CYBERSEC
EXPO & FORUM

DUAL-USE TECHNOLOGY – CROSS-SECTOR COOPERATION IN THE CYBER SECURITY SECTOR

POLICY BRIEF

Table of contents

Dear Ladies and Gentlemen,

This document is the third *policy brief* resulting from the letter of intent signed during **CYBERSEC EXPO & FORUM 2024** on June 19th in Kraków, in the presence of Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski. The agreement was concluded between the **Kosciuszko Institute** and the **European Cyber Security Organisation (ECSO)** regarding the organization of a series of events focused on the priorities of digital and technological policy during Poland's Presidency of the EU Council.

The third meeting in the *Road to the Polish Presidency* series was dedicated to addressing challenges and overcoming obstacles in dual use technology.

In recent years, dual use technologies have become increasingly critical for economic competitiveness, national security, and technological sovereignty. Rapid advancements in areas such as artificial intelligence, quantum computing, and advanced digital systems offer transformative potential. However, they also introduce challenges, including regulatory fragmentation, export control complexities, and the need for effective collaboration across sectors. Furthermore, geopolitical tensions and evolving global security threats have highlighted the importance of fostering a balanced, coordinated, and forward-looking approach to dual use innovation and deployment.

Drawing from a meeting held on November 26, 2024, attended by representatives of the Ministry of Digital Affairs of Poland, the European Cyber Security Organisation (ECSO), the private sector, academia, and the Kosciuszko Institute, together we were able to identify key challenges and solutions surrounding regulatory harmonization, export controls, cross-sector collaboration, and innovation support for dual use technologies. We would like to express our heartfelt gratitude to all members of the working group whose dedication, knowledge, and experience contributed to the creation of this document. The developed recommendations represent a significant step in building a digital and secure society. We extend our sincere thanks to the Ministry of Digital Affairs for their invaluable support and commitment, which played a crucial role in the realization of our initiative. We greatly appreciate your professionalism, openness to cooperation, meaningful contributions, and support of our shared mission.

We would also like to extend our heartfelt gratitude to all partner institutions and experts for their invaluable support in both the substantive and organizational aspects of our efforts, with our deepest appreciation reserved for our esteemed partner, Deloitte.

Deloitte.

Members of the working group:

1. **Izabela Albrycht** – AGH University of Science and Technology, NATO DIANA
2. **David Antunes** – European Defence Agency
3. **Wojciech Burian** – Łukasiewicz Research Network – Institute of Non-Ferrous Metals
4. **Jonas Cederlöf** – European Commission
5. **Dr Claire Gray** – League of European Research Universities
6. **Marietta Gieroń** – Kosciuszko Institute
7. **Paulina Górska** – Kosciuszko Institute
8. **Łukasz Jędrzejczak** – Deloitte
9. **Col Marcin Mazur** – Polish Space Agency
10. **Marco Marsili, PhD** – Ca' Foscari University of Venice
11. **Tom Dallas McSorley** – NATO DIANA
12. **Matteo Mole** – European Cyber Security Organisation
13. **Jana Novohradska** – CERAI – Committee on Ethics and Regulation of Artificial Intelligence
14. **Krzysztof Sierański** – Information Security Foundation Poland
15. **Adam Szczukocki** – Ministry of Digital Affairs
16. **Paul Timmers** – University of Oxford
17. **Mariusz Ustyjańczuk** – Deloitte
18. **Aleksandra Wójtowicz** – The Polish Institute of International Affairs
19. **Dr hab. Przemysław Wywiał** – Government Security Center

Please note that the challenges and recommendations outlined in this document are the outcome of collaborative discussions and do not represent the official positions, endorsements, or commitments of individuals and organisations contributing to the working group. They are intended solely for informational and exploratory purposes.

THEME I:

Utilizing dual use technology – challenges for the upcoming years

Dual-use technology poses a range of pressing challenges today and in the near future. Currently, issues include ensuring responsible development, preventing misuse, and navigating complex international regulations that very across borders. In the coming years, challenges will likely intensify with the rapid advancement of emerging and disruptive technologies as they risk falling into unintended hands or exacerbating global power imbalances.

DEFINING DUAL USE TECHNOLOGY

The concept of dual use technology has grown increasingly complex. While traditionally defined as technologies intended for civilian use but with potential military applications, this understanding no longer fully captures today's reality. Technological development now flows in multiple directions—innovations originating in the private sector are increasingly adopted for military and public use, while traditional military technologies also find civilian applications.

Defining dual use technology requires a focus on context and application. Technologies such as software, cybersecurity tools, and artificial intelligence may serve civilian purposes but can be repurposed for defense, espionage, or other unintended uses. Static regulatory lists, while a useful baseline, are not enough to keep pace with emerging challenges. A risk-based approach—assessing the likelihood of misuse and understanding how technologies evolve—is increasingly necessary.

The challenge lies in balancing innovation with security. Technologies must remain accessible to foster economic and societal progress while ensuring safeguards against misuse. Monitoring research outcomes, improving regulatory flexibility, and addressing vulnerabilities are essential steps to manage risks without hindering technological growth. A clearer, context-driven approach to dual use technology will provide a foundation for effective policies that reflect both current challenges and future technological realities.

CHALLENGE: IDENTIFYING BIGGEST THREATS IN TERMS OF DUAL USE TECHNOLOGY

It is crucial to maintain the discussion about the threats and risks posed by dual use technologies, as their misuse by hostile actors can lead to significant security breaches, cyber-attacks, espionage and violations of privacy and human rights. A recent example highlights the risk of glocalization data, such as military personnel's jogging routes near sensitive facilities being exploited to infer critical information. Dual use technologies can also be weaponized by non-state actors or hostile states like Russia or North Korea, destabilizing national security and undermining trust in these innovations.

Regulatory inconsistencies, particularly in international frameworks, further exacerbate these risks by creating enforcement loopholes. For example, the EU's AI Act regulates high-risk civilian AI but exempts military applications, creating a regulatory gap that leaves dual use technologies vulnerable to misuses. Civilian-developed AI systems, such as drones and surveillance tools, could be repurposed for military or intelligen-

ce use, bypassing human rights protections and posing risks to European and NATO security. This gap is compounded by asymmetries in veracity and cybersecurity requirements between military and civilian applications, with the adoption of less accurate, probabilistic systems from civil domain posing additional threats.

Broad fields like AI and quantum computing complicate regulation, and the rapid pace of technological advancement presents challenges for universities and research to stay informed. Addressing these issues requires stronger oversight, harmonized regulations and systemic approaches to risk mitigation, ensuring technologies align with both ethical principles and security needs.

RECOMMENDATIONS:

1. It is recommended to conduct ongoing assessments of the usage and associated risks of dual use technologies. The development of advanced risk assessment frameworks is essential for effectively addressing these challenges. Introducing comprehensive, tailored models to identify potential vulnerabilities, including misuse scenarios by hostile actors, is critical. Such assessments should be integrated into the processes of technology development and deployment to ensure responsible innovation and risk mitigation.

2. Developing real-time threat monitoring systems to identify and detect potential misuse of dual use technologies, such as unauthorized access to sensitive data or the weaponization of civilian technologies, is essential. These systems should provide early warnings and support rapid response efforts to mitigate risks effectively.

3. Universal standards for dual use AI in the military context should be immediately set up. The lack of such standards exacerbates risks, including ethical practices, regulatory gaps and potential misuse by hostile actors. Without a unified framework, the deployment of AI in military settings may lead to heightened security vulnerabilities, reduced interoperability among allied nations and challenges in ensuring accountability and transparency.

4. Expanding the AI Act should be considered and complemented by a cohesive international framework to regulate AI across all sectors, ensuring the protection of human rights and the preservation of global stability.

5. It is recommended to clarify the legislative scope by specifying whether it encompasses technologies subject to export controls (e.g., Annex 1 in the EU), critical technologies, or a broader category that includes all STEM-related innovations with potential military or civilian applications.

6. Skills gap should be addressed by developing and implementing comprehensive training programs on dual use issues at all levels within universities. These programs should equip responsible individuals, who often lack prior experience, with the necessary knowledge and tools to manage dual use concerns effectively.

7. It is recommended that Europe draw on the lessons learned from countries like the US, Canada, and Australia in addressing dual use issues, using their approaches as inspiration to enhance policies and practices at all levels.

CHALLENGE: COOPERATION ON THE EU AND TRANSATLANTIC LEVEL

The level of transatlantic cooperation will largely depend on the approach of the new US administration. Nevertheless, pursuing the highest possible level of collaboration remains essential. The Transatlantic Trade and Technology Council (TTC) has already established a foundation for addressing regulatory barriers in trade and compliance, including issues related to export-controlled dual use items.

To enhance cooperation, it is crucial to build on this foundation by adopting key principles and strategies that address shared security concerns while balancing economic and regulatory differences. This approach will ensure a strong and secure transatlantic partnership.

The ultimate goal should not only be to strengthen mutual security but also to set a global standard for responsible innovation in dual use technologies, ensuring these advancements benefit society while minimizing potential risks.

RECOMMENDATIONS:

1. The EU and transatlantic partners, especially the United States, should work together on harmonizing policies related to dual use technologies, including those concerning export controls, cybersecurity standards, and AI governance. This process would also help to close loopholes and ensure consistent enforcement across borders. By aligning regulatory frameworks, both regions can reduce barriers to collaboration and ensure that dual use technologies are governed by robust and compa-

tible standards that protect human rights and national security. A unified approach can strengthen overall security and compliance.

2. It is recommended to leverage the Trade and Technology Council as a platform for enabling the EU and U.S. to proactively address challenges associated with dual use technologies with an ongoing dialogue, collaborative investments, and unified policy measures to tackle emerging technological threats, enhancing transatlantic resilience against shared challenges.

3. Promoting joint research and development (R&D) initiatives between the EU and the US can accelerate technological innovation while ensuring advancements align with shared security and ethical standards. By pooling resources and expertise in areas such as AI, cybersecurity and other emerging dual use technologies, both regions can foster innovation that benefits both defense and civilian sectors. Horizon Europe and joint projects aimed at developing secure and resilient technologies can serve as platforms for collaborative efforts, driving innovation while reinforcing transatlantic ties.

4. Developing common standards for export controls is crucial to mitigate the risks associated with dual use technologies, particularly their acquisition by hostile actors, including state and non-state entities. The EU and the U.S. should work through frameworks, for example, the Wassenaar Arrangement to establish coordinated export control policies that prevent unauthorized access to sensitive technologies. Harmonizing these controls can involve creating joint screening mechanisms, fostering multilateral partnerships, implementing international standards, supporting capacity building, advancing joint research initiatives, and enhancing information sharing to ensure a robust and unified approach.

5. Building ethical and transparent AI governance frameworks is essential as AI becomes increasingly integrated into dual use technologies, particularly in military and security contexts. The EU and the U.S. should collaborate to develop frameworks that emphasize transparency, accountability, and the protection of fundamental human rights, with clear guidelines for AI's military applications. Drawing on initiatives such as the EU's Artificial Intelligence Act and the U.S. National AI Initiative, both regions can work toward shared ethical principles. In parallel, it is crucial to address the legal challenges associated with technological development, including intellectual property rights (IPR), the regulation of access to critical raw materials and their substitutes, and the ongoing review and updating of relevant legislation. Investments in talent development and creating optimal conditions for professional growth will further support these efforts.

6. Beyond government-to-government collaboration, the EU and U.S. should actively involve industry stakeholders, academic institutions, and civil society in discussions on dual use technologies. Engaging with the private sector can provide valuable insights into emerging technological trends and help align innovation with security priorities. Simultaneously, contributions from civil society can ensure that policies governing dual use technologies uphold human rights and ethical principles.

CHALLENGE: IMPLEMENTING CYBERSECURITY MECHANISMS TO PROTECT THEM FROM POTENTIAL TAKEOVER BY HOSTILE ACTORS

With dual use technologies becoming increasingly integral to innovation and national security, the need for robust cybersecurity measures to protect them has grown significantly. These technologies are particularly vulnerable to cyberattacks that aim to steal sensitive information, disrupt critical operations, or seize unauthorized control. As the lines between civilian and military applications continue to blur, it is essential to implement well-defined safeguards that address their unique risks, and the high stakes involved.

RECOMMENDATIONS:

1. Enhanced threat detection and monitoring systems are critical for safeguarding dual use technologies, particularly those with military applications. Governments should deploy advanced systems leveraging AI and machine learning to detect cyber threats in real-time and establish dedicated monitoring units for these technologies. Centralizing log data, utilizing SIEM tools for analysis, and ensuring adequate logging to identify anomalies are essential steps. Collaborations with intelligence agencies and cybersecurity firms can improve data-sharing and bolster threat intelligence, ensuring readiness against the latest attack methods. Additionally, developing a comprehensive incident response plan will enable rapid and effective action during security incidents.

2. Investing in robust encryption and comprehensive data protection measures is essential for securing dual use technologies. Mandatory implementation of strong encryption standards should be enforced for both data at rest and data in transit, ensuring that information remains secure against unauthorized access. End-to-end encryption must be adopted alongside secure data-sharing platforms to minimize the risk of interception by hostile entities, especially when transmitting sensitive information between government systems or external partners. To prevent unauthorized data transfers and leaks, Data Loss Prevention (DLP) tools and processes should be implemented across all systems. These tools can monitor, detect, and block any suspicious data movement, providing an additional safeguard for sensitive assets. Regular backups of critical data, combined with periodic restoration tests, are necessary to ensure data integrity and availability in case of disruptions or cyber incidents. For technologies deemed highly sensitive, the Ministry should actively explore and invest in quantum-resistant encryption methods as they become available. These emerging encryption standards will provide a future-proof layer of protection against potential threats posed by advances in quantum computing. Proactively integrating these measures will bolster the security and resilience of digital systems managed by the Ministry, ensuring the protection of strategic assets in an evolving threat landscape.

3. Ensuring supply chain security and effective vendor management is critical for protecting dual use technologies. Governments should enforce stringent cybersecurity standards for all suppliers and third parties involved in their production and distribution. This includes mandatory security certifications, compliance with established security requirements, and regular supply chain audits to identify and mitigate risks, such as the insertion of malware or backdoors by hostile actors. Requiring suppliers to adhere to these standards reduces supply chain vulnerabilities and strengthens overall security.

4. Establishing clear and common rules for trading in dual use technologies is essential, encompassing procedural and technical requirements as well as the obligations of end-users. These rules should be supported by robust legal and regulatory frameworks that address the unique cybersecurity challenges associated with dual use applications. This includes updating national cybersecurity laws to counter emerging threats, penalizing unauthorized access and cyberattacks, and fostering international coordination to prosecute hostile actors involved in cyber intrusions. Together, these measures ensure a secure and transparent trading environment for dual use technologies.

5. Fostering public-private partnerships (PPP) and enhancing international collaboration are vital for securing dual use technologies. Governments should engage private sector expertise through joint R&D initiatives, threat intelligence sharing, and collaborative response strategies to strengthen defenses and drive innovation in cybersecurity solutions. Simultaneously, international cooperation is essential to address the global nature of dual use technologies. By working through organizations like NATO and the EU, governments can establish and enforce standardized cybersecurity protocols, harmonizing security measures across borders and closing regulatory gaps that could be exploited by hostile actors.

THEME II:

Dual use technology and the global competition

In the race to develop and control dual use technologies, Europe faces mounting pressure from major competitors like China. How can the EU navigate the global competition surrounding technologies with both civil and military applications.

CHALLENGE: FOSTERING INNOVATION AND COMPETITIVENESS WITHIN EUROPE, MANAGING DEPENDENCIES ON FOREIGN TECHNOLOGIES, ENHANCING RESILIENCE, AND BALANCING COLLABORATION WITH SECURITY AND SOVEREIGNTY CONCERNS

The challenge of fostering innovation within Europe, managing dependency on foreign technologies, and balancing collaboration with security concerns, requires a multi faced approach. Dependency on foreign technologies means that sectors are more susceptible to occurrences such as supply chain disruptions and geopolitical tensions. Such disruptions can hinder access to critical resources or technologies, causing significant economic and operational setbacks. Furthermore, placing essential services in the hands of foreign entities can put national security at risk by increasing the possibility of foreign malign actors exploiting the vulnerabilities of these technologies. It also exposes sensitive data and critical infrastructure to potential cyber threats.

This reliance can also stifle domestic innovation as foreign technologies might limit opportunities for local businesses and start-ups. Domestic innovation can both bolster the economy and national security by ensuring control over critical technologies and more attention should be brought to this area. Furthermore, the lack of education and support for research and development is constricting competitiveness within Europe and limiting the number of experts capable of driving such technological innovation. At the same time, partnerships between sectors and like-minded partners can accelerate innovation by combining resources, knowledge, and expertise while setting shared security and ethical standards. These partnerships enable the development of mutual safeguards to mitigate security risks, ensuring that collaborative advancements in critical technologies align with European values and priorities. Reducing reliance on foreign technologies is essential to secure Europe's digital and technological sovereignty.

RECOMMENDATIONS:

1. Expedite the establishment of Union Testing Facilities (UTFs) for the civil domain and interconnected cross-border digital infrastructure. Testing and Experimentation Facilities (TEFs) focused on AI systems and technologies at Technology Readiness Levels (TRL) 6-8 (pre-market and pre-certification stages) will allow oversight bodies to verify claims of potential technologies before they enter the market. Develop systemic frameworks to identify errors and failures, reduce existing error rates, and enhance the safety and quality of emerging technologies. Implement measures such as regula-

tory sandboxes, UTFs, and TEFs to accelerate time-to-market and lower certification costs.

2. Continue investing in strategic sectors such as semiconductors, artificial intelligence (AI), cybersecurity, quantum technologies, and biotechnology to reduce reliance on external sources. Initiatives like the European Chips Act can strengthen semiconductor production, ensuring resilience in supply chains. Prioritize the production of semiconductors within the EU to secure advanced computing technologies essential for AI and other critical fields. Develop local semiconductor manufacturing capabilities while engaging in strategic partnerships with trusted global manufacturers.

3. Foster public-private partnerships (PPPs) to accelerate innovation while ensuring security and ethical standards. Collaborations between EU-based tech firms and public institutions can advance AI and other technologies maintaining data privacy and cybersecurity. Streamline pathways for technology transfer from research institutions to industry to efficiently commercialize innovations. Promote startups and SMEs through innovation funds, R&D grants, and incentives to develop domestic technologies, especially in sensitive sectors.

4. Support educational programs, research funding, and career pathways in critical fields such as engineering, data science, AI, quantum technologies, and cybersecurity. Promote STEM education, specialized training, and programs for future skills development. Attract and retain talent by offering PhD and postdoctoral fellowships, competitive salaries, state-of-the-art research facilities, and funding for independent research. Creating attractive career opportunities will help retain European scientists and technologists and reduce reliance on imported expertise. Strengthen EU-wide research networks, such as the European Research Area (ERA), to facilitate knowledge sharing and resource pooling. Establish specialized centers for AI, quantum computing, and biotechnology to promote synergies among top researchers across Europe.

5. Ensure European data and AI infrastructure remain under EU jurisdiction by developing homegrown platforms and establishing strict data governance policies. Invest in Europe's own cloud services, high-performance computing, and quantum infrastructure to reduce dependency on foreign providers and enhance digital resilience.

6. Implement strong export control mechanisms, such as the EU Dual Use Regulation, to prevent sensitive technologies from reaching adversarial states or non-state actors. Develop a standardized framework for assessing and mitigating foreign investment risks in critical sectors to prevent hostile takeovers and undue influence over European tech firms.

7. Partner with trusted countries such as the U.S., Japan, and South Korea to enhance access to cutting-edge technology and develop a cooperative approach to global standards-setting. Such collaborations should include provisions for technology sharing and mutual safeguards against security risks.

8. Align regulatory processes across Member States to streamline R&D, production, and commercialization, ensuring that innovative products reach the market efficiently. Establish EU-wide ethical and security standards for AI, biotech, and other emerging technologies to ensure responsible development aligned with European values and enhance public trust.

CHALLENGE: STRENGHTENING THE COOPERATION TO BE LESS DEPENDENT

The EU faces significant challenges in building a resilient and sovereign technological ecosystem, particularly due to fragmented cross-border digital and technological infrastructure. Disparities in regulatory frameworks, procurement processes, and supply chain coordination across Member States hinder the efficient production and deployment of critical technologies like semiconductors and biotech. The absence of standardized procurement systems prevents the creation of a unified market that could incentivize local production and reduce reliance on third-party suppliers. Additionally, insufficient cross-border testing and regulatory tech infrastructure delays the verification and market entry of emerging technologies, limiting Europe's ability to respond swiftly to global technological advancements.

Another major challenge is the development of talent, research capacity, and innovation ecosystems that can keep pace with global competitors. While Europe boasts strong research initiatives, talent mobility and retention remain insufficient, with programs like Erasmus+ and Marie Skłodowska-Curie Actions needing expansion to meet the demands of fields such as AI, quantum computing, and cybersecurity. Attracting and retaining top talent is increasingly difficult without competitive career incentives, funding for high-risk deep tech projects, and a clear strategy for public-private partnerships. Furthermore, the lack of unified ethical

and cybersecurity standards across the EU complicates efforts to ensure responsible technology development and data sovereignty, leaving Europe vulnerable to external influences and technological dependencies.

RECOMMENDATIONS:

1. Develop cross-border digital regulatory infrastructure to streamline oversight, enhance cooperation, and ensure harmonized regulatory processes across Member States. Establish Pan-European production networks to strengthen supply chains for key technologies, such as semiconductors and biotech supplies, ensuring facilities are distributed across Member States. Standardize procurement processes to harmonize purchasing across the EU, fostering a unified market that encourages local production and reduces dependence on third-party suppliers.

2. Implement digital sovereignty policies that prioritize data protection, ethical AI, and cybersecurity infrastructure. Establish a European Center for Cybersecurity and Critical Technologies to coordinate cybersecurity and critical tech development, enabling the EU to collectively address emerging technological threats. Create a Coalition for Ethical AI and Cybersecurity Standards in collaboration with international allies. This coalition would promote transparency, security, and ethical practices in technology development, safeguarding European interests globally.

3. Create a European Venture Capital Fund for Deep Tech to support startups working in AI, quantum computing, and biotechnology. This pan-European fund would incentivize innovation by financing high-risk, high-reward projects. Foster public-private partnerships (PPPs) to accelerate innovation and stimulate private-sector involvement in high-tech sectors. Encourage collaborations between governments, industry, and research institutions to co-invest in advanced R&D and commercialize innovations effectively.

4. Support domestic innovation through targeted funding, including grants and incentives for startups and SMEs. Focus on high-impact sectors such as AI, semiconductors, and biotechnology to strengthen Europe's competitive edge. Promote internal cooperation by developing integrated systems that align Member States' regulatory and technological priorities. Collaborative efforts will enable the EU to build a competitive, resilient, and sovereign technological ecosystem.

CHALLENGE: ESTABLISHING A JOINT EU-NATO PLATFORM TO COORDINATE RESPONSES TO CYBER THREATS

Establishing a join EU-NATO platform could bring about many advantages, such as improved threat detection. A unified defense strategy, enhanced collaboration with other sectors, and collective security. However, creating such a platform comes with its challenges. The differences in the decision-making processes, as well as coming to a consensus on priorities and resource allocation, can become a major obstacle in such a cooperation. The sharing of sensitive information between the two organizations could also raise concern about the safety of data sharing platforms. This could greatly increase the risk for intelligence leaks which would affect more than one member state and could pose a threat to international security. Furthermore, differences in priorities between NATO's primarily military focus and the EU's civilian-economic focus could lead to misalignment in strategies and resource allocation. Shifts in geopolitical dynamics or disagreements among partners could undermine the platform's effectiveness. Finally, establishing and operationalizing a joint platform would require significant upfront investments in technology, personnel, and infrastructure and sustained funding and resource commitments from both organizations may prove challenging in the face of competing priorities. Despite the obstacles however, if implemented with care, the advantages could justify the need for such a platform.

RECOMMENDATIONS:

1. Form a dedicated EU-NATO task force focused on cyber threats to dual-use technologies, comprising representatives from both organizations and key member states. The task force would assess threats, coordinate responses, and develop joint cybersecurity protocols. The task force would also oversee partnerships with private sector companies that develop and maintain dual-use technologies. Collaboration with the private sector will ensure best practices are followed in securing supply chains and critical infrastructure against cyber threats.

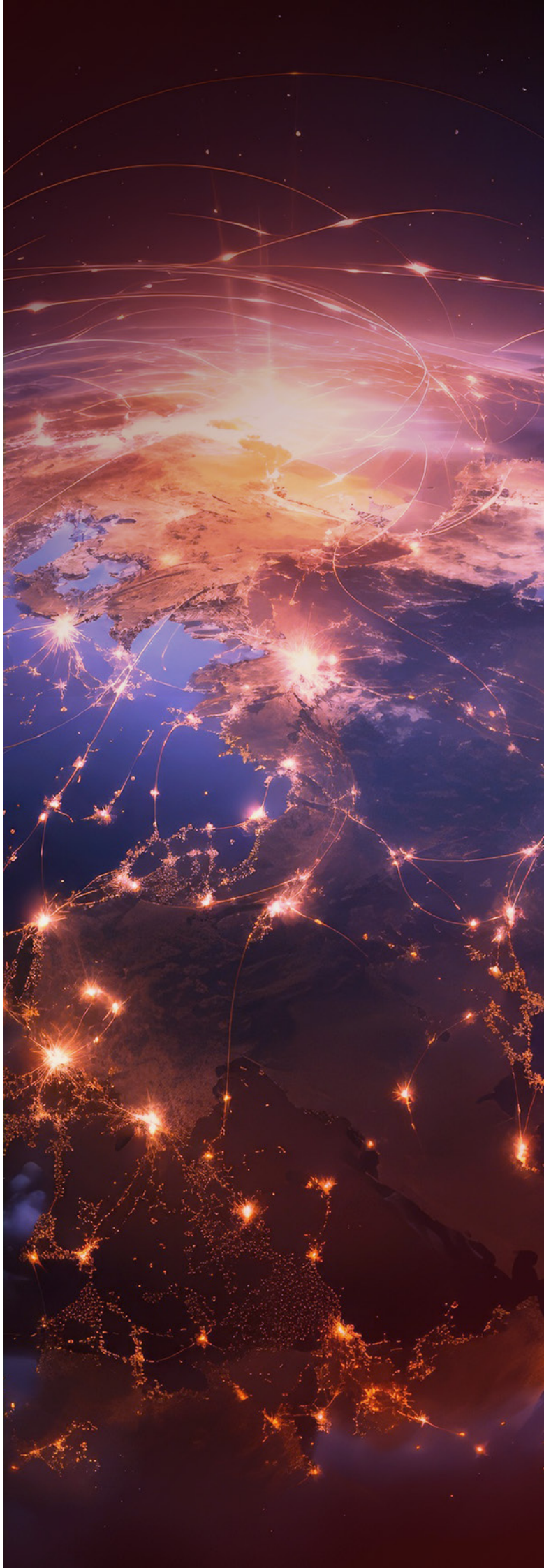
2. Create a secure digital platform for real-time threat intelligence sharing and communication between EU and NATO cybersecurity teams. This platform would enable both organizations to identify patterns, share information on vulnerabilities, and protect critical technologies such as AI and quantum systems. Connecting institutions to this platform should be mandatory to ensure comprehensive participation and maximize threat detection capabilities.

3. Develop common cybersecurity standards and best practices for dual-use technology suppliers to ensure robust security measures are implemented across critical technologies. This will help minimize vulnerabilities to cyber-attacks and strengthen the resilience of both civilian and military applications. Enrich cyber threat taxonomies and leverage platforms like the OECD AI Incident Monitor to share lessons learned, identify patterns, and enhance system-wide understanding of cyber risks.

4. Organize regular EU-NATO cyber defense exercises to test collaboration and readiness in responding to cyber threats targeting dual-use technologies. These exercises would identify weaknesses, improve coordination, and enhance response times in real-world scenarios. Incorporate insights from exercises to refine cybersecurity protocols, threat mitigation strategies, and interoperability between EU and NATO systems.

5. Create a network of military-focused laboratories in Europe that act as bridge institutions between academic research and military applications. This would facilitate the transition of civil-focused technological innovations with military potential into practical defense solutions. Support academic research on AI security by addressing key challenges, such as AI model manipulation, severe coding errors, and system risks. Focus on developing advanced error identification methods beyond current probabilistic systems, which are insufficient and can introduce new vulnerabilities.

6. Encourage collaboration with private sector partners to enhance cybersecurity across dual-use technologies. Engage industry leaders to implement security best practices, improve supply chain resilience, and safeguard critical infrastructure. Facilitate partnerships that foster innovation while ensuring alignment with EU-NATO cybersecurity standards and protocols.



THEME III:

Dual-use control export and regulations

Currently, inconsistent regulations across the EU lead to loopholes and uneven enforcement, weakening Europe's position in global technology security. Looking forward, emerging technologies such as AI, biotechnology, and quantum computing present new regulatory hurdles, as these rapidly evolve beyond existing frameworks.

CHALLENGE: STREAMLINING AND STANDATIZING EXPORT CONTROLS FOR DUAL-USE TECHNOLOGIES ACROSS THE EU

The regulatory inconsistency for dual-use technology export controls across the EU poses significant challenges to security, innovation and economic competitiveness. It created vulnerabilities that can be exploited by hostile actors and place an increased compliance burden on exporters.

To overcome these challenges, the EU must undertake coordinated actions to simplify and harmonize dual-use technology export control processes. A unified framework will enhance security by minimizing exploitation risks and strengthen Europe's position as a global leader in establishing robust technology governance standards. Moreover, streamlined processes will reduce costs for businesses and foster innovation within the EU.

RECOMMENDATIONS:

1. Establishing a unified EU export control framework is essential for streamlining and standardizing the regulation of dual-use technology exports across member states. Replacing fragmented national policies with a single, harmonized system will ensure clear rules and guidelines, eliminate regulatory discrepancies, and close loopholes. A consolidated framework should include a common monitoring system for dual-use technology exports, alongside updated regulations that enhance transparency and predictability, thereby strengthening the EU's common export control regime.

2. Enhancing the role of the EU Dual-Use Coordination Group (DUCG) is critical to ensuring the uniform application of export controls and improving coordination among member states. The DUCG's mandate should be expanded to include oversight of emerging technologies, mediation of disputes, and providing clear guidance. Additionally, establishing a centralized database, fostering stronger cooperation between member states, conducting regular consultations, and supporting joint decision-making will further streamline enforcement and strengthen the EU's dual-use export control framework.

3. Introduce robust enforcement measures to prevent unauthorized exports, including regular audits, enhanced penalties for violations, and improved cooperation between national customs authorities.

A centralized EU enforcement unit could support these efforts by investigating cross-border cases.

4. Developing a centralized EU export licensing system is essential for streamlining the application and approval processes for dual-use technology exports. A shared digital platform would allow businesses to submit requests through a single portal, reducing bureaucratic delays and ensuring consistency in licensing decisions across the EU. Leveraging advanced technologies, such as AI, data analytics, and secure communication channels, can enhance the system's efficiency and user experience while strengthening the overall reliability of export controls.

5. Expanding and updating the EU Dual-Use Control List to include advancements in emerging technologies such as AI, quantum computing, and biotechnology is essential to ensure export controls remain effective in addressing advancements that could be exploited for malicious purposes.

6. Providing regular training and resources for businesses and exporters is vital to ensuring compliance with export controls. Comprehensive training programs should educate stakeholders on the risks associated with dual-use technologies and offer clear guidance on licensing requirements. Additionally, fostering public-private collaboration through partnerships between governments, academia, and private sector stakeholders can align export controls with industry practices. This cooperation helps identify potential risks and ensures that regulations remain practical and balanced, avoiding undue burdens on businesses.

CHALLENGE: ESTABLISHMENT OF A CENTRAL EU INSTITUTION TO COORDINATE AND MONITOR COMPLIANCE WITH EXPORT CONTROL REGULATIONS

The creation of a central EU institution to coordinate and monitor compliance with export control regulations could bring significant advantages to addressing current inconsistencies and enforcement gaps across member states. However, it would also come with challenges related to sovereignty, bureaucracy, and resource allocation.

There are some arguments in favor of this. The creation of this kind of institution could address significant challenges currently facing the EU. First of all, it could bring consistency and harmonization. A centralized institution would ensure uniform application of export control regulations, eliminating discrepancies between national-level policies and closing loopholes that adversaries could exploit. A centralized oversight would facilitate real-time monitoring of dual-use exports, improving enforcement against unauthorized transfer. A specialized unit to investigate and address violations across the EU could be established within the institution. A central body would be also better positioned to regularly update regulations to address new technologies, such as AI, quantum computing and biotechnology, ensuring that controls remain relevant. Lastly, smaller member states, which can lack the resources to enforce export control effectively would benefit significantly from the shared expertise and centralized resources provided by such an institution.

However, creating a central EU institution to coordinate and monitor compliance with export control regulations could face some challenges. Member states may be hesitant to relinquish control over sensitive aspects of trade and security, citing concerns over national sovereignty. Additionally, implementing such an institution would require substantial investments in infrastructure, staffing, and training, posing significant financial and logistical hurdles. There is also a risk that a centralized body could become overly bureaucratic, leading to inefficiencies and delays in decision-making, including export approvals. Furthermore, striking the right balance between security and innovation remains a critical concern, as excessively stringent controls could stifle innovation and reduce the competitiveness of European industries in global markets. The establishment of such an institution presents certain challenges. Nevertheless, the potential benefits it offers make it a consideration worth pursuing.

RECOMMENDATIONS:

1. The institution's responsibilities, focusing on harmonization, monitoring and enforcement while respecting national prerogatives, should be clearly outlined. Its primary focus would be on harmonizing export control regulations across member states, ensuring consistency in interpretation, application, and enforcement. It would monitor compliance with dual-use export controls, facilitate real-time reporting and intelligence sharing, and provide a central hub for addressing violations efficiently. Additionally, the institution should act as a resource center, offering technical support and expertise to member states, particularly smaller ones. Importantly, its operations must respect national sovereignty by working within a framework that allows member states to retain final authority over sensitive national security matters.

2. Representatives from all member states should collaborate to ensure transparency and inclusiveness. Regular forums, reporting mechanisms, and advisory committees should be established to facilitate dialogue, address member state concerns, and strengthen cooperation. A rotating leadership model or equal representation could enhance trust and ensure that diverse national interests are taken into account, fostering ownership and alignment of export control measures across the EU.

3. The private sector and academia should be involved to ensure that regulations align with technological realities and industry needs. Regular consultations with businesses and research entities will help ensure that regulations are practical, aligned with technological realities, and do not impose excessive burdens that could stifle innovation. Advisory panels or working groups comprised of industry experts, policymakers, and academics should be created to provide guidance on updating regulations, identifying emerging risks, and developing balanced measures that enhance security without hindering competitiveness.

4. It is recommended to adopt a phased implementation approach, starting with a pilot program to centralize oversight for selecting high-risk technologies and expanding it gradually as needed. The program can initially focus on high-risk technologies such as AI, quantum computing, or cybersecurity tools, where consistent oversight is most urgently needed. This would allow the institution to test centralized coordination mechanisms, establish protocols for reporting and enforcement, and identify potential obstacles before scaling operations. Lessons learned from the pilot phase would inform adjustments and improvements, ensuring a smooth, gradual rollout. Over time, the institution's scope can be expanded to cover additional technologies and sectors, as required.

5. Coordination and interoperability with NATO are needed in this area to align export control measures with transatlantic operations, and active collaboration with all stakeholders. Dual-use technologies often have strategic importance in transatlantic defense and security efforts, and inconsistent regulations could hinder joint operations or create vulnerabilities. The institution should prioritize coordination with NATO to ensure interoperability of policies, facilitate intelligence sharing, and harmonize approaches to dual-use technology exports. This collaboration would enhance Europe's strategic autonomy while reinforcing its role as a reliable transatlantic partner.

6. The Agency for the Cooperation of Energy Regulators could serve as a model. The Agency for the Cooperation of Energy Regulators (ACER) serves as a successful precedent for creating centralized EU-level oversight while maintaining national authority in a critical sector. Like ACER, the proposed institution could function as a coordinator and facilitator, ensuring uniform enforcement while empowering member states to retain operational control where necessary. ACER's governance structure, funding model, and mechanisms for collaboration across national authorities provide valuable lessons for building an institution that is both efficient and adaptable.

CHALLENGE: ADAPTING EU REGULATIONS TO RAPIDLY EVOLVING TECHNOLOGIES

Adapting EU regulations to address rapidly evolving technologies, such as AI and biotechnology, requires proactive, dynamic, and forward-looking measures. These technologies evolve much faster than traditional regulatory frameworks, necessitating a shift towards flexible and anticipatory governance.

By implementing recommended measures, the EU can create a robust, adaptable regulatory framework that balances innovation with security concerns. These steps will ensure the EU remains a leader in responsibly governing rapidly evolving technologies while mitigating risks to global stability. Some stakeholders argue that expanding export controls to cover all emerging technologies, such as AI and biotechnology, could create unnecessary burdens and stifle innovation. Therefore, a careful approach is needed to ensure that export controls are applied only where strictly necessary, while exploring alternatives like soft law for broader, less critical technologies.

RECOMMENDATIONS:

1. Adopting an adaptive regulatory framework is essential to keep pace with rapidly evolving technologies. This framework should include modular regulations that can be easily updated as technologies and their applications change, along with provisional guidelines to enable interim compliance while permanent regulations are developed. Regulatory sandboxes should be implemented to test and refine regulations in controlled environments, providing valuable insights to improve regulatory approaches. Regular reviews, a flexible risk-based assessment approach, and enhanced international cooperation—such as multilateral collaboration,

information sharing, and joint research initiatives—are crucial for staying ahead of emerging challenges. Investment in expertise, technological tools, and cybersecurity capacity building is also necessary, as is fostering public-private partnerships that involve industry, academia, and civil society to ensure a balanced and forward-looking regulatory system.

2. Enhancing risk assessment and categorization is crucial for managing dual-use technologies effectively. An EU-wide risk classification system should be developed to evaluate emerging technologies based on their potential dual-use applications, incorporating input from scientific, ethical, and technological experts to identify potential misuse and security risks. This system should be continuously monitored, with regular reviews and updates to reflect advancements in technology and evolving threat landscapes. Additionally, dual-use projects should be consistently monitored, and risks mitigated through legislation at the EU level. To ensure effectiveness, the regulatory impact must be evaluated regularly, with policies adjusted in response to emerging challenges and feedback from stakeholders.

3. Expanding expert networks and strengthening public-private collaboration are essential for effectively managing dual-use technologies. The EU should establish a permanent Expert Advisory Council on Emerging Technologies, drawing on diverse perspectives from academia, industry, and international organizations to maintain up-to-date knowledge and expertise. AI and biotechnology experts should be actively involved in export control decision-making processes. Simultaneously, fostering public-private partnerships by engaging with technology companies, academic institutions, and civil society can facilitate information sharing on potential misuse and compliance challenges. Incentivizing innovation in 'export control-friendly' technologies that minimize dual-use risks will further support a balanced approach to security and innovation.

CHALLENGE: RISK MANAGEMENT MECHANISMS TO SUPPORT THE RESPONSIBLE USE OF DUAL-USE TECHNOLOGIES

Managing the risks associated with dual-use technologies requires robust and harmonized mechanisms to address potential misuse while fostering secure and ethical applications. At both the national and EU levels, there is a pressing need to shift from being risk-averse to becoming risk-aware, recognizing that no collaboration or technological advancement is entirely without risk. The focus should be on effectively mitigating these risks through comprehensive strategies and measures, such as clear contractual obligations, data-sharing restrictions, personnel vetting, and adaptable exit clauses.

Currently, the lack of harmonization in existing risk management mechanisms and the limited availability of automated tools represent significant challenges. Many market operators developing dual-use technologies may lack expertise in cyber risk management, further underscoring the need for standardized approaches and accessible tools. Additionally, a broader conversation is needed across the EU to raise awareness of the risks and foster discussions around effective mitigation strategies. By integrating risk management into national and EU strategies, governments can ensure that innovation progresses responsibly, aligned with EU values and global security objectives.

RECOMMENDATIONS:

1. Addressing the challenges of deploying AI technologies developed for civilian purposes in military contexts requires robust mechanisms, including the establishment of Civil-Military Testing and Experimentation Facilities to adapt and evaluate these technologies in controlled environments. An integrated risk assessment framework is essential, combining threat analysis—based on misuse likelihood, geopolitical implications, and ethical considerations. Effective risk control mechanisms must ensure oversight of technology usage, verification of its effects, and acceptance of defined risk levels. Regulatory systems should be introduced to govern the export of dual-use technologies, balancing national and EU security priorities with ethical considerations. Complementary monitoring and audit mechanisms would provide ongoing oversight, ensuring accountability and fostering trust in the responsible use of dual-use technologies.

2. Enhancing oversight and monitoring of dual-use technologies requires coordinated efforts at both national and EU levels. National watchdog agencies should be established to oversee compliance and conduct risk assessments, while a centralized EU body could harmonize monitoring efforts across member states and coordinate responses to emerging risks. A shared EU database would further strengthen these efforts by tracking the production, sale, and export of dual-use technologies, enabling data-driven decision-making. Leveraging

real-time data analytics would allow for the identification and mitigation of vulnerabilities across supply chains, ensuring a proactive and unified approach to managing dual-use technology risks.

3. Partnerships between governments and technology firms can help identify vulnerabilities, share threat intelligence, and implement best practices for safeguarding technologies. Offering incentives, such as tax breaks or grants, can encourage companies to invest in secure and ethical dual-use applications. Additionally, engaging civil society organizations, academic experts, and industry leaders in the policymaking process ensures diverse perspectives are considered. Regular forums and consultations can further refine risk management strategies by incorporating valuable feedback and fostering a collaborative approach to addressing challenges.

4. Enhancing ethics and compliance in dual-use technologies requires targeted training and investment in research and innovation. Mandatory training programs should be developed for stakeholders in industries handling dual-use technologies, emphasizing export controls, compliance, and ethical usage. EU-wide certification schemes can standardize these programs, ensuring consistent understanding across sectors. Simultaneously, supporting R&D initiatives is crucial for advancing technologies with built-in risk management features. Funding research into ethical AI, secure biotechnology, and quantum computing will promote responsible innovation while addressing the unique challenges posed by dual-use technologies.

5. Strengthening international cooperation is vital for aligning risk management practices and establishing global standards for dual-use technologies. Collaboration with organizations like NATO and the United Nations can ensure a cohesive approach, while bilateral agreements with allies can facilitate the exchange of knowledge, best practices, and resources. Effective risk control measures must accompany these efforts, including stringent oversight of technology usage, verification of its effects, and acceptance of defined risk levels. Monitoring and audit mechanisms should be integrated to support these goals, ensuring that international cooperation is underpinned by robust and transparent risk mitigation strategies.

THEME IV:

Financing dual-use technology development and innovation

Funding is a key aspect of dual-use technology development, especially in the context of Europe's ambitious goals for innovation, competitiveness and technological independence. Stable and targeted funding can enable acceleration of research, development of key capabilities and strengthening of public-private cooperation.

CHALLENGE: SOURCES OF FUNDING

To effectively support the development of dual-use technologies and enhance Europe's technological security, a balanced approach to funding that leverages national, EU, and private sources is recommended. Each funding source plays a complementary role, and prioritizing their integration can maximize innovation and strategic outcomes.

RECOMMENDATIONS:

1. Given the strategic importance of dual-use technologies, funding should prioritize a mix of EU, national, and private sources to ensure financial stability and sustainable support. EU funds should remain the dominant funding source, complemented by national investments, with countries like Poland encouraged to increase their contributions to R&D in key and sensitive technologies. Dedicated support programs should be established, guided by an EU-level strategy that sets priorities and appropriate security requirements for financing paths. This balanced approach will mitigate risks, foster innovation, and provide the stability needed to advance critical dual-use projects.

2. National governments should foster tailored investments by allocating funds to address country-specific technological priorities and security concerns, while ensuring alignment with broader EU goals. For dual-use technologies with military applications, national defense budgets should support innovation in critical areas such as cybersecurity, quantum computing, and AI. Additionally, governments can leverage public procurement policies to stimulate local industries and strengthen resilience in strategic sectors, fostering both national security and economic growth.

3. EU funds play a crucial role in enhancing cohesion and scaling innovation across member states. Programs like Horizon Europe should be prioritized to fund collaborative research and innovation projects, fostering cross-border advancements in dual-use technologies. Increased investment in the European Defense Fund (EDF) is essential to support dual-use R&D and strengthen the EU's defense technological base. Additionally, Cohesion Funds should be directed toward regions lagging in technological development, ensuring a more equitable innovation landscape and bridging gaps across the EU.

4. A balanced funding approach is essential to ensure stable and sustainable support for dual-use technologies. Public-Private Partnerships (PPPs)

should be facilitated to bridge gaps between public funding and private investment, aligning financial efforts with EU strategic goals. Match funding mechanisms can encourage participation in EU programs by leveraging national funds to complement EU grants, allowing countries to address both national priorities and broader EU objectives. Additionally, dedicated innovation hubs for dual-use technologies, supported by pooled EU and national funds, can streamline development and funding processes. This mix of national, EU, and private funds, guided by an EU-level strategy that sets priorities and security requirements, will provide a diverse and resilient financing path. Such a balanced approach mitigates risks, supports innovation, and enhances overall financial stability across the EU.

5. Private sector funding plays a critical role in driving innovation in dual-use technologies. Creating an environment that attracts venture capital and supports startups through tax incentives, public-private partnerships (PPPs), and innovation hubs can accelerate investment in high-potential projects. Encouraging corporate R&D investments will ensure that large companies integrate dual-use research into their strategies while maintaining compliance with EU security regulations. Blended finance models, which combine public and private funding, can help mitigate risks for investors, particularly in high-potential but high-risk dual-use projects. Facilitating robust PPPs will further bridge the gap between public funding and private investment, ensuring alignment with EU strategic priorities and fostering a sustainable ecosystem for dual-use innovation.

6. Funding strategies for dual-use technologies must align with broader EU priorities to ensure technological independence, resilience, and ethical innovation. Emphasis should be placed on reducing reliance on non-European technologies, particularly in critical sectors such as semiconductors, AI, and cybersecurity. Funding should also prioritize projects that integrate robust cybersecurity measures to protect dual-use innovations from potential threats posed by hostile actors. Additionally, all investments must uphold European values by fostering ethical and sustainable innovation, ensuring that funded technologies respect human rights and promote environmental sustainability while advancing the EU's strategic goals.

CHALLENGE: CREATION OF A SPECIAL EU FUND EXCLUSIVELY DEDICATED TO DUAL-USE TECHNOLOGIES

Opinions are divided when it comes to the creation of a special EU fund exclusively dedicated to dual-use technologies. Some argue that such a fund would streamline financing, reduce fragmentation, and prioritize strategic projects in areas like AI, biotechnology, and quantum computing, allowing Europe to maintain its technological edge while addressing emerging challenges. They emphasize the need for faster allocation of resources, particularly in response to evolving security threats, and highlight the benefits of incentivizing public-private partnerships to foster collaboration and share risks.

On the other hand, critics express concerns about adding complexity to an already crowded funding landscape. They argue that existing frameworks should be leveraged and simplified rather than creating additional layers of bureaucracy. Some suggest a hybrid approach, where dual-use projects remain integrated within broader civil R&D programs, while military-specific initiatives are handled separately with clear interconnections. Safeguards must also be in place to ensure researchers retain autonomy and are not pressured into developing technologies they do not wish to pursue. Areas like materials science, drones, and space technologies have been identified as priorities, regardless of the funding structure.

RECOMMENDATIONS:

1. On one hand, creating this kind of fund could be a strategic move to enhance Europe's ability to address pressing technological challenges, ensure security, and maintain competitiveness in global markets. Such a fund would streamline financing processes, prioritize urgent and strategically important projects, and provide a focused approach to innovation in this critical area. It could act as a cornerstone of Europe's strategy to maintain resilience, security, and leadership in critical technology domains. By focusing resources on key areas and fostering a collaborative ecosystem, the fund would reinforce Europe's position in the global technology race while addressing emerging challenges.

2. On the other hand, there are opinions it would add extra complexity to the already crowded funding landscape, and we should focus on simplification rather than the other way around. The model proposed by the FP10 High-Level Group, which suggests a division between civil and dual-use projects and a separate military category with interlinks,

provides a balanced approach. This structure allows for mutual exploitation of innovations between sectors without the need for an entirely separate fund. Dual-use technologies can instead be categorized within the broader framework for supporting R&D projects, ensuring integration while maintaining flexibility. If a more defined separation is required, it could focus on areas like materials and material technologies, drones, space technologies, artificial intelligence, and quantum technologies. Additionally, safeguards must be in place to protect researchers from being pressured into developing items against their will, ensuring ethical and voluntary participation.

CHALLENGE: FINANCING MECHANISMS FOR THE BEST SUPPORT OF INTERNATIONAL COOPERATION BETWEEN THE EU AND TRANSATLANTIC ALLIES FOR JOIN TECHOLOGY PROJECTS AND INNOVATIVE SECURITY SOLUTIONS

Fostering international cooperation between the EU and its transatlantic allies, particularly European NATO members, for joint technology projects faces significant challenges due to political and financial complexities. Not all EU nations may support such initiatives, which could hinder consensus and collective action. The lack of a unified governance structure for overseeing funding distribution and monitoring project progress risks undermining transparency and accountability, creating distrust among stakeholders. Additionally, ensuring equal financial commitment from partners—such as through 50-50 co-financed projects—is essential but can be difficult to achieve, especially when nations prioritize differing security and technological objectives.

Strategic alignment poses another challenge, as projects must address shared threats like cyber risks, supply chain vulnerabilities, and the misuse of dual-use technologies, all while adhering to ethical standards and democratic values. Furthermore, building capacity through workforce development and technology-sharing programs requires dedicated resources, which may face delays or fragmentation. The lack of flexible and agile funding mechanisms limits the EU's ability to respond swiftly to emerging technological opportunities and global security challenges. Without overcoming these barriers, the EU risks missing opportunities to strengthen transatlantic ties, enhance technological sovereignty, and accelerate the development of critical dual-use innovations that serve both civilian and military needs.

RECOMMENDATIONS:

1. Create EU-NATO Innovation Funds to co-finance dual-use technology projects in key areas such as AI, quantum computing, biotechnology, and cybersecurity. Implement matching contributions from the EU, NATO, and individual member states to pool resources efficiently and maximize impact. Develop co-investment strategies that allow partners to share risks and resources, strengthening collaboration and driving innovation.

2. Expand the Horizon Europe framework to include transatlantic calls for proposals, enabling joint research and development efforts with global allies. Establish partnerships with the U.S. Defense Advanced Research Projects Agency (DARPA) to fund research on high-risk, high-reward technologies, fostering innovation in critical areas.

3. Negotiate specific agreements with the U.S and Canada to co-fund projects in strategically vital fields, such as cybersecurity, advanced materials, and AI. Include funding for technology transfer programs to leverage each partner's strengths while safeguarding intellectual property.

4. Introduce joint EU-NATO or EU-U.S. innovation challenges to identify and fund groundbreaking ideas in security-related technologies. Award winners with seed funding and opportunities for further development in collaborative research labs, promoting cutting-edge solutions in dual-use innovation.

CHALLENGES: HOW EXISTING EUROPEAN FUNDS CAN BE OPTIMIZED TO INCREASE THEIR IMPACT ON DUAL-USE TECHNOLOGY DEVELOPMENT AND EFFECTIVELY MEET THE STRATEGIC NEEDS OF THE EUROPEAN UNION?

Optimizing existing European funds like the European Defence Fund (EDF) and Horizon Europe to support dual-use technology development presents several challenges. A lack of strategic alignment and coordination across these programs leads to inefficiencies and duplication, hindering their ability to target emerging technologies like AI, quantum computing, and advanced materials. Administrative complexity, including burdensome application and reporting processes, further limits accessibility, particularly for SMEs and start-ups that drive innovation. Additionally, fragmented funding mechanisms and unclear definitions of dual-use technologies create barriers to effective

implementation and resource allocation, slowing innovation cycles and reducing the EU's ability to respond quickly to strategic defense and security needs.

Another critical challenge is ensuring that funding mechanisms are flexible and risk-mitigated to address the unique demands of dual-use technologies. While public-private collaboration and blended financing mechanisms hold promise, they remain underutilized, limiting private sector participation and co-investment. Establishing thematic funding calls, regional innovation hubs, and workforce development programs is essential but requires better integration and focus. If these challenges are addressed, the expected impact would be significant: greater EU resilience and sovereignty in critical technologies, accelerated innovation cycles with direct applications in security and defense, and strengthened strategic autonomy, reducing reliance on foreign technologies. By refining and aligning existing funds, the EU can position itself as a global leader in dual-use innovation and strategic security while fostering participation from diverse actors across its ecosystem.

RECOMMENDATIONS:

1. Enhance strategic coordination across funding programs, such as the European Defence Fund (EDF) and Horizon Europe, to align objectives with dual-use priorities. Focus on technologies critical to both civil and military applications, including AI, quantum computing, advanced materials, and biotechnology. Create synergies between these funds to reduce duplication, encourage interdisciplinary projects, and maximize resource efficiency.

2. Use EDF and Horizon Europe funds to establish regional innovation clusters focused on dual-use technologies. These hubs will foster collaboration among universities, industry, and government institutions, driving localized innovation. Diversify projects geographically by prioritizing development in areas like Southern and Eastern Europe, ensuring broader regional participation and innovation.

3. Allocate specific funding streams within Horizon Europe and EDF for dual-use R&D projects through thematic calls in priority areas such as cybersecurity, autonomous systems, and biotechnology. Utilize blended finance mechanisms, such as combining public funding with private investments, matching grants, and risk-sharing instruments to support high-impact projects. Enable fast-track funding procedures for projects that can scale quickly to address strategic EU defense and security needs.

4. Simplify application and reporting procedures to attract a broader range of stakeholders, particularly SMEs and start-ups, which are key drivers of dual-use innovation. Introduce centralized platforms for funding applications to enable better coordination, monitoring, and transparency across programs.

5. Increase funding for public-private partnerships to leverage industry expertise and accelerate the commercialization of dual-use innovations. Incentivize private co-investment through tax benefits or matching grants tied to EU strategic priorities, fostering a collaborative innovation ecosystem.

6. Allocate funding to workforce training programs that prepare researchers, engineers, and technicians to work on dual-use technologies. Partner with universities to integrate dual-use technology considerations into academic curricula, ensuring a steady pipeline of skilled talent to meet future needs.

7. Foster cross-border cooperation with transatlantic allies and other global partners while maintaining EU security standards. Dedicate EDF funding to joint projects that enhance interoperability within NATO and promote global leadership in dual-use technologies.

8. Dedicate portions of funding to risk assessments and technology export control compliance to ensure adherence to EU security guidelines. Develop monitoring frameworks to track technological advancements, address vulnerabilities in real time, and mitigate risks related to dual-use innovations. Establish a joint monitoring effort between public and private stakeholders to enhance transparency, share intelligence, and ensure a coordinated response to emerging risks.

CHALLENGE: ATTRACTING GREATER PRIVATE SECTOR INVESTMENT

The EU faces significant challenges in fostering a thriving dual-use technology ecosystem due to fragmented regulatory frameworks, limited financial incentives, and insufficient coordination. Complex and inconsistent certification processes across Member States create barriers to market entry, slowing innovation and increasing costs for companies. Additionally, while intellectual property protections and export control regulations exist, they remain inadequate in fully safeguarding dual-use innovations, reducing investment attractiveness. Balancing security requirements with innovation, such as implementing mandatory security assessments, further complicates efforts

to streamline regulatory processes and promote private sector participation.

Another critical challenge is the fragmented funding landscape for cybersecurity and dual-use R&D. Cybersecurity suffers from dispersed and uncoordinated funding, which limits its impact. Financial tools like tax incentives, grants, and low-interest loans are underutilized or inconsistently applied, preventing the EU from attracting sufficient private investment in high-risk, high-reward technologies like AI, quantum computing, and biotechnology. Moreover, the lack of cohesive public-private partnerships and secure information-sharing mechanisms hinders collaboration and slows the adoption of innovative solutions. Addressing these challenges requires the EU to harmonize regulations, focus funding, and create a clear, supportive environment for dual-use technology development.

RECOMMENDATIONS:

1. Provide clear and supportive regulatory frameworks that encourage private sector participation in dual-use technology development. Develop regulatory sandboxes to allow companies to test dual-use technologies in controlled environments, accelerating innovation while ensuring compliance with security standards. Introduce streamlined export control compliance processes for firms adhering to EU regulations, reducing administrative burdens without compromising security. Establish an EU-wide security certification framework for dual-use technologies, enabling compliant firms' easier access to funding, procurement opportunities, and markets. Balance security with innovation by implementing mandatory security assessments for private investments in dual-use technologies to ensure responsible use and prevent misuse by hostile actors.

2. Offer R&D tax credits, deductions, and reduced tax rates for companies investing in critical dual-use areas such as AI, quantum computing, and biotechnology. Provide tax breaks for companies demonstrating compliance with EU security standards. Implement matching grants where public funding complements private investments in dual-use R&D, encouraging companies to scale projects. Offer competitive grants (targeted funding) and block subsidies for high-potential dual-use innovation projects. Provide low-interest loans through instruments like the European Investment Bank (EIB), prioritizing SMEs and start-ups working on dual-use technology projects. Additionally, develop co-investment schemes in partnerships with venture capital firms to support high-risk, high-reward dual-use technologies. Create public-private partnership Funds, pooling resources between governments and private firms to finance large-scale innovation projects. Finally, establish EU-wide innovation prizes to reward breakthroughs in dual-use technologies that address strategic priorities, such as energy resilience and cyber defense.

3. Strengthen intellectual property protection laws to safeguard dual-use innovations, incentivize private sector investments, and protect European patents. Provide regulatory support to facilitate the monetization of solutions developed in dual-use R&D projects. Offer private companies, preferential access to EU-funded defense and infrastructure projects if they meet dual-use technology standards.

4. Ensure cyber funding is focused, coordinated, and less fragmented, given its horizontal and cross-cutting nature. Dual-use technologies, particularly in cybersecurity, require concentrated financial and strategic support to mitigate risks effectively. Prioritize funding for R&D programs and establish strategic areas of focus, ensuring dual-use projects align with EU security and technological autonomy goals. Facilitate public-private information-sharing frameworks to allow the private sector access to government insights on emerging threats and vulnerabilities.

5. Expedite access to the market for dual-use technologies by reducing the cost and complexity of the certification process. Develop mechanisms like regulatory sandboxes and enhance implementation policies to accelerate the commercialization of dual-use technologies.

Summary of key recommendations

Dual-use technology is vital to national and global security, economic competitiveness, critical infrastructure resilience, and the collaboration between the civilian and military sectors. They hold significance in multiple sectors and should be at the forefront for policy makers. As dual use technologies advance rapidly, ensuring their responsible use while maintaining innovation is essential. Key issues include the risks of misuse, such as cyber threats, espionage, and the spread of misinformation, which can undermine security, public trust, and democratic stability. Regulatory gaps further exacerbate these risks, as outdated or insufficient frameworks leave emerging technologies vulnerable to exploitation, hindering their safe and equitable deployment. Moreover, the fragmented nature of regulations across different regions and sectors creates inefficiencies, stifles innovation, and complicates international collaboration.

To address these challenges, there is a growing need for clear, adaptable regulations that can keep pace with technological advancements, alongside improved oversight mechanisms to ensure accountability and transparency. Enhanced international collaboration is equally critical to align global standards, share best practices, and mitigate cross-border risks effectively. The creation of joint institutions and platforms should be considered in order to ensure the safe development of such technologies. Furthermore, creating funds and investing more into this area can drive innovation and the expansion of new technologies. By balancing security with innovation, fostering cross-sector cooperation, and aligning national and regional strategies, Europe can build a more resilient and integrated technological ecosystem, boost its competitiveness, and establish global leadership in the responsible development and use of emerging technologies.

Deloitte.

Challenges of the NIS2 Directive

The NIS2 Directive, which aims to increase the level of security of network and information systems in the European Union, poses new challenges for organizations. These include both the adaptation of existing processes and the implementation of new technical, legal and organizational solutions. Failure to comply with the requirements may result in high financial penalties and damage to the company's reputation. Therefore, it is worth taking action now to ensure compliance with the new regulations.

Key challenges of the NIS2 Directive

1. Security Gap Analysis: Organizations must conduct a comprehensive assessment of current systems and processes to identify areas for improvement.

2. Implementation of new requirements: The implementation of technical safeguards, such as threat detection systems or incident management, requires time, resources and appropriate know-how.

3. Legal compliance: The directive imposes the obligation to meet certain formal requirements, such as incident reporting or risk management.

4. Maintaining Compliance: Organizations must constantly monitor their systems and adapt procedures to changing legal and technological requirements.

How can Deloitte help?

Deloitte specializes in comprehensive support for organizations in the process of meeting the requirements of the NIS2 directive. Our services include:

1. Gap analysis:

- We conduct detailed audits, identifying areas where the organization does not meet NIS2 requirements.
- We prepare a report with recommendations, indicating specific steps to take.

2. Requirements Implementation:

- We help you implement appropriate technical measures, such as information security management systems (ISMS), and processes in accordance with best practices.
- We support the development and implementation of business continuity plans and incident response strategies.

3. Legal and organizational consulting:

- We cooperate with legal experts to ensure full formal and legal compliance.
- We advise on risk management and creating a safety culture in the organization.

4. Maintaining Compliance:

- We offer monitoring, training and process update services to ensure long-term compliance with the Directive.

Why is it worth acting now?

The NIS2 directive imposes strict deadlines for implementing the requirements, and the process of adapting the organization is time-consuming. Starting action now allows you to avoid rushing, minimize the risk of fines, and build a solid foundation for digital security.

Take action today! Contact Deloitte for a free consultation and to find out how we can help your organization meet the requirements of the NIS2 directive.