SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Future threat landscapes: The impact on intelligence and security services

Mikael Weissmann

mikael.weissmann@fhs.se

https://orcid.org/0000-0001-5426-8238

Department of Systems Science for Defence and Security, Swedish Defence University, Drottning Kristinas väg 39, 11428 Stockholm, Sweden

Abstract

This article examines the evolving nature of antagonistic threats in the context of intelligence and security services, with a focus on small and medium-sized countries. It explores the impact of hybrid threats and non-linear warfare in an increasingly blurred security landscape between war and peace. The study aims to understand the emerging dynamics of the grey zone and the new challenges these evolving threats pose to intelligence and security services. The article adopts a qualitative methodology, drawing on global examples and including the strategic use of hybrid warfare by both state and non-state actors. In addition, the study examines technological advancements, particularly in artificial intelligence (AI) and machine learning (ML), to assess their role in shaping modern threats. The article argues that modern antagonistic threats differ from traditional ones in both intensity and complexity. Hybrid threats operate across multiple domains, blending military and non-military tactics while exploiting societal vulnerabilities. The article highlights the growing importance of AI and ML in both offensive and defensive strategies as well as the challenges posed by rapid technological advancements beyond state control. The article concludes that intelligence and security services must adapt to these multi-dimensional threats by embracing flexible integrated strategies. Enhanced international collaboration, advanced technological integration, and a focus on resilience will be the key to countering hybrid threats. The findings underscore the need for intelligence services to operate beyond traditional boundaries to effectively manage the complexities of future security environments.

Keywords:

national security, PNR, counterintelligence, border security, TRAVINT, hybrid threats, artificial intelligence, strategic intelligence, security challenges, intelligence services

Article info
Received: 22 September 2024
Revised: 6 December 2024
Accepted: 11 December 2024
Available online: 25 January 2025

Citation: Weissmann, M. (2025) 'Future threat landscapes: The impact on intelligence and security services', *Security and Defence Quarterly*, 49(1). doi: 10.35467/sdq/197248.

Introduction[1]

This article addresses the future challenges that intelligence and security services will face, focusing on small and medium-sized countries. It explores the impact of emerging threats, including hybrid threats and non-linear warfare, which increasingly blur the traditional distinction between war and peace and demand a rethinking of existing security paradigms.[2]

Whereas many studies have often focused on specific threats or great power dynamics, this study takes a holistic view of the multifaceted threats confronting small and medium-sized countries, thereby contributing new insights to existing research. In doing so, the article emphasises the increasingly complex and blurred distinctions between war and peace, focusing on how hybrid threats and non-linear warfare dominate the evolving security environment. By examining these dynamics, it provides critical insights into the challenges these threats pose to the intelligence community. This holistic approach moves beyond examining isolated elements, addressing instead the systemic interactions and broader implications that shape today's security landscape.

These future threats, often operating in the "grey zone" between war and peace—a space where traditional binaries of war and peace or conventional and unconventional warfare no longer apply—pose significant challenges to traditional security paradigms (Palmgren, 2020; Weissmann, 2019a, 2021). In this grey zone, state and non-state actors employ hybrid strategies that challenge dominant military powers through military and non-military tactics, including cyberattacks, information warfare, and proxy conflicts.

Against this backdrop, the article aims to support the intelligence and security services in navigating these emerging challenges by providing insights into the evolving threat landscape, the prevalence of grey zone activities, and the growing interdependence among states. To achieve this, the article adopts a qualitative methodology, drawing on global examples and including state and non-state actors' strategic use of hybrid methods. In addition, the study examines technological advancements, particularly in artificial intelligence (AI) and machine learning (ML), to assess their role in shaping current and future

---

[1] *This article is an abridged and developed translation of a chapter published by the author in a report originally published in Swedish (Weissmann, 2024). It stems from a project examining the challenges facing the military security and intelligence service in the context of Sweden's rebuilding of total defence and crisis preparedness, resulting in a report published by the Swedish Defence University (Häggström, 2024). The report brought together some of Sweden's leading experts in the field to analyse, from different perspectives, how modern threats, new technologies, legislation, the rebuilding of total defence, membership in the North Atlantic Treaty Organization (NATO), and the demands for cooperation across borders and with other authorities and companies affect the future of the activities of the military security and intelligence service. It features chapters on antagonistic threats in peacetime (Petersson, 2024), the impact of future threats on security services (Weissmann, 2024), legitimacy and legality (Karlson, 2024b), defence intelligence legislation in Sweden, Finland, Norway, and Denmark (Viksten, 2024), the role of international co-operation (Corneliusson, 2024), the military security services and total defence (Karlson, 2024a), and human resources for the future military security services (Annell and Lilja-Lolax, 2024). The research was supported by funding from the Swedish Armed Forces. The views and opinions presented in this article are those of the author alone and do not necessarily represent those of the Swedish Defence University or the Swedish Armed Forces. During the preparation of this work, the author has used a number of generative AI and AI-assisted technologies in the writing process, including DeepL, Google Translate, ChatGPT, and Grammarly. These tools were employed to support the translation and writing process and to enhance and refine the text. The author carefully reviewed, edited, and validated the content to ensure its accuracy and integrity and takes full responsibility for the final published work.*

[2] *In this article, the term "non-linear warfare" is used interchangeably with hybrid warfare and refers to "…the use of military and non-military tools in an integrated campaign designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure" (International Institute for Strategic Studies [IISS], 2015, p. 5). For a deeper discussion, see, for example, Bērziņš, 2020; Friedman, 2018; Galeotti, 2016a, 2016b; Weissmann, 2019a.*

threats. It also examines the effects of the ongoing global redistribution of economic power, which is driving a shift in the international order. The article integrates perspectives from military studies, political science, military technology, systems science for defence and security, and geopolitical analysis. This enables a comprehensive examination of emerging threats' complex and interconnected nature and their implications for security and intelligence services.

The article is framed around two key questions:

- What will modern antagonistic threats look like, and what will characterize them?
- What new demands will these evolving threats place on intelligence and security services, including their defensive capabilities and ability to influence threat actors in various domains?

By examining these forces, the study highlights the need for security and intelligence services to adapt their strategies, tools, and methods to effectively counter emerging challenges.

Modern antagonistic threats[3]

In recent years, the international security environment has evolved into a volatile and increasingly large grey zone between war and peace. Security challenges and antagonistic threats arising from various hybrid threats and non-linear warfare are high on today's security agenda in Europe and worldwide.

The combined military resources of the United States and Europe remain significantly superior to those of Russia and China, driving these and other actors to develop and combine less resource-intensive methods to compete globally. Non-linear warfare and hybrid threats are common strategies among many actors, including Russia, China, Iran, and North Korea, as well as some non-state actors, primarily the Islamic State and Hezbollah, used to challenge the West's global hegemony.

Russia's actions in Ukraine before the invasion on 24 February 2022 manifested this paradigm as a good example of the problem of thinking of war and peace as binary categories. How does a country or group of countries handle threats and aggression in this grey area, such as "little green men" appearing in uniform but without national insignia and refusing to disclose their origin, election interference operations, or cyberattacks, to name just a few possible examples?

This does not mean that the West cannot combine various political means in a manner that can be described as non-linear warfare or a hybrid threat. The debate may have flaws and ambiguities but does challenge the West's binary perspective on war and peace as well as conventional and unconventional warfare. It has contributed to a better understanding of how an adversary can innovatively combine different tools to exploit specific vulnerabilities in Western societies and bypass existing defence structures. This, in turn, has increased the West's ability to handle antagonistic threats.

How do these threats differ from traditional threats? Threats of the 21st century differ from traditional threats and warfare in intensity and degree rather than in their nature.

[3] *This section is based on Weissmann et al. (2021), in particular Chapters 1, 5, and 17.*

The exception is the virtual and digital realms, where many new tools have been created, and the startup cost for using them has decreased (e.g. unmanned aerial vehicles (UAVs) and surveillance cameras). Adversaries frequently introduce new threats aimed at achieving their objectives without resorting to war; for example, they may disrupt, undermine, or damage a target's political system and social cohesion through a combination of control, manipulation, violence, subversion, and the dissemination of false information (Treverton *et al.*, 2018, p. 10). These threats target the opponent's society, not combatants (Pawlak, 2017).

Hybrid threats and non-linear warfare also mean a range of possible contradictory means, from the threat of war to propaganda and everything in between. Thus, they contain several power and influence instruments but emphasise non-military and military threats that operate in the grey zone below the threshold of an open war. These forms of threats and warfare do not allow for a clear distinction between different types of actors—whether they are state or non-state, soldiers or civilians, organised violence, terrorism, crime, or war—in the traditional sense. Regardless of the actor from which the threat originates, it has become common for such actors to combine and tailor a mix of conventional and irregular means to achieve maximum effect.

Intelligence and security services undoubtedly play a central role in analysing and addressing antagonistic threats. These threats are not only directly aimed at the armed forces or national security interests but also include understanding and preventing indirect effects and threats that are, or risk becoming, a danger to these security interests. Operating under the assumption that an adversary is neither unwise nor inclined to predict is essential. This underscores the utility of reverse targeting because understanding what needs to be protected and anticipating how an adversary might likely target these assets are often more effective than merely tracking the actors themselves, all else being equal. Intelligence and security services must collaborate nationally and internationally, as future antagonistic threats in the grey zone must be addressed collectively to achieve success (see Häggström, 2021 on multilateral intelligence cooperation). In this context, intelligence and security services within the framework of total defence are particularly important.

Future threats: Drivers, challenges, requirements, and countermeasures

To understand future challenges and associated threat landscapes that intelligence and security services face, it is beneficial to start with two global megatrends reshaping our world today. These developmental processes will have significant consequences for all forms of organisations, industries, and the broader society and consequently for the challenges and threats that intelligence and security services will need to manage in the future.

Technological breakthroughs, especially in AI and ML, are central to the world's development and critical for intelligence and security services. The redistribution of economic power from north to south and west to east alters the world order, the global context in which antagonistic threats exist, and the context within which intelligence and security services must operate. What challenges do these megatrends pose to intelligence and security services?

Technological breakthroughs

Technical breakthroughs, particularly in AI and ML, represent domains with significant opportunities and challenges that intelligence and security services must

monitor. This field will be critically important in the fully digitalised and connected world we are moving towards. However, technological development poses an inherent problem—knowing what is fundamental for the future and what constitutes mere technological "fads". Because it is not possible to know in advance what will be most important, it is crucial to adopt a broad perspective. To succeed, it is necessary to understand that we are dealing with a complex or "wicked" problem here, not just a complicated whole that needs to be analysed (see, e.g. Interaction Design Foundations, n.d. Also see Conklin, 2005; Rittel and Webber, 1973). Therefore, a broader range of areas are discussed below that may or may be likely to impose new demands on intelligence and security services to create the required defence capabilities and influence various threat actors across different domains.

AI and ML

One area requiring special attention is the development of AI and ML. What is central here is that AI and ML is not an area where the Western world is guaranteed to maintain technological superiority, even though this has traditionally been the case. Significant investments are being made in AI within the Western armed forces and their intelligence and security services. For example, the US Department of Defense significantly increased its unclassified investments in AI, rising from just over $600 million in 2016 to approximately $1.8 billion in the fiscal year 2024, and now oversees more than 685 active AI projects in total (Sayler, 2024, p. 4).

However, this investment is relatively small compared to that of the private sector. To illustrate the scale, in 2023 the global AI market was valued at over €130 billion and is projected to grow to nearly €1.9 trillion by 2030 (European Parliament, 2024). To provide a concrete example, in 2023, Microsoft announced that it would invest $10 billion in OpenAI, the Creator of ChatGPT (Metz and Weise, 2023).

Moreover, it is not only the West that focuses on and invests in AI. Putin stated "[w]hoever becomes the leader in this sphere will become the ruler of the world" (RT International, 2017). According to the Congressional Research Service (CRS), Russia's development in AI significantly lags behind that of the United States and China (Sayler, 2020c). Russia wants to close this gap and has published a national strategy to enhance its AI expertise, educational programs, datasets, infrastructure, and legislation (Office of the President of the Russian Federation, 2019). China's position is stronger and is generally considered the closest competitor to the United States in AI (Lee, 2018). China's "Next Generation AI Development Plan" from 2017 describes AI as a "strategic technology" that has become a "focus of international competition" (China State Council, 2017; also see Jones, 2022; Sheehan, 2023).

In summary, much of the development in this area has occurred outside the control of Western states, presenting challenges and demanding flexibility from intelligence and security services. This is especially true because the distinction between state and private entities is not always clear or transparent, and there is often a significant overlap between sectors. In countries such as Russia, China, Iran, and North Korea, there is no division among commercial companies, the research environment, the military, and the central government.

The differences between narrow and broad AI systems are important. Narrow AI systems are limited to handling only the specific tasks they have been trained to conduct. General AI systems do not yet exist and may never be developed; however, they can perform a wide range of tasks, including those they have not been specifically trained for

(see, e.g. Bostrom, 2014, Sayler, 2024). Intelligence and security services must follow the broad development of AI by focusing on both open and secret advancements. AI systems have successfully developed, imposing new demands on intelligence and security services. Handling lightning-fast self-learning systems with broad cognitive human capabilities is a wicked problem for which one can never be fully prepared.

Narrow AI has already been integrated into many civilian and military systems today and is used by both friendly states and competitors. Its applications are found not only in intelligence, surveillance, and reconnaissance (Smagh, 2020) but also in logistics, cyber operations, command and control as well as in semi-automated and automated vehicles. Understanding the potential impacts on defensive and offensive capabilities is crucial, as both sides utilise narrow AI systems.

Technologies designed to augment or replace human operators are not inherently offensive or defensive; the key is understanding and using them best and more effectively than the adversary. Intelligence and security services must ask themselves, what role their analysts and operators should play in this brave new world. Will the analyst's future role be to analyse independently or pose the correct questions to the AI system? Should the operator control or provide instructions to an AI system? Will the major issue in the future revolve around law and ethics as limiting factors, and, if so, how in a world where systems are virtually limitless? Which systems should be developed? How broad are these systems? These questions are particularly pertinent when broader AI systems are being developed.

It is clear, to cite Sayler (2024, p. 2):

> AI-enabled systems could (1) react significantly faster than systems that rely on operator input; (2) cope with an exponential increase in the amount of data available for analysis; and (3) enable new concepts of operations, such as swarming (i.e. cooperative behaviour in which unmanned vehicles autonomously coordinate to achieve a task) that could confer a warfighting advantage by overwhelming adversary defensive systems.

AI's role in defence now includes applications such as Generative AI and Explainable AI (XAI). Generative AI, exemplified by models such as GPT-4, is increasingly used by intelligence and security services for various tasks, including content triage and assisting analysts (Konkel, 2024). XAI is becoming crucial for military and intelligence agencies in ensuring transparency and trust in AI-driven decisions, which are critical in high-stake situations (on XAI, see e.g. Ali *et al.*, 2023; European Data Protection Supervisor (EDPS) Technology and Privacy Unit, 2023).

Another important issue is the risk that AI algorithms may produce unpredictable and unconventional results, which could lead to unexpected inaccuracies if incorporated into military systems (Sayler, 2024, p. 3). This phenomenon is often illustrated by an example where researchers combined an image that an AI system correctly identified as a panda with random distortions labelled by the computer as a "nematode," where although the differences in the combined image are imperceptible to the human eye, the AI system misclassified it as a gibbon with 99.3% confidence (Ilachinski, 2017, p. 61).

There must be awareness and, above all, a critical approach to the results and recommendations provided by AI. It is also essential for intelligence and security services to consider that adversaries can exploit these vulnerabilities in every possible manner, broadly

disrupting one's own AI dependencies or, more specifically, affecting target identification, selection, and engagement.

Another AI-related area that will significantly impact intelligence and security services is AI's role in enabling increasingly realistic digital forgeries or "deepfakes"; see, for example, Deepfake Queen: 2020 alternative Christmas message (Channel 4, 2024). For example, Britain's Channel 4 (2020) created an alternative version of the Queen's annual Christmas speech, intended as "[a] comedic parody which serves as a stark warning about misinformation and fake news in a digital age. The Queen speaks 'plainly and from the heart'. Is what we see and hear always the same as it seems?"

The danger of deep fakes should not be underestimated. For example, a climate change study examining five populations of American students, educators, and the general adult public found that 33–50% of people could not distinguish between authentic and fake video clips (Doss *et al.*, 2023).

The technologies presented above pose enormous challenges for intelligence and security services in the grey zone and future wars. Concerns about how AI technology can generate false news reports, influence the public, and erode public trust, and potentially even blackmail government officials, are as important as they are challenging to address (Rempfer, 2018; Sayler, 2020a). What are reality and truth if it is no longer possible to tell the difference? What happens if official channels, such as Emergency Service websites, Public Service radio, TV, etc. are blocked or taken over if the prime minister or the king speaks, but it is a deep fake? To what extent should intelligence and security services (and society) use deep fakes?

It is essential to consider both direct and indirect effects, as this largely concerns the struggle in the information environment about which narrative is true and how reality should be understood and interpreted. The COVID-19 pandemic has demonstrated how heavily people rely on diverse sources and platforms for information, many of which fall outside official channels. For example, individuals with immigrant backgrounds may prefer media from their country of origin. In contrast, others turn to digital channels and social media or seek information broadly, both within and outside the border of the country of residence. It also shows how information influences from both state and non-state origins (and everything in between) can occur in a broad sense. Additionally, as more content becomes restricted behind paywalls, the risk increases that adversaries can gain significant influence simply by offering free access to their information.

The information environment

It is often stated that future wars will be decided within the information environment, claiming that future conflicts will revolve around strategic communication and the struggle over narratives will be central. Given the relevance of the information environment, intelligence and security services must address and manage it, which is challenging considering that they have traditionally tended to be secretive and cautious about the information they disclose regarding their knowledge and perceptions of reality.

If intelligence and security services are not active in a public information environment where the narrative battle is constantly unfolding, they risk losing its significance. However, excessive openness may expose vulnerabilities and reduce defence capabilities. Deciding whether and how to engage requires careful consideration and continuous efforts.

Because all actors are active in the information environment and continuously attempt to utilise all available tools, this environment must be understood as a central aspect of the grey zone and integrated with other domains. Everything converges in the information environment, making constant analysis by intelligence and security services necessary. Here, various forces are met, such as AI and ML, cyberattacks, deception and influence operations, and the application of biometrics.

Management of a vast amount of information flow is also crucial. Intelligence and security services must ensure that they develop tools to handle the dynamics of information flow, continuously ongoing assessments, information overspread, and forward-looking operational advice in an environment with virtually unlimited information. This requires managing information flows from a range of sources, including Human Intelligence (HUMINT), signal intelligence (SIGINT), communication intelligence (COMINT), imagery intelligence (IMINT), geospatial intelligence (GEOINT), measurement and signature intelligence (MASINT), and open-source intelligence (OSINT) (see, e.g. Clark, 2016; US Naval War College (USNWC), n.d.). To this end, social media intelligence (SOCMEINT), the latest addition to the intelligence family, must be included (see, e.g. Omand *et al.*, 2012).

The space domain

Intelligence and security services must monitor space domain developments, which are closely linked to other technological developments. Information flows, and the entire cyber domain is intimately connected to what happens in space, as are large parts of intelligence-gathering capabilities.

The space domain is both a threat and an opportunity. When used intelligently, those with the greatest capacity have the greatest potential to gain advantages in maximising their defence capabilities and influencing adversaries, even beyond the space domain. The fact that the previous dominance of the United States, both military and civilian, is no longer assured is significant for intelligence and security services to consider. It is not guaranteed that developments in space will always favour the Western world when it is not only major powers like Russia and China but also other actors who have their space programs (Colucci, 2021; Goswami and Garretson, 2020; O'Connell and Salter, 2021).

Developments in space are also important because they open up new potential conflicts, as several major powers have developed space-based weapon systems. This makes space a possible battlefield and creates uncertainty, as our entire society and lifestyle today rely on functioning systems in space for navigation, communication, mobile telephony, and weather forecasting, to name a few examples. The robustness of these systems is threatened as more states have the capability to disable satellites (Chekinov and Bogdanov, 2013; Manson and Shepherd, 2020; Mehta, 2020).

Space is a potential future battlefield and, together with cyber technology, affects most of what we do on the Earth. Beyond this, space is particularly important to intelligence and security services because it reflects the increasing intertwining of civilian and military interests. There is a possibility for the dual use of civilian satellites and technologies; however, what happens in space, even if it affects civilian areas primarily, will have significant indirect impacts on the security interests of the armed forces. Remembering that we live in a grey zone where warfare is ongoing and is also essential.

Biotechnology, biometrics, and quantum technology

Biotechnology is another area imposing new demands on intelligence and security services. These technologies alter biological systems. Biotechnology leverages bioscience for technical applications and is an area with potentially significant implications for the security interests of not least, but not limited to, the armed forces. Biotechnology has opened up the possibility of altering genes and creating DNA to modify plants, animals, and humans. Moreover, the spread of synthetic biology has expanded the number of actors capable of producing chemical and biological weapons (Sayler, 2020c; also see Bellasio *et al.*, 2021).

Intelligence and security services should closely monitor this area to understand the threats they face and when there is a need to actively influence an adversary's development. This area also requires ethical reflection on what should and should not be done and what is legal. This is particularly important because it can be assumed that the ethical standards differ among actors. Remembering that these technologies are not confined to state actors is also essential.

The use of biometrics is crucial for intelligence and security services. These technologies enhance our ability to eliminate the anonymity of individuals and non-state actors through automated identification of behaviours and biological characteristics (Lunan, 2018; Sayler, 2021). Although biometric techniques have used unique attributes "such as DNA, fingerprints, cardiac signatures, voice or gait patterns, and facial or ocular measurements" to identify individuals for decades, AI and ML and Big Data analytics advancement have dramatically expanded their applications (Sayler, 2021, p. 1). Biometrics could prove revolutionary. This area also raises significant legal and ethical questions that intelligence and security services must address.

The development of quantum technology presents another challenge for future studies. These technologies translate the principles of quantum physics into technical applications. The US Defense Science Board (DSB), an independent advisory function of the US Department of Defense, has identified three applications as the most critical from a defence perspective: quantum sensing, quantum computing, and quantum communication. Among these, quantum sensing is the most advanced and is close to deployment. It offers the potential to provide alternative positioning, navigation, and timing methods, which could allow military operations to function effectively, even in environments where Global Positioning System (GPS) is unavailable. Quantum sensors are also expected to play important roles in intelligence, surveillance, and reconnaissance. Although quantum computing remains nascent, it can revolutionise ML and other advanced computational processes. In addition, quantum computers may eventually be able to crack encrypted data, including classified and controlled unclassified information. At the same time, quantum communication could also pave the way for a secure network that links quantum sensors, computers, and other military systems. However, the practical deployment of quantum technologies is likely to face challenges owing to the fragility of quantum states, which are highly sensitive to disruptions from environmental factors, such as minor movement and temperature fluctuations (Sayler, 2020b).

In summary, quantum technology has the greatest potential to aid or hinder intelligence and security services. The magnitudes are immense; the difference between perfectly encrypted information and the complete decryption of one's encrypted information is

groundbreaking. The same applies to quantum sensing and the ability to continue operating at full performance in GPS-denied environments. In other words, as abstract as this area may be, intelligence and security services must allocate resources to ensure they do not fall behind in the quantum field.

A changing world order

Technological challenges have created new demands on intelligence and security services. We are currently living in a time of shifting world order. There is an ongoing shift in economic, political, and military power from the West to the East, and from the North to the South, altering the global balance of power and potentially transforming the entire existing world order (see, e.g. Bajpai, 2021; Christensen, 2016; Kanet and Moulioukova, 2022; Nordin and Weissmann, 2018; Weissmann, 2019b; Weissmann and Li, 2019; Carlsson *et al.*, 2015).

The global economy is undergoing a significant transformation, with Asia emerging as the largest trading region. This shift is driving the growth of a newly prosperous population and a distinct category of businesses. Together, China and India make up 36% of the global population and contribute 25% of worldwide GDP. As the world's economic focus continues to move towards Asia, India and China are poised to claim an increasing share of global output. By 2035, China's GDP is expected to surpass that of the United States, while India's GDP could exceed the United State's by 2075. This trend will likely result in a reorganisation of the global economic landscape, with the non-Organisation for Economic Co-operation and Development (OECD) countries projected to account for 57% of global GDP by 2030 (Sydney Business Insights, 2024).

As outlined by the European Commission (2020), the economic dominance of the G7 countries (USA, UK, France, Germany, Japan, Canada, and Italy) is expected to shift towards the Emerging 7 (China, India, Indonesia, Brazil, Russia, Mexico, and Turkey). By 2040, the combined economies of the E7 are projected to be twice the size of the G7 economies, compared to being equal in 2015 and only half as large in 1995. At the time of writing, in 2020, the European Commission estimated that China was likely to surpass the United States as the world's largest economy shortly before 2030. In contrast, the economies of Europe, Japan, and Russia are expected to experience a continued gradual decline in relative terms.

However, the post-COVID-19 developments have raised questions about China's capacity to overtake the United States economically (see, e.g. Carbonaro, 2024; Huang, 2024; Martin, 2024). After COVID, there have been publications, also from the European Commission, suggesting that the earlier consensus on China's inevitable rise to surpass the United States may now need to be reconsidered (see, e.g. Vandermeeren, 2024).

Nonetheless, as reported by *The Economist* (2023), forecasts from reputable sources, including from the OECD, the Lowy Institute, and the Centre for Economics and Business Research, project that China's GDP will eventually overtake America's at some point in the 2030s. *The Economist*'s own economist intelligence unit (EIU), for example, now thinks it will happen by 2039.

The Russian invasion of Ukraine has fundamentally changed and worsened Europe's security situation. This instability has been further aggravated by Israel's war against Hamas and the uncertainty in the Middle East. The unstable political situation in the United States has also contributed to the deterioration of the global security picture.

Intelligence and security services must operate within and manage an environment. Although opinions differ on the outcome of this power struggle, it is a fact that the world is changing, whether one likes it or not, and this is the reality that intelligence and security services must navigate and respond to. This uncertainty is evident because emerging economies, such as Brazil and Russia, which have shown rapid growth, have entered a recession. China, once the engine of global growth, slowed, while India continued to grow. Consequently, development in Africa has been severely affected by falling commodity prices. In addition, developments in Ukraine, Iran, the South China Sea, Taiwan, Afghanistan, and Iran do not automatically inspire optimism. The same can be said for countries in Russia's neighbouring regions (see Nilsson and Weissmann, 2024).

At the same time, the growing influence of the Global South, marked by increasing assertiveness in international forums, such as the United Nations and the G20, underscores its rising impact on global decision-making. Notably, the expansion of BRICS with the invitation of five new members joining in January 2024 or having been invited to join (Egypt, Ethiopia, Iran, and the United Arab Emirates) or invited to join (Saudi Arabia) is of significance as it challenges Western hegemony (Azevedo *et al.*, 2024; Melvin, 2023). It is estimated that BRICS+, the often-used informal name for the organisation following its expansion, now represents 37.3% of the global GDP, which is over double the EU's share (14.5%) (Jütten and Falkenberg, 2024, p. 1). BRICS' global significance can be expected to rise further following the January 6, 2025 announcement that Indonesia—the world's fourth most populous country and the first full member from Southeast Asia—has been admitted as a full member of BRICS. Jakarta's bid was approved by the bloc in 2023, nevertheless Jakarta did not ask to join until after a change in government following its presidential election in 2024 (Reuters, 2025).

In this shifting order, new actors seek their roles, and new power balances are established. Intelligence and security services must address new demands and challenges from the myriad of actors seeking new roles, including Iran, North Korea, Belarus, and the countries in Central Asia and Southern Caucasus as well as major powers, such as Russia and China, and managing the emergence of countries, such as India, Turkey, Brazil, Indonesia, Qatar, and Dubai, as well as the old powers seeking new roles in future world order. The choices made by countries such as Japan, the United Kingdom, and Australia have significant implications for European security interests; even if there is no direct negative intent towards friendly countries, the indirect consequences could be considerable.

Furthermore, intelligence and security services must remember that it is crucial to monitor and, when necessary, act on the rise of non-state actors. How these actors evolve and what they do have significant direct and indirect impacts on the security interests that intelligence and security services must protect. The necessity of dealing directly with antagonistic actors such as ISIL/ISIS and al-Qaeda and various forms of proxy-based intelligence operations, crime, sabotage, subversion, and terrorism is obvious. However, many other areas are not necessarily directly antagonistic, but they still affect the security interests of the armed forces. The development of megacities that act politically on the global stage and in areas traditionally within the domain of states and large corporations and billionaires acting independently of the global stage is significant for security interests.

The explosion of private military companies and private actors' involvement in warfare and conflicts should also be mentioned. Their role and the size have grown, and nothing indicates that this trend will change. Private actors have become integral to state military operations and warfare. At the same time, these risks alter how military operations and

warfare are conducted and, in the long term, challenge the monopoly and role of states, as they may eventually open up the possibility for companies, individuals, and other actors with monetary resources to acquire their military capabilities. Overall, the line between civilian and military becomes blurred in this area. This applies both within and outside Western countries (for a detailed review of the emergence of a privatised military industry, see McFate, 2017; Singer, 2008).

Conclusion: The way forward

There is no definitive recipe for protecting against hybrid threats and non-linear warfare, nor is there a single way to build resilience. No single actor or organisation can succeed in this task alone. We must continuously adapt as our adversaries and threats evolve.

How, then, do we address these challenges in practice?

The work must be pragmatic and flexible, involving many actors beyond intelligence and security services across various national and international sectors and levels. International cooperation must occur both within and beyond the North Atlantic Treaty Organization (NATO) framework. Good international cooperation outside the NATO framework is crucial, with like-minded allies and among the members. Such cooperation is particularly important because intelligence sharing has often been problematic within the NATO framework for confidentiality reasons. Hybrid operations are designed to surprise the adversary. When countermeasures succeed, the adversary changes its attack pattern, which requires a strategy encompassing all relevant actors and considering both short- and long-term perspectives. One potentially successful model is the development of comprehensive defence capabilities—the greater a society's resilience and recovery capability, the more effective are the countermeasures.

Intelligence and security services must collaborate closely with key international and regional partners within and outside their operational areas. Enhanced cooperation among different sectors and levels is crucial, as weaknesses in defence against future grey zone antagonist threats are often found in the gaps between them—gaps that adversaries can exploit to maximise their chances of success.

Therefore, it is important to build a platform for cooperation between and within the military, political, and economic spheres, including civil society, in defence and resilience building. Considering the increased importance of the information sphere and the increasing use of different types of cognitive warfare, actors within this sphere should be included regardless of whether in the public or private sector. Moreover, it is also essential to cover actors at all levels, from local and regional to national and international levels.

In conclusion, security and intelligence services must adapt to multi-dimensional threats by embracing flexible integrated strategies. Enhanced international collaboration, advanced technological integration, and a focus on resilience are vital to countering hybrid threats. The findings underscore the need for intelligence and security services to operate beyond traditional boundaries to effectively manage the complexities of future security environments.

Funding

The research was supported by funding from the Swedish Armed Forces.

Data Availability Statement

Not applicable.

Disclosure Statement
No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

References

Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J.M., Confalonieri, R., Guidotti, R., Del Ser, J., Díaz-Rodríguez, N. and Herrera, F. (2023) 'Explainable artificial intelligence (XAI): What we know and what is left to attain trustworthy artificial intelligence', *Information Fusion*, 99. doi: 10.1016/j.inffus.2023.101805.

Annell, S. and Lilja-Lolax, K. (2024) 'Personalförsörjning för den framtida militära säkerhetstjänsten—Utmaningar och möjligheter' [Staffing the future military security service—Challenges and opportunities], in Häggström, H. (ed.) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan, pp. 147–171. doi: 10.62061/OVWF1511.

Azevedo, D., Bakliwal, S., Chen, C., Gilbert, M., Koch-Weser, I., Lang, N. and McAdoo, M. (2024) *An evolving BRICS and the shifting world order*. Available at: https://www.bcg.com/publications/2024/brics-enlargement-and-shifting-world-order (Accessed: 05 September 2024).

Bajpai, K.P. (2021) *India versus China: Why they are not friends*. New Delhi: Juggernaut.

Bellasio, J., Slapakova, L., Huxtable, L., Black, J., Ogden, T. and Dawaele, L. (2021) *Innovative technologies shaping the 2040 battlefield*. Study/Panel for the Future of Science and Technology. Brussels: European Union. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690038EPRS_STU(2021)690038_EN.pdf (Accessed: 21 September 2024).

Bērziņš, J. (2020) 'The theory and practice of new generation warfare: The case of Ukraine and Syria', *The Journal of Slavic Military Studies*, 33(3), pp. 355–380. doi: 10.1080/13518046.2020.1824109.

Bostrom, N. (2014) *Superintelligence: Paths, dangers, strategies.* Oxford: Oxford University Press.

Carbonaro, G. (2024) 'China's chances of overtaking US economy "declining"', *Newsweek*, 6 February. Available at: https://www.newsweek.com/china-chances-overtaking-us-economy-declining-1866979 (Accessed: 03 December 2024).

Carlsson, M., Oxenstierna, S. and Weissmann, M. (2015) *China and Russia: A study on cooperation, competition and distrust.* Stockholm: Swedish Defence Research Agency.

Channel 4 (2020) *Queen's annual Christmas speech*. Available at: https://www.channel4.com/programmes/alternative-christmas-message/on-demand/19302-001 (Accessed: 05 September 2024).

Channel 4 (2024) *Deepfake Queen: 2020 alternative Christmas message*. YouTube. Available at: https://www.youtube.com/watch?v=IvY-Abd2FfM (Accessed: 05 September 2024). Real address available at: https://www.youtube.com/watch?v=zL9JR0A4yCU (Accessed: 05 September 2024).

Chekinov, S.G. and Bogdanov, S.A. (2013) 'The nature and content of a new-generation war', *Military Thought*, 22(4), pp. 12–23.

China State Council (2017) *A next generation artificial intelligence development plan*. English translation available at: https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ (Accessed: 21 September 2024).

Christensen, T.J. (2016) *The China challenge: Shaping the choices of a rising power*. New York, NY: W.W. Norton.

Clark, R.M. (2016) *The five disciplines of intelligence collection*. Washington, DC: CQ Press.

Colucci, L. (2021) *Great power strategic competition on earth and in space*. Available at: https://www.afpc.org/publications/articles/great-power-strategic-competition-on-earth-and-in-space (Accessed: 05 September 2024).

Conklin, E.J. (2005) *Dialogue mapping: Building shared understanding of wicked problems*. Chichester: John Wiley.

Corneliusson, L.-O. (2024) 'Internationelltsa marbete, enförutsättning för framgång inom underrättelse-och säkerhetstjänst?—"Need to Cooperate"' [International cooperation, a prerequisite for success in intelligence and security services?—"Need to Cooperate"], in Häggström, H. (ed.) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan (Swedish Defence University), pp. 111–130. doi: 10.62061/OVWF1511.

Doss, C., Mondschein, J., Shu, D., Wolfson, T., Kopecky, D., Fitton-Kane, V.A., Bush, L. and Tucker, C. (2023) 'Deepfakes and scientific knowledge dissemination', *Scientific Reports*, 13(1). doi: 10.1038/s41598-023-39944-3.

European Commission (2020) *Economic power shifts*. Available at: https://knowledge4policy.ec.europa.eu/foresight/topic/expanding-influence-east-south/power-shifts_en (Accessed: 2 December 2024).

European Data Protection Supervisor (EDPS), Technology and Privacy Unit (2023) *TechDispatch: Explainable artificial intelligence*. Available at: https://www.edps.europa.eu/system/files/2023-11/23-11-16_techdispatch_xai_en.pdf (Accessed: 05 September 2024).

European Parliament (2024) *AI investment: EU and global indicators*. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA(2024)760392_EN.pdf (Accessed: 05 September 2024).

Friedman, O. (2018) *Russian "hybrid warfare": Resurgence and politicisation*. London: Hurst & Company.

Galeotti, M. (2016a) 'Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"?', *Small Wars & Insurgencies*, 27(2), pp. 282–301. doi: 10.1080/09592318.2015.1129170.

Galeotti, M. (2016b) *Hybrid war or gibridnaya voina? Getting Russia's non-linear military challenge right*. Prague: Mayak Intelligence.

Goswami, N. and Garretson, P.A. (2020) *Scramble for the skies: The great power competition to control the resources of outer space*. Lanham: Lexington Books.

Huang, Y. (2024) 'Tipped power balance: China's peak and the US resilience', *Council on Foreign Relations*, 22 February. Available at: https://www.cfr.org/blog/tipped-power-balance-chinas-peak-and-us-resilience (Accessed: 02 December 2024).

Häggström, H. (2021) 'Hybrid threats and new challenges for multilateral intelligence cooperation', in Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. (eds.) *Hybrid warfare: Security and asymmetric conflict in international relations.* London: I.B. Tauris, pp. 132–144.

Häggström, H. (ed.) (2024) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan. doi: 10.62061/OVWF1511.

Ilachinski, A. (2017) *AI, robots, and swarms: issues, questions, and recommended studies*. Available at: https://www.cna.org/archive/CNA_Files/pdf/drm-2017-u-014796-final.pdf (Accessed: 05 September 2024).

Interaction Design Foundations (n.d.) *Wicked problems*. Available at: https://www.interaction-design.org/literature/topics/wicked-problems (Accessed: 21 September 2024)

International Institute for Strategic Studies (IISS) (2015) *The military balance 2015*. Abingdon: Routledge, for IISS.

Jones, H.H. (2022) *When AI rules the world: China, the U.S., and the race to control a smart planet*. New York, NY: Bombardier Books.

Jütten, M. and Falkenberg, D. (2024) *Expansion of BRICS: A quest for greater global influence?* (PE 760.368). Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760368/EPRS_BRI(2024)760368_EN.pdf#page=2.53 (Accessed: 02 December 2024).

Kanet, R.E. and Moulioukova, D. (eds.) (2022) *Russia and the world in the Putin era: From theory to reality in Russian global strategy*. New York, NY: Routledge.

Karlson, G. (2024a) 'Den militära säkerhetstjänsten och totalförsvaret' [The military security service and total defence], in Häggström, H. (ed.) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan (Swedish Defence University), pp. 131–145. doi: 10.62061/OVWF1511.

Karlson, G. (2024b) 'Legitimitet och legalitet för säkerhetstjänsten idag och imorgon' [Legitimacy and legality of security services today and tomorrow], in Häggström, H. (ed.) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan (Swedish Defence University), pp. 69–84. doi: 10.62061/OVWF1511.

Konkel, F. (2024) 'The US intelligence community is embracing generative AI', *Nextgov/FCW,* 3 July. Available at: https://www.nextgov.com/artificial-intelligence/2024/07/us-intelligence-community-embracing-generative-ai/397849/ (Accessed: 05 September 2024).

Lee, K.-F. (2018) *AI superpowers: China, Silicon Valley, and the new world order*. Boston: Houghton Mifflin Harcourt.

Lunan, M. (2018) 'Biometrics', *The Three Swords Magazine*, 33, pp. 37–41. Available at: https://www.jwc.nato.int/images/stories/threeswords/Biometrics_2018.pdf (Accessed: 20 September 2021).

Manson, K. and Shepherd, C. (2020, 1 September) *US military officials eye new generation of space weapons*. Available at: https://www.ft.com/content/d44aa332-f564-4b4a-89b7-1685e4579e72 (Accessed: 05 September 2024).

Martin, N. (2024) *Will China ever overtake the US economy?*, 15 July. Available at: https://www.dw.com/en/will-china-ever-overtake-the-us-economy/a-69591117 (Accessed: 03 December 2024).

McFate, S. (2017) *The modern mercenary: Private armies and what they mean for world order*. Oxford: Oxford University Press.

Mehta, A. (2020) 'What is a space weapon, and who has them?' *C4ISRNet*, 27 May. Available at: https://www.c4isrnet.com/battlefield-tech/space/2020/05/27/defining-what-a-space-weapon-is-and-who-has-them/ (Accessed: 05 September 2024).

Melvin, N. (2023) *Building up the BRICS: An emerging counter-west order?*. Available at: https://www.rusi.org/explore-our-research/publications/commentary/building-brics-emerging-counter-west-order (Accessed: 05 September 2024).

Metz, C. and Weise, K. (2023) 'Microsoft to invest $10 billion in OpenAI, the creator of ChatGPT', *The New York Times,* 23 January. Available at: https://www.nytimes.com/2023/01/23/business/microsoft-chatgpt-artificial-intelligence.html (Accessed: 05 September 2024).

Nilsson, N. and Weissmann, M. (eds.) (2024) *Russian warfare and influence: States in the intersection between East and West*. New York, NY: Bloomsbury Academic.

Nordin, A.H.M. and Weissmann, M. (2018) 'Will Trump make China great again? The belt and road initiative and international order', *International Affairs*, 94(2), pp. 231–249. doi: 10.1093/ia/iix242.

O'Connell, K. and Salter, A.W. (2021) 'Great power competition in the final frontier: How to keep the peace in space', *National Review, 0*4 May. Available at: https://www.nationalreview.com/2021/05/great-power-competition-in-the-final-frontier-how-to-keep-the-peace-in-space/#slide-1 (Accessed: 05 September 2024).

Office of the President of the Russian Federation (2019) *Decree of the president of the Russian Federation on the development of artificial intelligence in the Russian Federation*. Available at: https://cset.georgetown.edu/publication/decree-of-the-president-of-the-russian-federation-on-the-development-of-artificial-intelligence-in-the-russian-federation/ (Accessed: 21 September 2024).

Omand, D., Bartlett, J. and Miller, C. (2012) 'Introducing social media intelligence (SOCMINT)', *Intelligence and National Security*, 27(6), pp. 801–823. doi: 10.1080/02684527.2012.716965.

Palmgren, A. (2020) 'Gråzonsproblematik [Grey zone problem]', *The Royal Swedish Academy of War Sciences Proceedings and Journal*, January–March (1), pp. 156–159. Available at: https://kkrva.se/hot/2020:1/palmgren-grazonsproblematik.pdf (Accessed: 05 September 2024).

Pawlak, P. (2017) *Cyber security woes: WannaCry?* Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_13_Cyber.pdf (Accessed: 06 March 2020).

Petersson, O. (2024) 'Antagonistiska hot ifredstid' [Antagonistic threats in peacetime], in Häggström, H. (ed.) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan, pp. 17–37. doi: 10.62061/OVWF1511.

Rempfer, K. (2018) 'Ever heard of "deep fake" technology? The phony audio and video tech could be used to blackmail US troops', *Military Times*, 19 July. Available at https://www.airforcetimes.com/news/your-air-force/2018/07/19/ever-heard-of-deep-fake-technology-the-phony-audio-and-video-tech-could-be-used-to-blackmail-us-troops/ (Accessed: 21 September 2024).

Reuters (2025) 'Indonesia joins BRICS bloc as full member, Brazil says', *Reuters*, 7 January. Available at https://www.reuters.com/world/indonesia-join-brics-bloc-full-member-brazil-says-2025-01-06/ (Accessed: 09 January 2025).

Rittel, H. and Webber, M. (1973) 'Dilemmas in a general theory of planning', *Policy Sciences* 4(2), pp. 155–169. doi: 10.1007/BF01405730

RT International (2017) *Whoever leads in AI will rule the world': Putin to Russian children on Knowledge Day*, *0*5 September. Available at: https://www.rt.com/news/401731-ai-rule-world-putin/ (Accessed: 05 September 2024).

Sayler, K.M. (2020a) 'Artificial intelligence and national security', *Congressional Research Service*, R45178, updated 10 November 2020. Available at: https://sgp.fas.org/crs/natsec/R45178.pdf (Accessed: 21 September 2024).

Sayler, K.M. (2020b) 'Defense primer: Emerging technologies', *Congressional Research Service*, IF11105, updated 30 November 2020. Available at: https://crsreports.congress.gov/product/pdf/IF/IF11105/6 (Accessed: 21 September 2024).

Sayler, K.M. (2020c) 'Emerging military technologies: Background and issues for congress', *Congressional Research Service*, R46458, updated 10 November 2020. Available at: https://crsreports.congress.gov/product/pdf/R/R46458/5 (Accessed: 21 September 2024).

Sayler, K.M. (2021) 'Biometric technologies and global security', *Congressional Research Service*, IF11783, updated 30 March 2021. Available at: https://www.everycrsreport.com/files/2021-03-30_IF11783_3e6876685b08bb19fd644d543cebf72064466b7b.pdf (Accessed: 21 September 2024).

Sayler, K.M. (2024) 'Emerging military technologies: Background and issues for Congress', *Congressional Research Service*, R46458, updated 22 February 2024. Available at: https://sgp.fas.org/crs/natsec/R46458.pdf (Accessed: 03 September 2024).

Sheehan, M. (2023) *China's AI regulations and how they get made*. Available at: https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en (Accessed: 5 September 2024).

Singer, P.W. (2008) *Corporate warriors: The rise of the privatized military industry*. Ithaca, NY: Cornell University Press.

Smagh, N.S. (2020) 'Intelligence, surveillance, and reconnaissance design for great power competition', *Congressional Research Service*, R46389, updated 04 June 2020. Available at: https://sgp.fas.org/crs/intel/R46389.pdf (Accessed: 21 September 2024).

Sydney Business Insights (2024) *Economic power shift: Megatrends*. Available at: https://sbi.sydney.edu.au/megatrends/economic-power-shift/ (Accessed: 02 December 2024).

The Economist (2023) 'When will China's GDP overtake America's? Daily chart', *The Economist*, 7 June. Available at: https://www.economist.com/graphic-detail/2023/06/07/when-will-chinas-gdp-overtake-americas (Accessed: 05 September 2024).

Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K and McCue, M. (2018) *Addressing hybrid threats*. Stockholm: Swedish Defence University.

US Naval War College (USNWC) (n.d.) *Intelligence studies: Types of intelligence collection*. Available at: https://usnwc.libguides.com/c.php?g=494120&p=3381426 (Accessed: 05 September 2024)

Vandermeeren, F. (2024) *Understanding EU-China economic exposure*. Single Market Economics Briefs, No. 4. Luxembourg: European Union, Publications Office. Available at: https://single-market-economy.ec.europa.eu/system/files/2024-01/EconomicBrief_4_ETBD_23_004ENN_V2.pdf (Accessed: 03 December 2024).

Viksten, R. (2024) 'Försvarsunderrättelse lagstiftning i Sverige, Finland, Norge och Danmark – en jämförelse och en del nyheter' [Defence intelligence legislation in Sweden, Finland, Norway, and Denmark – a comparison and some updates], in Häggström, H. (ed.) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan, pp. 85–109.

Weissmann, M. (2019a) 'Hybrid warfare and hybrid threats today and tomorrow: Towards an analytical framework', *Journal on Baltic Security*, 5(1), pp. 17–26. doi: 10.2478/jobs-2019-0002.

Weissmann, M. (2019b) 'Understanding power (shift) in East Asia: The Sino-US narrative battle about leadership in the South China Sea', *Asian Perspective*, 43(2), pp. 223–248. doi: 10.1353/apr.2019.0009.

Weissmann, M. (2021) 'Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone', in Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds.) *Hybrid warfare: Security and asymmetric conflict in international relations*. London: I.B. Tauris, pp. 61–82.

Weissmann, M. (2024) 'Framtida hotbilders påverkan för säkerhetstjänsterna' [Impact of future threats on security services], in Häggström, H. (ed.) *Framtidens säkerhetstjänst i totalförsvaret* [*The future of security services in total defence*]. Stockholm: Försvarshögskolan, pp. 38–67. doi: 10.62061/OVWF1511.

Weissmann, M. and Li, M. (2019) 'Introduction to the special issue', *Asian Perspective*, 43(2), pp. 215–221. doi: 10.1353/apr.2019.0008.

Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds.) (2021) *Hybrid warfare: Security and asymmetric conflict in international relations*. London: I.B. Tauris.