

Artificial intelligence in hybrid threat operations: How AI empowers the existing adversarial playbook



Hybrid CoE Strategic Analyses address timely questions concerning hybrid threats and can serve as an opening for a theme that requires further research. They aim to identify gaps in knowledge and understanding, explain processes behind a phenomenon, and highlight trends and future challenges.

The European Centre of Excellence for Countering Hybrid Threats

tel. +358 400 253800 www.hybridcoe.fi

ISBN (web) 978–952–7591–46–8

ISBN (print) 978–952–7591–47–5

ISSN 2670–2282 (web)

ISSN 2814–7243 (print)

October 2026

Cover photo: ercan senkaya / shutterstock.com

The European Centre of Excellence for Countering Hybrid Threats

(Hybrid CoE) is an autonomous network-based international expert organization dedicated to addressing hybrid threats. Hybrid CoE's mission is to enhance the security of its 35 Participating States, the European Union and NATO by providing expertise, training and networks to counter hybrid threats. Its core values are excellence, integrity and respect. The Centre is based in Helsinki, Finland.

Responsibility for the views expressed in this paper ultimately rests with the authors.

Contents

- 1. Introduction..... 4
- 2. Understanding the threat landscape: Hybrid threats and the CORE ecosystem..... 4
 - 2.1 What makes a threat “hybrid” 4
 - 2.2 The CORE model as an analytical lens..... 5
 - 2.3 AI capability clusters..... 5
- 3. AI capability cluster 1: Generate and amplify 5
 - 3.1 CORE impact assessment..... 6
 - 3.2 Example: Russia’s AI-assisted information operations in Ukraine (2022–2024)..... 6
- 4. AI capability cluster 2: Probe and exploit 7
 - 4.1 CORE impact assessment 7
 - 4.2 Example: Volt Typhoon as a pre-AI baseline 8
- 5. AI capability cluster 3: Sense and target..... 8
 - 5.1 CORE impact assessment..... 8
 - 5.2 Example: Drone and autonomous system use in the Nagorno-Karabakh and Ukraine conflicts..... 9
- 6. Compounding problem: AI enables cross-space simultaneity..... 9
- 7. Conclusion 10
- Authors 11

Artificial intelligence in hybrid threat operations: How AI empowers the existing adversarial playbook

In recent years, artificial intelligence (AI) has become integrated into people's daily lives. The technology has improved rapidly, while regulations have failed to keep up. This Hybrid CoE Strategic Analysis explores how AI technology is affecting the hybrid threat landscape. The paper demonstrates that AI not only adds tools to hybrid threat operations but structurally alters existing threats.

1. Introduction

In March 2022, a deepfake video was posted on social media, showing Ukrainian president Volodymyr Zelenskyy urging his troops to surrender to the Russian invaders.¹ Although the video was quickly identified as fake, this example illustrates the challenge democracies face: AI-assisted technology has become widely available, amplifying content generation and lowering the skill threshold for hybrid threat operators.

The paper uses the Comprehensive Resilience Ecosystem (CORE) model, developed by the European Commission's Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), as an analytical lens to examine how the application of AI affects civic, governance and services spaces in various ways. The paper is structured around three capability clusters that examine various forms of AI-enabled hybrid threat activity, presented as illustrations rather than as a defined taxonomy of AI capabilities.

AI-assisted technology has become widely available, amplifying content generation and lowering the skill threshold for hybrid threat operators.

2. Understanding the threat landscape: Hybrid threats and the CORE ecosystem

2.1 What makes a threat "hybrid"

Hybrid threats can be difficult to detect and define because deniability is part of their design, and they aim to create cascading effects to maximize impact. At their core, hybrid threats target democracies and democratic values, combining various tools and methods. A co-authored paper by Hybrid CoE and the JRC describes hybrid threat actors as having

¹ Reuters, 'Deepfake footage purports to show Ukrainian president capitulating', 17 March 2022, <https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/> (accessed 5 August 2026)

three main goals: undermining and harming the integrity and functioning of democracies; manipulating established decision-making processes; and maximizing impact by creating cascading effects.² To achieve this, hybrid threat operators can apply different types of AI in various ways, from fabricating disinformation to automating military systems. This paper uses these criteria to describe hybrid threats and apply the CORE model to understand how AI is used in the hybrid threat landscape.

2.2 The CORE model as an analytical lens

The CORE model splits society into three spaces, depending on the object of threat. They are civic, governance and services, with levels ranging from local to national and international. The civic space represents the population's cohesion and beliefs; the governance space represents legitimate institutions and authorities; the services space represents the material and technical capacity required for society to function.³ The CORE model outlines 13 domains that can be used to target the three underlying spaces across three levels. These domains are interconnected, and hybrid threats often target multiple domains simultaneously; effects from one domain can also influence other domains, spaces and levels. This paper uses the CORE model as a diagnostic tool to

explore how AI-enabled threats can affect the ecosystem.

2.3 AI capability clusters

AI is a broad term that can be used to describe computer systems that are trained on large quantities of data to generate outputs. These outputs include text, video, audio, and pictures. Instead of acting on predefined instructions, AI requires real-time human interaction. Large language models (LLM) are a subset of AI that are trained on huge amounts of data to generate language in the form of text, summaries or even conversations.⁴ To illustrate the different capabilities AI can offer, this paper introduces three capability clusters that are assessed as complementary functions: shaping societal perception (generate and amplify); penetrating digital systems (probe and exploit); and directing effort (sense and target).

3. AI capability cluster 1: Generate and amplify

AI has empowered influence operations, acting as a “force multiplier” for disinformation and election interference, as low-cost, scaled-up, audience-specific content is effectively generated, with targeting and dissemination consolidated into a single low-budget pipeline.⁵

2 Rainer Jungwirth et al., *Hybrid Threats: A Comprehensive Resilience Ecosystem* (Luxembourg: Publications Office of the European Union, 2023), 42, <https://doi.org/10.2760/37899>.

3 Jungwirth et al., *Hybrid Threats*, 42.

4 Cole Stryker and Eda Kavlakoglu, ‘What Is Artificial Intelligence (AI)?’ IBM, last updated 15 June 2026, <https://www.ibm.com/think/topics/artificial-intelligence>.

5 Heidi Hanhijärvi, ‘Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian Approaches’, Hybrid CoE Paper 29 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, March 2026), 5, 25, 27, <https://www.hybridcoe.fi/wp-content/uploads/2026/03/Artificial-Intelligence-and-Foreign-Information-Manipulation-Hybrid-CoE-Paper-29.pdf>.

An analysis of seven recent studies has shown that 17,422 participants were equally affected by LLM- and human-created messages.⁶ The main difference was in the sheer volume of personalized messages that LLMs could generate compared with a group of humans. The improvement of these messages has mirrored the evolution of AI. Video and audio generation capabilities have been improving since 2022,⁷ while coordinated proxy networks disseminate this content at machine speed.⁸

The improvement of these messages has mirrored the evolution of AI.

3.1 CORE impact assessment

This cluster targets the civic space, spanning the information and societal domains, threatening political responsibility and accountability, stability, and foresight capabilities. Entering at the national layer, it contests nations' political coherence, cascades to the local layer to target local communities by exploiting existing divisions, and is amplified through transnational groups. The impact then spills over into the governance space, degrading decision makers'

information environment. This assessment is anticipatory: these spaces and layers are exposed rather than currently degraded, as it is reach rather than the content's quality or volume that dictates the cluster's impact.

3.2 Example: Russia's AI-assisted information operations in Ukraine (2022–2024)

Contrary to the 2022 "Zelenskyy" deepfake example mentioned in the introduction, the three AI-generated videos of Valerii Zaluzhnyi, the former Ukrainian Commander-in-Chief, in November 2023 were more difficult to identify as fake, showing a remarkable improvement in AI's generation capability, though some giveaways remained. In contrast with the broad mass-audience targeting of the 2022 Zelenskyy deepfake, future operations targeted specific and smaller audiences; an AI-generated video call by opposition MP Petro Poroshenko succeeded in deceiving International Legion members, while an AI-constructed voice clip of Oleksiy Danilov, who was then National Security and Defense Council Secretary, discussing the Crocus City Hall attack was aired on Gazprom-owned NTV.⁹ Separately, the scale of these operations grew, even if the campaigns narrowed their targeting. The infamous Meliorator bot farm, led by an RT deputy

6 Lukas Hölbling, Sebastian Maier, and Stefan Feuerriegel, 'A Meta-Analysis of the Persuasive Power of Large Language Models', *Scientific Reports* 15, article 43818 (2025), <https://doi.org/10.1038/s41598-025-30783-y>.

7 Roman Osadchuk, 'AI Tools Usage for Disinformation in the War in Ukraine', Digital Forensic Research Lab (DFRLab), 9 July 2024, <https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine>.

8 'State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity', Joint Cybersecurity Advisory, U.S. Federal Bureau of Investigation and Cyber National Mission Force, 9 July 2024, <https://www.ic3.gov/CSA/2024/240709.pdf>; U.S. Department of Justice, Office of Public Affairs, 'Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm', press release, 9 July 2024, <https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners>.

9 Osadchuk, 'AI Tools Usage for Disinformation in the War in Ukraine'.

editor-in-chief and overseen by a Russian FSB-affiliated unit, produced 968 posts on X (formerly Twitter) between 2023 and its seizure in July 2024.¹⁰ DFRLab assessed that these operations were still unable to achieve the desired impact,¹¹ and Hanhijärvi assesses AI as an add-on to existing and tested tools and tactics, techniques, and procedures (TTP), not as a replacement.¹²

4. AI capability cluster 2: Probe and exploit

As with the previous cluster, AI condenses vulnerability discovery and the generation of applicable exploits in an automated workflow. It also reduces the cost of managing capability, broadening its use and reducing the proficiency required of would-be users.

According to M-Trends 2026 (Mandiant's annual threat intelligence report, now part of Google Cloud) the mean time to exploit newly discovered software vulnerabilities has decreased to an estimated minus seven days, compared with 63 days in 2018. This means adversaries exploit software flaws before vendors or defenders can mitigate them.¹³ Furthermore, Google's Threat Intelligence Group has reported an increase in AI-supported vulnerability discovery and research among People's Republic of China (PRC)- and Democratic People's Republic of Korea (DPRK)-linked threat actors, though the first

AI-developed zero-day, a flaw unknown to the vendor, originated from a criminal actor.¹⁴ This was previously a capability reserved for state-supported threat actors; CERT-EU assesses that it has now spread to less sophisticated actors.¹⁵

4.1 CORE impact assessment

This cluster targets the services space, spanning both the cyber and infrastructure domains, compromising operational and information technology's reliability and availability, and in turn affecting political stability and foresight capabilities. Entering at the connections level, exploiting the point where global supply chains meet dependent national entities, it cascades to the clusters layer at the point of service delivery. The impact then spills over into the governance space, as prepositioned access becomes leverage for potential future developments. This means undiscovered digital artefacts within systems remain dormant and unnoticed by defenders because the adversary takes no action.

4.2 Example: Volt Typhoon as a pre-AI baseline

An example of this is the PRC state-sponsored Volt Typhoon threat actor, which has established and maintained persistence within US communications, energy, transport, and water sector networks for at least five years.

10 Joint Cybersecurity Advisory, 'State-Sponsored Russian Media Leverages Meliorator Software'; U.S. Department of Justice, 'Justice Department Leads Efforts'.

11 Osadchuk, 'AI Tools Usage for Disinformation in the War in Ukraine'.

12 Hanhijärvi, 'Artificial Intelligence and Foreign Information Manipulation'.

13 Jurgen Kutscher, 'M-Trends 2026: Data, Insights, and Strategies From the Frontlines', Google Cloud Blog (Mandiant), 23 March 2026, <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026/>.

14 Google Threat Intelligence Group, 'Adversaries Leverage AI for Vulnerability Exploitation, Augmented Operations, and Initial Access', Google Cloud Blog, 11 May 2026, <https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access>.

15 CERT-EU, 'AI Is Changing the Economics of Vulnerability Discovery. Defenders Should Adapt Now', 21 April 2026, <https://www.cert.europa.eu/blog/ai-vulnerability-discovery-defenders-must-adapt>.

The advisory assessed that adversaries used living-off-the-land techniques, tools and processes already in the system rather than installing new malware, making the activity blend in with normal use,¹⁶ as preparation for disruptive attacks in the event of a future escalation or crisis. This case has not been attributed to AI; separately, of 1,061 vulnerabilities attributed to AI-assisted discovery in the first half of 2026, 1.3 per cent were confirmed as exploited, which does not deviate from the pre-AI rate.¹⁷ Vulnerability discovery has industrialized; exploitation [still] has not.

Vulnerability discovery has industrialized; exploitation [still] has not.

5. AI capability cluster 3: Sense and target

The amount of information available online is increasing daily. From social media posts to legal documents and handbooks, it can be difficult for a human being to find and determine which data are useful, legitimate or even accurate. Nevertheless, widely available LLMs have made this task easier.

LLMs can sort the relevant information and produce actionable intelligence. Open-source intelligence (OSINT) can now be automated

and used for tasks such as guiding drones and analysing drone images at scale.¹⁸

5.1 CORE impact assessment

The cluster targets both the governance and services spaces: the infrastructure domain at the national and local layers in the former; and the military defence domain at the international layer in the latter. Although not directly connected, automated systems and AI-enabled intelligence enable persistent surveillance, allowing threat actors to continuously monitor, analyse and target these systems with little to no human oversight. In the infrastructure domain, this concerns the energy distribution and transport sectors; in the military defence domain, AI is used to discover valid military targets, with varying levels of success. The impact spills over into the civic space because civilian and military technology increasingly overlap. This blurring is a characteristic of hybrid threats, causing diffused responsibilities and delayed reaction times.

5.2 Example: Drone and autonomous system use in the Nagorno-Karabakh and Ukraine conflicts

The use of AI-assisted drones in the Nagorno-Karabakh conflict in 2020, when Azerbaijan overwhelmed Armenia's defences, shows how AI can use commercial technology to alter dynamics. Drones were used both to perform reconnaissance and to carry out strikes

16 Cybersecurity and Infrastructure Security Agency, National Security Agency, and Federal Bureau of Investigation, 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure', AA24-038A, 7 February 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

17 Patrick Garrity, 'VulnCheck State of Exploitation 1H-2026', VulnCheck, 28 July 2026, <https://www.vulncheck.com/blog/state-of-exploitation-1h-2026>.

18 Eado Hecht, 'Drones in the Nagorno-Karabakh War: Analyzing the Data', Military Strategy Magazine Volume 7, Issue 4 (January 2022), <https://doi.org/10.64148/msm.v7i4.5>.

in a single loop, as onboard sensors and AI-augmented automatic target recognition identified Armenian military assets. AI decreased the time from detecting to engaging a viable target.¹⁹ Both sides in Ukraine use this type of technology, deploying drones with varying autonomous and AI-facilitated capabilities to survey and target in ways otherwise unattainable without aerial superiority. For example, news footage showing a partial view of a window shape, along with a few other minor details, can be enough to identify a building, as seen in a strike on a workshop at a Kyiv tank factory. A pro-Russian Telegram group reviewed the news footage, identified the precise location and posted it online. A few days later, the building was struck by a Russian PGM, destroying the workshop and killing several workers.²⁰

6. Compounding problem: AI enables cross-space simultaneity

As the examples have shown, the three capability clusters do not operate in isolation; they are not generated by AI but are enhanced and supported by it, which enables them to operate in parallel and effectively place pressure on specific domains.

Although only one of the clusters targets governance directly, all three affect it. “Generate and amplify” erodes public trust and limits political decision making; “probe and exploit” compromises services and systems, degrading

institutions’ ability to respond; “sense and target” enables military actions that have a direct impact on civilian populations. This highlights the intertwined nature of AI-empowered hybrid threats, and the assessment ultimately reveals that decision makers simultaneously face a compromised information environment, prepositioned access held as dormant leverage and compromised command capacity.

In practice the defender’s disadvantage is both structural and technical. Coordinating cross-space or even cross-domain activities and operations was once reserved for nation-state actors; it has now proliferated to less sophisticated entities. CERT-EU’s judgement is that AI mainly affects who can operate at this frequency: software patch cycles run thirty to sixty days against exploitation that now precedes the patch, and the operational burden of using these tools falls on the defender.²¹ The near-term challenge is the advent of agentic AI, which is already underway. It affects these clusters, as agentic systems can run multiple actions simultaneously and continuously without the need for real-time human input. This decreases the time and number of operators required to sustain campaigns.

In practice the defender’s disadvantage is both structural and technical.

19 Nino Kemoklidze, Lala Jumayeva, and Badri Belkania, ‘The Future of Military Doctrine: Lessons on AI and Autonomy from the 2020 Karabakh War’, *Defence Studies* (June 17, 2026): 1–24, <https://doi.org/10.1080/14702436.2026.2686613>.

20 Centre for Information Resilience, ‘Killer Coordinates: How a Russian Missile Hit Kyiv with the Help of Online Sleuths’, *Eyes on Russia*, 15 June 2022, <https://www.info-res.org/eyes-on-russia/reports/killer-coordinates-how-a-russian-missile-hit-kyiv-with-the-help-of-online-sleuths/>.

21 CERT-EU, ‘AI Is Changing the Economics of Vulnerability Discovery’.

7. Conclusion

AI has assisted actors with limited resources and capabilities by changing the economics of hybrid threat operations: lowering costs and raising productivity. At the same time the nature and logic of hybrid threat operations remain the same. Using the CORE model to analyse the threat, it becomes evident that the real danger lies in cross-space cascading effects rather than any single AI capability cluster. An effective response requires stronger collaboration not just across domains but across spaces. Single and disconnected responses will therefore have a limited effect, causing us to lose sight of the bigger picture. An applicable example

of a concerted response is the planning and execution of cross-space tabletop exercises (TTX) that integrate the concerns into an AI-enabled attack across domains. When we consider the capability clusters, a viable scenario is an AI-generated information campaign that would coincide with an AI-enabled cyber intrusion, targeting physical operational technology systems, training defenders to address cascading rather than isolated events. This is something NATO/EU TTXs have already tried to emulate. Just as the CORE model has been applied here to analyse the threat, it can be used to build effective resilience across spaces, layers and domains.

Authors

Tinna Þuríður Sigurðardóttir is a cyber specialist in the Financial Stability Department at the Central Bank of Iceland, focusing on preparedness and threat intelligence by leading a sectoral working group and organizing exercises. Between 2024 and 2026, she was Iceland's secondee and a senior analyst at Hybrid CoE, specializing in the intersection of hybrid threats, cybersecurity and emerging technologies. She also has professional experience of working in various cyber roles from threat research to SOC analysis, cybersecurity management and cyber awareness. She has an MSc in AI and Language Technology and a BSc in Computer Science and Psychology.

Martin Cvetko is a senior military specialist from the Slovenian Armed Forces, currently working as a strategy researcher and coordinator for Cyber Intelligence Research at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. He has a bachelor's degree in Telecommunications Engineering and a master's degree in Cybersecurity, providing him with both a technical understanding of cyber threats and an operational and strategic perspective on managing cybersecurity and understanding the cyber threat landscape. His professional background includes experience of working in a Security Operations Centre (SOC), providing him with a solid understanding of SOC processes. His main area of work focuses on Cyber Threat Intelligence and by extension Cyber Intelligence, with a particular emphasis on methodology, taxonomy, best practices, and sector-agnostic common frameworks.



Hybrid CoE
The European Centre of Excellence
for Countering Hybrid Threats