IMPLICATIONS OF ARTIFICIAL INTELLIGENCE FOR INTELLIGENCE ORGANIZATIONS IN THE CONTEXT OF GLOBAL SECURITY TRANSFORMATIONS

Mihai CIOBANU*

Abstract:
The period in which artificial intelligence (AI) was treated in a speculative way in the field of national security appears to be over. The current dynamics on the geopolitical stage generated new technological needs which stimulated innovation even further, contributing to an increased inter-play between supply and demand. Between 2023 and 2025 AI moved from image and video generation to broader and more interactive environments, all in the light of new players and new models joining in the race. This article synthesizes developments and assesses the implications of AI advancement over national security and especially over intelligence agencies. The acceleration of AI capabilities and global reactions over large-scale deployment have prompted intelligence agencies to explore the implications for national security and have also led to organizational changes. AI is truly an agent of change, with the potential to bring organizational transformations in intelligence work, all while also being an agent of multiplication and creation of new risks, both external and internal, for national security agencies.

Keywords*: artificial intelligence; national security; intelligence; Geopolitics; technology; transformation.*

Introduction

AI's accelerated development is reshaping the national security and the everyday practice of intelligence. Generative systems now produce not only text and images but also video, interactive digital environments and applications designed for specific tasks. All of these

* PhD candidate, "Mihai Viteazul" National Intelligence Academy Bucharest, email: ciobanu.mihai@animv.eu. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

developments affect how data is collected, processed and used, at a scale and speed that exceeds human capacity. In addition, there is also a need to protect data. For intelligence agencies, AI represents a dual challenge: on one hand, it increases the volume and quality of collection and analysis processes and on the other hand, it is a catalyst for new vulnerabilities: through the public exposure of sensitive information, new types of cyber-attacks, disinformation and influence operations. In this article we will refer to developments from 2023 to the first part of 2025. During this period, the *DeepSeek* episode was a global stress test for governments and regulators in the western world. Our aim is to identify and analyse various factors that make up the problems that intelligence agencies must manage in relation to AI development and deployment. At the same time, we will focus on operational and organizational implications for intelligence agencies, brought by these factors. Finally, we will explore the perspective of congruence and intersections between AI and the intelligence domain. The text relies both on an analysis of the specialized literature, using techniques specific to the content analysis and semantic meta-analysis method, as well as on our observations during the research.

Accelerating the evolution of AI capabilities

To talk about AI just a few years ago meant to talk about emergence. The advancements brought by competition led to a very fast paced evolution of AI capabilities. If the year 2023 was associated with text and image generation at a very wide scale, 2024 brought rapid progress in video and music generation. By early 2025, both research and industry shifted their interest and concern towards connecting different environments in an interactive matter, the best example being the possibility of creating playable game experiences from 2D sketches. This tendency alone is an indicator that content generation is experimenting with the convergence of planning and drafting with simulation (O'Donnel, Heaven, and Heikkilä, 2025). Of course, these kinds of shifts are enabled by development and improvements in hardware, expanding the feasible size and responsiveness of AI models, making way for new functionalities.

In parallel with the AI industry and as a natural response to technological advance, organizations started reframing their approach to operating with huge amounts of data. The literature notes an increased interest in tools that perform specific tasks, whose impact is quantifiable in various professional environments. Intelligent functionalities are increasingly related to workflows and workload and less to generic content generation (Davenport and Bean, 2025).

Davenport and Bean (2025) identify five trends for AI in 2025 that place emphasis on:

1. reassessing the promises of the industry regarding capabilities and advancements of AI models and agents;
2. moving from perception-based enthusiasm to systematic evaluation of generative AI;
3. prioritizing new data production and its management;
4. investing in leadership and governance models regarding managing lots of data and AI models;
5. clarifying responsibilities and implementing oversight across organizations in regard to AI models use.

An equally significant trend has been noted in the gradual shift of organizations toward what is now known as data-driven cultures. Davenport and Bean (2025) noted that 2024 marked a doubling in the number of companies that prioritized AI data management and AI training data management, establishing practices in this regard, The same authors noted that 2025 brought a slowdown, with only 33% of the companies maintaining the same pace of establishing internal policies and cultivating a culture related to AI implementation. A survey cited by the same authors showed that cultural and the management of change remained the primary obstacles in consolidating AI adoption by individuals. This indicates, of course, that the success of AI integration is not only dependent on innovation, but on the ability of organizations to reshape their own cultures and workflows as well. Domanska (2025) emphasizes that in the very close future organizations will need to appoint specialized AI officers who should watch be responsible for the implementation of AI and for formulating and changing principles and procedures regarding the use of AI in their organizations.

The overall picture is one in which AI models (and maybe AI agents in the near future) and organizational practices need to co-evolve and adapt to one another. As AI models demand broader, higher-quality data, organizations must increase investment in quality assurance and data security, as well as adapt the management perspective. The co-integration of these components directly affects the feasibility and the quality of deploying AI within intelligence agencies, where ownership, availability, reliability and timeliness of data are crucial. The rapid pace of AI development became visible not only in the market or in the industry but also in public reactions across the globe.

Global architects of public policies on AI

Progress and implementation of AI brought the need for policies and legal frameworks all around the globe. In this capacity USA, EU and China claimed the leader position, be it verbally or by action, their efforts setting them, one by one, as global leaders in research, development, implementation, use and AI governance in general. Each one has a different tone regarding governance and competition, publicly recognized or just assumed. Different authors note that this leadership race influences not only development and innovation, but also policy making around the globe, with an attentive focus on security matters (Clegg, 2024; Bhuiyan, 2024; China Aerospace Studies Institute, 2023).

The USA adopted a practical approach to AI policies between 2024 and 2025, focused on inter-organizational cooperation for the advancement of the USA. In October 2024 the White House adopted a document[1] through which public institutions were directed to establish policies regarding AI implementation and use, with the aim of strengthening governance mechanisms and safeguarding all of the technological developments from various external threats. The document anchored policy making in democratic values and cooperative principles, pragmatically setting a balance between innovation and resilience (Durland and Siegmann, 2024). In November 2024 *Meta* announced that

[1] Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence.

national security agencies of the USA would be granted access to the open-source version of its *Llama* LLM, further reinforcing the tone set by the memorandum in October 2024. Meta's justification revolved around adherence to democratic principles of ensuring transparency and accountability, in the greater interest of the general public, by sustaining national security (Bhuiyan, 2024; Clegg, 2024). July 2025 brought the current administration's view over AI governance, with the adoption of a new document called *Winning the Race – America's Action Plan*. Starting with the title, the entire content of the document reflects that USA's final goal is maintain global leadership over AI in general. This document sets a very clear path of AI experimentation and learning through practice, in line with principles and values specific to democracies (The White House, 2025). A complementary perspective is brought by Walker (2025), who affirmed that USA has to prioritize AI governance on three coordinates: 1) investments in hardware and software infrastructure, 2) integration of AI in defence and in intelligence domains and 3) strategic coordination of state investments in order to ensure leadership over China. This vision further reflects a pragmatic orientation, in line with recent governmental and presidential initiatives. All of these facts state clearly that USA is on a trajectory of aligning principles and values with pragmatism, ensuring a fluid AI governance policy making process, as long as the results provide global strategic advantages for the USA.

In contrast with USA's practical orientation, the EU has methodically advanced a policy and law driven approach to AI governance. The peak of this fact is the adoption of EU AI Act, the biggest and most comprehensive legal framework designed so far, which regulates AI development, implementation and use across member states (Desmarais, 2025). This act reflects EU's philosophy of governance, that of where innovation must be infused with certainty, responsibility, transparency and, above all, respect and protection of fundamental rights. In February 2025, at the *Paris AI Action Summit*, the Commission President stated that EU's advantage lies in combining cooperation between member states with open and common principles and values, all of which provide a framework that is not a general constraint, but a driver of responsible competition and safe innovation (von der Leyen, 2025). Desmarais (2025) states that a coalition of about 20 companies

reserved 150 billion euros for building an EU specific AI ecosystem, in collaboration with the EU Commission and under regulatory frameworks that combine advancements with oversight. In this matter, EU has a combined agenda, wanting to create trustworthy datasets, central and cross-members governance mechanisms, aligning AI policies with EU's fundamental principles of human-centricity. EU's AI leadership model is about adopting rules and norms, sacrificing rapid experimentation and deployment for ensuring individual, collective, state and union security and global trust.

China followed a different AI policy trajectory, further highlighting the contrasts in the global AI governance landscape. The document *Interim Measures for the Management and Generative AI Services*, emitted in July 2023, established strict AI related requirements that stretch from content moderation to security related reviews and interventions (China Aerospace Studies Institute, 2023). The Chinese approach is characterized by state control and oversight exercised through an extensive regulatory framework, public and not public. China doesn't see AI just as a means and a goal towards global leadership, it sees AI as a tool designed for governmental and social use, in accordance with national priorities. The regulatory framework aims to provide social stability and, above all, national security. Of course, the Chinese way is one of pursuing great economic and industrial achievements and in this case, AI is being treated as a catalyst of achieving global supremacy (Zhu, 2025; Lee, 2025). The Chinese model uses regulations both as instruments of internal control and as a platform of pushing international leadership and influence further. Considering this, we could say that the Chinese way is that of state driven over regulation, where every step in AI development has to be of value to the country and has to be subordinated to national interests. This development is always under the close oversight of authorities, AI providers being obliged to serve national interests first, aligning innovation and deployment with the governmental views and goals.

We called these major powers AI architects because they design AI's advancement in the world. These three major actors – USA, EU, and China – ground their strategies in different ways and approaches:

- USA sets principles and values aligned with democracy while advancing AI through practice, experimentation and public-private cooperation, all while seeking global leadership, which we call *the practical social approach to AI*.
- The EU treats AI governance in line with laws and policies, infusing AI with a normative framework that prioritizes compliance with fundamental rights; which we call *the practical normative approach to AI*.
- China adopts a state-first policy, prioritizing oversight over AI providers and users, all in the name of national interests, for economic and strategic supremacy; which we call *the practical over-regulated approach to AI*.

For intelligence agencies and for national security communities, these differences are not only words or mere theories. They are the reality in which AI tools are shaped and made available both in the benefit of society and for doing harm. Understanding regulatory frameworks and global views on AI is essential in navigating across different logics, used both by allies and by adversaries. In this regard, intelligence agencies might be able to build resilience through emulation of each approach, in order to sustain cooperation and to be prepared for adversarial usage of AI. One episode of great importance towards illustrating all of the above was generated by the deployment of a new app, called *DeepSeek*, which debuted in 2025 and took over the world rapidly. This fact alone exemplified how quickly a technological innovation can evolve into a real test of institutional resilience at a global scale.

DeepSeek: a global stress test

The emergence of the Chinese made *DeepSeek* Large Language Model (LLM) in late 2024 and early 2025 crystallized many of the dynamics between development and regulation into a single, highly visible episode, representing a practical manifestation of the accelerated development and adoption of AI capabilities. In early 2025, it became one of the first global scale tests of how different governments and different intelligence communities respond when new AI models spread faster than organizations can adapt. *DeepSeek* serves as a case study of institutional resilience in front of rapid innovation and slow public policy

adaptation. It was reported that by 13 February 2025, *DeepSeek* was the most downloaded application globally, available in approximately 156 states, with around 22.15 million daily active users and approximately 33.7 million monthly active users in January 2025. Half of those users were based in China, India, and Indonesia (Backlinko, 2025). The speed and the scale of adoption raised national security concerns, especially around data handling in general and personal data in particular. Different governments responded in different ways, for example: Italy's data protection agency suspended personal data processing for Italian citizens; Australia banned the app from all government cell phones claiming national security risks; Taiwan imposed similar restrictions, banning *DeepSeek* altogether, concerned about risks to their national security. Other countries, such as Belgium, The Netherlands, South Korea and the state of Texas opened investigations into how the Chinese made LLM manages data and interactions (Canales, 2025; del Rosario, 2025; Smalley, 2025; Sterling, 2025; The Brussels Times with Belga, 2025; Data General, 2025). A survey conducted under Euractiv (2025) showed that Cyprus, Czech Republic, Estonia, Hungary, Lithuania, Malta, Romania and Sweden reported no registered complains, while Austria, Bulgaria, Denmark, Finland, Latvia, Portugal, Slovakia and Slovenia did not respond to the survey. All of the other European states either took some measures or started investigations through their legitimate institutions.

Beyond the multiple ways in which states responded to *DeepSeek*, the debate around this app converges on national security implications. Different authors (Canales, 2025; Booth, Krupa, and Giuffrida, 2025) note that suspicions arise from the Chinese way of collecting and processing information which pose serious concerns if personal data and strategic data is involved. As plausibly presumed, the privacy and individual data protection issues are more present in the European discourse, while other political regimes treat things differently, with bans and limitations that have the role to prevent and protect. As we sweep over the literature, we see variations in the global public positions regarding *DeepSeek*, spanning from personal and general data protection to national security concerns. In both cases risks and vulnerabilities can rapidly become active threats which intelligence services and police agencies have to deal with. Starting from those reasons alone, intelligent

technologies have to be treated seriously, not only as consumer technologies, but also as potential vectors of vulnerabilities, risks and threats posed both to individual, collective and national security.

The literature indicates several types of specific vulnerabilities. These include the possibility of losing human control over intelligent technology and the risk of AI making undesirable autonomous decisions (Galliot and Scholz, 2020; Rowe, 2022; Zhou, 2024). Other risks are related to uncontrolled data collection and poor data management, which can lead to: compromised confidentiality, data alteration, and malicious use of data (Roberson, și alții, 2022; Klaus, 2024). The literature also contains numerous references to the lack of transparency of algorithms and the possibility that AI may adopt and reproduce human biases, leading to discrimination and solutions that are disproportionate to the requests (Michel, 2023; Bode and Bhila, 2024). Zhou (2024) also mentions the risk of escalating military conflicts against the backdrop of armament with intelligent technology.

DeepSeek's fast adoption amidst reasonable questions regarding personal and collective security provides at least three valuable lessons for debate in and around intelligence services:

1. the operational landscape is both national and transnational. AI apps grow and spread fast, while the organizational response can and usually is slower. Getting ready to respond to the unknown is essential and remains a constant of intelligence work. This alone is a sufficient argument for fast strategic debates that have to lead to harmonised tactical and operational responses;
2. the most acute and present risk revolves around data management, data security and dependencies that support the collection and the administration of huge data amounts. This alone brings concerns regarding potential new threats and national security risks revolving around all that is placed under the AI umbrella;
3. for adversaries, legal action and political decided bans might be an indicator of organizational readiness. Intelligence agencies might have to assess what effects would public declarations

and normative actions produce both on their own organizations and on the adversaries. The debate, in this matter, is about how public action can help or slow down the efforts of ensuring national security.

Beyond its controversies, the *DeepSeek* case highlights the strategic implications of AI on national security and for intelligence agencies. It demonstrates that vulnerabilities and risks can also emerge from rapid and uncontrolled diffusion of technology across various jurisdictions. For intelligence services, *DeepSeek* represents an important turning point, showing how various transnational approaches by different state actors are shaping a new operational landscape. In this new operational landscape, debates on global technological advances and global official public positions are mixed with new operational challenges in creating and securing national security.

AI and operational risks in intelligence

Just as *DeepSeek* was treated by some countries as a potential risk to national security, when viewing AI as a whole from a national security perspective, it is imperative to see that in addition to capabilities and opportunities, AI also brings risks. Intelligence agencies have to adapt and learn how to manage both of these two different sides of AI. Aside from pure risks, various authors (Walker, 2025; Bendett, 2024; Bond, 2024) have warned that AI could become a risk multiplier, especially in domains where automation, speed and scale can grant great advantages. The best example to this date is that of generative models that are being used widely for large-scale influence operations and disinformation. Thus, national security adversaries gain the ability to produce rapid, diverse and well-tailored narratives, supported by convincing photos and videos. AI also has the potential to lower costs and to offer precision and speed in support of malicious cyber operations (Walker, 2025). Amongst all of these, the current geopolitical situation generates great interest in infusing military tools with AI, directly affecting the way intelligent technology develops (Bond, 2024; Bendett, 2024). Bendett (2024) claims that even small progresses made in enhancing military capabilities with AI can shift tactical and operational balances, suggesting that the modern battlefield might see great disproportions

in relation with what the military expects. Considering all of these situations we might have to see AI not just a simple tool, but as a real catalyst of wide societal and historical change.

For intelligence agencies, all of the above create a very urgent need to become resilient before malicious actors can gain any kind of advantage. Despite all identified risks, it appears that for now, with the exception of disinformation and influence campaigns, adversaries have not fully exploited AI for offensive actions. Walker (2025) suggests that national security agencies still have a strategic advantage and can gain the upper hand, particularly in collection, detection and response. However, the author suggests that this period of opportunity is probably coming to an end soon. As the industry formed around AI develops more advanced hardware and more sophisticated software, more powerful and diverse models will appear, with diverse applications. Eventually, these models will spread and it is a matter of time until they will start being used for harm. Intelligence must act proactively, focusing greatly on monitoring how adversaries think, direct, innovate, implement and use AI. This is probably easier said than done, as the effort must be conjoined with a strong support from public policy makers. If we note the fact that intelligence organizations have to follow laws and ethical codes while some adversaries have no such limitations, the urgency for dialogue and for creating supporting legal frameworks becomes even greater.

The complexity of operational risks derivate from the bivalent way of using AI. Systems that are designed for benign use can become malicious in hands of malicious actors. This bivalence complicates the task of intelligence agencies, as they not only need technical expertise and legal frameworks, but a profound support from targeted research as well. Research in this field should be able to provide extensive contextual knowledge of how allies and adversaries see, develop, adapt, implement and use intelligent technology. The fact that AI can bring both opportunities and vulnerabilities creates a paradox that has to be carefully managed so that the adoption of AI at all levels of society does not produce more harm than good. Intelligence agencies must be ahead in this game and have to produce strategies that ensure resilience in providing and maintaining national security.

Organizational change and data management in intelligence

Another aspect of great importance for intelligence agencies comes from within. While the operational risks posed by AI are related to external influence and the specific nature of national security information, organizational change and adaptation are related to the influence of AI implementation in intelligence organizations. This is another perspective related to the interaction between AI and intelligence in our effort to investigate change at the level of intelligence agencies.

While looking at the private sector, Davenport and Bean (2025) documented that the year 2024 saw a doubling of organizations that made a priority out of data governance. The reality of data driven decision making is now being automatized and promises in this field might increase AI financing and adoption. While the 2024 data showed a doubling of organizations reporting data-driven culture, the 2025 survey results – which reflect responses at the time of study – suggest some regression or stagnation, with only 37% of respondents claiming to work in a data and AI driven organizations. The same moment in 2025 showed that the momentum of adopting data governance policies has slowed, with only 33% of all respondent organizations stating that they would develop data governance strategies. An interesting fact is that 92% of the questioned organizations affirmed that obstacles to full adoption and integration of AI reside in cultural views and management of change barriers. Another study conducted by McKinsey (2025) confirms the trend observed by Davenport and Bean, according to which organizations are becoming increasingly open to adopting AI, with some even becoming dependent on AI in certain internal processes. The study revealed that more than three-quarters of respondents say that their organizations already use AI solutions in at least one process. Among these processes, McKinsey (2025) highlights the automation of certain tasks, data analysis, and decision support. At the same time, the management levels of organizations are seeking to establish internal policies to ensure AI governance. The issues that AI brings to organizations are related to security, privacy, and transparency. McKinsey's (2025) conclusions argue that the success of AI integration depends both on technological innovation and on adapting the

organizational culture in terms of taking responsibility and adopting clear internal policies related to AI. We can clearly see that even though technology can rapidly advance, it is of no use if institutions that implement it are not ready for that. Without being ready, organizations will probably misuse or underutilize sophisticated tech capabilities. The problems of organizational culture and management of change are more acute in intelligence agencies, which usually operate within strict legal limits and with secrecy. This alone can make agencies more conservative. Implementation of AI will probably pose challenges in changing tools, methods, workflows, ways of treating and operating with data, all under adapted strategies and policies. As Davenport and Bean (2025) note, organizational transformations need sustained investment in human capital and in management transformation. The authors talk about cultivating trust, responsibility and adaptability, being aware of the fact that organizational cultures change at a slow pace. Intelligence organizations cannot always have the luxury of changing at a slow pace, the security landscape through which they have to navigate generating the need of fast and precise action. Therefore, intelligence agencies have to find a balance between creating resilience in front of new risks and introducing new technologies in their own ranks.

Another key issue regarding AI adoption in intelligence for national security is related to data. Roose (2024) showed that availability of high-quality data for AI training is becoming more and scarcer. Models need to continuously train; therefore, new data has to be gathered or crated. For the data to become high-quality, it needs to be cleaned, curated and structured, otherwise it could infect models with factual mistakes, biases, wrong connections and with all the consequences that this entails. According to Davenport and Bean (2025), in 2025 organizations started to realize that being competitive is not only about buying or developing the best AI models, but in data governance and data security. Intelligence services already practice collection, cleaning, structuring, verifying and analysis of data, producing high-quality information. For AI to bring scale, speed, accuracy and reliability, intelligence agencies need to gain new professional skills and orient themselves towards interdisciplinary collaboration; this fact alone

would probably be one major driver of serious cultural changes within organizations.

Organizational change will probably be a result of AI implementation and integration in various work environments. Without data governance and data security, management support and adaptive, open cultures, intelligence agencies risk becoming slow and inefficient in front of technical advancements of both their allies and their adversaries. As different authors note, success is not only about gaining cutting-edge hardware and software, but in transforming the way organizations approach AI regarding accountability, responsibility and ethical data governance (Davenport and Bean, 2025; Domanska, 2025; Walker, 2025). For intelligence agencies alone this means that their future successful missions would surely depend on internal cultural updates and normative reforms.

Conclusions

The accelerated creation and evolution of AI models between 2023 and 2025 has demonstrated that progress has the potential of not being dependent on specific industries any more. Everyone, with little or no training at all, can now generate images, videos, music and can even design interactive environments such as games and applications. Malign use of generative models has now become the main driver for disinformation, influence, control and manipulation. For intelligence agencies, this acceleration of evolving and rapid implementation of AI poses great challenges, as collection and analysis of national security relevant data now requires a new approach and a new mentality within the intelligence field of work.

At a global scale, from the perspective of policy architects and frameworks, the global race is led by three major actors, providing three distinct models. USA anchors AI development in democratic values while pursuing global leadership. This creates the need for private-public cooperation, practical lessons and great strategic investments, leading to a real *social practice* regarding AI. The EU approach is constructed around legal frameworks and specific regulations, seeing the norm as the fundamental base for trust in AI development. This leads to a *normative*

practice. China, on the other hand, believes that state driven regulation and implication is the way, prioritizing national interest in pursue of global leadership. Their ambition of gaining geopolitical supremacy and their way of over-implicating public institutions in everything creates an *over-regulated practice*, in which AI development has to have the first and ultimate goal of sustaining national interests.

The *DeepSeek* moment taught the world that a well promoted new application can take over the world with an unseen rapidity. With this kind of challenges, states are usually slow in response, as national action can only be taken after rigorous assessments and strategic analysis, a very important part of it being usually carried by intelligence communities. The key lesson here is that AI models can become matters of concern for national security, not only because new technological functionalities, but because of their potential security consequences.

Just as *DeepSeek* exemplified, from an operational perspective, AI creates a clear path for new vulnerabilities, risks and threats that intelligence have to take account of. Various authors warned about AI's potential to enhance cybercrime, to conduct disinformation and influence campaigns, to shift battlefield balances, to manipulate and control. Even though adversaries have not yet fully exploited all of AI's possibilities, the rhythm of accelerated innovation and the wide availability of models creates the need for intelligence services to anticipate and be prepared for malign use of AI as well as to develop means and methods of reaction.

For intelligence organizations to fully benefit from AI, they would have to be ready and adapt to cultural changes, while finding the best ways of assuring data governance. As the studies cited in this article have shown, public and private institutions attempted to create this type of change, only to slow down for the moment. Knowing that Intelligence agencies are slower in cultural change, both strategic management and operational layer have to be aware and acknowledge that AI governance has to be quickly assessed and implemented, so the risk of misutilization or underutilization of intelligent technology remains low.

Considering all of the above, we can come to the conclusion that AI development and deployment, global regulatory actions and organizational challenges brought by AI brought altogether pose a significant challenge for intelligence agencies. Their slower way of

adapting to cultural changes while still having to provide foresight, profound and clear knowledge of reality and rapid response mechanisms pose a problem. The mission of assuring national security in the age of AI is as hard as it gets for intelligence agencies because of different and varied currents and influences that arrive from different points. Agencies have to: adapt to new intelligent technology, finding benefits and assessing threats; navigate through various policies, that govern their own activity and that govern their adversaries' activities; be ready to respond to very rapid deployment and adoption of AI models in various domains; adapt and overcome their own inside difficulties regarding AI-brought change in organizational culture; be ready to learn how to use AI effectively to enhance their methods of assuring national security. Intelligence has to find ways of adapting from within while being ready for imposed changes from outside of their professional world. Integrating, using and understanding AI effectively has to be subordinated to the ultimate goal of assuring national security.

While the global race regarding AI supremacy brings huge investments and creates rapid innovation and implementation, it also raises one fundamental question: *how should we develop and use AI for the benefit of humanity and not against our collective interests and, above all, against our collective security?* Considering AI's potential of reshaping every aspect of social life as we know it, we should collectively try to be more cautious and more in control of our needs and wants, so that AI becomes one of our greatest instruments so far, rather than one of our greatest failures.

References:

1. Backlinko. (2024). *DeepSeek AI Usage Stats.* https://backlinko.com/deepseek-stats

2. Bendett, S. (2024). *The Role of AI in Russia's Confrontation with the West.* Center for a New American Security. https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west

3. Bhuiyan, J. (2024). "Meta to let US national security agencies and defense contractors use Llama AI." *The Guardian*. https://www.theguardian.com/

technology/2024/nov/05/meta-allows-national-security-defense-contractors-use-llama-ai

4. Bode, I., and Bhila, I. (2024). "The problem of algorithmic bias in AI-based military decision support systems." *Red Cross – Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2024/09/03/the-problem-of-algorithmic-bias-in-ai-based-military-decision-support-systems/

5. Bond, S. (2024). *How Russia is using artificial intelligence in its propaganda operations.* https://www.npr.org/2024/06/25/nx-s1-5019381/how-russia-is-using-artificial-intelligence-in-its-propaganda-operations

6. Booth, R., Krupa, J., and Giuffrida, A. (2025). "DeepSeek blocked from some app stores in Italy amid questions on data use." *The Guardian*. https://www.theguardian.com/technology/2025/jan/29/deepseek-blocked-some-app-stores-italy-questions-data-use

7. Canales, S. B. (2025). "DeepSeek banned from Australian government devices amid national security concerns." *The Guardian*. https://www.theguardian.com/technology/2025/feb/04/deepseek-banned-from-australian-government-devices-over-national-security-concerns

8. China Aerospace Studies Institute. (2023). *Interim Measures for the Management of Generative Artificial Intelligence Services*. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2023-08-07%20ITOW%20Interim%20Measures%20for%20the%20Management%20of%20Generative%20Artificial%20Intelligence%20Services.pdf?utm_source=chatgpt.com

9. Clegg, N. (2024). *Open Source AI Can Help America Lead in AI and Strengthen Global Security.* https://about.fb.com/news/2024/11/open-source-ai-america-global-security/

10. Data General. (2025). *South Korea: PIPC announces investigation into DeepSeek.* https://www.dataguidance.com/node/641139

11. Davenport, T., and Bean, R. (2025). *Five trends in AI and Data Science for 2025.* https://sloanreview.mit.edu/article/five-trends-in-ai-and-data-science-for-2025/

12. del Rosario, S. (2025). "DeepSeek faces federal investigation over how it got its AI chips: Report." *Straight Arrow News*. https://san.com/cc/deepseek-faces-federal-investigation-over-how-it-got-its-ai-chips-report/

13. Desmarais, A. (2025). *Here's what has been announced at the AI Action Summit.* EuroNews. https://www.euronews.com/next/2025/02/11/heres-what-has-been-announced-at-the-ai-action-summit

14. Domanska, O. (2025). "Why more businesses are hiring Chief AI Officer." *Avenga*. https://www.avenga.com/magazine/chief-ai-officers-role-decoded/

15. Durland, H., and Siegmann, E. (2024). "The 2024 National Security Memorandum on AI: A Timeline and Index of Responsibilities." *Georgetown Security Studies Review*. https://georgetownsecuritystudiesreview.org/2024/11/04/the-2024-national-security-memorandum-on-ai-a-timeline-and-index-of-responsibilities/

16. Galliot, J., and Scholz, J. (2020). "The Case for Ethical AI in the Military." *The Oxford Handbook of Ethics of AI The Oxford Handbook of Ethics of AI*.

17. Klaus, M. (2024). "Transcending weapon systems: the ethical challenges of AI in military decision support systems." *Red Cross – Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2024/09/24/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems/

18. Lee, C. (2025). "Russia turns to China to step up AI race against US." *VOA News*. https://www.voanews.com/a/russia-turns-to-china-to-step-up-ai-race-against-us/7931829.html

19. McKinsey and Company. (2025). *The state of AI: How organizations are rewiring to capture value.* https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai?utm_source=chatgpt.com

20. Michel, A. H. (2023). "Inside the messy ethics of making war with machines." *MIT Technology Review*. https://www.technologyreview.com/2023/08/16/1077386/war-machines/

21. Moreau, C. (2025). "DeepSeek making a splash with EU data protection bodies." *EURACTIV.* https://www.euractiv.com/section/tech/news/deepseek-making-a-splash-with-eu-data-protection-bodies/

22. O'Donnel, J., Heaven, W. D., and Heikkilä, M. (2025). "What's next for AI in 2025." *MIT Technology Review*. https://www.technologyreview.com/2025/01/08/1109188/whats-next-for-ai-in-2025/

23. Roberson, T., Bornstein, S., Liivoja, R., Ng, S., Scholz, J., and Devitt, K. (2022). "A method for ethical AI in defence: A case study on developing trustworthy autonomous systems." *Journal of Responsible Technology,* vol. 11.

24. Roose, K. (2024, Iulie). "The Data That Powers A.I. Is Disappearing Fast." *New York Times.* https://www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html

25. Rowe, N. (2022). "The comparative ethics of artificial-intelligence methods for military applications." *Frontiers in Big Data vol. 5*.

26. Smalley, S. (2025). "Texas investigating DeepSeek for violating data privacy law." *The Record.* https://therecord.media/texas-investigating-deepseek-privacy

27. Sterling, T. (2025). "Dutch privacy watchdog to launch investigation into China's DeepSeek AI." *Reuters*. https://www.reuters.com/technology/

artificial-intelligence/dutch-privacy-watchdog-launch-investigation-into-chinas-deepseek-ai-2025-01-31/

28. The Brussels Times with Belga. (2025, Ianuarie). "Investigation opened into possible privacy violations by DeepSeek." *The Business Times*. https://www.brusselstimes.com/1419622/investigation-opened-into-possible-privacy-violations-by-deepseek

29. The White House. (2025). *America's AI Action Plan*. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

30. von der Leyen, U. (2025). "Speech by President von der Leyen at the Artificial Intelligence Action Summit." *European Comission Press Corner*. European Comission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_471

31. Walker, K. (2025). *AI and the future of national security.* Google Threat Intelligence Group. https://blog.google/technology/safety-security/ai-and-the-future-of-national-security/

32. Zhou, W. (2024). "Artificial intelligence in military decision-making: supporting humans, not replacing them." *Red Cross – Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-decision-making-supporting-humans-not-replacing-them/

33. Zhu, S. (2025, Ianuarie). *Transforming industries with AI: Lessons from China's journey.* World Economic Forum. https://www.weforum.org/stories/2025/01/transforming-industries-with-ai-lessons-from-china/