

Innovation, adaptation and the future force: translating Ukraine's lessons for NATO

**12
10**

Co-organised with



Event report

As Ukraine's battlefield experience continues to reshape modern warfare, NATO and its allies face a practical challenge: how to translate lessons in digitalisation, rapid innovation and adaptation into practice, and whether their institutions, processes and partnerships are equipped to absorb and apply them at the pace required. Friends of Europe's high-level online policy discussion titled "Innovation, Adaptation and the Future Force" brought together Ukrainian, NATO and key European defence practitioners to examine how Ukraine's wartime experience can inform the future of allied armed forces.

Moderated by **Dharmendra Kanani**, Chief Spokesperson and Chief Operating Officer at Friends of Europe, the discussion featured **Oksana Ferchuk**, Ukraine's Minister of Digital Transformation; **Valeriya Izhyk** of the Boryviter Center of Excellence; **Nikos Loutas**, NATO's Director of Innovation; and **Sven Weizenegger**, leader of the Bundeswehr Cyber Innovation Hub.

The discussion focused on three interconnected challenges: translating battlefield lessons into lasting institutional change, shortening the path from operational need to deployed capability, and strengthening the interoperability and industrial capacity needed for a more adaptive future force.

Battlefield digitalisation, rapid innovation cycles and cyber resilience

Ukraine's Minister of Digital Transformation, **Oksana Ferchuk**, highlighted two pillars of Ukraine's wartime adaptation: digitalisation of the battlefield and rapid innovation cycles. Digitalisation relies on resilient connectivity, sensors, shared situational awareness through Delta (Ukraine's situational awareness and battlefield control system), civilian technologies and AI to support operations and decision-making.

On innovation, she said the cycle from field use and feedback to an improved product can take around four weeks, while decentralised procurement can take seven to ten days. She stressed that allies need to adopt an integrated operational ecosystem – rather than just purchase new equipment – and make experimentation part of routine military life. Ferchuk also said Ukraine faces an estimated 3,000–6,000 cyberattacks annually against government, defence and civilian services. She noted that AI-enabled attacks are evolving and learning rapidly, making cyber defence a constant race. She emphasised the need to work with international cybersecurity companies to test and improve protective tools against real-world attacks.

Ferchuk's remarks suggest that allies should treat digital transformation and rapid innovation as **core operational capabilities**, not separate modernisation projects. The following recommendations can be drawn from her examples:

- 1. Build an integrated, secure digital battlefield.** Invest in resilient connectivity, sensors and a shared operational picture that connects frontline users and commanders. Use dual-use technology and AI where appropriate, and develop the digital skills needed to make these tools part of routine military practice.
- 2. Accelerate the path from battlefield need to fielded capability.** Create a direct feedback channel between frontline users and suppliers and use operational data and after-action reviews to identify what needs to change. Let authorised units order from an approved digital marketplace, with decentralised delivery. Establish an accelerator to turn battlefield problems into clearly defined challenges for companies and start-ups, support pilots with grants, and define a route from successful testing to a state contract.
- 3. Develop AI sandboxes with Ukraine.** Support Ukraine as a practical environment for testing AI-enabled public and defence services, including on sovereign infrastructure. Use pilots to identify effective approaches and potential risks, then share the lessons with European partners. Design the approach to enable responsible experimentation while avoiding unnecessary regulatory friction that could slow innovation.

Preserving human and operational context in defence lessons-learned systems

Valeriya Izhyk of the Boryviter Center of Excellence argued that turning Ukrainian battlefield experience into lasting capability requires preserving the human and operational context behind lessons, not just collecting data. Lessons also need clear owners and accountability to ensure they inform doctrine, training and procurement; she cited JATEC as a mechanism to strengthen exchange between Ukraine and NATO. She emphasised that the deepest gap is cultural: peacetime institutions are built around planning cycles measured in years, while battlefield tactics can change every 30 days. Armed forces reviewing doctrine and training on a two-year cycle cannot keep pace with that change, and attending more training alone will not close the gap.

NATO innovation mechanisms, industrial scaling and interoperability standards

Nikos Loutas, NATO's Director of Innovation, said the Alliance is adapting its future force by combining legacy capabilities with new technologies, including unmanned systems, and by experimenting continuously rather than relying on periodic modernisation. Through its Rapid Adoption Action Plan, NATO has established Innovation Ranges, where technology innovators, operational users and procurement specialists work together to test and mature solutions, assess their potential operational value and consider pathways to adoption.

Loutas situated the Ranges within a broader innovation ecosystem: DIANA helps companies enter the defence market, the NATO Innovation Fund supports their growth, and NATO Engine connects defence firms with available commercial manufacturing capacity. Loutas said procurement should embed established standards wherever possible to support interoperability, while remaining flexible on emerging technologies; closer collaboration with industry can help develop standards for areas such as AI and next-generation networks.

User-led defence innovation: from field testing to capability scaling

Sven Weizenegger, the leader of the Bundeswehr Cyber Innovation Hub, described the Hub as a bridge between soldiers, government and industry. Its position within a commercial IT provider gives it advantages in recruitment and management, while its direct links to Ministry of Defence leadership help connect innovation work to strategic and operational needs. A key advantage, he said, is that soldiers are not just asked to identify problems; they become part of the solution. They participate in testing and improving technologies, creating a direct feedback loop with developers. Weizenegger cited the Laser Dome counter-drone trial as an example and described a process for helping successful projects scale beyond testing and bridge the gap to procurement. If a trial succeeds, the hub can help move the capability towards initial scaling, giving the unit a usable capability and the company a paying customer while informing a later full procurement decision.

From the audience, **Lauri Kangas**, Chief Technology Officer at the Finnish Aerospace and Defence Industries, noted that Finland's long border with Russia, reservist force and operationally informed engineers provide a strong foundation for defence innovation, but that adaptation must still accelerate. Finland's new defence innovation unit launched to help start-ups enter the defence market and explore new technologies, is still working with technologies at relatively low technology-readiness levels. Industry also needs clearer pathways from NATO Innovation Ranges into member states' procurement.

Štefan Füle, co-founder of U&C UAS, former Special Envoy to the OSCE and the Western Balkans and former EU Commissioner for Enlargement and a Trustee of Friends of Europe, described the EU-Ukraine Drone Alliance as an industry-led platform intended to bring Ukrainian and European defence companies together, but said the rules for sharing Ukrainian know-how with it remain unclear. He contrasted it with Ukraine's separate "drone deal" framework, which he said permits know-how transfers to companies in the EU or in agreed third-countries, in return for 20% of contract proceeds allocated to Ukraine. Füle argued that the two initiatives are not yet compatible and that further work is needed to establish clear rules for know-how transfer.

Key ideas to take forward:

- 1. Make continuous adaptation part of force readiness.** Build regular cycles of experimentation, feedback and revision into military life – not only into occasional exercises. Allies cannot match Ukraine's wartime conditions, but they can make adaptation more routine and reduce the gap between changing tactics and updating doctrine, training and capabilities.
- 2. Turn battlefield lessons into accountable action.** Capture the operational and human context behind lessons, then assign owners and deadlines for applying them to doctrine, training and procurement. Strengthen mechanisms such as JATEC around concrete outputs and follow-through, rather than treating attendance or reports as evidence of change.
- 3. Treat digitalisation as an operational ecosystem.** Connect resilient communications, sensors, shared situational awareness, AI-supported analysis and trained users. Plan for cybersecurity from the start, including protection of civilian and defence services against rapidly evolving, AI-enabled attacks.
- 4. Shorten the route from user need to deployed capability.** Establish a structured, user-led process that enables military end-users to define capability gaps, work directly with developers, and participate in testing and refinement. Pair this feedback loop with clear, time-bound pathways for procuring and scaling solutions that demonstrate operational value.
- 5. Make standardisation and interoperability practical priorities.** Embed established standards in procurement where possible so capabilities can work across allied forces. Where standards for emerging technologies are still developing, maintain flexibility and work with industry and partners to shape them – including in areas such as AI and next-generation networks.



Friends of Europe

Connect. Debate. Change.

info@friendsofeurope.org
friendsofeurope.org

Friends of Europe is a leading think-tank that connects people, stimulates debate and triggers change to create a more inclusive, sustainable and forward-looking Europe.

