EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure

Brussels, 29 June 2023

The EU and NATO share a common interest in preventing disruptions to critical infrastructure that provides essential services to citizens and supports our economies. Russia's war of aggression against Ukraine has brought new risks, physical and cyber-attacks, often combined as a hybrid threat.

The EU and NATO have stepped up their cooperation with the launch of the EU-NATO Task Force on resilience of critical infrastructure on 16 March 2023. The EU-NATO Task Force has now presented a **final assessment report**, which maps out the current security challenges and identifies four key sectors of cross-cutting importance: **energy, transport, digital infrastructure and space**. The report presents targeted recommendations to strengthen the resilience of critical infrastructure.

I. Key findings:

1. **Energy:** The sabotage of the Nord Stream pipelines illustrated the vulnerability of energy infrastructure. Energy security is more challenging in the current geopolitical environment. Moreover, military activities significantly rely on civilian energy networks and supplies. Energy infrastructure is also networked, so disruption in one location can have a broader impact. Decisive steps were taken by Member States and Allies to reduce our dependence on Russian energy. The growing use of renewable energy sources and electrification can also strengthen resilience because it increases the diversity of sources and autonomy and reduces reliance on a single central system. On the other hand, the new infrastructure and connections also bring new challenges in terms of infrastructure protection. The increased reliance on renewable energy also brings potential supply chain vulnerabilities since many of their critical components are still largely concentrated outside of NATO and the EU.

2. **Transport:** Transport infrastructure, including airports and seaports, is also vulnerable to cyber-attacks, which can inflict substantial economic damage and possibly cause disruptions for use by the military. Our militaries rely heavily on civil and commercial transport infrastructure to deploy their activities. Furthermore, the transport sector is affected by and has a significant impact the other sectors covered in this report, and these interdependencies are growing. The increasing electrification of transport will lead to a greater reliance on the electricity grid, batteries and associated infrastructure, in addition to existing dependencies on pipelines for hydrocarbon products that will remain part of the energy mix for the foreseeable future. Moreover, transport infrastructure is increasingly digitalised, making it more vulnerable to malicious cyber activities and disruptions.

3. **Digital infrastructure:** A wide range of infrastructure is required to provide information and communications services, from underground and undersea fibre-optic cables to cellular base stations and satellites. The reliance on undersea cables and 5G networks poses risks due to limited repair capabilities and increased vulnerability. Moreover, digital infrastructure relies on global supply chains. These are vulnerable to accidental and intentional disruptions, which could impact global networks and introduce security risks.

4. **Space:** Space infrastructure encompasses both space-based assets and ground-based systems, which can be vulnerable to various human-induced and natural risks. Space assets can be owned and operated by the EU (Galileo, Copernicus), Member States, Allies and, increasingly, commercial entities. Strategic competitors and potential adversaries are developing counter-space capabilities that could threaten NATO and the EU's access to and freedom of operation in space, potentially disrupting critical infrastructure.

II. Recommendations:

The EU and NATO experts have identified several key recommendations to enhance the resilience of critical infrastructure. These relate in particular to the need to ensure resilience and build on their cooperation by:

1. **Increased engagement, while making full use of synergies,** for instance in the case of a major hazard or a significant change in the security context; Promoting engagement among Allies, Member States and the private sector, including on security by design for critical infrastructure; Holding dedicated scenario-based discussions, including through the EU-NATO Foresight Seminar and with the support of the European Centre of Excellence for Countering Hybrid Threats.

2. **Strengthening the Structured Dialogue on Resilience** and the **Structured Dialogue on Military Mobility**, and expanding existing staff talks on cyber, space, maritime and energy, as well as between NATO's International Military Staff and the EU Military Staff.

3. **Promoting best practices, assessments, and enhancing monitoring for security implication and cooperation,** including between civilian and military actors; carrying out regular Parallel and Coordinated Assessments of the threats to critical infrastructure, building on the one conducted in spring 2023.

The EU-NATO Structured Dialogue on Resilience will coordinate the implementation of these recommendations.

Next steps

EU and NATO staff will take forward the recommendations of this report on the basis of long-standing cooperation and in full respect of the agreed guiding principles enshrined in the three Joint Declarations on EU-NATO cooperation. The EU-NATO Structured Dialogue on Resilience will ensure coherence of the follow-up work of the Task Force.

Background

On 11 January 2023, President **von der Leyen** and NATO Secretary General Stoltenberg jointly announced an EU-NATO Task Force on Resilience of Critical Infrastructure to reinforce our common security, which was launched on 16 March 2023. The Task Force is fully embedded in the EU-NATO Structured Dialogue on Resilience and is composed of staff from the European Commission, the European External Action Service and NATO International Staff. The Structured Dialogue on Resilience was launched by EU and NATO staffs in January 2022, in the framework of the implementation of 74 common actions and the well-established cooperation on resilience.

On 5 October 2022, President **von der Leyen** presented a 5-point plan to enhance the resilience of critical infrastructure. Based on this plan, on 18 October 2022, the Commission also proposed recommendations to accelerate work in three priority areas: preparedness, response and international cooperation.

Already in 2020, the Commission had proposed a significant upgrade to the EU's rules on the resilience of critical entities and the security of network and information systems. On 16 January, two key directives on critical and digital infrastructure entered into force with the purpose of strengthening the EU's resilience against online and offline threats, from cyberattacks to crime, risks to public health or natural disasters – the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) and the Directive on the resilience of critical entities (CER Directive).

For More Information

Final assessment report: EU-NATO Task Force on the resilience of critical infrastructure

Recommendation on Critical Infrastructure Resilience

Launch of the EU-NATO Task Force

Directive on the resilience of critical entities (CER Directive)

Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)

IP/23/3564

Quotes:

Our critical infrastructure faces increasingly complex security threats. We need to step up our efforts to ensure its resilience. This is crucial to protect essential services for citizens and support our economies. I'm glad that with Secretary General Stoltenberg we launched an EU-NATO Task Force and today I'm proud that we are presenting the outcome of its work. The Task Force has identified key security challenges in the areas of energy, transport, digital infrastructure and space, and proposes targeted recommendations. We will follow up and continue working together.
Ursula von der Leyen, President of the European Commission - 29/06/2023

Disruption of critical infrastructure can have massive consequences for our economies, our societies, the security of our citizens, potentially causing disruptions for the military. We must ensure that strengthening resilience of critical infrastructure is an integral part of both civilian and military work. So it is only natural that it is a key part of EU-NATO cooperation. The report prepared by our Task Force provides a solid basis to work together, combining our respective strengths and tools for the benefit of Europe's and our partners' security.
High Representative/Vice-President Josep Borrell - 29/06/2023

I thank President von der Leyen for her leadership, and the European Commission and the European External Action Service for their support as part of the NATO-EU Task Force on the resilience of critical infrastructure. This is an excellent example of our cooperation in action. The Task Force's Report sets out the importance of resilience in energy, transport, digital infrastructure, and space, and makes a number of key recommendations to deepen NATO-EU cooperation even more.
Jens Stoltenberg, Secretary General of NATO - 29/06/2023

Press contacts:

Eric MAMER (+32 2 299 40 73)
Christian WIGAND (+32 2 296 22 53)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email