Dual-use innovation and critical infrastructure resilience: prospects of bulgaria's defense innovation center

Antoaneta Simeonova, Angel Krumov
Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences,
67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria [1]

Abstract: *This paper examines the prospective role of Bulgaria's newly established Defense Innovation Center at Sofia Tech Park in strengthening critical infrastructure resilience. Designed in line with NATO and EU standards, the Center is expected to test emerging technologies and develop prototypes, with an initial focus on unmanned aerial vehicles (UAVs) and advanced defense systems. The analysis adopts a conceptual approach, outlining potential applications of these dual-use technologies across the energy, communications, cyber, and transport sectors. It also highlights key risks, including funding sustainability, dual-use dilemmas, and continued dependence on external technological ecosystems. By situating the initiative within the broader NATO and EU innovation landscape, the paper underscores both the opportunities and uncertainties of integrating defense-driven innovation into national resilience strategies.*

KEYWORDS: *DUAL-USE INNOVATION, CRITICAL INFRASTRUCTURE, RESILIENCE, BULGARIA, NATO, EU, UAVS.*

1. Introduction

In an era defined by hybrid threats, geopolitical uncertainty, and rapid technological change, the protection of critical infrastructure (CI) has become a central pillar of national security policy. Energy grids, communication networks, transport systems, and cyber infrastructure form the backbone of modern societies, yet they are increasingly vulnerable to disruption, sabotage, and cyberattacks. For small and medium states such as Bulgaria, these vulnerabilities are further amplified by limited defense-industrial capacity and dependence on external technological ecosystems. Strengthening infrastructure resilience therefore requires not only robust security policies but also the ability to integrate innovation and advanced technologies into national defense and civil protection frameworks.

Against this backdrop, Bulgaria has recently established a Defense Innovation Center at Sofia Tech Park, designed in alignment with NATO and European Union standards. The initiative aims to stimulate research and development in dual-use and defense technologies, fostering cooperation between the armed forces, academia, and the private sector. According to official statements, the Center will serve as a platform for testing cutting-edge technologies and developing prototypes, with an initial focus on unmanned aerial vehicles (UAVs) and advanced defense systems. Although the Center's operational activities are still in the early stages, its creation signals Bulgaria's growing ambition to enhance strategic autonomy, bridge the gap between defense and innovation, and build technological capacity within the national security ecosystem.

This paper examines the prospective role of the Defense Innovation Center in strengthening the resilience of Bulgaria's critical infrastructure. It adopts a conceptual and forward-looking approach, exploring how innovations in dual-use technologies – particularly drones and secure communications – could contribute to the protection and recovery of key systems across the energy, communications, cyber, and transport sectors. At the same time, the paper acknowledges that the integration of advanced technologies may introduce new risks and vulnerabilities, especially when security is not embedded by design.

The study thus seeks to address the following research question:

In what ways can innovations emerging from Bulgaria's Defense Innovation Center strengthen, or potentially compromise, the resilience of national critical infrastructure?

By situating the Bulgarian case within the broader NATO and EU defense innovation landscape, the paper highlights both the opportunities and uncertainties of leveraging dual-use technologies for national resilience in a small-state context.

2. Conceptual Framework

2.1. Critical infrastructure resilience (EU/NATO/BG policy context)

Across the European Union, critical infrastructure resilience refers to the capacity of "critical entities" that provide essential services to prepare for, withstand, respond to, and recover from disruptive incidents – including natural hazards, terrorism, insider threats, sabotage, and major public-health events. This policy framing is codified in the Critical Entities Resilience (CER) Directive (Directive (EU) 2022/2557), which requires Member States to designate critical entities, run risk assessments, and ensure organizational, physical, and operational measures that strengthen continuity of essential services. Member States had to transpose CER into national law by 17 October 2024. [1]

In parallel, the NIS2 Directive (Directive (EU) 2022/2555) sets a high common level of cybersecurity for network and information systems across a broad set of sectors. NIS2 obliges covered entities to adopt risk management measures and incident reporting, thereby reinforcing the cyber dimension of resilience for operators of essential and important services. [2] Together, CER and NIS2 articulate an integrated EU approach in which organizational resilience and cybersecurity are treated as mutually reinforcing requirements for critical infrastructure protection.

Bulgaria's domestic framework aligns with this EU architecture. The Cybersecurity Act (2018) organizes national cybersecurity governance and defines "network and information security" as the ability of systems to resist actions that negatively affect availability, authenticity, integrity, or confidentiality of data and related services – concepts that dovetail with NIS/NIS2 obligations. [3] Disaster-management legislation (the Disaster Protection Act) embeds the notion of critical infrastructure and "European critical infrastructure," anchoring CI protection within national emergency-management and continuity planning. [4]

2.2. Dual-use innovation

Dual-use innovation denotes technologies with both civilian and military applications – particularly relevant where defense-driven R&D can spill over to civilian CI protection (e.g., surveillance, secure communications, autonomy, sensing). [5] Within NATO, the Defense Innovation Accelerator for the North Atlantic (DIANA) explicitly targets dual-use deep tech and collective resilience challenges, providing acceleration, test centers, and challenge-driven calls to translate prototypes into deployable solutions. This

positions defense innovation as a lever for allied resilience, not solely for traditional military capability development. [6]

At EU level, the European Defense Fund (EDF) – established by Regulation (EU) 2021/697 – finances collaborative R&D to strengthen the European defense technological and industrial base (EDTIB). While the EDF is a defense instrument, its emphasis on competitiveness, efficiency, and innovation capacity creates channels through which defense R&D can influence adjacent civilian technologies relevant to CI resilience (e.g., sensors, secure networks, autonomy). [7] The 2025 interim evaluation underscores this ecosystem-building function and provides evidence on implementation progress. [8]

3. Case: Bulgaria's Defense Innovation Center

In June 2025, the Council of Ministers of the Republic of Bulgaria officially adopted a decision to establish a Defense Innovation Center (DIC) as a unit within Sofia Tech Park AD.

The Center is designed to operate as a hub for testing emerging defense and dual-use technologies and developing prototypes with an initial focus on unmanned aerial vehicles (UAVs) and advanced defense systems. [9]

According to official sources, the DIC aims to leverage the strategic location and infrastructure of Sofia Tech Park, strengthen cooperation among government bodies (including the Ministry of Defense, Ministry of Innovation and Growth, and Ministry of Economy), and integrate the national defense research sector – notably the Defense Institute "Prof. Tsvetan Lazarov" – with private sector innovation.

Funding for the Center is expected to come via EU "shared management" instruments and national investment, though operational specifics (e.g., full staffing, prototype programs) remain at the planning phase. [10]

Officials emphasize that the Center is part of Bulgaria's strategy to enhance strategic autonomy and align national innovation efforts with both NATO Defense Innovation Accelerator (DIANA) and European Defense Fund mechanisms. As one deputy minister put it, it will "ensure Bulgaria's strategic independence through dual-use research and development." [11]

Taken together, the DIC represents a structural effort to bridge defense innovation and critical infrastructure resilience in Bulgaria – yet because it has only recently been established, our analysis treats it as prospective rather than evaluating realized outcomes.

4. Prospective Pathways to Infrastructure Resilience

The following section outlines prospective pathways through which technologies developed or tested within Bulgaria's Defense Innovation Center could contribute to strengthening national critical infrastructure resilience. Given that the Center is still in its formative stage, the discussion is necessarily conceptual and grounded in the broader NATO and EU frameworks that link defense innovation with civilian resilience. Each subsection highlights one critical sector – energy, communications, cyber, and transport – and considers how dual-use technologies such as unmanned aerial vehicles (UAVs), secure communications, and autonomous systems might enhance operational continuity, while also recognizing the potential vulnerabilities such innovations may introduce.

4.1. Energy

UAVs can augment situational awareness and maintenance in the power sector by enabling rapid, remote inspection of assets such as transmission lines, wind turbines, and pipelines – especially in hard-to-reach areas. This improves fault detection speed and reduces personnel risk during adverse conditions. [12]

From a systems perspective, electricity networks also need cyber-resilience measures – governance, testing, incident response, and recovery planning – to cope with increasingly digital grid operations and interdependencies. Authoritative guidance stresses structured risk management and drills for cyber-physical contingencies in the power sector. [13]

In NATO's ecosystem, challenge areas such as Energy and Power point to dual-use R&D opportunities (e.g., sensing, autonomy, data-driven maintenance) that could flow from defense innovation into civilian grid resilience. [14]

4.2. Communications

For communications infrastructure, spillovers from defense-grade secure communications – hardening against interception, jamming, and spoofing – could support continuity of telecom services and emergency communications. At EU level, the 5G Security Toolbox sets out coordinated risk-mitigation measures for mobile networks [15], complemented by ENISA's technical threat analyses for 5G. [16] These frameworks clarify vulnerabilities and required controls, providing a policy baseline for any dual-use innovations that interface with telecoms.

Recent Global Navigation Satellite System (GNSS) interference incidents over Europe (including a widely reported event over Bulgaria) [17] underscore the reality of contested electromagnetic environments for aviation and communications – highlighting the need for resilient PNT (positioning, navigation, timing) and anti-jamming/anti-spoofing approaches that defense innovation programs already prioritize. [18]

4.3. Cyber

Across sectors, EU threat-landscape assessments emphasize a steady tempo of cyber incidents targeting essential services and their supply chains. [19] This supports a design premise: prototypes emerging from a defense innovation hub must embed "security-by-design," align with NIS2-style risk management, and assume persistent threat activity.

In practice, dual-use capabilities relevant to cyber resilience include advanced detection and response (e.g., anomaly detection on OT/IT boundaries), secure update mechanisms for connected devices, and rigorous testing environments. Energy-sector guidance from international bodies details how tabletop exercises, red-teaming, and restoration planning strengthen cyber-physical preparedness – methods that a national testbed could institutionalize. [20]

NATO's DIANA challenge areas (e.g., Advanced Communication Technologies, Contested Electromagnetic Environments, Data-Assisted Decision Making) align closely with these needs, signaling a pathway for Bulgarian projects to target dual-use cyber-resilience solutions. [21]

4.4. Transport

Drones already see regulated civilian use for inspection of rail lines, bridges, and roads, enabling rapid assessment after incidents and improving maintenance cycles – capabilities directly relevant to transport continuity.

At the same time, transport systems are prominent cyber targets in Europe, and sector guidance highlights the necessity of coordinated incident response, supply-chain security, and testing against operational disruption. Any defense-derived autonomy, sensing, or secure-comms solution deployed into transport must therefore account for sector-specific cyber risks and interdependencies. [22]

Because many transport services rely on Global Navigation Satellite System (GNSS) and resilient communications, the documented rise in jamming/spoofing incidents further argues for dual-use R&D on navigation resilience, interference detection, and fail-safe procedures in mobility operations. [23]

Taken together, these pathways illustrate both the promise and the complexity of integrating defense innovation into the civilian infrastructure landscape. Dual-use technologies such as UAVs, secure communications, and autonomous systems could meaningfully enhance monitoring, responsiveness, and system redundancy across key sectors. However, the effectiveness of these applications will depend not only on technological capability but also on governance, funding, and secure implementation. The next section therefore examines the principal challenges and risks that may shape – or constrain – the Defense Innovation Center's potential to deliver tangible resilience benefits.

5. Challenges & Risks

While the establishment of Bulgaria's Defense Innovation Center (DIC) represents a strategic step toward integrating defense innovation with national resilience goals, its potential impact will depend on the country's ability to navigate several structural and operational challenges. These include issues of funding and sustainability, dual-use governance dilemmas, dependence on external technological ecosystems, and the inherent vulnerabilities that new technologies can introduce.

5.1. Funding and sustainability

Early-stage innovation hubs often struggle after initial launch unless there's predictable multi-year financing and the capacity to win competitive EU/NATO calls. The European Defense Fund (EDF) regulation makes clear that projects require collaborative consortia and co-funding to strengthen the EU's Defense Technological and Industrial Base (EDTIB) – opportunities, but also administrative and capacity hurdles for smaller states. [24] Sustained national budgeting and project-building capacity will be decisive for Bulgaria's DIC.

5.2. Dual-use governance and export controls

Bulgaria must balance openness for R&D collaboration with obligations under the EU's Dual-Use Regulation (recast), which establishes controls on the export, brokering, transit and transfer of dual-use items and related technical assistance. This framework is intended to prevent misuse/proliferation while not unduly constraining legitimate research and trade – creating a policy tension that DIC projects will need to manage from the outset. [25]

5.3. Strategic dependence on external ecosystems

The EU openly frames defense-industrial competitiveness and technological/industrial base development as collective aims (EDF) [26], while NATO's DIANA provides transatlantic accelerators and test centers rather than purely national pipelines. [27] For Bulgaria, interoperability and allied access are strengths – but they also imply reliance on external supply chains, standards and financing, which can become constraints during shocks.

5.4. Technological vulnerabilities and "security-by-design" gaps

New capabilities (UAVs, autonomy, secure comms) expand the attack surface if security is not embedded from design through deployment. ENISA's threat-landscape work highlights persistent targeting of essential services and the need for systematic risk management and incident reporting under NIS2 – requirements that should shape any prototypes/testbeds associated with the DIC. [28]

5.5. Communications resilience: jamming/spoofing as a live risk

Recent European aviation advisories and reporting document increased GNSS jamming/spoofing affecting operations, with high-profile incidents over Bulgaria. [29] This underscores the need for resilient PNT, anti-jamming/spoofing measures, and robust procedures in any dual-use comms/navigation solutions the DIC may touch.

5.6. Governance and coordination

Complex cross-ministerial ecosystems falter without clear mandates, shared standards, and transparent funding flows. OECD guidance on innovation governance stresses coherent roles and coordination to avoid fragmentation – principles directly relevant to steering Bulgaria's multi-actor defense-innovation effort (MoD, innovation agencies, Sofia Tech Park, academia, firms). [30]

These risks are not arguments against the DIC; they are the conditions that will determine whether a promising policy initiative matures into a durable capability for critical-infrastructure resilience – and they provide the criteria for future empirical evaluation once the Center is fully operational.

6. Conclusion

The establishment of Bulgaria's Defense Innovation Center represents an important policy signal: a recognition that technological innovation is now inseparable from national security and critical infrastructure resilience. By aligning with NATO and EU frameworks, the Center positions Bulgaria within a wider ecosystem that views defense research not only as a matter of capability development but also as a driver of societal resilience. The initiative's declared focus on dual-use technologies – such as unmanned aerial vehicles and advanced defense systems – illustrates the growing convergence between civilian and military innovation domains.

Yet, the analysis in this paper underscores that such convergence also introduces complex challenges. Sustainable funding, effective governance, and coherent integration with European regulatory regimes will be decisive for the Center's success. Moreover, the very technologies that promise to enhance resilience can simultaneously create new vulnerabilities if not secured by design, expanding the attack surface of critical systems. Managing these trade-offs will require a policy approach that prioritizes security, transparency, and interoperability from the earliest stages of innovation.

As of 2025, the Defense Innovation Center remains at an early stage of development. Its future impact will depend on whether Bulgaria can transform this institutional initiative into a functioning innovation ecosystem – one that connects defense needs with industrial capacity, research expertise, and infrastructure protection. Continued observation and empirical evaluation will be necessary to determine whether the Center evolves into a sustainable contributor to national resilience or remains primarily a strategic alignment gesture within NATO and EU frameworks.

Ultimately, the Bulgarian case illustrates a broader lesson for small and medium states: defense innovation can strengthen national resilience only when technological ambition is matched by long-term investment, secure design practices, and coordinated governance across both military and civilian domains.

References

1. European Commission. "Critical infrastructure resilience at EU-level". 11 September 2025. Available at: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en Accessed 10 November 2025.

2. EUR-Lex. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 Accessed 10 November 2025.

3. Cybersecurity Act. 7 November 2018. Available at: https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf Accessed 10 November 2025.

4. Disaster Protection Act. 19 December 2006. Available at: https://www.mi.government.bg/file/2011/08/zakon_zashtita_bedstvia_07_2020.pdf Accessed 10 November 2025.

5. European Commission. "Dual-use technologies". Available at: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/dual-use-technologies_en Accessed 10 November 2025.

6. NATO. "Defence Innovation Accelerator for the North Atlantic (DIANA)". 26 June 2025. Available at: https://www.nato.int/cps/en/natohq/topics_216199.htm Accessed 10 November 2025.

7. Regulation (EU) 2021/697 of the European parliament and of the council. 29 April 2021. Available at: https://eur-lex.europa.eu/eli/reg/2021/697/oj/eng Accessed 10 November 2025.

8. Interim evaluation of the European Defence Fund. 17 June 2025. Available at: https://defence-industry-space.ec.europa.eu/document/download/50cb88a0-7a4b-4f41-9649-f6272ca987ca_en Accessed 10 November 2025.

9. Bulgarian News Agency. "Government Establishes Defence Innovation Centre". 24 June 2025. Available at: https://www.bta.bg/en/news/bulgaria/917179-government-establishes-defence-innovation-centre Accessed 10 November 2025.

10. Epicenter. "The government created a Center for Innovation in Defense.". 24 June 2025. Available at: https://epicenter.bg/en/article/Pravitelstvoto-sazdade-Tsentar-za-inovatsii-v-otbranata/390901/2/0 Accessed 10 November 2025.

11. Bulgarian News Agency. "Defence Innovation Centre to Guarantee Bulgaria's Strategic Independence - Deputy Innovation Minister". 24 September 2025. Available at: https://www.bta.bg/en/news/bulgaria/973081-defence-innovation-centre-to-guarantee-bulgaria-s-strategic-independence-deput Accessed 10 November 2025.

12. European Union Aviation Safety Agency. "Inspecting Infrastructure". Available at: https://www.easa.europa.eu/en/domains/civil-drones/privacy/case-studies/inspecting-infrastructure Accessed 10 November 2025.

13. International Energy Agency (IEA). "Enhancing Cyber Resilience in Electricity Systems". Electricity Security 2021. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/04/enhancing-cyber-resilience-in-electricity-systems_38dbad0f/e00ae407-en.pdf Accessed 10 November 2025.

14. NATO DIANA. "NATO DIANA unveils 10 new challenges to accelerate dual-use technology breakthroughs". 2 June 2025. Available at: https://www.diana.nato.int/connect/nato-diana-unveils-10-new-challenges-to-accelerate-dualuse-technology-breakthroughs.html Accessed 10 November 2025.

15. European Commission. "The EU toolbox for 5G security". Available at: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security Accessed 10 November 2025.

16. European Union Agency for Cybersecurity. "ENISA Threat Landscape for 5G Networks Report". December 2020. Available at: https://standict.eu/sites/default/files/2021-02/ENISA%205G%20Threat%20Landscape%20-%20Update.pdf Accessed 10 November 2025.

17. The Associated Press News. "Russia is suspected of jamming navigation on EU leader's plane above Bulgaria, official says". 1 September 2025. Available at: https://apnews.com/article/europe-leyen-plane-radar-russia-jammed-51fa78294c2d0464dce5fd24dd4f273b Accessed 10 November 2025.

18. TIME. "NATO Says It's Working to Counter Russian GPS Jamming After Interference With European Commission President's Plane". 2 September 2025. Available at: https://time.com/7313738/russia-plane-gps-interference-suspected-president-european-commission/ Accessed 10 November 2025.

19. ENISA. ENISA Threat Landscape 2025. October 2025. Available at: https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf Accessed 10 November 2025.

20. International Energy Agency (IEA). "Enhancing Cyber Resilience in Electricity Systems". Electricity Security 2021. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/04/enhancing-cyber-resilience-in-electricity-systems_38dbad0f/e00ae407-en.pdf Accessed 10 November 2025.

21. NATO DIANA. "NATO DIANA unveils 10 new challenges to accelerate dual-use technology breakthroughs". 2 June 2025. Available at: https://www.diana.nato.int/connect/nato-diana-unveils-10-new-challenges-to-accelerate-dualuse-technology-breakthroughs.html Accessed 10 November 2025.

22. ENISA. Transport. Available at: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/transport Accessed 10 November 2025.

23. Jakub Trýba, Jakub Hospodkaa. "GNSS Interference and Security: Impacts on Critical Infrastructure and Mitigation Strategies". ScienceDirect, Procedia Computer Science 253 (2025) 2635–2644. Available at: https://www.sciencedirect.com/science/article/pii/S187705092500331X Accessed 10 November 2025.

24. EUR-Lex. "European Defence Fund (2021-2027)". Available at: https://eur-lex.europa.eu/EN/legal-content/summary/european-defence-fund-2021-2027.html Accessed 10 November 2025.

25. EUR-Lex. "Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)". Available at: https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng Accessed 10 November 2025.

26. EUR-Lex. "Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092 (Text with EEA relevance)". Available at: https://eur-lex.europa.eu/eli/reg/2021/697/oj/eng Accessed 10 November 2025.

27. DIANA NATO. "Defence Innovation Accelerator for the North Atlantic". Available at: https://www.diana.nato.int/ Accessed 10 November 2025.

28. ENISA. ENISA Threat Landscape 2025. October 2025. Available at: https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf Accessed 10 November 2025.

29. The Associated Press News. "Russia is suspected of jamming navigation on EU leader's plane above Bulgaria, official says". 1 September 2025. Available at: https://apnews.com/article/europe-leyen-plane-radar-russia-jammed-51fa78294c2d0464dce5fd24dd4f273b Accessed 10 November 2025.

30. OECD. OECD Working Papers on Public Governance No. 37. "The Public Sector Innovation Lifecycle". 2020. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/05/the-public-sector-innovation-lifecycle_2359c685/0d1bf7e7-en.pdf Accessed 10 November 2025.