The American Journal of Political Science Law and Criminology
ISSN 2693-0803 | Open Access

TYPE Original Research
PAGE NO. 40-48
DOI 10.37547/tajpslc/Volume07Issue06-08

Check for updates

# Implementation Of Dual-Use Technologies in Defense and Public Security

**Kristijan Ilovača**
CEO of Sky Fort Systems d.o.o Croatia, Zagreb

**OPEN ACCESS**

SUBMITED 11 April 2025
ACCEPTED 26 May 2025
PUBLISHED 18 June 2025
VOLUME Vol.07 Issue 06 2025

CITATION

Kristijan Ilovača. (2025). Implementation Of Dual-Use Technologies in Defense and Public Security. The American Journal of Political Science Law and Criminology, 7(06), 40–48. https://doi.org/10.37547/tajpslc/Volume07Issue06-08



**Abstract:** This paper presents a comprehensive analysis of the mechanisms for introducing dual-use technologies into defense and public-security frameworks. The topic's relevance stems from rapid advances in technical solutions that blur the traditional lines between civilian and military applications—creating new opportunities to boost efficiency across multiple sectors, while simultaneously posing significant risks of international destabilization and threats to national integrity. The study aims to survey contemporary models for integrating dual-use technologies, to identify regulatory, economic, and ethical constraints, and to pinpoint the most promising practices for strengthening defense capabilities and enhancing public protection in a holistic manner. Emphasis is placed on technological domains such as artificial intelligence, biological systems, cybersecurity, and autonomous unmanned platforms. Drawing on current research, the paper demonstrates how adaptive management strategies for dual-use technologies can deliver flexible responses to rapidly evolving challenges. Special attention is given to the need for robust interagency and transnational coalitions, as well as the creation of legal frameworks that simultaneously foster innovation. The findings will benefit defense-policy and security-management professionals, technology-transfer experts, and representatives of governmental bodies and high-tech firms seeking balanced solutions in an era of technological turbulence.

**Keywords:** dual-use technologies; defense; public security; innovation; artificial intelligence; cybersecurity; technology transfer; national security; risk management; export control.

**Introduction:** Dual-use technologies (DUT)—capable of operating in both civilian and military domains—have become a focal point in discussions of national and international security [1, 2]. Their rapid development and widespread adoption are reshaping established approaches to defense policy and law enforcement, opening new opportunities while simultaneously introducing serious challenges for state institutions [3]. The urgency of analyzing DUT implementation mechanisms is driven by the need to recalibrate governance strategies in response to swift technological change [6].

Recent R&D dynamics reveal a tight interweaving of civilian and defense innovations. Consequently, commercial solutions frequently outpace specialized military analogues in functionality or serve as their foundation—a phenomenon known as "spin-on" and "reverse spin-off" [4, 5].

In the public-security sphere, dual-use technologies already see broad deployment: video-surveillance systems with machine-vision analytics, big-data platforms for crime forecasting, and more [8, 9]. The use of drones for emergency response, search-and-rescue operations, and terrain mapping has become standard practice in many countries [10].

At the same time, the expanded use of DUT entails significant risks: from the leakage of information vital to national interests to the intensification of technological races and the emergence of ethical dilemmas surrounding autonomous systems and pervasive surveillance [11, 12]. Uncontrolled proliferation of such technologies can undermine stability at both regional and global levels [13].

The aim of this paper is to analyze the processes by which dual-use technologies are integrated into defense and law-enforcement contexts, drawing on current data and scholarly publications.

The scientific novelty lies in a systematic examination of the relationships among the pace of technological innovation, the flexibility of regulatory regimes, and the strategic priorities of national security as they pertain to DUT.

The author's hypothesis is that optimal strategies for implementing dual-use technologies should rest on principles of proactive risk management, close cooperation among government, academia, and industry, and the development of international partnerships to establish unified standards and codes of conduct for key dual-use technologies.

## MATERIALS AND METHODS

The study employs a system-structural analysis combined with an interdisciplinary synthesis of knowledge. Its empirical base comprises leading monographs, peer-reviewed journal articles, and official documents and analytical reports from major international organizations and government bodies.

Within the regulatory and legal domain, control over dual-use technologies is exercised through national and multilateral regimes. A CNAS report [1] recommends strengthening U.S. export controls on high-technology components. The European Commission [2] emphasizes the need to coordinate national control regimes to counter technological risks, while source [5] examines public-security considerations within the single market. Whang C. [15] identifies differences in evaluation criteria and decision-making procedures between the U.S. and the EU. The Wassenaar Arrangement [25] and U.N. conventions [18, 19] codify universal obligations to update lists of controlled technologies.

In the biotechnology sector, WHO guidelines [26] set out principles for responsible management of research projects, with particular focus on biothreat assessment at each stage. Xue Y., Yu H., and Qin G. [27] explore adaptive control mechanisms to support sustainable development.

Reis J. et al.'s Quintuple Helix model [4] illustrates the interaction among university, industry, civil society, government, and ecology in EU defense innovation—a linkage corroborated by the EDA Annual Report 2024 [28] and increased IT project funding in the Pentagon budget [20]. Kasikci T. and Yetim M. [11] underscore the necessity of balancing innovation with disarmament.

Source [6] documents shifts in the AI market alongside the development of "Responsible AI" principles by SIPRI [13] and examines ethical risks associated with AGI

(Bikkasani D. C. [12]) and strategic threats (CSET [21]). Psycho-moral aspects of remote military operators are analyzed by Rauch M. and Ansari S. [3], predictive policing practices by Sandhu A. and Fussey P. [8], and the applicability of AI solutions in jurisprudence by Grimm P. W., Grossman M. R., and Cormack G. V. [9]. Rosenberg I. et al. [24] investigate defenses against adversarial-ML attacks, while ICRC [29] highlights a legal vacuum in regulation. Svoboda O. [14] critiques export controls in the context of digital surveillance.

Unmanned systems are governed by CAA regulations [7] and see active deployment in emergency response operations (Daud S. M. S. M. et al. [10]), with the commercial drone market expanding in OEM and service segments [30].

Cyber-threats in space are assessed by the CFR [17], state preparedness by the ITU [22], and ENISA identifies key trends for 2023 [23].

Quantum computing as a dual-use technology is characterized by its scaling potential and barriers, as examined by Memon Q. A., Al Ahmad M., and Pecht M. [16].

## RESULTS AND DISCUSSION

The integration of dual-use technologies (DUT) into defense and public-security domains has achieved significant milestones while confronting a variety of technical, regulatory, and ethical barriers. Since 2001, the Florida Attorney General's Office, in partnership with the Florida Department of Law Enforcement (FDLE), formed an interagency task force dubbed "LEGIT" (Law Enforcement Getting Identity Thieves) to uncover and halt crimes involving identity theft. The team comprised five full-time FDLE agents and regional officers from local and federal agencies, all trained in investigating these offenses and conducting statewide workshops for their peers. A landmark success came in collaboration with the Hernando County Sheriff's Office, the State Attorney's Office, and SSA/OIG: an offender who had assumed a California resident's identity for over twelve years—purchasing and selling real estate, opening bank accounts, and evading arrest three times—was finally apprehended. LEGIT's coordinated effort led to the annulment of all illicit transactions and restoration of the victim's reputation and legal rights. Once its active mission concluded, LEGIT's procedures were folded into routine law-enforcement operations, and the task force was disbanded.

Today, a different suite of solutions is in use, built on a variety of innovative platforms. In artificial intelligence, for example, systems combine deep-learning algorithms, multi-module data processing, and adaptive control frameworks to deliver precise intelligence analysis and broaden the capabilities of autonomous platforms. Militaries employ AI not only to optimize logistics and support real-time decision-making but also to automate cybersecurity tasks—such as intrusion detection and response [16, 20]. In public-safety applications, machine-learning algorithms sift through massive datasets to identify organized crime networks, perform real-time facial and object recognition in video streams, and enable predictive-policing methods [9]. At the same time, the rise of lethal autonomous weapon systems (LAWS) has provoked profound ethical and legal debates over accountability, compliance with international humanitarian law, and the risk of unintended civilian casualties [12, 28].

A broad spectrum of unmanned systems—ranging from micro-UAVs to heavy unmanned combat aerial vehicles, as well as autonomous ground and maritime platforms—is being integrated for both military missions (reconnaissance, target designation, preventive and strike operations) and emergency-response functions. These systems are deployed for border and crowd monitoring, search-and-rescue missions, and the delivery of critical supplies [7, 10]. According to forecasts in source [30], the commercial UAV market will expand from USD 5.32 billion in 2024 to USD 9.34 billion by 2030—an average annual growth rate of 11.2 percent between 2024 and 2030. Employing drones to inspect telecommunications towers, for instance, can achieve more cost-effective surveillance in a fraction of the time. Figure 1 illustrates the structure of the commercial UAV market for increased clarity.

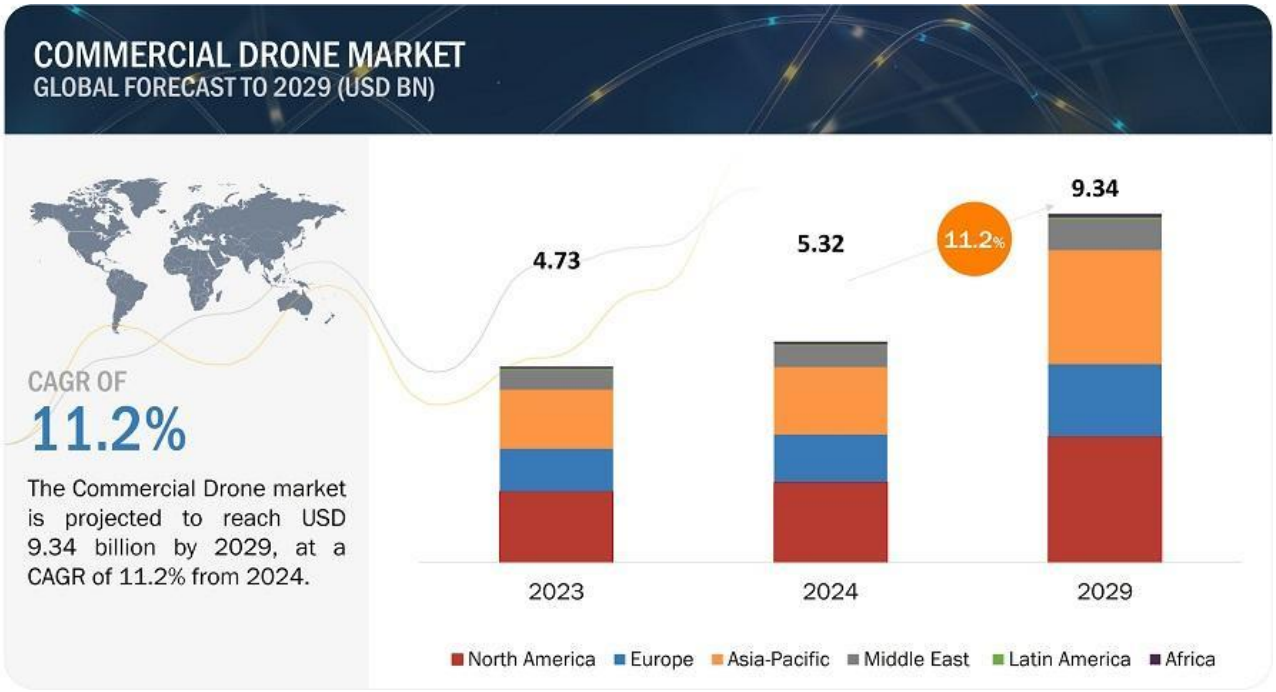


**Fig.1. The structure of the unmanned aerial vehicles market [30].**

Cybernetic technologies have become a key arena of confrontation between offensive and defensive tools in national and corporate security. The modern suite of dual-use technologies in this field includes infrastructures for proactive penetration testing, enhanced cryptographic protocols designed to resist quantum-computing threats, and multi-layered systems for detecting and preventing sophisticated attacks (SIEM, EDR, XDR) [22, 23]. At the same time, the rise in AI-driven cyberattacks demands the development of counter-AI technologies capable of identifying and neutralizing self-learning malicious agents [17, 24].

Recent advances in biotechnology—chiefly CRISPR-Cas9 and its improved variants for genome editing, synthetic biology, and neurotechnologies—open new frontiers in medicine, agriculture, and industry. However, these innovations also carry the risk of unintentionally or intentionally creating novel pathogens and biotoxins, underscoring the need for strict international biosafety mechanisms and early-warning systems for biological threats [25, 26]. The COVID-19 pandemic has vividly demonstrated the importance of global cooperation transparency, and rapid response in biocontrol.

**Figure 2 illustrates the dual-use technology implementation cycle and identifies the key stakeholders involved.**

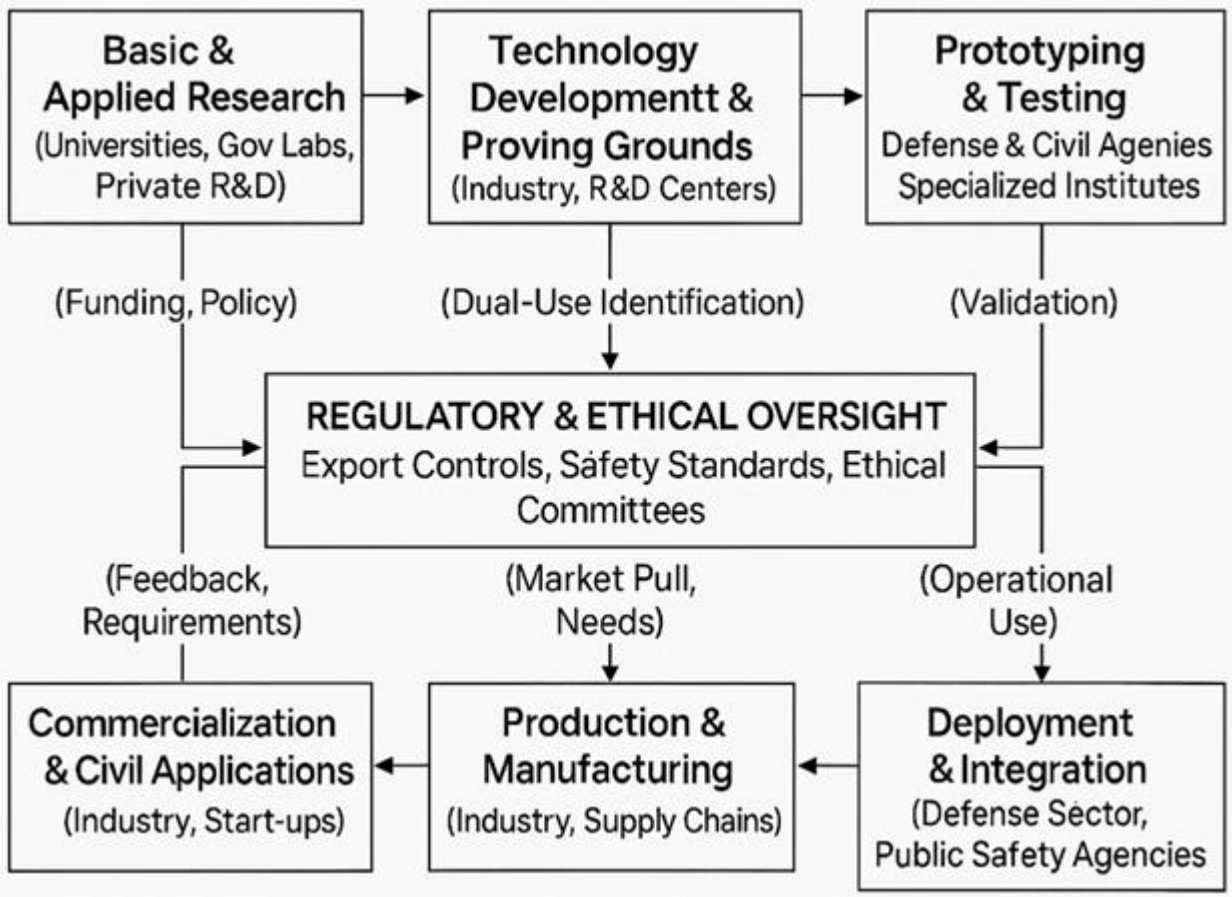


**Fig.2. The TD implementation cycle and key stakeholders [20, 21, 25, 26].**

Modern export-control regimes, designed in the era of heavy armaments, have proven insufficiently flexible to regulate effectively intangible assets—software and AI training datasets—and dual-use equipment with broad civilian applications [19]. The inability of institutions such as the Wassenaar Arrangement Secretariat to update assessment criteria for emerging digital technologies in a timely manner creates a dual effect: it increases the risk of unauthorized dissemination of strategically sensitive developments, while unduly hindering international trade and scientific–technical collaboration [25][14, 15].

Concurrently, large-scale deployment of intelligent algorithms in surveillance systems and autonomous combat platforms calls into question their compliance with existing norms of international humanitarian law and fundamental human rights. The absence of transparent audit procedures and clear lines of accountability for decisions made by autonomous systems heightens the risk of unintended conflict escalation and legal disputes. At the same time, the lack of universally recognized international standards for lethal autonomous weapon systems (LAWS) severely restricts the establishment of adequate control frameworks and legal oversight for these technologies [12, 18, 28].

Organizational barriers and technological divides between the civilian and military sectors are exacerbated by complex bureaucratic processes and mismatched industry standards. Innovative products often undergo lengthy approval and adaptation cycles to meet defense-agency requirements, delaying deployment and eroding competitive advantage. As a result, the most promising solutions are either held up indefinitely or deployed through unofficial channels, diminishing the overall efficiency of technology transfer [1, 4].

Finally, the intensification of geopolitical competition has given rise to “technological nationalism,” aimed at limiting foreign partners’ access to cutting-edge research and components. Yet the transnational nature of modern threats—from cybercrime to pandemics—

demands new forms of international coordination and collective response. This dual dynamic between the pursuit of monopoly control over technological resources and the imperative for global cooperation remains a principal challenge in shaping defense-industrial innovation strategies [3, 13].

**Table 1. Examples of dual-use technologies and associated challenges in defense and public safety [6, 7, 9, 10, 12, 20, 23, 25, 28, 29]**

| Technology | Use in Defense | Use in Public Security | Key Challenges (General) |
|---|---|---|---|
| Artificial Intelligence (AI) | Autonomous systems, intelligence analysis, cyber operations | Predictive analytics, facial recognition, chatbots | Ethics (LAWS, algorithmic bias), oversight, vulnerability to attacks, arms race |
| Unmanned Aerial Systems (UAS) | Reconnaissance, strike missions, logistics | Monitoring, search & rescue, delivery, mapping | Proliferation, airspace regulation, counter-UAS measures, privacy |
| Cyber Technologies | Cyber warfare, network defense, intelligence | Combating cybercrime, protecting critical infrastructure | Attack attribution, dual-use nature, data protection, international law |
| Biotechnology (genetic engineering) | Defensive measures, biosensors | Diagnostics, epidemiological surveillance | Bioweapon risk, genome-editing ethics, technology access controls |
| Quantum Technologies | Quantum computing (codebreaking), sensors, communications | Potential for secure communications | Quantum-supremacy race, high costs, threats to existing cryptography |

Establishing a flexible regulatory framework requires the regular review and rapid adjustment of legal instruments in line with the pace of technological change. Key tools include “regulatory sandboxes” and detailed cost–benefit analyses, which together provide a balanced assessment of the potential risks and advantages of deploying new dual-use technologies [14, 15].

Institutional partnerships rest on the synergy among government bodies, research institutes, and the private sector. To spur joint R&D and demonstration projects, targeted grant programs, tax incentives, and other support measures are recommended—with particular emphasis on engaging small and medium-sized innovative enterprises [5, 27].

The development of international platforms and multilateral dialogues aims to forge universally recognized standards of “responsible conduct” in the dual-use domain. It is proposed to establish high-level forums that bring together state authorities, industry associations, and NGOs to prevent an arms race in emerging technological niches and to oversee the transfer of sensitive technologies [3, 18].

Enhancing technological literacy and instituting mandatory ethical reviews call for systematic training and upskilling of both technical experts and policymakers. Recommended actions include the design of specialized educational curricula, regular workshops, and the creation of independent committees charged with evaluating the social, environmental, and legal dimensions of dual-use projects [12, 28].

Ensuring the resilience and security of global supply chains depends on diversifying sources of critical components, building strategic reserves, and

implementing digital registries of trusted suppliers. Such a multi-layered approach minimizes disruption risks and guarantees access to essential technologies regardless of geopolitical upheavals.

Together, these measures form a continuous, adaptive governance process for dual-use technologies—capable of responding to rapidly evolving technological and geopolitical conditions. A robust feedback mechanism, integration of multi-level risk-benefit analyses, and alignment of the international community's interests in fostering innovation while minimizing potential threats are vital prerequisites for this strategy's success.

## CONCLUSION

The implementation of dual-use technologies stands as a primary driver in transforming twenty-first-century defense systems and public-safety mechanisms. This study has shown that innovations such as artificial-intelligence algorithms, autonomous unmanned platforms, advanced cybersecurity solutions, and bioengineering frameworks open fundamentally new capabilities for accelerating monitoring, forecasting, and rapid response to both traditional and emerging threats. At the same time, the dual nature of these technologies introduces a host of associated risks: uncontrolled dissemination of critical know-how, misuse by hostile actors, and the emergence of unresolved ethical dilemmas that demand immediate legislative and institutional attention.

The findings confirm the initial hypothesis that effective management of dual-use technologies cannot be reduced to technical controls alone. A comprehensive strategy is required—one that fortifies the regulatory framework, implements flexible public–private cooperation mechanisms, and intensifies international partnerships.

Looking forward, it will be essential to strike an optimal balance between fostering innovation and ensuring security within an ever-evolving threat landscape.

## REFERENCES


Dual-Use Technology and U.S. Export Controls. [2025 Apr. 20]. Available from https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls.

Communication from the Commission to the European Parliament and the Council. [2025 Apr. 22]. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0249 .

Rauch, M., & Ansari, S. (2022). Waging war from remote cubicles: How workers cope with technologies that disrupt the meaning and morality of their work. Organization Science, 33(1), 83–104. https://doi.org/10.1287/orsc.2021.1555.

Reis, J., et al. (2022). Quintuple helix innovation model for the European Union defense industry—An empirical research. Sustainability, 14(24). https://doi.org/10.3390/su142416499.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. [2025 Apr. 23]. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0070 .

Artificial Intelligence Market Size. [2025 May. 23]. Available from https://www.fortunebusinessinsights.com/industry-reports/artificial-intelligence-market-100114 .

The Drone and Model Aircraft Code. [2025 Apr. 20]. Available from https://www.caa.co.uk/media/5d1otmqu/the-drone-code-march-2024.pdf.

Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. Policing and Society, 31(1), 66–81. https://doi.org/10.1080/10439463.2020.1803315.

Grimm, P. W., Grossman, M. R., & Cormack, G. V. (2021). Artificial intelligence as evidence. Northwestern Journal of Technology and Intellectual Property, 19, 9.

Daud, S. M. S. M., et al. (2022). Applications of drone in disaster management: A scoping review. Science & Justice, 62(1), 30–42. https://doi.org/10.1016/j.scijus.2021.11.002.

Kasikci, T., & Yetim, M. (2023). Disarmament. In The Palgrave Encyclopedia of Global Security Studies 299–302.

Bikkasani, D. C. (2024). Navigating artificial general intelligence (AGI): Societal implications, ethical considerations, and governance strategies. AI and Ethics, 1–16.

Responsible artificial intelligence research and innovation for international peace and security. [2025 Apr. 26]. Available from https://www.sipri.org/sites/default/files/2020-11/sipri_report_responsible_artificial_intelligence_research_and_innovation_for_international_peace_and_security_2011.pdf.

Svoboda, O. (2022). Building Surveillance State in a Digital Age and what export control can (not) do about it? In YSEC Yearbook of Socio-Economic Constitutions 2021: Triangulating Freedom of Speech. 231–253.

Whang, C. (2021). Trade and emerging technologies: A comparative analysis of the United States and the European Union dual-use export control regulations. Security and Human Rights, 31(1–4), 11–34.

Memon, Q. A., Al Ahmad, M., & Pecht, M. (2024). Quantum computing: Navigating the future of computation, challenges, and technological breakthroughs. Quantum Reports, 6(4), 627–663. https://doi.org/10.3390/quantum6040039.

Cybersecurity and the New Era of Space Activities. [2025 Apr. 27]. Available from https://www.cfr.org/report/cybersecurity-and-new-era-space-activities.

Convention on prohibitions or restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects. [2025 Apr. 29]. Available from https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_2_Advance_version.pdf .

Convention on prohibitions or restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects. [2025 Apr. 29]. Available from https://docs.un.org/en/CCW/GGE.1/2023/1.

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. (n.d.). FY2024 Budget Request Overview Book. [2025 Apr. 30]. Available from https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Budget_Request_Overview_Book.pdf .

Artificial Intelligence and National Security. [2025 Apr. 30]. Available from https://cset.georgetown.edu/publication/artificial-intelligence-and-national-security/.

Global Cybersecurity Index. [2025 May 1]. Available from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

ENISA Threat Landscape 2023. [2025 May 2]. Available from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Adversarial machine learning attacks and defense methods in the cybersecurity domain. ACM Computing Surveys (CSUR), 54(5), 1–36. https://doi.org/10.1145/3453158.

Wassenaar Arrangement Secretariat. (2021). [2025 May 1]. Available from https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf.

Global guidance framework for the responsible use of the life sciences: Mitigating biorisks and governing dual-use research. [2025 May 5]. Available from https://www.who.int/publications/i/item/9789240056107.

Xue, Y., Yu, H., & Qin, G. (2021). Towards good governance on dual-use biotechnology for global sustainable development. Sustainability, 13(24). https://doi.org/10.3390/su132414056.

EDA Annual Report 2024. [2025 Apr. 27]. Available from https://eda.europa.eu/docs/default-source/brochures/eda---annual-report-2024---webdfcdc23fa4d264cfa776ff000087ef0f.pdf.

ICRC position on autonomous weapon systems. [2025 May 15]. Available from

https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

Commercial Drone Market by Point Of Sale (OEM, Aftermarket). [2025 May. 23]. Available from https://www.marketsandmarkets.com/Market-Reports/commercial-drone-market-66171414.html.