

---

## MISSION STATEMENT

---

As a result of Russia's unprovoked war of aggression against Ukraine, the Tallinn Mechanism<sup>1</sup>, hereafter referred to as “*The Mechanism*”, aims to coordinate and facilitate civilian cyber capacity building to help Ukraine uphold its fundamental right to self-defence in cyber space, and address longer-term cyber resilience needs.

---

## SCOPE

---

1. The Mechanism acknowledges that the ongoing destruction of Ukraine’s critical infrastructure (CI) and the disruption of essential services caused by Russian cyber operations will require substantial multi-year assistance for Ukraine to maintain and strengthen its cybersecurity and cyber resilience capabilities.
2. Recognizing that disruptive Russian cyber operations and cyber activity are expected to continue well beyond any formal cessation of hostilities, the Mechanism is committed to supporting Ukraine’s cyber capacity building needs over the long-term.
3. The Mechanism is intended to serve as a focal point for Members’ civilian cyber capacity building support in order to help integrate/coordinate with other related areas of multinational support to Ukraine and overall increased situational awareness.
4. The Mechanism does not inhibit Members from engaging in other bilateral and multilateral cyber capacity building support to Ukraine in either a formal or an informal manner. Decision-making on general operational matters such as public statements and membership require consensus.
5. The Mechanism’s efforts to deliver cyber capacity building assistance to Ukraine should be coordinated and delivered across three mutually supportive Lines of Effort (LoE) to be effective: short (SUPPORT), medium (BUILD) and long-term (SUSTAIN).

---

<sup>1</sup> As endorsed by Canada, Denmark, Estonia, France, Germany, The Netherlands, Poland, Sweden, United Kingdom, United States on 30 May, 2023

6. Cyber capacity-building support is carried out with respect for international law and in full coordination with relevant Ukrainian counterparts. The principle “nothing about Ukraine without Ukraine” should be the guiding principle for the Mechanism.
7. The Mechanism is structured as a de-confliction and coordination group, voluntarily comprised of Members and Observers relying on a rotating lead nation mechanism consisting of a front and back-office<sup>2</sup>, and a coordination group.
8. Members of The Mechanism intend to improve coordination and delivery of civilian cyber capacity building across the three LoE, focused on assistance, recovery and resilience.<sup>3</sup>
9. The Mechanism’s LoE are intended to be separate, yet complementary, to military cyber capacity-building efforts and civilian efforts on digital development. The Mechanism aims to interface routinely with other donor initiatives around those efforts to coordinate and de-conflict. Members are encouraged to share information on assistance not affiliated with The Mechanism on a voluntary basis and in coordination with the front and back offices.
10. Private sector and non-governmental actors are encouraged to contribute to The Mechanism. Contributions provided via The Mechanism must align with its objectives and goals, including Points 4, 5 and 11 of this document, and complement Member-based efforts.
11. The coordination group intends to carry out regular lessons learned in order to develop recommendations to review and improve its functions.
12. The Members recognize the potential applicability of The Mechanism to future cyber assistance efforts.
13. Decisions will be taken by Members of the Mechanism, whereas Observers are limited to active participation in discussions. Membership applications will be considered on an Ad hoc basis; while being considered, candidates may be afforded interim Observer status.

---

<sup>2</sup> The front and back-office are expected to be responsible for developing, managing and reporting on the three LoE.

<sup>3</sup> This Mission Statement serves as a strategic document on the purpose of this mechanism. The exact delivery of cyber support measures, including information gained from activities undertaken within the mechanism, will be treated with the appropriate level of confidentiality. It will also be discussed between the members on a case-by-case basis.