Hybrid CoE Paper 13

# Digitalization and hybrid threats: Assessing the vulnerabilities for European security

Hybrid CoE

Daniel Fiott – April 2022

**Hybrid CoE Papers** are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

---

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

ISBN (web) 978–952–7472–32–3
ISBN (print) 978–952–7472–33–0
ISSN 2670–2053

April 2022

Cover photo: Nico El Nino / shutterstock.com

**Hybrid CoE's mission** is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

# Contents

# Summary

From artificial intelligence to quantum computing, emerging and disruptive technologies (EDTs) are being hailed as part of the next revolution in military affairs. However, it is not entirely clear how EDTs will shape the future of conflict or strategies aimed at countering hybrid threats. This Hybrid CoE Paper seeks to uncover what kind of role EDTs could play in European security, but it does so by contextualizing the emergence of EDTs in the broader process of digitalization. In this vein, it reveals important areas in which EDTs and digitalization could negatively and positively affect the European security landscape. To this end, the paper makes specific recommendations for the EU and NATO.

# Introduction

Advances in computing power, the increased use of automated systems or robots, artificial intelligence (AI) and hypersonic velocity vehicles have become regular objects of study for the strategic studies community. On the one hand, such emerging and disruptive technologies (EDTs) can be seen as a revolutionary step forward in the way that conventional and unconventional conflict is conducted, or the way that modern deterrence can function. Here, much is made of the ways in which EDTs may enhance communications, targeting or intelligence-gathering. On the other hand, there are those who believe that this so-called revolution in military affairs is overblown because it discounts the human factor in conflict and presumes that technological supremacy offers easier solutions to protracted crises. Wherever one may stand in this debate, it is clear that there is a need to understand how EDTs could impact Europe's future threat landscape.

However, this Hybrid CoE Paper argues that we cannot fully appreciate the importance of EDTs without contextualizing their development in light of broader technological processes such as digitalization. Focusing only on the development of individual EDTs without appreciating the implications of the digital transition could present risks to Europe's security landscape. In the field of economics, digitalization often refers to how business models are computerized to improve efficiency.[1] However, what is of relevance to discussions about Europe's security landscape is that digitalization represents a process of intensified interconnection between systems and enhanced information storage and management capacities.[2] On the one hand, this hyper-connectivity may serve to improve economic efficiency but, on the other, it may lead to vulnerabilities that can be exploited by state and non-state actors. This is particularly the case if EDTs such as AI or quantum computing are increasingly used to help manage and sustain critical infrastructure and strategically important economic sectors.

If digitalization does imply a process of intensified interconnection between systems, then there is a need to focus on the implications for countering hybrid threats. If one understands hybrid threats to mean malicious covert and overt actions by state and non-state actors, then digitalization may pose certain vulnerabilities that malicious actors can exploit. For example, the global trading system of goods is heavily reliant on digitalized logistics chains, which in turn could be vulnerable to cyberattacks and cause major security concerns (e.g. supply chokes for critical technologies and components).[3] Cyberattacks on computer networks, the spoofing and jamming of communications signals or the manipulation of data can also give rise to serious security concerns while providing a degree of deniability and cover for the perpetrators. In this respect,

1 See for example, G. Valenduc and P. Vendramin, 'Digitalisation, between Disruption and Evolution', *Transfer: European Review of Labour and Research* 23, no. 2 (2017): 121–134.

2 Daniel Fiott, 'Digitalising Defence: Protecting Europe in the Age of Quantum Computing and the Cloud', EUISS Brief, no. 4 (2020): 2, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%204%20Defence.pdf. [Unless otherwise indicated, all links were last accessed on 22 March 2022.]

3 Jukka Savolainen, 'Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?', Hybrid CoE Working Paper, no. 4 (2019): 8, https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Working-paper_WMDivers_2019_rgb.pdf.

there is a crucially important relationship between digitalization and cybersecurity, especially as digitalization is sustained through computer systems and data.

However, digitalization is not only a challenge due to covert malicious activities such as cyberattacks. As this paper will show, digitalization implies a wider range of security considerations that relate to critical infrastructure, access to raw materials, legislation, critical supply chains and energy management. In this sense, while cybersecurity is seen as a major element of the digital transition and digital security, a focus, say, on denial-of-service (DoS) attacks overlooks security issues such as technology dependencies, supply chain security, data encryption, extraction and manipulation and energy management. Hence, it pays to understand that the digital transition requires a broader security perspective that includes questions related to industrial policy and technological innovation.[4]

As a consequence, this paper intends to answer the following question: In what ways could digitalization affect Europe's security environment? To this end, the paper is divided into two parts. The first part looks at the relationship between EDTs, digitalization and hybrid threats in more detail, and seeks to provide some conceptual clarity in this regard. The second part looks at the wider implications of digitalization for European security. Here, the paper analyzes the importance of critical infrastructure, raw materials, legislation, critical supply chains and energy management as key elements of digitalization, but also highlights the vulnerabilities of each of these factors from the perspective of hybrid threats. The paper concludes with some policy considerations for the EU and NATO.

4 Thierry Breton, 'Technological Geopolitics: It's Time for Europe to Play its Cards', European Commission, 11 October 2021, https://ec.europa.eu/commission/commissioners/2019–2024/breton/blog/technological-geopolitics-its-time-europe-play-its-cards_en; Andrew Mumford, 'Ambiguity in Hybrid Warfare', Hybrid CoE Strategic Analysis, no. 24, 17 September 2020, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-24-ambiguity-in-hybrid-warfare/.

# Digitalization, EDTs and hybrid threats

Over the last few years, the strategic studies community has become accustomed to discussions about how EDTs such as AI, quantum computing, blockchain, 5G/6G and hypervelocity vehicles may alter the character of conventional and non-conventional threats.[5] Indeed, the NATO Science and Technology Organization (STO) surmises that EDTs are important for the future security environment for at least four reasons: 1) intelligence – the use of AI can enhance human intelligence and provide a more comprehensive and in-depth analytical picture of the battlefield; 2) interconnectedness – networks of sensors and the connection between the physical and virtual domains can enable effective battlefield connectivity; 3) distribution – a shift to decentralized data collection and analysis may give operatives greater battlefield autonomy; and 4) digitalization – the blending of information domains can enhance situational awareness and action.[6]

These four trends are not only relevant for the battlefield, however, as they can also aid our broader understanding of EDTs and digitalization. Indeed, digitalization is linked to questions about human-AI interaction, the interconnectedness of sensors and communication systems, centralized data storage, decentralized data usage and the connection of economic sectors and domains. The architecture of the digital transition is built on EDTs such as AI, big data, the internet of things, blockchain, 5G/6G and quantum and edge computing. These technologies are, in turn, reliant on a range of computing developments, industrial processes and supply chains, and they also rely on precious metals and energy sources for proper functioning. The key challenges facing Europe in light of EDTs and digitalization are:

1. to ensure that society and commerce benefit from more powerful, faster and interconnected computing power and processes;
2. to make sure that this interconnectedness does not lead to security vulnerabilities; and
3. to see to it that EDTs are used in a responsible manner.

Yet the trends reveal that EDTs and digitalization can pose security challenges. For example, the circulation of cryptocurrencies and the development of virtual spaces (such as the "metaverse") raise questions about additional cyber vulnerabilities and opportunities for non-state actors to manipulate currencies or to influence public opinion.[7] Indeed, in its recent Technology Foresight report, the European Defence Agency hypothesizes that the post-2040s may lead to home-delivered gene editing kits, crypto currency stock market manipulation, and the proliferation of small nuclear reactors and quantum computers.[8] In this sense, EDTs may allow non-state and state

5 See for example, Todd S. Sechser, Neil Narang and Caitlin Talmadge, 'Emerging Technologies and Strategic Stability in Peacetime, Crisis and War', *Journal of Strategic Studies*, Vol. 42, No. 6 (2019): 727–735.

6 NATO Science & Technology Organization, 'Science & Technology Trends: 2020–2040 – Exploring the S&T Edge', March 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020–2040.pdf.

7 World Economic Forum, 'Global Risks Report 2022', 11 January 2022, https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities.

8 European Defence Agency, 'EDA Technology Foresight Exercise 2021: Welcome to the Futures – Future Narratives', May 2021, https://eda.europa.eu/docs/default-source/documents/202105-edatechnologyforesightexercise-futuresnarratives_v5.pdf.

actors to manipulate data, DNA and energy production for malicious ends. It is also true that quantum encrypted systems may enhance the sophistication of cyberattacks, which raises the question of whether current cybersecurity measures are up to the challenge of defending against AI and quantum-enabled systems that may not even be controlled by humans.

Such threats necessitate a focus on what the STO calls "distribution". This is important because there is a growing understanding that EDTs such as AI may lead to a sort of proliferation of cutting-edge technology. This would imply a potential decentralization of technology usage, and without effective policy or regulation, states, private citizens or corporations could exert highly damaging and covert effects. Of course, one could also argue that the proliferation of technology could empower citizens to enhance societal resilience, especially if they play a role in the early warning of threats. However, given the blurring lines between commercial and public actors in certain countries, there is a risk that technology can be used for tracking, data manipulation, surveillance and other suspect activities such as supply disruption, election manipulation, and crime.

While much can be written about how individual EDTs can enhance or test European security, it is essential to consider how individual technologies may feed off and/or enable other technological phenomena. For example, quantum computing is not simply important in its own right, but because it has the potential to lead to greater advances in fields such as nano- and bio-technologies.[9] Part of the problem is adjusting the policy lens to deal with a "system of systems" approach where EDTs are seen to form a digital ecosystem of communication, sensing and automation capabilities. Obviously, this forces the EU and NATO to ensure the protection of cyber, 5G and AI-enabled systems, but the challenge for the Union and NATO may be much deeper given the skills deficit in European societies in terms of deep tech and IT know-how.[10] In particular, technological literacy has been identified as a key strategic shortfall, especially in terms of how EDTs should be employed and how best to mediate between technological effects and strategy.[11]

The growing relevance of EDTs and digitalization poses a range of questions for countering hybrid threats. On the one hand, being able to employ AI or quantum computing could enhance Europe's ability to encrypt data and ensure cybersecurity. On the other hand, a "system of systems" of EDTs and digitalization is leading to a widening of the hybrid attack surface. Most obviously, the centralization of data through big data and cloud technologies incurs a risk as far as cyberattacks are concerned. Malicious access to and manipulation of data can wreak havoc in key infrastructures in government, and in the finance and banking, energy, transport, and health sectors. Yet,

9 Ralph Thiele, 'Quantum Sciences – A Disruptive Innovation in Hybrid Warfare', Hybrid CoE Working Paper, no. 7, March 2020, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Working-Paper-7_2020.pdf.

10 Niels van der Linden et al., 'High-Tech Skills Industry: Increasing EU's Talent Pool and Promoting the Highest Quality Standards in Support of Digital Transformation', 2019, 8, https://skills4industry.eu/sites/default/files/2019–06/Brochure_Digiframe_final20190617.pdf.

11 Andrea Gilli, 'Future Warfare, Future Skills? Future Professional Military Education', NATO Defence College Brief, no. 18, November 2021: 3. Retrieved from https://www.ndc.nato.int/news/news.php?icode=1629.

in addition to the centralization of data, digitalization is based on a decentralization of data usage and communication (e.g. smart phones and 5G) to cater for evolving consumption patterns. Thus, although "smart cities" are designed to enhance efficiency and accessibility through digital interconnectivity, there are inherent security concerns that may have a cascading effect through urban, regional, national and transnational critical infrastructures.[12]

12 Trevor Braun et al., 'Security and Privacy Challenges in Smart Cities', *Sustainable Cities and Society*, vol. 39, (2018), 499–507.

# The digital ecosystem and hybrid threats

The growing development and use of EDTs and the evolving nature of digitalization pose significant security considerations for Europe. In particular, the digitalization of critical infrastructure invites policymakers and analysts to more clearly establish a link between economic sectors and security. Fortunately, this wider perspective has already been recognized by organizations such as NATO and the EU. Through its "baseline requirements", NATO is already working on seven areas for civil preparedness as part of its resilience efforts. In particular, the requirements related to continuity of government services, resilient energy supplies, resilient civil communication systems and resilient civil transportation systems all link to processes of digitalization.[13] In this respect, faced with the increasing "hybridization" of the threat landscape, the Alliance is investing in more joined-up situational awareness.[14] Furthermore, recognition of the interlinkages between critical infrastructure and European security has paved the way for closer EU-NATO cooperation to counter hybrid threats.

The EU has also made progress in developing policy to counter the potentially harmful effects of EDTs and digitalization on critical infrastructure. First, since October 2020, the EU's Foreign Direct Investment screening mechanism has served to monitor ownership of critical infrastructure such as 5G networks so that non-EU-owned mobile networks and operators do not undertake third-party interference, imperil privacy or disrupt services.[15] Second, the EU is currently working on revising and expanding the Network and Information Security (NIS) Directive to ensure greater cyber resilience. Among other things, the "NIS 2 Directive" is designed to expand cybersecurity measures and obligations to telecoms and social media services, as well as to enhance situational awareness by revised rules on the prevention and handling of large-scale security incidents.[16] Additionally, the European Commission has proposed a new Directive on the resilience of critical entities to cover a range of interdependent service sectors such as finance and banking, water, health, and space – the existing Directive from 2008 only applied to the energy and transport sectors.[17]

This more holistic approach to identifying vulnerabilities in Europe's digital infrastructure is long overdue. Indeed, the twin major transitions related to digitalization and climate change are having lasting effects on

13 Wolf-Diether Roepke and Hasit Thankey, 'Resilience: the First Line of Defence', *NATO Review*, 27 February 2019, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

14 Antonio Missiroli, 'From Hybrid Warfare to "Cybrid" Campaigns: the New Normal?', NATO Defence College Policy Brief, no. 19, September 2019: 4, https://www.jstor.org/stable/resrep19847?seq=1.

15 NIS Cooperation Group, 'Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures', January 2020: 7, https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf.

16 Mar Negreiro, 'The NIS2 Directive: A High Common Level of Cybersecurity in the EU', European Parliamentary Research Service Briefing, December 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

17 European Commission, 'Proposal for a Directive on the Resilience of Critical Entities', COM(2020) 829 final, Brussels, 16 December 2020, https://eur-lex.europa.eu/resource.html?uri=cellar:74d1acf7-3f94-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

economies and societies, which may provide further opportunities for malign hybrid threat campaigns. For example, consider that today electricity grids have been digitalized to ensure safer and more efficient allocation of electricity supply. Further still, energy markets today are not just more interconnected, they are also increasingly decentralized, as consumers are given more power over how they manage energy consumption. While this may be beneficial for the environment and energy security, it comes with an inherent risk: namely, without effective regulations, procedures and cybersecurity, it may become easier for competitors to infiltrate such critical infrastructures via hacking or service denial tactics.[18] Targeting the energy sector in this way could be an effective hybrid threat.

Much like the example of electricity markets, there are other areas where digitalization could lead to vulnerabilities to hybrid threats: think of the infiltration of smart phone sets, automated transport systems, air traffic control systems, and so forth. However, these vulnerabilities are not just a cause for concern in terms of technology usage, they also invite us to look into the specific causes of infiltration into and disruption of digital systems. Such an approach must begin with the recognition that the digital world is not simply "virtual", but sustained instead by "physical" supplies, materials and processes. Any analysis of vulnerabilities in the digital world must include a closer focus on supplies of raw materials, the management of supply chains, and the ownership of critical infrastructure. Indeed, increased digitalization is likely to lead to a greater dependency on raw materials for high-tech and strategic products and industries, but a number of these materials are held by strategic competitors or countries and regions marked by instability.[19]

This is a particular challenge for the defence sector, as raw material dependency for EDTs and digitalization becomes even more critical – particularly if it leads to the immobility of military units or the disabling of capability. In particular, the blurring lines between the civil and defence sectors mean that critical supply chains are more likely to be vulnerable to hostile actors that may seek to manipulate supply for political ends. What is more, the integration of civil technologies into the defence supply chain may be considered an inherent vulnerability. Given that defence supply chain management and supply inventories are increasingly digitalized, the risk of cyber vulnerabilities increases as strategic competitors and hostile actors look for ways to disrupt inventory management systems or even disable the use or accuracy of precision weapons, targeting systems and sensors.[20] This is not a hypothetical threat: the Belgian Ministry of Defence was

---

18 Daniel Fiott and Roderick Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', Chaillot Paper, no. 151, EU Institute for Security Studies, April 2019: 27, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf.

19 Joint Research Centre, 'Critical Raw Materials for Strategic Technologies and Sectors in the EU – A Foresight Study', 2020: 15, https://rmis.jrc.ec.europa.eu/uploads/CRMs_for_Strategic_Technologies_and_Sectors_in_the_EU_2020.pdf.

20 Benjamin Turnbull, 'Cyber-resilient Supply Chains: Mission Assurance in the Future Operating Environment', *Australian Army Journal* 14, no. 3 (2018): 48, https://search.informit.org/doi/pdf/10.3316/ielapa.344417545553155.

subject to a cyberattack in December 2021[21] and the 2021 Colonial Pipeline hack was another example of how vulnerable critical infrastructure is to cyberattacks.[22]

Yet even beyond the specifics of the defence sector, critical infrastructure vulnerabilities are giving rise to a broader focus on strategic domains by the EU and NATO. In particular, there is a greater focus on space, maritime and cyber domains, with the recognition that vulnerabilities in the digital systems in these domains may give rise to military vulnerabilities and economic crises. For example, NATO adopted a space policy on 17 January 2022 with the express objective of countering space-based threats that may enable hybrid attacks with a high degree of deniability.[23] In its Strategic Compass on EU security and defence, the Union has dedicated more time and resources to the vulnerabilities increasingly inherent in strategic domains. Not only will the Strategic Compass lead to an EU strategy for space and defence[24] and rapid cybersecurity response instruments, but the focus on maritime security promises to better shield the Union from maritime hybrid threats – an essential task given the economic weight of the EU.[25]

The growing hybrid threats in the maritime domain are becoming clearer. This domain is home to critical infrastructure such as undersea communications cables and energy pipelines, as well as offshore oil rigs and renewable energy installations. Additionally, an incomplete application of international law to the seas ensures regulatory "grey zones" that can be exploited by strategic competitors. In such cases, commercial fishing vessels or coastguards can play a strategic role in advancing the political objectives of hostile actors. The digitalization of marine systems and interconnectedness of maritime networks, hubs and vessels only contributes to a further vulnerability. As one study puts it, "[t]he pace of technological development in maritime systems, including navigational, surveillance and other operational systems, has been rapid".[26] This rapid digitalization also threatens to lead to vulnerabilities in the entire shipping industry, as ports, logistics chains and inventories are exposed to cyberattacks.

21 Laurens Cerulus, 'Belgian defense ministry hit by cyberattack', *Political Europe*, 20 December 2021, https://www.politico.eu/article/belgium-defense-ministry-hit-with-cyberattack/.

22 Valeria Insinna, 'Colonial Pipeline Hack Shows Peril of Ignoring Military Cyber Vulnerabilities: Kendall', *Breaking Defense*, 19 October 2021, https://breakingdefense.com/2021/10/colonial-pipeline-hack-shows-peril-of-ignoring-military-cyber-vulnerabilities-kendall/.

23 NATO, 'NATO's Overarching Space Policy', 17 January 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

24 Daniel Fiott, 'Securing the Heavens: How can Space Support the EU's Strategic Compass?', EUISS Brief, no. 9, April 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_9_2021_0.pdf.

25 Daniel Fiott, 'Naval Gazing? The Strategic Compass and the EU's Maritime Presence', EUISS Brief, no. 16, July 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_16_2021.pdf.

26 Tiia Lohela and Valentin Schatz (eds.), 'Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans', Hybrid CoE Working Paper, no. 5, November 2019: 13, https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf.

# Conclusions

This paper has shown how the use and development of EDTs and broader processes of digitalization pose serious security questions for the EU and NATO. Indeed, the analysis began with a single question: In what ways could digitalization affect Europe's security environment? The analysis has shown that digitalization is an irreversible process that promises to lead to economic gains, but also to security vulnerabilities. Digitalization and the use of EDTs implies an even more interconnected "system of systems" that is not only bringing different economic sectors (transport, energy, space, maritime, cyber, etc.) into close proximity, but is also leading to greater decentralization where – at least in open societies – consumers play a bigger role in managing service preferences and consumption. We have seen how this process can lead to hybrid threats, as a hyper-interconnected society is more susceptible to information and data manipulation, and hacking digital systems can lead to the collapse of critical infrastructure such as electricity grids.

Having established the importance of EDTs and digitalization for hybrid threats, this paper also drew attention to factors that require greater clarity. Indeed, EDTs can lure analysts and policymakers into thinking that disruptive technologies can deal with the intractable political challenges of resource allocation and decision-making. EDTs such as AI, quantum computing or hypervelocity vehicles should not be treated as solutions to the long-standing challenge of addressing political contestation. Such EDTs should also be seen as part of a wider technological ecosystem where technologies can enable new areas of research or development (e.g. nano-technologies, life sciences) and threats. In this respect, what is called for is an interdisciplinary approach to the challenge of EDTs and digitalization that brings together policymakers, political scientists, computing engineers, lawyers, and so forth.

Following the analysis, **one of the first recommendations that can be made is that EU and NATO decision-makers should not focus exclusively on the trajectory of individual EDTs. It is vital that any assessment of EDTs is placed in a broader context of digitalization, of which the principal hallmarks are the interconnectivity of systems, centralization of data, decentralization of data use and enhanced information storage and communications.** In this respect, there is growing recognition that the key aspect of EDTs that requires a policy response is data management, processing and use. We have seen that EDTs rely on data as "fuel" and the EU and NATO are already focusing on investments and strategies geared towards data management. However, as part of the EU's and NATO's policies to enhance resilience there is an increased need to focus on the constituent parts of digitalization.

In practice, this means that digitalization should not be seen as a "virtual" enterprise because in reality it cannot be sustained without resource inputs such as precious metals, or physical infrastructure such as subsea cables. In this respect, when thinking about EDTs and digitalization, there is **a need for the EU and NATO to continue to focus on the wider resource and supply chain ecosystems that sustain digitalization.** Proposed plans by the European Commission to develop a Critical Technology Observatory are a step in the right direction, as it will focus on supply chains and critical resources. In a broader context, this is an effective way to ensure technological resilience. However, **there is a clear need for the EU and NATO to communicate with each other on supply threats and challenges that may loom on the horizon.**

However, **one of the chief ways in which the EU and NATO can better prepare to counter the security vulnerabilities brought about by digitalization entails planning a more ambitious set of joint exercises and enhancing situational awareness.** Despite the obvious restrictions in EU-NATO cooperation, both organizations need to integrate digital and technological aspects into their respective (and potentially joint) strategic scenario and tabletop exercises. Further still, **there is an urgent need through investment to address the wide chasm between rapid technological developments and the resource base of Europe's armed forces.** There is a certain irony in calling for investments in hypervelocity vehicles, when Europe's armed forces still struggle to fill basic capability needs or are still using analogue systems for basic tasks.

**Finally, it is essential that a more comprehensive plan for societal resilience is developed.** The word "comprehensive" is, of course, overused but it should imply that policymakers are able to look at potential security vulnerabilities across a range of economic sectors. Through various pieces of legislation and investments aimed at boosting cybersecurity, protecting critical infrastructure and securing critical raw materials, the EU is moving in this direction. For its part, NATO is looking at the defence-specific aspects of digital vulnerabilities, and so too are bodies such as the European Defence Agency and the European Commission. What remains a challenge, however, is promoting a wider societal understanding of the risks and challenges that emerge with EDTs and through digitalization.

# Author

**Daniel Fiott** is Security and Defence Editor at the EU Institute for Security Studies, a position he has held since 2016, and where he focuses on European defence and questions related to capability development, the defence industry and technologies. He studied at the University of Cambridge and received his PhD from the Vrije Universiteit Brussel (VUB).

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats