EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE

FINAL ASSESSMENT REPORT

JUNE 2023

EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE
FINAL ASSESSMENT REPORT

Introduction

In light of the growing assertiveness of strategic competitors and the increasing complexity of security threats, ensuring the resilience of infrastructure that is critical to EU Member States and NATO Allies is an important element of the strategic partnership and cooperation between the two organisations. On this basis, on 11 January 2023 the President of the European Commission and the Secretary General of NATO announced the establishment of a dedicated NATO-EU Task Force on the resilience of critical infrastructure.

The EU-NATO Task Force is fully embedded in the existing NATO-EU Structured Dialogue on Resilience and further reinforces it. This report, produced by EU and NATO staffs, complements the 8th annual Progress Report on the implementation of the common set of proposals submitted jointly by the NATO Secretary General and the High Representative/Vice-President to the two Councils in June. It describes the importance of critical infrastructure, assesses the current security context characterised by a heightened level of risk and explores four key sectors (energy, transport, digital infrastructure and space), as well as cross-sectoral considerations. The report presents concrete recommendations on actions that could contribute to strengthening the resilience of critical infrastructure, in support of EU Member States and NATO Allies.

NATO and the EU will continue to work towards making critical infrastructure, technology and supply chains more resilient in the face of continuously evolving threats and risks, based on parallel and coordinated assessments, and to take action to mitigate potential vulnerabilities.

EU and NATO staffs 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 NATO-EU Structured Dialogue on Resilience will ensure coherence of the follow-up work of the Task Force, taking into account the political guidance of the respective Councils on the further development of this work.

THE IMPORTANCE OF CRITICAL INFRASTRUCTURE

Our economies and our democratic societies rely on critical infrastructure, which provides essential services to our citizens and underpins our economies. Military forces also rely to a great degree on public and private civilian infrastructure to be able to fulfil their tasks.

The resilience of Member States' and Allies' critical infrastructure is primarily a national responsibility. Resilience encompasses the ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services. This is particularly important for critical infrastructure because full protection is generally not possible. Infrastructure often crosses borders or provides services that do so. Therefore, cooperation at regional and international level, including through international organisations, is indispensable.

For NATO, the focus is on critical infrastructure that enables the fulfilment of the organisation's core tasks of deterrence and defence; crisis prevention and management; and cooperative security. Ensuring national and collective resilience is critical to all of NATO's core tasks and underpins NATO's efforts to safeguard Allies, their societies and shared values.

For the EU, critical infrastructure is not only closely related to policies and legislation ensuring the functioning of the internal market of the EU, but also to its security and defence agenda, including the strategic priority of the protection of the Union and its citizens and the EU's freedom of action. Critical infrastructure is needed for the provision of essential public services and economic activities in the internal market, as well as for security and defence.

Disruptions to critical infrastructure can have significant negative consequences for vital government functions, essential services to the population and economic activity in Allies and Member States. They can also hamper military activities, including exercises, deployment, reinforcement and sustainment. Moreover, complex interdependencies mean that a disruption to critical infrastructure can have cascading or mutually reinforcing effects. For example, a disruption to the electricity supply can affect public services and the supply of vital goods. Such consequences may also cross borders, due to the interlinkages of networks and the fact that in some cases the infrastructure itself spans more than one country.

Critical infrastructure is in many cases privately owned, managed or operated. Since it enables critical government services and essential services to the population and economic actors, while also in some cases serving a security and defence purpose, governments must ensure that it is resilient to disruption. This includes considering investment that may be necessary.

Member States and Allies are working to strengthen the resilience of their critical infrastructure. They are, for example, increasing awareness through monitoring and information sharing; preventing disruption through security measures and preparedness actions; minimising the effects of a potential disruption through swift and effective response, redundancy or back-up measures, including restore/repair capabilities; and ensuring timely recovery after a disruption through contingency planning and preparedness.

SECURITY CONTEXT

As a contribution to the work of the NATO-EU Task Force, the EU Hybrid Fusion Cell and the Hybrid Analysis Branch of NATO's Joint Intelligence and Security Division Intelligence Production Unit conducted a Parallel and Coordinated Assessment (PACA) of the threat landscape related to critical infrastructure, in line with the established practice of NATO-EU cooperation. It was released to EU Member States and NATO Allies in parallel.

Disruptions to critical infrastructure can come from many sources, both natural and human-induced. Moreover, due to an increasingly intertwined and connected economy and society, disruptions of critical infrastructure can have significant repercussions across sectors and borders.

Critical infrastructure is vulnerable to intentional attack or accidents. Many types of critical infrastructure are widely dispersed and some are easily accessible. Given the extent of private ownership and the need to ensure inter alia financial viability, strong security measures may not be feasible. Thus, critical infrastructure can be seen as a 'soft target' by an adversary, especially to hybrid tactics, which allow for such attacks to take place under a cloak of plausible deniability. Intentional attacks can also be timed to maximise the disruptive impact.

Russia's war of aggression against Ukraine has shown that critical infrastructure can be targeted in various ways: through espionage and intelligence gathering, physical attack, hostile reconnaissance, malicious hybrid and cyber activities, exploitation of dependencies or seizure. At the same time, Ukraine's example has both proven that it is possible to withstand even large-scale attacks and underscored how important resilient critical infrastructure and the continued provision of essential services are to a country's ability and determination to defend itself.

Russia has already demonstrated that it sees critical infrastructure as a target through its actions in Ukraine. It is also mapping critical infrastructure in the Euro-Atlantic area, which it could target. Russia and groups associated with it have used cyber attacks as a means to disrupt essential services in the Euro-Atlantic area.

Terrorist organisations also pose a threat to critical infrastructure. Various terrorist groups have targeted the transport infrastructure of Allies and of Member States several times.

Natural disasters or extreme weather can cause physical damage to infrastructure, thereby disrupting services. This challenge is increasing with climate change, which will expose infrastructure to rising sea levels, shifting weather patterns and more frequent extreme weather events.

In a context of growing strategic competition, it is important to identify and mitigate strategic vulnerabilities and dependencies that can be exploited. Foreign control of key technological and industrial sectors, critical infrastructure and strategic materials and supply chains, could allow foreign actors to gather sensitive information about NATO and EU activities, and potentially deny and disrupt access to critical infrastructure or impede the services it provides.

The seabed is a field of growing strategic importance, due to increasing reliance on undersea infrastructure and the particular challenges in protecting it from hybrid threats and physical damage.

SECTORAL ANALYSIS

Each essential services sector relies on specific critical infrastructure. Nevertheless, four sectors of cross-cutting importance have been identified as providing services that support and enable other sectors: energy, transport, digital infrastructure and space. These sectors face particular challenges that need to be addressed in order to bolster resilience.

ENERGY

Our economies and our societies depend on a reliable supply of energy from a mix of sources. Extensive energy trade links among Members States and Allies underline the importance of international cooperation on energy.

Energy security has become more challenging in the current geopolitical environment, as hostile actors and strategic competitors conduct malicious activities in cyberspace, manipulate energy supplies and employ economic coercion. Military activities depend to a significant degree on civilian energy networks and supplies, further underscoring the need to ensure security of critical energy infrastructure and supply chains.

The sabotage of the Nord Stream pipelines illustrates the vulnerability of energy infrastructure. The risk of shortages as a result of Russia's war of aggression against Ukraine has also heightened popular awareness of the potential damage to everyday life. Energy infrastructure spans long distances (e.g. pipelines, electricity cables), making it difficult to constantly monitor or protect; a one-off attack can be enough to do major damage, as in the case of a hydroelectric dam, as shown by the recent attack in Ukraine. Energy infrastructure is also networked, so disruption in one location can have an impact beyond that local area, and information about its location and routing is generally publicly available. As witnessed in previous incidents, significant investments in the digitalisation of energy infrastructure makes it potentially vulnerable to targeted cyber attacks as well as to general disruptions of digital infrastructure and services.

These challenges are compounded for undersea energy infrastructure, which is extensive and more difficult to survey and protect. Moreover, the network of undersea energy infrastructure in the Euro-Atlantic area is expected to grow as offshore energy platforms become more numerous.

Energy infrastructure is transforming as Allies and Member States take steps to both reduce their dependence on Russian energy and reduce emissions in response to climate change.

For example, the decisive steps taken by Member States and Allies to diversify away from Russian energy has led to an increased use of Liquefied Natural Gas (LNG), and an increased deployment of floating LNG terminals. These terminals comprise floating and land-based components, as well as connections between them.

Infrastructure is also transforming as the use of renewable energy sources and electrification grows. This can strengthen resilience because it increases the diversity of sources and autonomy, while the presence of numerous decentralised actors reduces the reliance on a single central system. On the other hand, the greater number of remote and dispersed sources of energy and energy storage, as well as the new connections they require, bring new challenges in terms of infrastructure protection.

The increased reliance on renewable energy also brings potential supply chain vulnerabilities because the production of solar panels, wind turbines, batteries and many of their critical components is still largely concentrated outside of NATO and the EU. The development of more offshore renewable energy infrastructure also makes it more challenging to monitor, but at the same time offers an opportunity to build resilience by design.

Moreover, the energy sector has specific characteristics that require tailored measures to ensure resilience, namely:

i. Real-time requirements: some energy systems need to react very fast, down to milliseconds in some cases, and do not allow for extra processing time.
ii. Cascading effects: a sudden failure in a power grid can induce a rapid domino effect of failures, which can quickly lead to the disruption of the supply of a large number of consumers across countries and sectors.
iii. Technology mix: legacy technology and infrastructure, with a lifetime of 30-60 years, will need to be maintained at the same time as new technologies and digitalisation are introduced.

TRANSPORT

Transport infrastructure is vital to our populations, our economies and our armed forces. Furthermore, it is extensive, comprising roads, railways, inland waterways, airports, seaports and inland ports. It can be state-owned, privately-owned or a result of public-private partnerships.

It is critical to maintain functional transport infrastructure, including the infrastructure identified in the trans-European transport network that represents the main arteries of transport throughout Europe and in neighbouring third countries. However, given the vast network of transport infrastructure across the territories of Member States and Allies, there is a great deal of redundancy and many alternate routing options are available, including intermodal transport solutions. Nevertheless, some key nodes are critical, including for military purposes, and not easily replaceable. This has become evident in recent years when natural hazards have led to disruptions that temporarily reduced accessibility to parts of the European transport network. These key nodes include major airports, seaports, main railway hubs and certain inland waterways, as well as the network of infrastructure that enables the transport of large quantities of outsized military cargo and dangerous goods, including ammunition. This infrastructure is also essential from a defence perspective. It will need to be further strengthened and upgraded to meet the demands of military activities, exercises and potential missions and operations, including in a contested environment.

Mass transit infrastructure has been the target of terrorist attacks in Allies and Member States. Security measures have been strengthened, but the need for transport infrastructure to remain accessible to the public limits the extent to which it can be protected.

Transport infrastructure, including airports and seaports, is also vulnerable to cyber attacks, which can inflict substantial economic damage and potentially disrupt or deny its use by the armed forces. Our militaries rely heavily on civil and commercial transport assets and infrastructure to deploy and to sustain their activities. Seaports, airports and robust inland intermodal connectivity are key prerequisites to rapidly deploy and sustain military forces into, across and from Europe. Although disruption to any node can have significant consequences for military operations, disruptions to the larger seaports would likely have greater implications because fewer options exist to mitigate the disrupted flow of bulk freight movement for both civilian and military purposes. Similarly, any significant disruption to a key airport could have an impact on the strategic and operational deployment of military forces, depending on the nature and location of the crisis. Access to infrastructure can change, so a secure exchange of information is needed between infrastructure owners/operators and users to keep up-to-date about issues such as planned maintenance or other activities that could reduce the availability of the infrastructure.

The transport sector is affected by and has a significant impact on each of the other sectors covered in this paper, 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 reliant on digital infrastructure and at the same time more vulnerable to malicious cyber activities and disruptions. Finally, transport infrastructure relies on space systems, in particular for positioning, navigation and timing. For example, even port equipment requires data provided by Global Navigation Satellite Systems to unload containers from ships.

DIGITAL INFRASTRUCTURE

Digital infrastructure provides the backbone for communications, which underpin all essential functions in society and the economy. Our citizens are increasingly reliant on digital infrastructure in their daily lives, and it is a key capability to enable governments to communicate with their citizens, especially in times of crisis.

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. Redundancy is to a large extent built into communications networks, although it remains important to plan for contingencies (for example, by identifying Primary, Alternate, Contingency and Emergency requirements). In addition, there are certain nodes that are critical for routing traffic or managing the network, including data centres and internet exchange points, and certain types of infrastructure that are not easily replaceable, including undersea cables.

Undersea communications cables are an essential part of the global communications network, carrying 95% of the world's internet traffic. Given their length and the difficulty in monitoring them, they may be seen as an attractive target for an adversary. The simultaneous disruption of multiple undersea communications cables would pose a significant risk to Member States and Allies, as repair capabilities are limited worldwide and, given the remote location of many of the cables, repairs take time.

5G networks increasingly provide the backbone for a wide range of services essential to public services and economic functions – such as energy, transport, banking and health, as well as industrial control systems. The dependence of many critical services on 5G networks, and on next generation networks in the future, would make the consequences of a systemic and widespread disruption particularly serious. 5G networks present a larger vulnerability surface that gives attackers more entry points, and therefore they require stronger security and resilience measures. Moreover, the major role of suppliers of network equipment and services makes it necessary to assess and address strategic risks, especially the risk of interference from specific third countries that have security laws and corporate governance that pose potential risks to the security of Allies and Member States.

Governments and armed forces rely to a large extent on digital infrastructure owned and operated by private sector companies. There is therefore a growing understanding of the importance of ensuring the security and resilience of this infrastructure, as well as gaining better knowledge of where data is stored and processed.

Some of the digital infrastructure used by governments and armed forces is also owned and operated by them. While fully a national competence, it is paramount to increase its resilience too, in particular military and law enforcement digital infrastructure. Existing legislation and policies applying to the public sector could be relevant for the military domain, and vice versa.

Moreover, digital infrastructure relies on supply chains that span the globe. This makes them vulnerable to accidental disruption, whether due to weather or human error, as well as to intentional disruption for political, military, financial or criminal gain. Critical components sourced from outside the EU or NATO may also not meet the same standards in terms of security or data protection, and could introduce vulnerabilities into Allies' or Members States' networks.

SPACE

Space infrastructure includes both space-based assets and ground-based systems, including data and other radio frequency links, all of which can be vulnerable to different kinds of human-induced and natural risks. Space assets can be owned and operated by the EU (Galileo, Copernicus, IRIS), Member States, Allies and, increasingly, commercial entities.

Strategic competitors and potential adversaries are investing in, developing, testing and operationalising sophisticated counter-space capabilities and doctrines that could threaten NATO's and the EU's access to and freedom to operate in the space domain, impair our defence and harm our security. By targeting civilian and military infrastructure, they could disrupt, degrade, deceive, deny or destroy space capabilities and services on which other critical infrastructure of Member States and Allies depends. In addition, space-based infrastructure faces unique risks from space debris, which can both cause collateral damage and reduce the accessibility and usability of orbits. Space weather can also affect both elements in orbit and terrestrial communications and electricity networks.

Many essential services – including energy, transport, finance and digital infrastructure – rely on space data, products and services, which provide connectivity, facilitate precision timing, enable accurate positioning, support monitoring and forecasting and enable earth observation. This is likely to increase given the dynamic evolution of the space sector and the increased accessibility of space, including through private sector actors. Disruptions in access to these data, products and services can have implications for the resilience of Allies and Member States, hampering the delivery of services, reducing efficiency and raising costs.

Resilience to disruptions can be strengthened through redundancy. In this context, the space data, products and services provided by Member States and Allies, as well as by the EU's space capabilities, are complementary.

CROSS-SECTORAL CHALLENGES

The sector-specific elements raised above point to the strong physical and digital interlinkages that exist between sectors, including others outside the scope of the current analysis (for example public health, water supply or agriculture, to name a few). Due to this high degree of interdependence among different types of infrastructure, the effects of disruption in one sector can cascade, affecting critical infrastructure in other sectors as well. These linkages need to be better understood in order to anticipate potential cascading effects, identify measures to mitigate them and facilitate an effective and complementary response through civilian and military means, including those available through the Union Civil Protection Mechanism (UCPM).

The fast-growing digitalisation of each of the four sectors assessed above makes them vulnerable to malicious cyber activities. Cyberspace is contested at all times. Malign actors have shown increasing willingness to conduct malicious cyber activity against critical infrastructure to achieve their strategic objectives, including by conducting extensive reconnaissance; carrying out attacks, including against supply chains; exploiting vulnerabilities in hardware and software; and taking advantage of poor cyber hygiene and security awareness in both public and private organisations.

Ownership or control by potential adversaries of critical infrastructure and supporting supply chains in Allies and Member States also poses a potential challenge. This could give access to data and information or it could be used to degrade, disrupt or deny access or withhold services. For example, ownership or control of transport infrastructure could be used to gain information about military equipment or operations or to hamper or delay deployments.

CONCLUSIONS AND RECOMMENDATIONS

The EU and NATO share a common interest in preventing disruptions to critical infrastructure that provides essential services to citizens and supports our economies. Through the work of the NATO-EU Task Force on the resilience of critical infrastructure, the staffs have confirmed that they have a shared view of the potential threats and risks. The two organisations will continue to cooperate in a complementary and mutually-reinforcing manner to build resilience and be prepared to manage disruptions from any source.

EU Member States and NATO Allies continue to enhance their preparedness to confront disruptions to critical infrastructure. Both NATO and the EU support their members with guidance, facilitate the exchange of best practices, conduct exercises, provide resources and offer complementary tools to build resilience. EU Member States and NATO Allies are encouraged to use them to the fullest.

The staffs of NATO and the EU have identified the following recommendations to build on their cooperation:

1. Ensuring swift engagement between high level EU and NATO officials in the case of an identified major hazard to critical infrastructure or a significant change in the security context;
2. Developing regular Parallel and Coordinated Assessments of the threats to critical infrastructure, building on the one conducted in spring 2023;

3. 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, with a view to:
   a) Deepening the understanding of the relevant tools and processes that are available to each organisation;
   b) Analysing observations from Russia's war of aggression against Ukraine regarding the resilience of critical infrastructure;
   c) Further analysing and undertaking a deeper assessment of the implications for the security of critical infrastructure of relevant supply chains, the energy transition and new technologies.
4. Making full use of synergies between respective processes deriving from EU and NATO critical infrastructure policies and programmes, including, through regular cross-briefings to the EU Critical Entities Resilience Group and Politico Military Group, and NATO's Resilience Committee;
5. Systematically taking into account the resilience of critical infrastructure in any future parallel and coordinated exercises;
6. Holding dedicated scenario-based discussions between staffs to better understand challenges, interdependencies and cascading effects, including through the EU-NATO Foresight Seminar and with the support of the European Centre of Excellence for Countering Hybrid Threats;
7. Enhancing awareness of the security implications of the participation in or control of critical infrastructure by entities from strategic competitors, as well as the potential risks related to suppliers from those countries, including in 5G networks;
8. Exploring possibilities for exchanges on how to improve the monitoring and protection of critical infrastructure in the maritime domain by relevant authorities, and discussing ways to enhance maritime situational awareness;
9. Promoting the exchange of best practices between civilian and military actors on the implementation of relevant cyber-related policies and legislation, including on relevant legislation aimed at enhancing the cyber resilience of critical infrastructure for a more resilient military;
10. Exchanging best practices on enhancing the resilience of critical infrastructure and identifying potential ways to strengthen it further, for example by assessing the need, relevance and feasibility of specific requirements for certain transport infrastructure for the purpose of accommodating the weight, size or scale of military transport;
11. Identifying alternative transport routes for both civilian and military purposes in case of a significant disruption to a particular route;
12. Promoting engagement among Allies, Member States and the private sector, including on security by design for critical infrastructure;
13. Promoting exchanges on the management of cross-sectoral consequences of major disruptions of critical infrastructure, in particular through increased cooperation between NATO and the EU's Emergency Response Coordination Centre (ERCC).
14. Identifying synergies and potential areas of cooperation in security research activities related to critical infrastructure, including challenges related to new technologies or supply chain security.

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