Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4278-cd

Cyber sovereignty and the (multitude of the) industrial metaverse

Marte Høiby

SINTEF Digital, Norway. E-mail: marte.hoiby@sintef.no

Tor Olav Grøtan

SINTEF Digital, Norway. E-mail: tor.o.grotan@sintef.no

Digital profiling and tracking in the age of attention economy and surveillance capitalism implies intricate and subtle ways of profiling and influencing people, but also industries, organizations and societies. The nature and full impact of this is only partially recognized at the civic level, receiving rather slack attention at the political/legal level, and scarcely addressed as a safety/security issue in industrial and societal contexts and corresponding critical roles and positions of individuals. These aspects carry serious challenges for the ambition of industrial participation in the private-public domain for national security, and for total defense approaches. In this paper, we explore the rise of vulnerabilities released by new industrial digitalization paradigms and practices, and their potential impact on society and state security from a cyber sovereignty and resilience perspective. Accompanied by growing concern for industrial and national sovereignty in cyberspace and burgeoning geopolitical instability, this constitutes a gap which urgently needs recognition. By investigating the concept of cyber sovereignty and the growing interest for the industrial metaverse on a global scale, we discuss to which extent cyber resilience thinking may be a counterweight to the vast digital vulnerabilities and challenges that can be envisaged. Although the exploration is brief and results tentative, reflecting the inherent complexity and dynamism in the field due to both technological, economic and geopolitical factors, we argue that both practical and theoretical (envisaged) approaches to cyber resilience may fall short towards the pace of change in the cyber domain. This may have serious implications for the prospect of industrial contribution to national security.

Keywords: cyber sovereignty, cybersecurity, cyber resilience, industrial metaverse, hybrid threats, national security

1. Introduction

The rise of surveillance capitalism was predicted by Zuboff (2019) and its successful conquest and might over the business-to-consumer (B2C) domain was signified and visualized beyond any doubt by the collective presence of the "tech bros" at the US Presidential inauguration in January 2025. Their conquest has not reached an endpoint in the B2C domain, but it may be overshadowing a forthcoming wave in its infancy of applying the same principles in the "business-to-business" (B2B) domain. The connection between B2C and B2B is exemplified by the British Military Intelligence section 5 warning about state sponsored espionage targeting industries using fake social media profiles to obtain classified information (BBC, 2021). However, these and similar incidents are just the tip of an iceberg.

While the implications for state security from digital tracking and profiling are largely unattended (Berrefjord, 2022), we can only assume the additional consequences from similar patterns in the B2B domain. Grøtan (2018) addressed such vulnerabilities in the energy domain through the "Big Cyber" paradigm; the composite threat landscape forged by the Big Brother (state surveillance), the Big Other (surveillance capitalism), the Big Five (psychological profiling), the Big Data (and its application in AI), and the Big Innovation (the appetite for disruptive potential). Today, the Big Cyber perspective is manifested in the world-wide attention to the "metaverse". In this paper, we will narrow our focus to the *industrial* metaverse (IMV), and its potential implications for societal safety and security through collaboration in the public-private sector.

Initiatives like Industry 4.0, Industry 5.0, and recently, the IMV, emerge from an engineering perspective of increasingly powerful concepts to combine the powers of AI, digital

twins, etc. From a societal perspective, the scenarios that may be envisaged have by far surpassed the worries from Orwell's (1948) "1984". Huxley's (2013) "Brave New World" originally published in 1932 is probably a better mirror for both the enthusiast and the worrisome.

Our societal security focus is more limited, but still extensive. Considering the more important role of industrial enterprises as contributors to national security or total defense, either by law or from seeing commercial opportunity in countering hybrid threats, a pressing issue persists: how safe is it to depend on a total defense built on premises forged primarily on economic interests? What are the consequences of building private industrial growth on the IMV in terms of societal security and total defense? What kind of knowledge will be necessary to answer such a question, and will an "industrial FOMO" ("fear-of-missing-out") pre-emptively render the options as very few?

This is the overall issue we want to explore in this paper. Several concerns loom in the horizon, e.g., will the IMV further accelerate the tracking and profiling capabilities towards individuals as well as organizations and enterprises? Historically, businesses have kept their cards close to the chest, if not to protect national interests, then at least to avoid leaking competitive advantage. However, when the obtainable scope of competitive advantage diminishes with the exponential pace of the global tech-race and its open-source based innovations, do we need other means to protect national interests and prioritize them over businesses' interests? What are the consequences of this to some extent uncontrolled exposure of business- and social infrastructure? Is it possible to mobilize cyber resilience concepts that can effectively counter these new challenges?

This paper explores current trends and discusses the possible impact of this development.

2. Method & Ambition

Conceptualizing this relatively new phenomenon in a theoretical frame of modern hybrid war- and conflict, this paper aims to elaborate, without offering definite solutions, on how the cyber sovereignty needed to trust industrial contributions to societal security will fit the emerging IMV.

The method is to compare brief descriptions of cyber sovereignty and the ambition of the IMV, seen both from an international economic perspective (WEF/EU), from an engineering perspective (IEEE), and from an industrial actor perspective (e.g., Nokia, Siemens), based on open sources. Contrasting issues will be interpreted both from a national sovereignty perspective, with attention to surveillance, and from a (cyber) resilience point of view.

However, conclusions are tentative, and mainly useful as directions for further research.

3. Cyber Sovereignty: Theoretical framework

3.1 Cyber Sovereignty

Sovereignty refers to supreme authority over one or more subsets in a hierarchy. As state sovereignty refers to territorial authority, both in terms of a nation state's jurisdiction and responsibility, cyber sovereignty is a concept contested by its interconnected infrastructure, global outreach and complex sociological environment. "Cyber Sovereignty reveals **how states have pursued new methods and tactics** to fuel the distribution of authority and control in the cyber field" (Kadlecová, 2024). Although cyber sovereignty when referring to infrastructure is to be considered a part of state sovereignty, this too is contestable by the structure and ownership of powerful multinational companies, such as some of the largest social media platforms. Thus, referring to the content within this infrastructure, data sovereignty is a term that has emerged with increasing complexity of structures surrounding nation-states' claimed space, presence, assets or values – i.e., social, political, economic etc. – in the virtual domain. Data sovereignty refers to a nation-state or region's jurisdiction over intellectual property, financial data, or personal information.

While academic discussions about cyber sovereignty is mostly concerned with the applicability of International Humanitarian Law (IHL) in cyberspace, states do not appear to apply neither sovereignty nor cyber sovereignty in their national cybersecurity policies – while there have been claims related to control internet content (Baezner & Patrice, 2018). This suggests there are different conceptions about what constitutes cyber – its structure or its content – or both.

The cyber domain was the latest addition to the doctrine of the North Atlantic Treaty Organisation (NATO), in 2016, added to its other established domains of warfare, i.e., air, sea, space and land (which also have unclear or disputed territorial borders and jurisdiction). Whether or not *cognitive* warfare, namely threats posed by the *perceptual influence* made increasingly effective and far-reaching with the emergence of cyberspace should be considered a sixth domain in NATO's doctrine, has been subject to evaluation in the NATO Allied Command Transformation (ACT) over the past years. A final version of the cognitive warfare concept was projected to be finalized in late 2024 (NATO Allied Command Transformation, 2023). However, NATO (2025) recognises the possibility of using cognitive tactics as a so-called "Instrument of power": "*Cognitive Warfare includes activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviours, by influencing, protecting, or disrupting individual, group, or population level cognition, to gain an advantage over an adversary. Designed to modify perceptions of reality, whole-of-society manipulation has become a new norm, with human cognition shaping to be a critical realm of warfare*".

Chinese authorities describe Cognitive Warfare as "the use of public opinion, psychological operations, and legal influence to achieve victory" (Ibid.). While all abovementioned definitions sum up parts of what has earlier been addressed as a matter of cyber sovereignty and security, the confusion seems to be laying in the fact that influence operations and -activities increasingly are executed through cyberspace, or via or against cyberdriven systems and infrastructure. So-called Influence Cyber Operations (ICOs) is frequently used to term such actions in cyberspace and may be understood as a specific subset of Influence Operations (Brangetto & Veenendaal, 2019) – of which an attack ultimately becomes a cyberattack.

3.2 Cybercrime and state activity

One of the issues of cyber sovereignty lays in the domain's flexibility to operate in time and space, and consequential opportunity for actors to launch attacks over distance while escaping attribution. When declaration of war is undesirable for any given party to a conflict, destruction and destabilization can still be achieved through activity within and through cyberspace.

Literature on cybercrime suggests that cybercrime too is poorly defined and variously applied among European law enforcement, used to describe any kind of actions in, via or against cybertechnology (Meland et al., 2024). Still, a divide between what is committed against and directed towards cybertechnology, such as computers, versus crime that is committed through cybertechnology, is a common distinction. The literature terms them cyber-dependent and cyber-enabled (Ibid).

3.3 Technology and hybrid threats

State power projection and interstate conflict escalation are increasingly characterized by elements of opportunity in cyber space. With unattributable sabotage attacks, espionage, surveillance, influence campaigns and election intervention, malign actors can influence societies in geographically distant locations. Such activity is often in politics and mainstream media termed as *hybrid threats* (HT). Hybrid CoE defines hybrid threats as "harmful activities that are planned and carried out with malign intent [aiming] to undermine a target, such as a state or an institution, through a variety of means, often combined" (Hybrid CoE, 2024).

Hybrid threats do not necessarily target state armies but society at large, and operations can combine conventional military and non-military methods, exploit economic and political superiority with coercion or force, and influence societal cognition through manipulation of democratic processes. Such tactics are made increasingly possible as result of 'hyperdigitalisation' pushing cybertechnology faster and further for industrial digital integration and automation, with consequent societal expectancy and dependency.

Aspects of organized crime to a greater extent intersect with state interference today than before – both in cyberspace and in the physical domain. Again, the core is the opportunities brought by with cybertechnology that allow actors to escape attribution for operations. With unprecedented force and highly diverse motives, this "cyber crossover" poses escalatory threats to geopolitical stability and security in Europe (Saalman et al., 2023). The cyber-asynchronicity also allows for (manmade) operations to await and coincide with natural and unexpected events

to boost force and impact (Ibid). As illegal virtual marketplaces proliferate, malware is sold on the black-market (i.e., cybercrime-as-a-service) along with assistance from criminal hack groups who partake in wars through cyberspace (Saalman et al., 2023).

While the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual), and its section on cyber sovereignty in particular, is the best regulatory framework that exists to steer power projection within cyberspace, a pressing question is whether and how the manual can contribute to regulate power while contradicting globally interconnected economic interests. Scholars argue that cyberspace is left poorly regulated because it is in neither stakeholders' nor state powers' interest to limit the room for maneuver which it provides: regulation is pending because of a dual interest among state actors to pursue their goals within cyberspace and thus the strongest actors have interest in keeping advantage (Moulin, 2023).

4. The Industrial Metaverse (IMV)

The IMV denotes a very optimistic projection of a metamorphosis of a number of technologies that are already available. Thus, it is also a potentially major enabler of hybrid threats that exploit lack of cyber sovereignty.

In this brief overview, we will give a few snapshots of how the rise of the IMV is seen, and which IMV imperatives are raised from different positions (of power) in the landscape of private-public cooperation. The overview is based on open sources.

4.1 Economic imperatives (WEF/EU)

We start with the World Economic Forum (WEF). WEF (2025) presents itself as "*the International Organization for Public-Private Cooperation. It provides a global, impartial and not-for-profit platform for meaningful connection between stakeholders to establish trust, and build initiatives for cooperation and progress*".

However, while the platform may be "not-for-profit", the arena and the activities conducted are more multifaceted and not necessarily oriented towards the "common good" in the broadest sense. Roose (2019), reporting from the 2019 Davos meeting with the banner of "committed to improve the state of the world", observe that executives on one side take part in panel discussions about building "human-centered A.I." and talk about the need to provide a safety net for people who lose their jobs as a result of automation. However, in private settings, including meetings with the other leaders of consulting and technology firms, they tell a different story, "*racing to automate their own work forces to stay ahead of the competition, with little regard for the impact on workers*".

This apparent double standard is hardly surprising and can only just be denoted a "hidden agenda". A reading of the WEF stance to the IMV must thus be done in a kind of Dylanesque hermeneutic: "*I'm a man of contradictions, I'm a man of many moods. I contain multitudes*" (Dylan, 2020). In other words, we may expect some inherent contradictions or shortcomings, rather than an ideally balanced blueprint for resolving our research issue.

Nevertheless, a blueprint is precisely what WEF, in collaboration with Accenture, is offering. The extensive WEF (2024a) "insight report" report *Navigating the Industrial Metaverse: A Blueprint for Future Innovations* offers the reasons for leaders to "act now"; the keys to unlocking the value in the IMV, a look into the future of the IMV, and advice for realizing the full potential for the IMV. The prospective IMV future is seen through the leading use cases implemented by large companies across the world (ibid, p54), namely digital twins, design and simulation, immersive learning, training and sales, and tamper-proof supply chains. According to the report, governmental fostering of the IMV is conducted by the EU (focusing on giving people the tools and the skills to safely and confidently use virtual worlds), China (emphasizing advanced technologies, a thriving 3D interactive ecosystem and comprehensive support), and the United Arab Emirates (robust government backing of metaverse adoption, including blockchain).

Moreover, to realize the full potential of IMV, safety and security must be enhanced, e.g., to ensure virtual environments do not compromise the well-being of the industrial workforce. Digital identity is a cornerstone, in which "*users have portable identities, complete with their data and history*" (WEF, 2024a, p76), in contrast to "siloed" identities linked to specific platforms or companies. The risk of

impersonation and fraud is acknowledged, with a call for digital identity governance and multi-factor authentication to enhance trust. However, accompanied with a taste for AI-powered avatars, it is fair to say that the "insider threat" aspects will not disappear with IMV, neither will the privacy issues for the IMV user, skilled or not. In that respect, the EU focus on providing humans with tools and skills, is at least promising.

However, for EU, the IMV prospect, also denoted the "Web 4.0 and virtual world", has not triggered any concerns so far that incite proposed new regulation in the short to medium-term. Rather, EU will "*connect virtual world developers with industry users, invest in the uptake and scale-up of new technologies, and give people the tools and the skills to safely and confidently use virtual worlds*" (Peets et al., 2023). Hence, seen in combination with the Draghi (2024) report on EU competitiveness, it is tempting to assume that the EU stance (multitude) reflects an "industrial FOMO" which they will try to mitigate by focusing on human skills.

Except for attention to "self-sovereign identity" of users as provided by industrial actor Bosch, the WEF "blueprint" does not address cyber sovereignty specifically. However, another WEF (2024b) report addresses 9 ways national security and economic cooperation are evolving. Without addressing the IMV, this report argues that despite the emerging multipolar world, mutual interdependence is still economically preferable. Diversification strategies may mitigate some harm to the rules-based trading system, and although trading partners may turn into adversaries, pragmatism must rule over rigid ideology, and dual-use technology is inevitable. To address the lack of trust stemming from (the view that) the playing field is tilted in favor of the largest players, active multistakeholder dialogues will be fruitful in order to "*bridge the gap of understanding between national security and economic cooperation*".

Hence, also here it appears that the IMV-related "industrial FOMO" persists, to the disfavor of attention to an emerging threat to cyber sovereignty. The WEF *multitude* is thus still tilted towards the presumption that the joint economic advances, which continuation will depend on the IMV boost, will persist in overriding other concerns.

4.2 Professional (engineering) imperative

The Institute of Electrical and Electronics Engineers (IEEE, 2025a) is the world's largest technical professional organization. IEEE's membership has long been composed of engineers, scientists, and allied professionals

Not unexpectedly, the IEEE (2025b) see the IMV as "*…a visionary and powerful concept, redefining the way industries operate*". Pointing to the role of major tech companies, for which IMV "*represents an unprecedented avenue of opportunity, challenge, and collective effort for a better, digitized future*", the IEEE envisage that the IMV is "*a powerful and revolutionary concept*", that "*has the potential to reshape various industries, aid business, and stimulate significant economic growth*".

However, IEEE (2025b) acknowledge the "*questions still remain about the necessary legal and ethical guidelines to regulate behavior and protect individual rights within this virtual domain*". They acknowledge that potential risks can emanate from the IMV, e.g., ethical concerns such as privacy invasion and data security, and societal effects. Examples of the latter are exacerbating digital disparity, the digital divide or contributing to an unhealthy dependence on virtual realities. However, the role of the IMV related to cyber sovereignty, national or other, remains in a void.

4.3 Industrial imperatives

For the world-wide industrial giant Siemens (2025), the IMV "*will be a place where we innovate at the speed of software*" (sic!), and "*will offer enormous potential to transform our economies and industries*". Besides being naturally focused on the technical issues, Siemens appear at least equally eager to emphasize the business model impact and urgency by claiming that "*the race is on*", with "*Leaders, Challengers, Explorers, and Observers*". Accordingly, the IMV "*isn't just a concept – it's quickly becoming a digital reality that's transforming the way industries operate*". The prospected impact from the IMV is framed as "*how it will revolutionalize the way we work and live, build and produce*". No less. However, cyber sovereignty or national security interests appear to be out of scope.

Also, industrial actors with more narrow focus and technical portfolios, such as the data network-centric Nokia (2025), directs attention to the "*endless possibilities for the future of both*

industry and society". Nokia's industrial focus is thus also accompanied by the alleged impact of "*turning the public good into the public great*", and "*transforming the way cities and nations defend, protect and thrive*". Interestingly, example areas addressed by Nokia are, inter alia, government services, defense, and public safety, however without any explicit focus on cyber sovereignty in the IMV.

4.4 A thought on IMV security

The format of this paper does not allow even a brief judgement of the actual security in IMV implementations so far. However, the global reaction to the introduction of the DeepSeek AI engine surprisingly launched in January 2025 in terms of massive access to a service with critical security flaws (Nagli, 2025), is another indicator that the *multitude* of the IMV expectations is clearly biased towards "FOMO" rather than precautionary safety and security concerns.

5. Discussion

5.1 The IMV can host a variety of activities challenging cyber sovereignty

Cognitive manipulation has existed for a long time and is inherently not a new concept. Still, a major difference lies in that the cyber technology which hosts such human influential potential has become far more potent and is now outside of institutional control (Høiby, 2022).

Especially with the inclusion of AI, it is clear that the IMV can harbor the full range of cyber influence, from classical cyber-attack to intentional bias in AI models to composite cognitive operations. This may threaten cyber sovereignty in any form. Moreover, the IMV raise a number of "insider" issues. They are usually divided into espionage cases, industrial or economic disloyalty, and insider actions, the latter paying existential attention to the psychological trait of the human being and development of personality tests. The literature does only to a limited extent acknowledge the blurring lines that divide information available on the inside and the outside, and even less any given actor's opportunity to operate on the outside while accessing what is on the inside (Høiby et al., 2022, 2024). The line between the "inside" and the "outside" is blurred (Ibid). Adding to this is the potential "nudging" of organizational behavior stemming from (B2B) tracking and profiling of organizational and individual behavior (B2C).

The IMV may be used for a variety of hybrid threats and operations. Meanwhile, these issues do not have an apparent priority in the IMV imperatives we have sampled. Similarly, the European initiative *Gaia-X*, instigated by concern for the sovereignty of European digital infrastructure dominated by (US) hyperscalers (e.g., Amazon, Microsoft, Google), allegedly has reduced its scope towards digital sovereignty through secure dataspaces across Europe to stimulate economic growth (Gooding, 2024). Thus, neither *Gaia-X* nor the *Fiware* initiative ("*a curated framework of Open Source Platform components to accelerate the development of Smart Solutions*" (Fiware, 2025), appear to make a difference for cyber sovereignty. The projected economic benefit reigns in the multitude of issues on the table, and international law has no mention of neither *hybrid warfare* nor *proxy warfare* (ICRC, 2024)

5.2 A cyber resilience perspective

The term resilience accommodates a variety of legacies, presumptions and pragmatic interests. The "Resilience ABC" taxonomy (Grøtan et al., 2022), comprises three different explanations or theories on the origin of resilient outcomes in the cyber domain. Put simply, Theory A attributes resilient outcomes of absorption of or rebound from disturbance to technical capabilities such as redundance, fault-tolerance and feedback control. Theory B attributes similar outcomes to existing, well-defined practices of, e.g., risk management, emergency preparedness and business continuity. Theory B also encompasses the idea of a *reactive* adaptive capacity, expressed, e.g., though the metaphor of biological systems developing immunity (Linkov and Kott. 2018).

Theory C departs from the other two by focusing on sustained *proactive* adaptive capacity at boundaries of preparedness as a distinct phenomenon and practice, grounded in complexity theory. Theory C stands out as representative for the (resilience engineering) idea that resilience is not a static trait but an active and evolving, forward-looking effort that enables graceful extensibility in boundary conditions, by being "*poised to adapt*" (Woods, 2018). Theory C is thus not focused on specific adaptations, but the sustained capacity to adapt.

The WEF (2024a, p4) aim *"to assist stakeholders in navigating the complexities and realizing the transformative opportunities of the industrial metaverse*" may in principle be associated with the ambition of Theory C. The accompanying "insight" of "*embracing innovation to withstand a myriad of disruptions*" reinforces such an impression. However, only until the subsequent statement that "*Leaders are doubling down on innovation to fortify themselves against disruptions*", employing technologies that "*promise enhanced data simplicity, transparency, interaction, collaboration and efficiency in business processes*". This indicates that the IMV is not intended to remain in the "adaptive universe" of Theory C but rather is aiming for a solidified state in which the planned robustness and rebound capacity of Theory A and B is sufficient. Based on the previous discussion, we find it hard to expect that to happen, not at least due to security challenges. Thus, it is more likely that the IMV will harbor a multitude requiring a degree and scale of Theory C resilience that is beyond any implementation known so far, requiring an unprecedented level of systemic, cross-scale interaction at or beyond the boundaries of recommended cyber security practice such as the EU NIS2 Directive. Initiatives such as the Cyber Resilience Pledge (WEF, 2022) are useful as they demand attention and action from top level management, but the scope is limited in the sense that it does not refer to practices beyond Theory B resilience. Hence, it may legitimate an IMV move into landscapes of becoming "robust yet fragile" (Woods, 2015). In the IMV, the consequences of fragility may potentially be huge and irreversible, as illustrated by the DeepSeek episode already mentioned (Nagli, 2025).

6. Conclusion

Despite the methodological limitations due to our high-level approach, we point at a growing divide between business development and national security interests. This is not promising for the role of IMV for societal safety and security.

With the blurred cyber sovereignty concept largely left unattended, the IMV might harbor hybrid threats and unleash "insider" challenges in a manner that is not sustainable in the current geopolitical situation. With this, we suggest recognition of the fact that resilience theories deployed in practice are not only static, but passive, in their lack of taking full advantage of the capacities of human agency. System-security thinking (Theory A, B) may not be enough to meet the challenges of cyberspace exactly because the virtual reality hosts cognitive environments beyond what can be balanced through resilience and any form of adaptive capacity. Cyber deterrence and cyber offensive operations are the new turn in cyber military strategic thinking such as the US "defend forward" doctrine (Friis, 2020) perhaps for some of these reasons.

The path to IMV-based societal safety and security in the private-public domain will be challenging, as the economic motivation will persist to be the main driver in any IMV multitude. Resilience as *proactive* adaptive capacity is, *in theory*, a conceivable pathway but will require a mindset and a systemic approach that challenges paradigms embedded in the IMV.

Acknowledgement

The paper is part of the project TECNOCRACI, funded by the Research Council of Norway (grant no. 03489).

References

Baezner, Marie; Robin, Patrice (2018). Cyber sovereignty, Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.

Berrefjord, V. (2022). Kommersiell sporing – nasjonal risiko. Internasjonal Politikk 80 (1): 24

Brangetto, P., Veenendaal, M.A., (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operation, in: 2016 8th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn.

Draghi, M. (2024). The future of European competitiveness: European Commission. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en . . Accessed at Febr 5th, 2025

Dylan, B. (2020). Lyric from "I contain multitudes" from the musical album "Rough and Rowdy Ways"

Gooding, M. 2024. https://www.datacenterdynamics.com/en/analysis/gaia-x-has-europes-grand-digital-infrastructure-project-hit-the-buffers/

Grøtan, T.O. (2018). Building Cyber Resilience through a Discursive Approach to "Big Cyber" Threat Landscapes. In Safety and Reliability – Safe Societies in a Changing World. Proceedings of ESREL 2018

Fiware. 2025. https://www.fiware.org/about-us/

Friis, K. (2020). *Offensive cyberoperasjoner: Den nye normalen?* Økonomi & politik. 2020, 93 (3), 30-44

Hybrid CoE. (2024). Hybrid threats as a concept. *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats*. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Huxley, A. 2013. Brave New World. Everyman's Library

Høiby, M. (2022). War and Military Journalism. In G. Borchard (Ed.), The SAGE Encyclopaedia of Journalism (2nd edition, March 2022). SAGE Publications, Inc. ISBN: 9781544391151

Høiby, M., Brennhovd, P. & Øren, A. (2024). En metastudie om innsidetrusselen. Academic report. Oslo: SINTEF Publications.

Høiby, M., Vatn, D., Fiskvik, J. & Thaulow, K. (2022). Kunnskapsgrunnlag om bevisstgjørings-strategier som skal motvirke rekruttering av ubevisste innsidere i norske virksomheter. Rapport nr. 2022:01518. ISBN: 978-82-14-07977-7ICRC

ICRC (2024) International humanitarian law and the challenges of contemporary armed conflicts: compliance for IHL to protect humanity in todays and future conflicts. https://www.icrc.org/sites/default/files/media_file/2024-10/4810_002_CH%202.pdf . Accessed at Febr 5th, 2025

(IEEE) Institute of Electrical and Electronics Engineers (2025a). Website. https://www.ieee.org/about/ieee-history.html . Accessed at Febr 5th, 2025

(IEEE) Institute of Electrical and Electronics Engineers (2025b). What Is Industrial Metaverse and Why It Is Important. https://metaversereality.ieee.org/publications/articles/what-is-industrial-metaverse-and-why-is-it-important . Accessed at Febr 5th, 2025https://www.ieee.org/about/ieee-history.html . Accessed at Febr 5th, 2025

Kadlecová, L. (2024). *Cyber Sovereignty: The Future of Governance in Cyberspace*. 1st Ed. Standford University Press.

Linkov, I. and A. Kott. 2018. Cyber Resilience of Systems and Networks. Springer Nature

Meland, PH.; Bjørge, N.; Møllerstuen; Høiby, M. & Kilskar, S. (2024). Kunnskapsoversikt cyberkriminalitet. SINTEF Rapport 2023:01331.

Moulin, T. (2023) *Cyber-Espionage in International Law: Silence Speaks.* Manchester University Press. Pp 312.

NATO Allied Command Transformation (2023). Accessed at https://www.act.nato.int/activities/cognitive-warfare/

Nagli, G. (2025). Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History. Wiz Blog. https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak . Accessed at Febr 5th, 2025

Nokia (2025). Powering the industrial metaverse. https://www.nokia.com/metaverse/industrial-metaverse/ . Accessed at Febr 5th, 2025

Orwell, G. (1948). 1984. Commons

Peets, L., Szewczyk, B. & Sa J. Choi. (2023). European Commission Publishes New Strategy on Virtual Worlds. Global Policy Watch. https://www.globalpolicywatch.com/category/metaverse/ . Accessed at Febr 5th, 2025

Roose, K. (2019). The Hidden Automation Agenda of the Davos Elite. Article in New York Times. https://www.nytimes.com/2019/01/25/technology/automation-davos-world-economic-forum.html . Accessed at Febr 5th, 2025

Siemens (2025). The Industrial Metaverse. https://www.siemens.com/global/en/company/digital-transformation/industrial-metaverse.html . Accessed at Febr 5th, 2025

World Economic Forum (WEF) (2022). Cyber Resilience Pledge. https://initiatives.weforum.org/cyberresilienceindustries/the-pledge Accessed at Febr 6th, 2025

World Economic Forum (WEF) (2024a). Navigating the Industrial Metaverse: A Blueprint for Future Innovations. https://www.weforum.org/publications/navigating-the-industrial-metaverse-a-blueprint-for-future-innovations/ . Accessed at Febr 5th, 2025

World Economic Forum (WEF) (2024b). 9 ways national security and economic cooperation are evolving. https://www.weforum.org/stories/2024/06/9-ways-national-security-and-economic-cooperation-are-evolving / . Accessed at Febr 5th, 2025

World Economic Forum (WEF) (2025). https://www.weforum.org/about/world-economic-forum/ . Accessed at Febr 5th, 2025

Zuboff, S. (2019) The Age of Surveillance Capitalism. Profile Books.

Woods, D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability engineering & system safety, 141, 5-9. https://doi.org/10.1016/j.ress.2015.03.018

Woods, D. 2018. 'The Theory of Graceful Extensibility: Basic Rules That Govern Adaptive Systems'. *Environment Systems and Decisions* 38 (4): 433–57.