This digest has been developed by the Tallinn Mechanism Project Office (TMPO) as part of the Tallinn Mechanism — an international initiative aimed at strengthening Ukraine's cybersecurity, enhancing cyber resilience, and protecting critical and civilian infrastructure through coordinated international assistance.

THE DIGEST PROVIDES UPDATES AND INSIGHTS ACROSS SIX AREAS FOR THE PERIOD FROM JUNE 5 TO JULY 18:

The information contained herein is intended to inform stakeholders and partners of ongoing activities related to international cyber assistance for Ukraine.

You have received this digest because your email address is included in the contact list of participants of the Tallinn Mechanism. If you have suggestions for improving the digest or wish to unsubscribe from future mailings, please contact Tetiana Riasna, TMPO's Communication Manager, at riasna@tmpo.com.ua

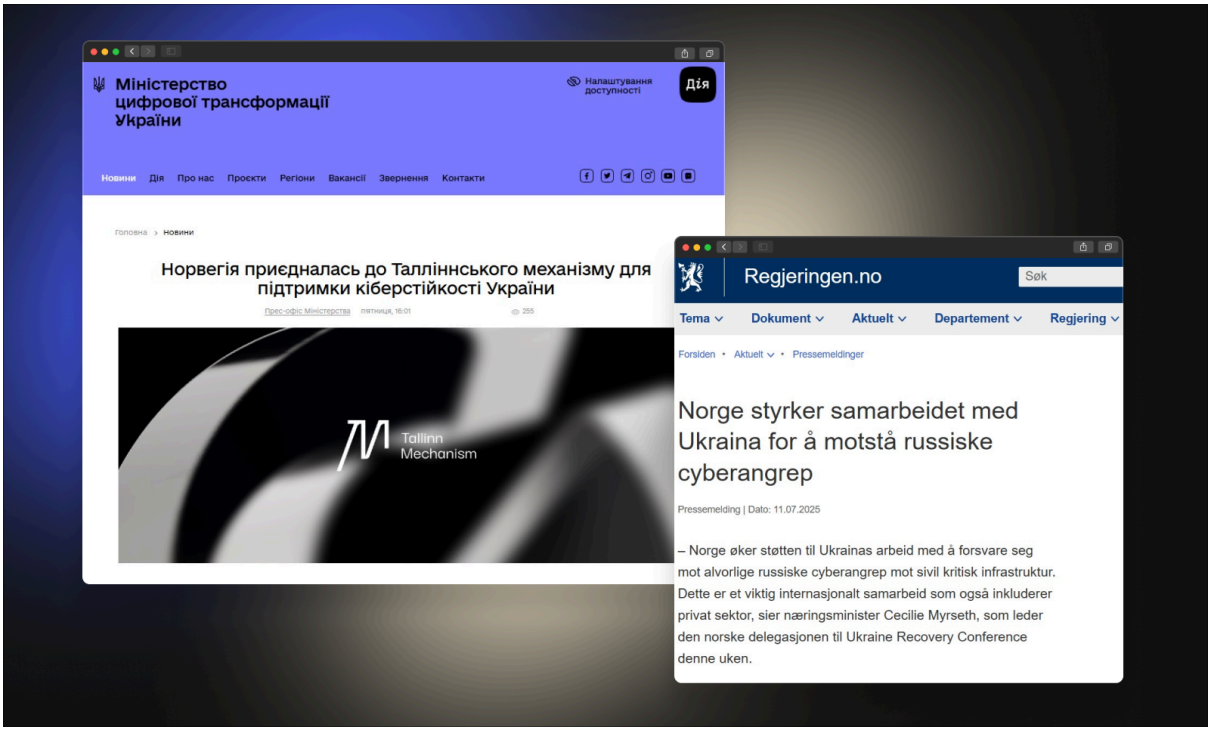
TALLINN MECHANISM UPDATES

Norway Joins the Tallinn Mechanism to Support Ukraine's Cyber Resilience

Norway has become the 12th country to join the Tallinn Mechanism. As part of this partnership, Norway plans to allocate over NOK 25 million (more than €2.1 million) in 2025 to support projects that aim to improve the cyber resilience of Ukraine's civilian and critical infrastructure.

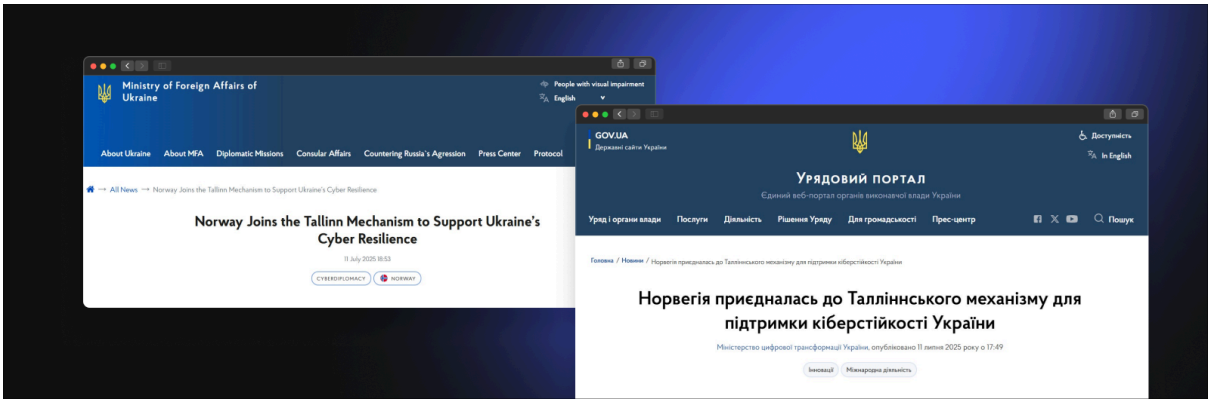
Norway was officially accepted as a member of the Tallinn Mechanism on July 2. Prior to that, the country participated in the initiative as an observer. The official announcement was made during the Ukraine Recovery Conference.

> *Ukraine demonstrates an impressive ability to defend itself against Russian cyberattacks targeting civilian critical infrastructure, government institutions, and businesses. The Tallinn Mechanism is the leading international tool for enabling Ukraine to defend against these attacks and build long-term digital resilience. The Norwegian government has now allocated NOK 25 million annually from the civilian component of the Nansen Program. This support is long-term and scalable.*
>
> ***Espen Barth Eide**, Minister of Foreign Affairs of Norway*



The announcement of Norway joining the Tallinn Mechanism was made public on July 11, drawing significant attention from Ukraine's leading business and tech media. The story was shared by Ukrainian and Norwegian authorities and covered by over 50 media, with total engagement exceeding 205,400 people.

Ukraine thanks the Norwegian partners for their continued support in enhancing the country's digital resilience and strengthening its cybersecurity.

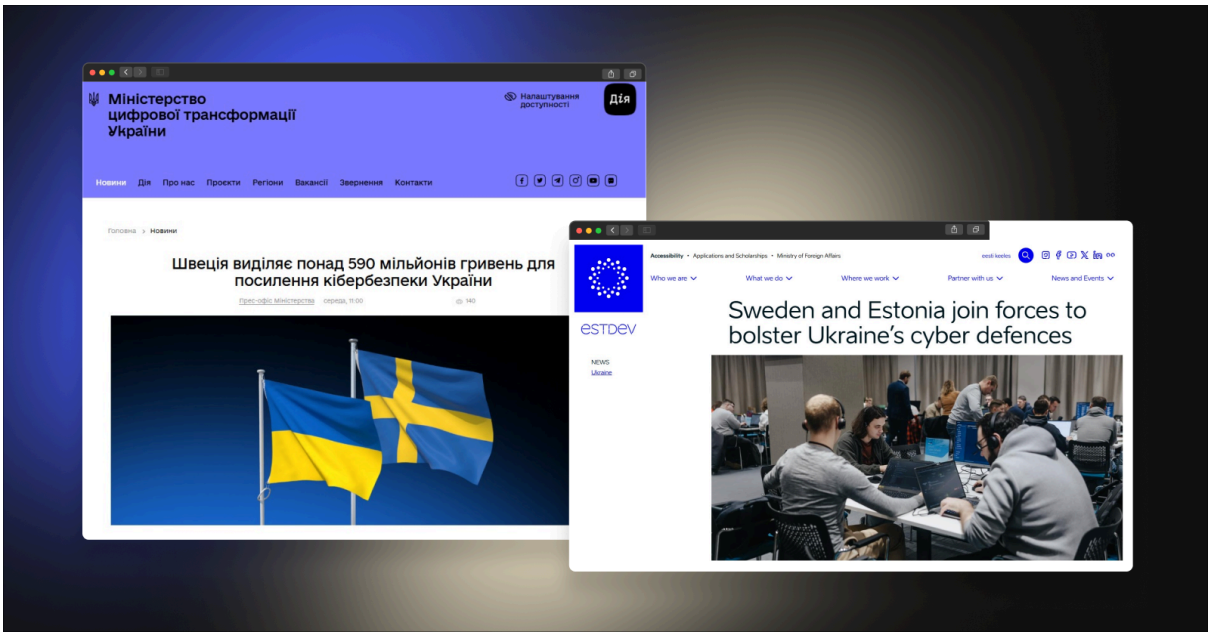


Sweden Allocates SEK 135 Million to Improve Ukraine's Civilian Cybersecurity under TM

The Swedish International Development Cooperation Agency (Sida) is providing a support package of SEK 135 million (approximately €12.2 million) to strengthen Ukraine's cyber resilience under the Tallinn Mechanism. Sida's contribution will be implemented via ESTDEV (Estonian Centre for International Development).

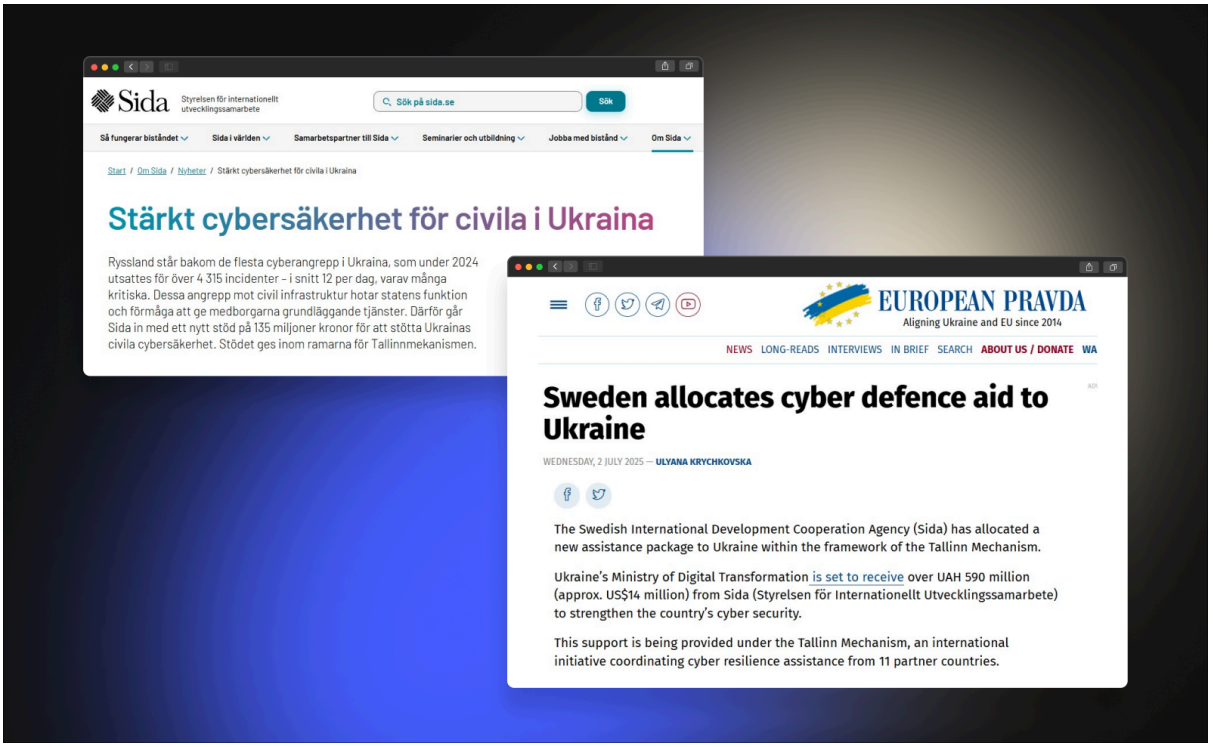
Sweden's support will focus on Ukrainian government authorities that Sida has previously collaborated with. Sida's funding will support a wide range of projects, in particular, IT infrastructure upgrades, improved email and application security, and staff training across key government institutions.

> *It is crucial that Ukraine can continue to provide citizens with basic public services, access to information, and digital services in areas such as education, healthcare, and social care. Sweden is now making a significant contribution to invest in cybersecurity. This will make Ukraine more resilient against future attacks.*
>
> ***Benjamin Dousa,** Minister for International Development Cooperation and Foreign Trade of Sweden*



The news on Sweden's support was publicly announced on July 2, and attracted significant attention from leading Ukrainian business and tech media, underscoring the importance of cybersecurity and global partnerships. The story was covered by Ukrainian and Sweden authorities, ESTDEV, and more than 90 media outlets, with total engagement exceeding 61,000 people.

Ukraine thanks the Sweden partners for their continued support in advancing the country's digital transformation and strengthening its cybersecurity.



Exploring New Modalities of Cooperation with the World Bank

On June 27, the TMPO team and the Ministry of Digital Transformation of Ukraine held a working meeting in Kyiv with representatives of the World Bank, led by Michel Kerf, Regional Director for Digital Transformation for Europe and Central Asia, and Latin America and the Caribbean.

The World Bank officially joined the Tallinn Mechanism as an observer on May 20, 2025. The meeting focused on exploring potential modalities for future collaboration.

TALLINN MECHANISM TRAINING INITIATIVES

🇫🇷 France

On June 16–18, June 23-25, and June 30 - July 2, Expertise France conducted cybersecurity training for cybersecurity professionals. The program consists of three consecutive training sessions. It covers the fundamentals of intrusion detection, configuration and use of SIEM systems, as well as the core principles of SOC analyst operations. Participants gained practical skills in monitoring, incident analysis, and cyber threat response.

This program is part of the French-led initiative “Cybersecurity Capacity Building for Ukraine” (CCBU), funded by the French Ministry for Europe and Foreign Affairs under the Tallinn Mechanism and implemented in collaboration with CDTO Campus.

🇩🇪 Germany

- **Monarch:** Basic Information Assurance Course (June 24–25)
- **Monarch:** Advanced Information Assurance Course (June 26–27)

The courses provided specialists responsible for implementing and maintaining information security policies with in-depth knowledge and practical skills. The curriculum covered risk management, compliance, policy development, organisational context, effective communication, and other critical aspects.

The educational program was organized under the Tallinn Mechanism by Monarch, a leading German company specializing in innovative cybersecurity solutions, funded by the Federal Republic of Germany, and implemented in collaboration with CDTO Campus.

TMPO ACTIVITIES

Strengthening Connection with the GovTech Community

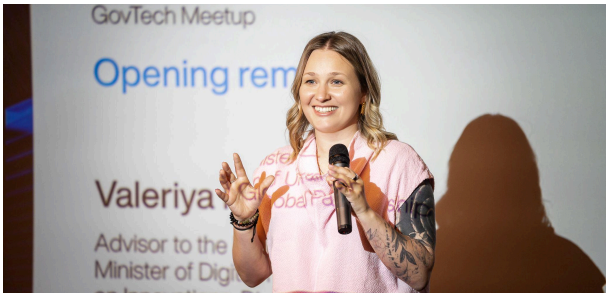
On June 11, the TMPO team joined the third GovTech Meetup, hosted by the Global Government Technology Centre (GGTC) Kyiv — the world's second GovTech centre. Established as a joint initiative of the World Economic Forum and Ukraine's Ministry of Digital Transformation, GGTC Kyiv has become a global platform for collaboration and knowledge exchange in the field of digital governance.

Participants explored how AI and digital reforms are transforming public institutions, with particular focus on insights and best practices from Estonia, Slovenia, and Ukraine.

Keynote speakers included:

- Luukas Ilves, Advisor to the Minister of Digital Transformation of Ukraine on AI and former Government CIO of Estonia
- Mark Boris Andrijanič, former Minister for Digital Transformation of the Republic of Slovenia and Senior Fellow at the Atlantic Council
- Valeriya Ionan, Advisor to the Deputy Prime Minister — Minister of Digital Transformation of Ukraine on Innovations, Digitalisation and Global Partnerships

> *All the remarkable progress Ukraine has achieved in digital transformation over the course of nearly six years — from launching Diia to building an integrated, nationwide digital public infrastructure — has been possible thanks to the synergy between government, international partners, and a private sector that operates digital by default.*
>
> ***Valeriya Ionan***

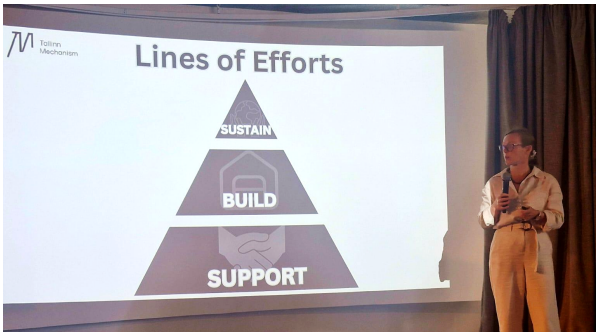


Fostering Digital Transformation in Ukraine and Beyond

On June 27, Olesya Danylchenko, Head of the Tallinn Mechanism Project Office, presented the Mechanism's priorities and initiatives at the Global Government Technology Centre (GGTC) event Informal Exchange on Digital Priorities.

Olesya described the Tallinn Mechanism as an example of digital diplomacy built on international solidarity, trust, and knowledge sharing. It is structured around three Pillars or Lines of Effort — Support, Build, and Sustain. Their aim is to address urgent cyber threats, strengthen institutional capacity, and ensure long-term resilience. While governments remain the core stakeholders (G2G), the Mechanism also encourages collaboration with private sector actors (G2B) and NGOs (G2NGO) to implement cybersecurity projects.

The keynote speaker was Michel Kerf, Regional Director for Digital Transformation for Europe and Central Asia and Latin America and the Caribbean at the World Bank, who visited Ukraine for the first time. Michel Kerf shared global insights on supporting digital futures.



EVENTS & STRATEGIC ENGAGEMENTS

Expending Partnership with Sida

On July 11, during the Ukraine Recovery Conference in Rome, Valeriya Ionan, Advisor to the Deputy Prime Minister on Digitalisation, Innovation, and Global Partnerships, met with Jakob Granit, Director General of Sida.

The discussion focused on advancing joint digital projects, launching innovative initiatives, and expanding cooperation following Sweden's accession to the Tallinn Mechanism. Sweden continues to actively support Ukraine's digital transformation and innovation efforts, and Ukraine looks forward to implementing new joint activities.

Strengthening EU–Ukraine Cyber Cooperation

On June 5, Anton Demokhin, Deputy Foreign Minister and Chief Digital Transformation Officer, held a meeting with Benedikta von Seherr-Thoss, Managing Director for Peace, Security, and Defence at the European External Action Service (EEAS). The meeting focused on current priorities of cooperation between Ukraine and the EU in the field of cybersecurity, strengthening cyber resilience, and joint efforts to counter threats in cyberspace.

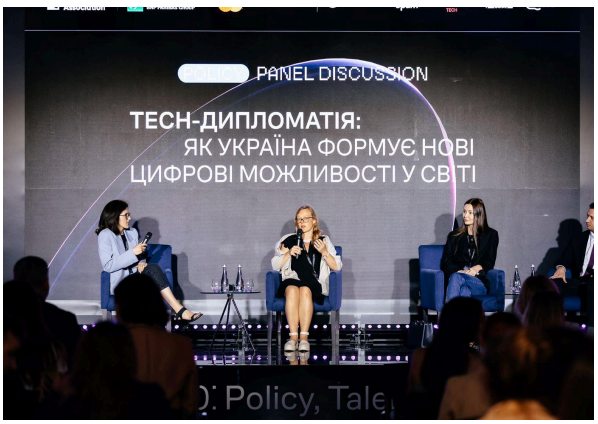
Benedikta von Seherr-Thoss commended Ukraine's progress in implementing reforms and the pace of transformation on its path toward EU membership. She also highlighted the effectiveness of cooperation within the framework of the Tallinn Mechanism, underlining its key role in coordinating international support for Ukraine in the digital domain.

Tech and Cyber Diplomacy in Action

On June 17, Olesya Danylchenko, Head of the Tallinn Mechanism Project Office, and Anton Demokhin, Deputy Foreign Minister and Chief Digital Transformation Officer, participated in the discussion “Tech Diplomacy: How Ukraine Is Shaping New Digital Opportunities Worldwide” at the Tech360 conference.

The event was organized by the IT Ukraine Association, and brought together representatives from the public and private sectors: over 50 thought leaders and experts as speakers, with more than 600 attendees joining both offline and online.

> *The Tallinn Mechanism is a coordination framework where technical assistance meets diplomacy. To foster successful cooperation with international partners, active interaction between the public and private sectors is also significant. Ukraine keeps sharing its unique experience in cybersecurity, and TM shows how this approach can really make a difference.*
>
> ***Olesya Danylchenko***

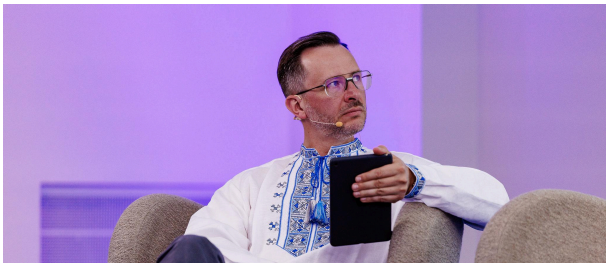


Tallinn Mechanism as a Case Study in Global Cyber Diplomacy

On June 16-20, the Tallinn Mechanism was presented as a case study during the Tallinn Cyber Diplomacy Summer School – an EU-funded programme supporting global capacity building and the development of inclusive, secure digital policies.

The Summer School is co-organised by the European Commission, the Estonian Ministry of Foreign Affairs, the e-Governance Academy, and ESTDEV. It gathered government officials and cyber policy professionals to explore practical tools for strengthening cyber resilience worldwide.

The panel discussion “Cyber Assistance to Ukraine – the Role of Public-Private Partnerships in Building National Cyber Resilience: Tallinn Mechanism and IT Coalition” showcased how coordinated support models can make a tangible impact. Speakers included Lauri Luht (Tallinn Mechanism Project Manager and Cyber Attaché at the Estonian Embassy in Kyiv), Ihor Malchenyuk (Director of Cyber Defense Department at the State Special Communications Service of Ukraine), Heli Tiirmaa-Klaar (Chair of IT Coalition Steering Group), Lilian Georgieva-Weiche (Strategic Advisor at German Federal Foreign Office), and Nikolas Ott (Project Manager for Cybersecurity Policy and Digital Diplomacy at Microsoft).



UKRAINE'S CYBERSECURITY INDUSTRY NEWS

Russian Cyber Threats Remain Consistently High

According to the latest update from Ukraine's National Cybersecurity Coordination Center, the threat landscape remains consistently high-risk due to the ongoing activity of russian hacker groups and special units. These actors continue targeting the information systems of Ukraine's government agencies, military leadership, and public officials to gather intelligence.

Phishing (via email and messaging apps like Signal and WhatsApp) remains the most common attack vector. Russian actors conserve sophisticated exploits for destructive operations, favoring phishing for routine intrusions. Malware such as HomeSteel, Remcos RAT, NetSupport RAT, MassLogger RAT, and DC RAT has been actively used in recent campaigns.

DDoS attacks by russian proxy hacktivist groups have also intensified, targeting government websites, media outlets, and critical infrastructure in Ukraine, NATO-affiliated entities, and countries such as the Netherlands and Israel.

Tracking Ukraine's Digital Transformation

Vox Ukraine and the Global Government Technology Centre (GGTC) in Kyiv released a new report titled "Reform Radar: Tracking Ukraine's Digital Transformation". It covers the years 2019–2024. The research offers an in-depth look at Ukraine's digital progress and outlines key strengths and challenges. The report aims to support policymakers, international partners, and digital reform advocates in advancing secure and sustainable transformation.

One section focuses on cybersecurity and provides a detailed overview of key regulatory documents shaping the sector, including:

- Cabinet of Ministers Resolution No. 518 (2019) on general cybersecurity requirements for critical infrastructure;
- Presidential Decree No. 447/2021 approving Ukraine's Cybersecurity Strategy for 2021–2025.

The documents in the section are essential for aligning Ukraine's cyber policy with EU, NATO, and NIST international standards.

The full report is available via **the link**.