CSC 2.0

September 2026

Strengthening NATO Through Military Mobility and Critical Infrastructure Cybersecurity

By Jiwon Ma

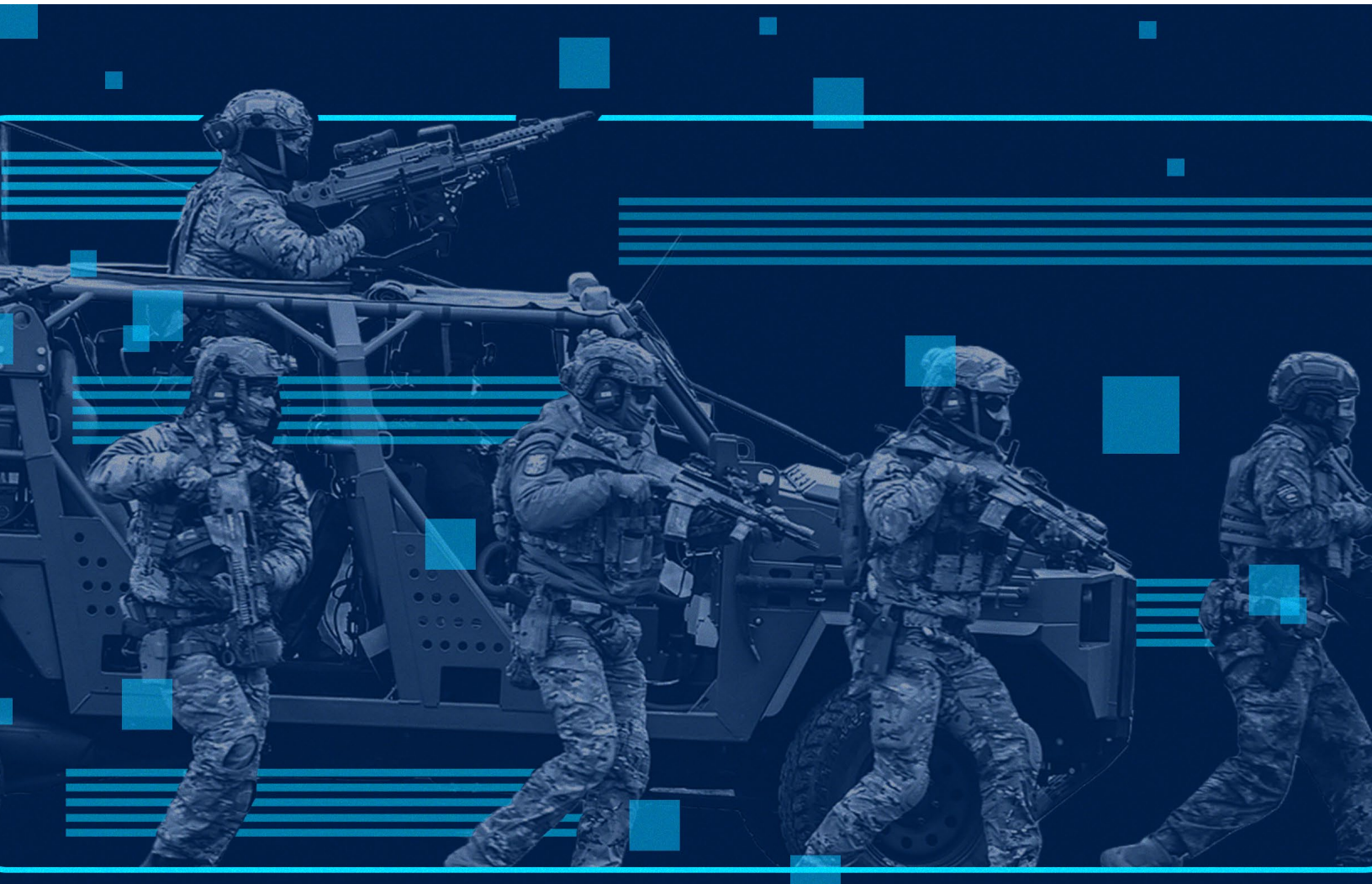
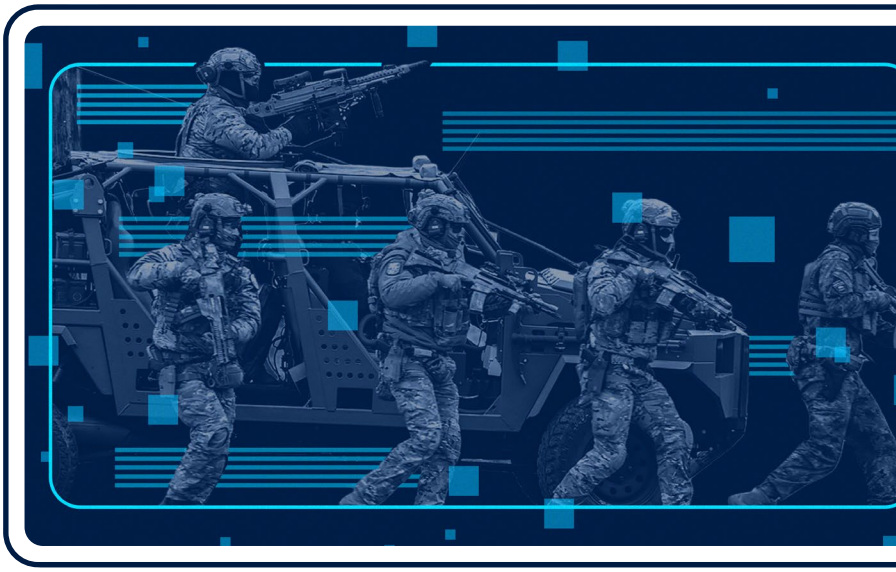


Table of Contents

Executive Summary



An FDD design by Liz Sunshine featuring armed forces during the NATO exercise Steadfast Dart (Hristo Rusev via Getty Image).

NATO's military capacity rests on its ability to swiftly concentrate combat power at decisive points, rapidly moving forces and materiel to the battlefield. That ability depends not only on roads, railways, ports, and airfields but also on the cybersecurity of the civilian systems that enable military movement. It could be the difference between preventing Russia from rapidly seizing NATO territory and having to fight hard to retake lost territory. Yet since the end of the Cold War, Europe's defense-related infrastructure investment has declined alongside its defense spending, leaving much of the continent's transportation network ill-suited for today's heavier forces.[1] Narrow roads, limited rail capacity, and incompatible rail gauges — the distance between rails of a railway track — continue to delay reinforcement and constrain operational readiness.[2]

Meanwhile, the alliance's ability to move forces — including U.S. forces based or arriving in Europe — increasingly depends on civilian digital networks that NATO neither owns nor directly regulates. Fragmented cybersecurity governance across NATO, the European Union, and national authorities leaves the civilian transportation operators on which alliance forces depend without consistent security standards or oversight. The result is a growing disconnect between NATO's operational requirements and the resilience of the infrastructure supporting them.

Adversaries have already demonstrated a willingness to digitally target logistics and transportation systems to disrupt movement without crossing the threshold of armed conflict. Foreign ownership further compounds these risks. Chinese state-linked firms hold stakes in more than 30 European port terminals, including facilities designated to receive U.S. military forces and equipment. The risk from these terminals falls directly on American forces, not only European ones. In a crisis, Beijing could exploit these dependencies to delay or restrict NATO access. Such investments also create potential digital avenues for intelligence collection and operational disruption.

Because allies retain sovereign responsibility for national infrastructure, this report finds that no single actor is responsible for keeping reinforcement corridors operational when under attack. NATO identifies the infrastructure and mobility capabilities its forces require and can coordinate national efforts but lacks the authority to impose binding standards on civilian operators. By contrast, the European Union can impose binding standards on civilian operators, but member states retain control over defense priorities and infrastructure investment. As a result, NATO forces cannot move as rapidly as they may need, and investment for upgrades lags behind NATO's reinforcement requirements. If NATO fails to align spending with reinforcement requirements, its ability to deter and defend will remain at risk. The alliance should thus pair its defense- and security-related spending commitment with a process that directs investment toward projects that enhance the physical and cyber resilience of assets integral to military mobility.

Defining Critical Infrastructure

While the United States, the European Union, and NATO recognize that critical infrastructure is essential to national security, economic stability, and public health and safety,[3] they identify and organize critical infrastructure and resilience priorities differently and impose different requirements and guidelines on operators.[4] This decentralized approach reflects, in part, NATO's reliance on national responsibility under Article 3 of its founding treaty, which calls on allies to maintain their capacity through "continuous and effective self-help and mutual aid."[5] The variability of these definitions and requirements results in inconsistent protection of civilian critical infrastructure across NATO mobility corridors.

The United States designates 16 infrastructure sectors as critical, including energy, transportation systems, information technology, and financial services. The European Union uses different sector classifications, covering 11 sectors under its critical entity framework for physical resilience and 18 sectors under its cybersecurity framework.[6] (See Table 1.)

NATO, by contrast, does not designate a comparable set of critical infrastructure sectors. Instead, the alliance assesses national resilience against NATO's seven baseline requirements — such as robust energy, transportation, and communications infrastructure — that are indispensable to its military operations.[7] In June 2023, though, a joint EU-NATO task force on critical infrastructure resilience did identify four sectors — energy, transportation, digital infrastructure, and space — as particularly important to both bodies for providing services that support and enable other sectors.[8]

In this context, the most consequential challenge for NATO is the uneven implementation of resilience requirements across its members. NATO sets alliance-wide resilience requirements and objectives, assesses allied preparedness, and works with the European Union on shared resilience priorities, but implementation and enforcement remain national responsibilities by individual member states. Because the civilian transportation systems that support military mobility depend on digital networks, the cybersecurity of civilian transportation infrastructure on NATO mobility corridors depends on the national standards of the member states through which those corridors run.

To be sure, for the 23 NATO member states that are also EU member states, EU law establishes binding requirements through the Critical Entities Resilience (CER) Directive and the Network and Information Security Directive 2 (NIS2). The CER directive obligates member states to ensure that designated critical entities implement physical resilience measures, while the NIS2 directive requires member states to impose cybersecurity risk management and reporting requirements on covered entities.[9] Member states were required to transpose — or incorporate into national law — both directives by October 17, 2024, and apply their national implementing measures beginning on October 18, 2024. CER required member states to identify critical entities by July 17, 2026, with the directive's entity-level resilience obligations applying 10 months after an entity is notified of its designation.[10]

In practice, however, EU member states have implemented NIS2 and CER unevenly.[11] On July 8, 2026, the European Commission, the European Union's main executive body, referred Ireland, Spain, France, and the Netherlands to the Court of Justice of the European Union for failing to transpose NIS2 by the October 17, 2024, deadline.[12] Three months earlier, the commission referred Bulgaria, France, Luxembourg, the Netherlands, Poland, Spain, and Sweden for failing to transpose the CER by the same deadline.[13]

Still, another law may achieve better results. The European Union's 2024 Cyber Resilience Act establishes mandatory cybersecurity requirements as well as vulnerability and incident reporting requirements for products with digital elements, satellite terminals, smart cameras, and control software for ports and airfields.[14] The legislation entered into force on December 10, 2024, but provides a three-year transition period for covered entities to adapt to the cybersecurity requirements, which will not begin to apply until December 11, 2027.[15] However, the law's vulnerability and incident reporting obligations took effect earlier, on September 11, 2026.[16] Manufacturers must now report "actively exploited vulnerabilities and severe incidents" through the Single Reporting Platform launched by the European Union Agency for Cybersecurity (ENISA), the EU agency responsible for supporting cybersecurity policy and implementation.[17]

Critical Infrastructure and Resilience Frameworks: United States, European Union, and NATO				
	United States	**European Union**	**NATO**	**EU-NATO Task Force**
Classification	**Critical Infrastructure Sectors (16)**	**Critical Infrastructure Sectors** **CER: 11 sectors, NIS2: 18 sectors total (covering 11 CER sectors plus seven more)**	**Seven Baselines for Level of Preparedness**	**Priority Areas**
Areas Covered	▸ Energy ▸ Transportation Systems ▸ Communications ▸ Information Technology ▸ Financial Services ▸ Healthcare and Public Health ▸ Water and Wastewater ▸ Government Services and Facilities ▸ Commercial Facilities ▸ Critical Manufacturing ▸ Dams ▸ Defense Industrial Base ▸ Emergency Services ▸ Food and Agriculture ▸ Nuclear Reactors, Materials, and Waste ▸ Chemical	**CER:** ▸ Energy ▸ Transport ▸ Digital Infrastructure ▸ Banking ▸ Financial Markets ▸ Health ▸ Drinking Water ▸ Wastewater ▸ Public Administration ▸ Space ▸ Production, Processing, and Distribution of Food **NIS2:** ▸ ICT Service Management ▸ Postal and Courier Services ▸ Waste Management ▸ Manufacture, Production, and Distribution of Chemicals ▸ Manufacturing ▸ Digital Providers ▸ Research	▸ Assured Continuity of Government and Critical Government Services ▸ Resilient Energy Supplies ▸ Ability to Deal Effectively With the Uncontrolled Movement of People ▸ Resilient Food and Water Resources ▸ Ability to Deal With Mass Casualties and Disruptive Health Crises ▸ Resilient Civil Communications Systems ▸ Resilient Transportation Systems	▸ Energy ▸ Transport ▸ Digital Infrastructure ▸ Space
Requirements	Varies by sector; includes some federal requirements, some state- and local-level regulation.	Binding regulatory frameworks enforced by national authorities designated by each member state.	Nonbinding; member states self-assess national preparedness against NATO's Seven Baseline Requirements through the NATO Defence Planning Capability Survey.[18]	No separate binding requirements.

Table 1: A comparison of how the United States, European Union, NATO, and the European Union-NATO Task Force organize critical infrastructure and resilience priorities and establish related requirements. Unlike the United States and the European Union, NATO does not designate critical infrastructure sectors but instead assesses national preparedness against seven baseline requirements.

Nevertheless, even legal transposition is not a reliable proxy for operational resilience. ENISA reinforced the distinction in its May 2026 NIS360 assessment, an annual evaluation of cybersecurity maturity across NIS2-regulated sectors. ENISA found that the transportation sector continues to remain below the appropriate level of cybersecurity maturity despite falling within NIS2's regulatory scope.[19]

Thus, NATO faces a fundamental coordination challenge. Assets that are operationally essential for NATO military mobility receive different levels of physical protection and cybersecurity attention depending on where they are.

The Military Mobility Challenge in Europe

At the June 2025 NATO summit in The Hague, leaders committed to spending 5 percent of gross domestic product (GDP) on defense by 2035, including up to 1.5 percent of GDP on defense-related investments, such as critical infrastructure, industrial base protection, and cybersecurity-related investments.[20] However, while NATO requirements inform European Union infrastructure planning, such expenditures do not ensure that national spending will be directed toward those priority corridors or address urgent bottlenecks.

That is because NATO's ability to reinforce allies and sustain operations relies on a complex network of civilian transportation infrastructure, digital systems, regulatory processes, and commercial operators that enable personnel, equipment, and supplies to move to and across Europe at speed. The military mobility challenge in Europe can thus be understood across four interconnected dimensions: physical infrastructure constraints, regulatory and investment shortfalls, technology modernization and cybersecurity gaps, and Chinese influence over Europe's critical infrastructure.

Physical Infrastructure Constraints

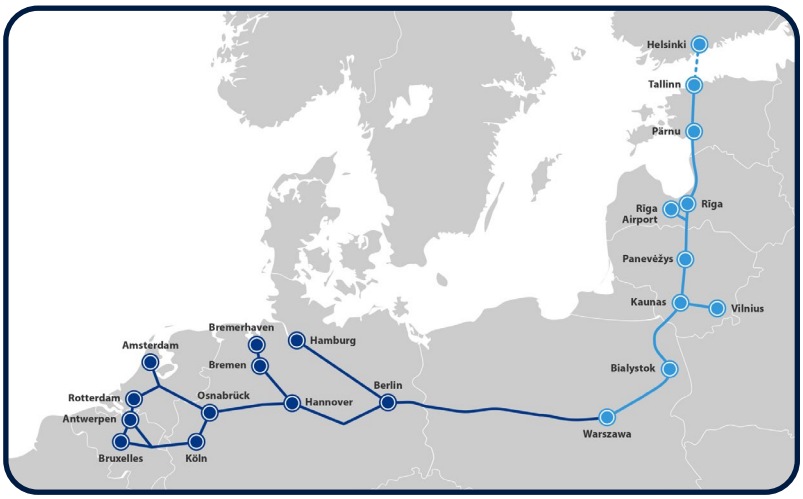
The European transportation infrastructure NATO depends on for military mobility has not been significantly updated since the Cold War. Much of it, particularly in Central and Eastern Europe, is poorly aligned with the alliance's current force posture and reinforcement routes for deployments. Constraints at ports, airfields, and railheads can compound delays across every mode of operational movement. Physical disruption to the energy and communications infrastructure that supports reinforcement creates an additional vulnerability. Roughly 500 mobility "hotspots," identified through NATO-EU staff mapping as priority infrastructure for investment — including bridges, tunnels, ports, airfields, and rail chokepoints — already hinder NATO exercises in peacetime and could paralyze reinforcement flows during conflict.[21]

NATO exercises have repeatedly identified shortcomings across Europe's transportation network. Armored units have been forced to reroute because bridges could not bear their load, while military convoys have experienced delays due to customs paperwork requirements and slow permitting systems for border crossings.[22] For example, in 2024, the French Institute of International Relations, a Paris-based foreign policy think tank, estimated it would take an average of 60 days to transport an equipment convoy from a French military site to the Cincu training garrison in Romania along a NATO reinforcement path — roughly 2,000 kilometers across six countries.[23] That timeline rivals a roundtrip transatlantic freight shipping voyage.

However, preparations for Dacian Fall 2025, a large-scale NATO exercise held in October 2025, showed that the journey can be made faster. Ahead of the exercise, which Romania led, France deployed a NATO-standard brigade from metropolitan France to Romania in 30 days. That faster pace required extensive advance planning and multimodal transportation, including shipping equipment from Toulon, France, to the Greek port of Alexandroupolis and trucking it into Romania.[24]

NATO also lacks an alliance-wide strategic rail system or shared fleet of railcars needed to move heavy equipment. Rail capabilities remain nationally owned and inconsistently maintained, with only a small number of members retaining dedicated wagons for military use.[25] For instance, one of the most acute chokepoints is the rail gauge break at Kaunas, Lithuania, which exemplifies a broader mismatch between Western European and Soviet-era rail infrastructure. The Baltic states operate on the 1,520 mm Soviet-era rail gauge, while Western Europe uses 1,435 mm. As a result, freight transported north of Kaunas must be reloaded onto wide-gauge trains, forcing NATO rail movements from Poland to halt at the Lithuanian border.[26] This transloading process can add up to 24 hours to a movement that would otherwise continue without changing trains.[27]

In the maritime domain, European deep-water ports can receive transatlantic reinforcements, but onward movement through inland ports and waterways presents challenges. Inland ports may lack suitable roll-on/roll-off ramps, adequate staging areas, sufficient water depth, or docking capacity needed to assemble and move brigade-sized formations at speed.[28] Most of Europe's ports are also commercial and often privately owned, meaning military movements must compete with civilian shipping traffic for berths, pilots, and tug support.[29] In peacetime and crises short of war, there is no automatic or enforceable military priority access to civilian port facilities.



Launched in 2019, Rail Baltica is integrating the Baltic states into the continental rail network by connecting Warsaw to Tallinn via an 870-km standard-gauge corridor, potentially reducing military transport times from one week to just 24 hours. Completion has slipped from 2026 to 2030, and estimated costs have quadrupled. Source: RB Rail AS.[a]

Air mobility infrastructure has faced similar limitations since the Cold War. To this day, European airfields designated for receiving military personnel and equipment frequently lack the ramp space, fuel storage, and ground handling capacity necessary to receive heavy-lift military cargo aircraft at surge rates. According to GLOBSEC, a pan-European security policy think tank, NATO has designated 14 civilian airports for military use in addition to 37 military airbases, yet only 31 airfields meet NATO runway length standards.[30] Not every airfield needs to meet this standard to support military airlift, but the shortfall reduces the number of locations able to accommodate the full range of strategic airlift operations, thereby reducing NATO's flexibility during large-scale or surge deployments.

Recent incidents in the Baltic Sea have intensified concerns about the vulnerability of critical undersea infrastructure as well. In October 2023, the Chinese-owned container ship *Newnew Polar Bear* damaged the Balticconnector gas pipeline and telecommunications cables linking Finland and Estonia after dragging its anchor across the seabed.[31] In November 2024, Swedish police opened an investigation into the Chinese bulk carrier *Yi Peng 3*, which had departed a Russian port after the vessel emerged as the primary suspect in the severing of the two major Baltic undersea telecommunications cables connecting Finland, Germany, Sweden, and Lithuania — cutting close to a fifth of Lithuania's internet capacity.[32] These incidents underscored how vulnerable critical energy and communications infrastructure remains to disruption in a region central to NATO reinforcement and deterrence operations.

Regulatory and Investment Shortfalls

NATO has treated military mobility as a core enablement challenge for years, but the European Union only began building a dedicated military mobility agenda in the last decade. Since then, Europe has made significant progress in planning military mobility, but investment has not kept pace with operational requirements.

In November 2017, the European Union launched its Military Mobility policy, which focused on upgrading the trans-European transport network (TEN-T) — major roads, railways, ports, airports, and inland waterways in the regional bloc — to serve both civilian and military purposes. In 2018, EU members launched the Permanent Structured Cooperation Military Mobility project to reduce cross-border military movement through digital permitting, standardized clearance templates, and information sharing among national authorities.[33]

Member states also voluntarily committed to process cross-border movement requests within five business days, a target later tightened to three business days, though neither pledge was legally binding.[34] However, by 2024, only half of EU member states were fully compliant with the original five-day target.[35] Some still require up to 45 days' advance notice, largely due to delays in granting movement permissions.[36] Thus, administrative delays can prevent forces from arriving within NATO's readiness timelines even when the infrastructure itself is available.

In 2021, the European Union's 2021-2027 budget allocated €1.69 billion (about $2 billion) under the Connecting Europe Facility (CEF) — the bloc's primary funding instrument for strategic transport, energy, and digital infrastructure — for dual-use transportation infrastructure. This funding marked the first-ever EU infrastructure funding explicitly reserved for this purpose.[37] However, the European Court of Auditors found that following Russia's February 2022 invasion of Ukraine, the European Commission frontloaded the available funding into the 2022 and 2023 funding rounds to accelerate dual-use upgrades, nearly doubling the 2022 round's original budget from €330 million (about $385 million) to €611.9 million (about $714 million) and putting the remaining funding into the 2023 round.[38] Thus, the €1.69 billion, intended to last through 2027, had already been fully allocated by 2023.

Consequently, demand for funding substantially exceeded supply. The 2023 round received 112 project proposals from 22 member states requesting about €3.7 billion (about $4.2 billion) in EU co-funding for dual-use transportation infrastructure projects against a €790 million (about $915 million) budget — 4.7 times more than was available.[39] The auditors warned that the European Commission therefore selected projects "piecemeal," improving isolated parts of corridors rather than the most strategically important chokepoints.[40]

This led the European Parliament, in 2024, to adopt a revised TEN-T regulation requiring member states to account for military mobility when building or upgrading infrastructure on the network.[41] The regulation also directed the European Commission to identify priority military mobility corridors.[42]

Building on that legal foundation, the Council of the European Union, which brings together ministers from EU member states to negotiate legislation and coordinate policies, identified four multimodal priority military mobility corridors in March 2025, spanning rail, road, sea, and air. These corridors give the European Union a common map for prioritizing investments that support short-notice, large-scale military movement.[43] However, the European Commission had already allocated most of the 2021-2027 military mobility funding before the Council of the European Union adopted the corridors, meaning the corridors were identified too late to guide those earlier investment decisions.

In this context, Europe has also begun pairing regulatory reforms with efforts to strengthen cybersecurity and physical resilience of infrastructure supporting military mobility. On November 19, 2025, the European Commission proposed the Military Mobility Package, which includes a proposed regulation that would create the first EU-wide harmonized rules for cross-border military movement. The regulation would cap clearance deadlines at three days and institute an emergency framework giving armed forces priority access to transportation infrastructure during a crisis.[44] Separately, the 2025 package would strengthen the cyber and physical resilience of strategic dual-use infrastructure along the priority corridors.[45]

However, the package is only a proposal: It must still be negotiated and adopted by both the European Parliament and the Council of the European Union before member states are required to implement its provisions. The Council of the European Union agreed on its negotiating position on the proposed regulation in June 2026, and the European Parliament cleared negotiations to begin on July 16, 2026. Legislators are aiming to reach an agreement by the end of 2026, with the goal of making the new emergency mobility system operational by 2028.[46]

For the 2028-2034 budget cycle, the European Commission has proposed increasing military mobility funding tenfold, from €1.69 billion (about $2 billion) to €17 billion (about $20 billion) under the CEF.[47] Much of this funding would go toward upgrading bridges, tunnels, railways, ports, airports, and other transportation infrastructure that cannot currently support the rapid movement of heavy military equipment.[48] Yet the European Commission's own estimate of the need has climbed from €70 billion (about $80 billion) in early 2025 to nearly €100 billion ($114 billion) in 2026, spread across more than 500 hotspot projects, according to its updated readiness roadmap.[49] A tenfold increase would cover less than a fifth of the commission's estimated €100 billion ($114 billion) investment need.

Moreover, past experience suggests that even the €17 billion is politically uncertain. In 2018, the European Commission asked for €6.5 billion (about $7.5 billion) for military mobility under the 2021-2027 CEF for dual-use transportation requirements. During budget negotiations, the European Council, which sets the European Union's priorities and general political direction, ultimately cut the allocation to €1.69 billion, a 74 percent reduction.[50]

No dedicated CEF military mobility funding is expected before 2028, roughly the same window in which European intelligence services warn that Russia could be ready to strike a NATO member.[51] Member states can partially fill the gap through reallocated cohesion funds[52] — the 27-member bloc's main regional development funding — or Security Action for Europe (SAFE) loans, a temporary EU instrument offering member states €150 billion (about $175 billion) in loans to finance defense investments.[53]

Likewise, NATO's June 2025 Hague summit commitment to spend up to 1.5 percent of GDP on defense-related infrastructure and resilience allows members to count investments in critical infrastructure, network protection, and resilience toward NATO's spending target. Even if the total proposed €17 billion CEF package were used for the European Commission's estimated €100 billion military mobility needs, roughly €83 billion would still need to be financed through national budgets or other EU programs. But eligible national investments could count toward NATO's 1.5 percent target. This creates a stronger incentive to fund the infrastructure and cyber upgrades that enable forces to move at scale. The new spending commitment could also shift more of the financial burden from limited EU programs to national budgets and accelerate upgrades before dedicated EU funding resumes in 2028.

Technology Modernization and Cybersecurity Gaps

NATO has repeatedly warned that the lack of interoperability of digital systems hinders the alliance's ability to mobilize and move forces quickly. These systems are also vulnerable to digital sabotage, a problem that criminal and state-backed hackers regularly exploit.

Over the years, NATO has acknowledged the need to improve how it shares real-time data rapidly and securely across the alliance.[54] In February 2025, NATO approved a Data Strategy for the Alliance, which aims to accelerate NATO's transition to data-centric operations and improve interoperability across domains. The strategy builds on initiatives such as the Alliance Data Sharing Ecosystem, a way for NATO and its trusted partners and allies to securely share and use interoperable data. NATO's strategy sets 2030 as the target completion date for the integration of this data-sharing ecosystem.[55] That leaves NATO dependent through 2030 on digital logistics that are not yet fully interoperable or secure.

NATO and allied transportation networks also depend on a small number of third-party technology providers to facilitate data sharing. A single provider being compromised can create cascading disruptions across geographically dispersed networks. For example, hours before Russia's February 2022 invasion of Ukraine, Russia-linked hackers attacked Viasat's KA-SAT satellite networks — a commercial satellite internet system serving Ukraine and parts of Europe — disrupting both civilian and military communications across the continent.[56] British intelligence assessed that the Ukrainian military was likely the primary target.[57]

Meanwhile, European operators — like their counterparts in many digitized nations — struggle to secure legacy operational technology, including industrial control systems, which automate the controlling and monitoring of physical processes in critical infrastructure. As a result, vendors bolt cybersecurity protections onto aging technology, which is often difficult to patch when researchers or attackers uncover software flaws. ENISA warned in 2023 that fewer than one-third of transportation critical infrastructure operators could remediate critical vulnerabilities within one week, with the rest taking at least a month, if not longer. That gives threat actors plenty of time to exploit a known vulnerability before operators can fix the problem.[58] And as artificial intelligence shrinks the time between discovery and exploitation of software flaws, one month is too long.

In its May 2026 NIS360 report, ENISA found that the transportation sector is still not closing this gap fast enough. Despite what ENISA described as rail's "growing role in military logistics,"[59] rail and maritime cyber resilience improved little over the past year. More than half of rail and maritime operators reported gaps in cybersecurity expertise, attributing them to workforce shortages and budget constraints. Furthermore, ENISA found that limited skills contributed to persistent weaknesses in access management across rail, maritime, and aviation systems.[60] Although ENISA rated the aviation sector's cybersecurity maturity higher, that finding was driven largely by major carriers. Small and medium-sized aviation entities face the same capacity constraints affecting the rest of the transportation sector.[61] The workforce shortage affects both the implementation of basic cybersecurity controls and the capacity of national authorities to ensure that operators meet security requirements.

Criminal and politically motivated attackers already target these systems for financial gain or to threaten disruption in response to government decisions. In July 2024, the Akira ransomware gang, a financially motivated cybercriminal group, disrupted the IT systems at Croatia's Split Airport, causing four flight cancellations and delays of 77 others.[62] In 2022, pro-Russian hacking group Killnet claimed distributed denial-of-service attacks against Lithuanian transportation systems and public institutions after Vilnius restricted sanctioned goods moving to Kaliningrad, the Russian exclave nestled between Poland and Lithuania.[63] In a crisis, these disruptions would create friction in mobilization timelines.

The bigger concern, however, is nation-state-backed hackers compromising these systems to conduct cyber espionage or disrupt NATO's ability to move forces while degrading local governments' ability to provide essential services. The 2024 Annual Threat Assessment of the U.S. Intelligence Community published by the Office of the Director of National Intelligence noted that China is gaining and maintaining access to U.S. critical infrastructure networks in advance of a crisis or conflict, pre-

positioning its hackers to disrupt essential services during a crisis or conflict.[64] In April 2024, then-FBI Director Christopher Wray noted during an interview that targeted critical infrastructure includes "telecommunications, energy, water, and other infrastructure sectors."[65]

Moscow, meanwhile, has demonstrated what that disruption looks like in practice. Within months following Russia's February 2022 invasion of Ukraine, the Kremlin-backed hacking group Sandworm launched ransomware attacks against transportation and logistics entities in Ukraine and Poland, encrypting files and deleting backups across all victims within an hour of each other. Microsoft's Threat Intelligence Center assessed in October 2022 that this ransomware attack increased risk for organizations transporting military and humanitarian supplies into Ukraine.[66]

Russia has also demonstrated how cyber operations can target energy systems that support civilian resilience and military mobilization. Transportation infrastructure and communications systems all depend on reliable energy to operate. Any prolonged outages could delay operational movement. In December 2025, Russian state-linked hackers deployed wiper malware against Polish renewable energy plants' operational technology and industrial control systems.[67] Polish officials said a successful attack could have left roughly half a million people without heating during near-freezing temperatures.[68]

Likewise, commercially deployed digital systems along NATO mobility routes can expose military infrastructure to adversary surveillance. In May 2025, for instance, allied cybersecurity agencies blamed Russia for a multiyear espionage campaign targeting the transportation sector across NATO member states. The campaign compromised thousands of internet-connected cameras near border crossings, rail stations, and military installations to monitor the movement of materiel. Russia has even conducted reconnaissance against railroads.[69] In November 2025, for example, Polish Prime Minister Donald Tusk blamed Moscow for a series of arson and sabotage attacks on Polish railroads.[70] Digital access can help adversaries identify movement patterns, select targets, and time acts of sabotage against the transportation nodes NATO would need most in a crisis.

Similarly, since 2022, persistent GPS jamming and spoofing has affected civilian GPS systems that NATO would rely on to move through Baltic and Nordic sea lanes and airspace. In its May 2026 assessment, ENISA identified aviation and maritime GPS jamming and spoofing as cyber-physical risks.[71] In June 2025, Finnish and Estonian authorities reported that vessels narrowly avoided accidents following global navigation satellite services disruptions in the Gulf of Finland that could "cause unexpected malfunctions" in vessel autopilot systems.[72] In July 2025, Sweden's Maritime Administration separately warned that spoofing can display a vessel in the wrong location or create an illusion "of being on a collision course" through incorrect data.[73] The Maritime Administration advised ships in the Baltic Sea to rely on radar and visual navigation after multiple signal interference reports, and Finnair temporarily suspended flights to Estonia over GPS disruptions affecting landings in 2024. Similar incidents near Russian territory have heightened concerns that persistent satellite jamming could disrupt reinforcement operations along NATO's northeastern flank.[74]

To address such challenges, the European Union has focused primarily on improving cybersecurity coordination and crisis response among member states. In 2022, the bloc activated the Cyber Rapid Response Teams (CRRT), which had reached full operational capability in 2021, to support Ukraine following Russia's invasion.[75] Their deployment showed that member states can mobilize cyber expertise across borders during a crisis. Similarly, the European Union established the Cyber and Information Domain Coordination Centre (CIDCC) in 2019 to improve coordination and situational awareness across the cyber and information domains.[76] Both programs, however, coordinate national capabilities rather than support commercial operators.

NATO has followed a similar path, strengthening its ability to defend the alliance's networks and support allies during cyber incidents. At the 2023 Vilnius Summit, allies launched the Virtual Cyber Incident Support Capability (VCISC), a mechanism NATO describes as a "clearinghouse" for mutual assistance in the event of a significant cyber incident.[77] At the 2024 Washington Summit, allies agreed to establish the NATO Integrated Cyber Defence Centre (NICC), which will inform military commanders about cyber threats to privately owned critical infrastructure that supports military activities.[78] NICC represents a more direct effort to connect cyber defense with NATO's operational dependence on civilian infrastructure, but it will not reach full operational capability until 2028.[79]

The consequences of civil-military coordination challenges are most visible in dual-use infrastructure, such as maritime ports. In July 2025, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) — a NATO-accredited cyber defense research, training, and exercise hub — published a policy brief on port cybersecurity. The brief found that NATO's Alliance Maritime Strategy — the alliance's doctrine that sets its security priorities in the maritime domain — had not been updated since 2011. It also found that the strategy contained no formal framework for cybersecurity coordination with commercial operators that

run Europe's ports.[80] In October 2025, NATO updated its strategy, calling for closer cooperation with commercial stakeholders to protect critical maritime infrastructure and for greater engagement with the maritime industry and international shipping community.[81] Nearly every NATO and partner country surveyed by CCDCOE reported cyberattacks on its port infrastructure over the previous five years.[82] These are the same ports that would receive U.S. reinforcements and heavy equipment during a crisis.

Unless NATO pairs digital modernization with stronger cybersecurity coordination between military planners and critical infrastructure operators that run these systems, efforts to accelerate military mobility could become more and more fragile.

Russia's Next-Generation Warfare

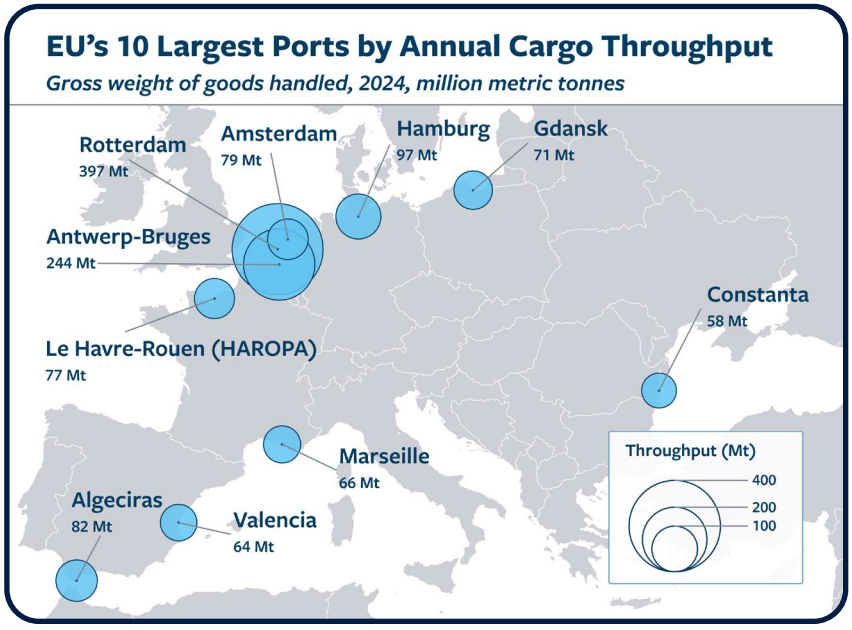
Russia's approach of next-generation warfare includes targeting critical infrastructure and information systems to disrupt an adversary's ability to coordinate operations and make decisions.[83] Attacks on logistics data, navigation signals, communications, or transportation systems could therefore create both operational disruption and uncertainty inside NATO's decision-making process.

For military mobility, this makes technological modernization a double-edged sword. More connected logistics networks can accelerate deployments, but they also give Russia more opportunities to alter routing data, obstruct coordination, and amplify confusion during a crisis. Therefore, NATO needs to pair interoperability with secure data exchange, trusted communications, system redundancy, and the ability to continue moving forces when digital services are degraded.

Chinese Influence Over Europe's Critical Infrastructure

Europe's military mobility vulnerabilities are compounded by the growing strategic footprint of Chinese state-linked entities across critical transportation and logistics infrastructure, energy infrastructure, and communications networks. Chinese laws requiring citizens and companies to cooperate with state intelligence agencies[84] — and Beijing's support for Russia's war in Ukraine — raise concerns that this footprint provides potential intelligence access or coercive leverage against NATO.

Chinese firms, many of them state-linked or state-owned, maintain direct or indirect stakes in at least 14 out of the 29 European ports located near NATO naval facilities or supporting NATO logistics operations.[85] A 2023 European Parliament study found that three Chinese conglomerates — COSCO Shipping Corporation, China Merchants Group, and Hutchison Port Holdings — own or operate terminals in roughly half of the EU ports considered critical to NATO operations,[86] including nearly 30 terminals across Europe and as many as 20 terminals within the 15 largest EU ports.[87]



Annual cargo throughput measures the total weight of goods moving through a port each year, providing a broad measure of a port's importance to EU logistics beyond container traffic alone. Source: Eurostat (online data code: mar_mg_aa_pwhd).[b]

COSCO, China's state-run shipping giant, maintains one of the largest footprints across European port terminals. The company acquired a 67 percent stake in Greece's Port of Piraeus between 2016 and 2021, giving Beijing influence over one of the Mediterranean's busiest commercial gateways and a critical entry point into southeastern Europe.[88] COSCO also holds 51 percent and 39.51 percent stakes in the largest container terminals at the Spanish ports of Valencia and Bilbao, respectively,[89] a 40 percent stake in Italy's Vado Ligure terminal,[90] and a 24.99 percent stake in Container Terminal Tollerort at Germany's Port of Hamburg.[91] In Belgium, COSCO owns a controlling stake in a container terminal in Zeebrugge and a minority stake in Antwerp.[92]

China Merchants Group, another Chinese state-owned enterprise, has a significant but largely indirect European port footprint through its subsidiary China Merchants Port Holdings (CMPort). CMPort owns a 49 percent stake in Terminal Link, a joint venture with French shipping company CMA CGM.[93] Through Terminal Link, CMPort's interest fans out across Europe, including Rotterdam, Antwerp-Bruges, Dunkirk, Le Havre, Fos-sur-Mer, Malta, Odessa, and Thessaloniki.[94] The exposure concentrates at several major gateways, including 44.59 percent of Dunkirk's Terminal des Flandres and 24.5 percent of terminals at Le Havre's Terminal de France and Marseille's Eurofos.[95] Because these interests are held indirectly and mostly as minority ownership stakes rather than outright control, they draw far less scrutiny than a direct acquisition would.

Separately, Hutchison Ports, headquartered in Hong Kong, controls a 20-hectare terminal at Poland's Port of Gdynia, a vital logistics node for NATO's eastern flank.[96] Alongside the Port of Rotterdam and Antwerpen-Zeebrugge, Gdynia is an arrival point for U.S. armed forces and would likely play a central role in reinforcing frontline allies during a contingency with Russia.[97] COSCO, China Merchants Group, and Hutchison all maintain stakes in terminals at Rotterdam, Europe's largest port and a major transatlantic logistics hub.[98]

Many of the ports in which Chinese firms maintain stakes sit along the same maritime and inland logistics corridors NATO would rely upon to move U.S. reinforcements, heavy equipment, fuel, and sustainment supplies across Europe during a crisis. This creates potential vulnerabilities at key chokepoints in the alliance's military mobility network. In 2024, researchers from ESET, a cybersecurity software company, identified malware deployed by a China-aligned hacker group, Mustang Panda, on systems across cargo shipping companies in Norway, Greece, and the Netherlands.[99]

The campaign demonstrates that Chinese cyber actors are already seeking access to European maritime logistics networks. Operators with access to port management systems, cargo manifests, and vessel scheduling platforms could potentially collect intelligence on military deployments, monitor logistics patterns, delay shipments, or disrupt port operations during periods of heightened tension. Likewise, the concentration of Chinese ownership across multiple strategically located ports also raises concerns about cumulative dependency risks within Europe's broader transportation infrastructure.

In addition, Chinese firms maintain a presence in Europe's digital and communication infrastructure. HMN Technologies (formerly Huawei Marine) and others have laid or serviced undersea fiber-optic cables near NATO naval facilities.[100] These cables carry both civilian and military logistics communications, meaning their compromise could disrupt command-and-control and sustainment operations during a crisis. In 2017, the state-linked company CITIC Telecom CPC acquired Dutch operator Linx Telecommunications, gaining control over key portions of Estonia's internet infrastructure, including a 470-kilometer undersea fiber-optic connection linking Estonia with Finland and Sweden.[101] The acquisition highlighted broader gaps in Europe's oversight of foreign investment in strategic digital infrastructure.[102]

Chinese enterprises also own positions in parts of Europe's energy infrastructure. In Portugal, State Grid Corporation of China owns a 25 percent stake in Redes Energeticas Nacionais (REN), the country's sole electricity transmission system operator,[103] which manages Portugal's high-voltage transmission grid and interconnection linking the Portuguese grid to Spain and the broader European network.[104] China Three Gorges Corporation is the largest single shareholder of Energias de Portugal (EDP),[105] one of Portugal's largest power companies and the operator of most of Portugal's electricity distribution network.[106] Collectively, Chinese entities own roughly 30 percent of Portugal's national grid operations.[107]

While these investments are commercial in nature, they create potential strategic dependence in sectors that NATO relies upon. This dependence mirrors broader lessons from cyber campaigns such as Volt Typhoon, which demonstrated how Chinese actors seek persistent access to civilian infrastructure systems that could be exploited during a future crisis. European Parliament researchers have also warned that Chinese port investments generate indirect political leverage over host governments.[108] The researchers noted that as national economies become increasingly tied to Chinese-operated logistics, energy, and communications networks, governments may become more hesitant to confront Beijing during periods of heightened geopolitical tension, particularly when disruption risks could impose significant economic costs.[109]

Recommendations

Keeping Europe's military mobility corridors operational under attack requires coordination that no current institution provides. The central problem is that European infrastructure investment consistently falls short and resilience initiatives are not aligned with NATO's operational requirements, EU regulation, and national enforcement. Each institution addresses part of the problem, but no coordinating mechanism assesses whether a complete reinforcement corridor can remain operational under attack. The most important solution is to align investment with NATO reinforcement plans. The recommendations below support that objective by establishing corridor-level resilience requirements, reducing strategic dependencies, and ensuring that civilian infrastructure can continue supporting military movement under disruption. The recommendations proceed from foundational reforms that better align infrastructure investment with NATO operational requirements to more targeted measures addressing specific vulnerabilities and capability gaps.

1. **NATO should obligate member states to show how investments contribute to collective defense.**

   NATO allies have agreed — as part of their broader commitment to invest 5 percent of GDP on defense by 2035 — to allocate up to 1.5 percent of GDP annually toward critical infrastructure protection, network defense, and civil preparedness and resilience.[110] Rather than prescribe another arbitrary spending target within the 1.5 percent category, NATO should require allies to show how qualifying investments address deficiencies identified in regional defense and reinforcement plans.[111] Member states already must submit annual plans demonstrating a credible path toward the broader spending commitment,[112] giving NATO a mechanism to use existing reporting to connect eligible investments to military needs. Those annual plans should include a military mobility annex identifying the operational problem each mobility investment addresses, the forces or routes that depend on the investment, and whether the project reduces delays or preserves movement during disruption.

   The European Court of Auditors found that the European Commission selected existing EU military mobility projects on a piecemeal basis and did not necessarily address the most strategically important locations.[113] NATO should therefore maintain a prioritized list of deficiencies whose failure would materially delay reinforcement, ranked by operational need rather than infrastructure type, and provide the European Union with sufficient military requirements to guide its funding decisions. NATO should then use its updated 2029 capability targets[114] — i.e., NATO's defense requirements specifying individual obligations of member states — to assess whether national investments are correcting those priority shortfalls. This would prevent allies from counting general transportation, digitalization, or infrastructure spending toward the 1.5 percent category without demonstrating its relevance to collective defense.

2. **NATO should operationalize the NICC around NATO battle plans.**

   NATO established the NATO Integrated Cyber Defence Centre (NICC) to inform military commanders about cyber threats and vulnerabilities affecting NATO and allied networks, including privately owned and operated critical infrastructure. NICC should organize that mission around ports, railways, airports, border systems, energy networks, communication services, and technology providers required by NATO reinforcement plans. Its assessments should explain the operational consequences of technical disruptions by identifying which movements are affected, how much capacity remains, how long the disruption can be tolerated, and whether commanders need to reroute or reprioritize forces. This would distinguish between cyber incidents that impose primarily commercial costs and those that threaten NATO's ability to execute a defense plan.

   NATO member states should designate national liaisons connecting transportation regulators, national cyber authorities, military movement officials, and NICC. Allies should also establish common protocols, standards, and policies that enable rapid, interoperable information sharing with NICC to support near-real-time situational awareness. NIS2 already covers major rail, aviation, and maritime entities and requires them to report significant cyber incidents to national authorities.[115] Allies should build on those existing reporting channels rather than create a parallel NATO reporting mandate for private operators. When an incident affects infrastructure supporting an alliance plan, the national liaison should provide NICC with details on impact and available workarounds. NICC should incorporate that information into the operational picture used by NATO logistics planners and commanders, ensuring that cyber reporting — rather than remaining a separate technical process — informs decisions about rerouting forces, adjusting schedules, or using alternative infrastructure.

3. The European Commission and EU member states should incorporate NATO logistics corridor designations as foreign direct investment (FDI) screening criteria.

The European Union's Military Mobility Package 2025 identifies foreign ownership risks as part of the broader resilience challenge affecting strategic dual-use infrastructure.[116] In this context, the union's FDI Screening Regulation establishes an EU framework for member states to review incoming FDI for security hazards. The regulation already provides a cooperation mechanism through which member states exchange information on screened investments and provide comments — the European Commission may issue opinions in response.[117]

On December 11, 2025, the Council of the European Union and the European Parliament reached a provisional political agreement on a revised regulation that requires all member states to maintain screening mechanisms with a common minimum mandatory scope covering dual-use items, military equipment, and critical entities in energy, transport, and digital infrastructure. The European Parliament approved the agreement on May 19, 2026, and the Council of the European Union formally adopted the revised regulation on June 8, 2026.[118] The regulation entered into force on July 16, 2026, but most provisions will apply beginning January 17, 2028.

However, although the revised regulation covers transportation infrastructure and TEN-T, it does not explicitly require heightened screening practices for investments affecting the four EU priority military mobility corridors, which were developed in close coordination with NATO.[119] Member states should therefore use the updated framework to prevent new dependencies while applying NIS2's supply chain security and business continuity requirements to high-risk technologies already in place.[120]

The United States already prohibits covered transportation entities from using Chinese-linked logistics platforms such as LOGINK.[121] The European Commission should update its guidance and coordination practice so that FDI involving operating stakes, contractual rights to operate or manage a terminal, access to sensitive logistics data or digital platforms, and other forms of control over rail nodes, ports, airports, and related logistics infrastructure is treated as presumptively warranting enhanced review. Designation of a transport corridor as part of NATO or EU military mobility corridors should function as an explicit trigger for national security consultation, with particular scrutiny of investments or operational dependencies linked to state actors like China.

4. NATO member states should establish a pooled multinational rail mobility capability.

Because NATO does not command most transport assets, day-to-day movement depends on voluntary contributions from allies and access to commercial transportation capacity. The Movement Coordination Centre Europe (MCCE) is an independent multinational military organization that functions as an "intelligent broker"[122] across 30 participant nations, matching available airlift, sealift, road, inland waterway, and rail capacity with nations that have transport needs.[123] MCCE improves visibility and efficiency, but it has no command authority over the assets it coordinates.[124] As a result, it can make better use of available rail capacity but cannot guarantee that sufficient rolling stock, or railway vehicles, will be available when several allies mobilize simultaneously.

Some allies have partially mitigated these gaps in specific domains. In the air domain, the European Air Transport Command (EATC) integrates more than 180 military transport assets drawn from seven member nations,[125] while NATO's Rapid Air Mobility initiative provides priority flight planning and airspace clearances for crisis deployment across allied territory.[126] Rail has no comparable mechanism combining pooled assets with pre-agreed access during a crisis, even though it is the primary means best suited for moving heavy armor on land over long distances. Europe's railway industry group — the Community of European Railway and Infrastructure Companies — estimates that moving a single light division of 15,000 soldiers requires up to 200 trains with roughly 8,400 wagons.[127] Participating allies should adapt the EATC pooling model by jointly procuring or designating, in coordination with the MCCE, a minimum pool of dual-use heavy-lift wagons.

5. NATO and EU member states should conduct exercises to build resilience against GPS jamming and spoofing.

Almost every form of military movement depends on satellite positioning and timing, making interference with these systems a growing operational vulnerability. Since 2022, deliberate jamming and spoofing has surged across the Baltic, Black Sea, and Arctic regions, with European governments attributing interference to Russia and Belarus. Roughly 40 percent of European air traffic now operates in heavily affected airspace,[128] and nearly 123,000 flights over the Baltic experienced navigation interference during the first four months of 2025.[129] Recent European initiatives have begun addressing this challenge. In 2025, the European Commission declared the Open Service Navigation Message Authentication of Galileo — the European Union's global navigation satellite system — operational, allowing users to detect manipulated navigation signals. However, it does not prevent spoofing or protect receivers against jamming.[130]

The bloc also launched the EU Governmental Satellite Communications program in 2026 to provide secure and resilient satellite communications to member states lacking sovereign satellite capabilities.[131]

Member states should therefore pair authenticated satellite services with alternative navigation, timing, communications, and routing procedures suited to each transportation mode. NATO and EU members should test these measures through exercises that disrupt several connected nodes on the same reinforcement corridor. ENISA's 2026 Cyber Europe exercise simultaneously disrupted port logistics, navigation systems, and cross-border rail operations, illustrating how failures in one transportation mode can compound problems elsewhere.[132] NATO exercises should also determine whether forces and equipment still reached their destinations within the required timelines. Each exercise should conclude with a corrective action plan and deadline for retesting so that identified vulnerabilities are corrected rather than repeatedly documented.

6. **NATO and EU member states should treat cybersecurity workforce shortages as a defense priority.**

NATO's resilience and military mobility objectives are constrained by a structural shortage of cybersecurity personnel across member states. The latest estimate by ISC2 — a global cybersecurity association that specializes in cybersecurity training and certifications — put the global cybersecurity workforce gap at roughly 4.8 million unfilled positions in 2024,[133] including roughly 424,000 across Europe[134] and nearly 300,000 within EU member states alone.[135] National deficits are significant even in advanced digital economies, including Germany, which projects a shortage exceeding 100,000 specialists,[136] and cyber-savvy countries like Estonia, which has reported a need for cyber talent equivalent to a substantial share of its workforce.[137] ENISA's 2025 NIS360 survey found that 45 percent of organizations reported difficulty finding qualified candidates as their primary hiring challenge.[138]

Member states should treat cyber talent as a defense capability and resource it accordingly. NATO and the European Union should expand government-funded training, scholarship, apprenticeship, and cyber reserve programs while creating accelerated pathways for military personnel and mid-career professionals to transition into cyber roles. Allies should also improve workforce interoperability through mutual recognition of certifications, shared training capacity, and joint exercises that build operational expertise across the alliance.

Recruitment alone, however, will not solve the problem. ENISA data show that workload, burnout, limited career advancement, and insufficient professional development remain major retention challenges.[139] Sustained investment in career development and retention will therefore be as important to long-term cyber resilience as attracting new talent.

Conclusion

Addressing Europe's military mobility infrastructure gaps and regulatory barriers is a test of whether NATO can move and sustain forces during cyber disruption, contested logistics, and attacks on the civilian systems that underpin reinforcement operations. While the European Union and NATO have made progress through mobility initiatives, cyber resilience programs, expanded infrastructure planning, updated operational plans and command structures, and more robust exercises, responsibility remains divided among NATO planners, EU regulators, national authorities, and private operators, and no actor currently ensures that an entire transportation corridor can remain operational under attack. Ensuring these transportation corridors work will require NATO to anchor resilience spending and cyber awareness to its reinforcement plans, and the European Union and member states should secure critical infrastructure along priority corridors. Ultimately, military mobility should be judged not by the number of projects funded or exercises conducted but by whether allied forces can still reach the battlefield at the speed and scale NATO's defense plans require.

Photo Credits and Notes

a. Estimated costs have risen from €5.8 billion to €23.8 billion. The Warsaw to Kaunas section is operational, but construction north of Kaunas remains unfinished. "Rail Baltica Map," *RB Rail AS*, November 15, 2017. (https://commons.wikimedia.org/wiki/File:RBINFO.png)

b. Based on 2024 Eurostat data, these ports rank among the European Union's largest by gross weight of goods handled. While throughput alone does not measure military handling capacity, these high-throughput ports are key freight nodes that could support the movement of equipment and supplies for military mobility. "Gross weight of goods handled in the top 20 European ports by direction," *Eurostat*, March 12, 2025. (https://ec.europa.eu/eurostat/databrowser/view/mar_mg_aa_pwhd/default/table?lang=en&category=mar.mar_m)

Endnotes

1. European Commission, "The economic impact of higher defence spending," May 19, 2025. (https://economy-finance.ec.europa.eu/economic-forecast-and-surveys/economic-forecasts/spring-2025-economic-forecast-moderate-growth-amid-global-economic-uncertainty/economic-impact-higher-defence-spending_en)

2. Arno Van Rensbergen, "How bureaucracy and underfunding undermine EU military mobility," *The Parliament Magazine*, February 17, 2025. (https://www.theparliamentmagazine.eu/news/article/bureaucracy-and-underfunding-undermine-eu-military-mobility)

3. Carol V. Evans, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner, *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency* (*NATO COE-DAT Handbook 1*), (Carlisle, Pennsylvania: U.S. Army War College Press, 2022), pages 1-4. (https://press.armywarcollege.edu/monographs/955)

4. European Commission, "CER and NIS-2 Directives enter into force to strengthen EU's resilience," October 26, 2022. (https://ec.europa.eu/newsroom/cipr/items/764849/en); The White House, Office of the Press Secretary, "Presidential Policy Directive/PPD-21," February 12, 2013, pages 10-11. (https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf); "Critical Infrastructure Sectors," *U.S. Department of Homeland Security*, *Cybersecurity and Infrastructure Security Agency*, accessed August 21, 2026. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors)

5. North Atlantic Treaty Organization, "The North Atlantic Treaty," April 4, 1949. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty)

6. "Critical Infrastructure Sectors," *U.S. Department of Homeland Security*, *Cybersecurity and Infrastructure Security Agency*, accessed August 21, 2026. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors); Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), *Official Journal of the European Union*. (https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng); "NIS2 Directive: securing network and information systems," *European Commission*, accessed August 21, 2026. (https://digital-strategy.ec.europa.eu/en/policies/nis2-directive); Consolidated text: Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), *Official Journal of the European Union*. (https://ec.europa.eu/commission/presscorner/detail/en/inf_26_679)

7. North Atlantic Treaty Organization, "2026 Resilience. Baseline Requirements," September 15, 2026. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/09/15/2026-resilience-baseline-requirements)

8. European Commission and North Atlantic Treaty Organization, "EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report," June 29, 2023, page 3. (https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf)

9. CER and NIS-2 Directives enter into force to strengthen EU's resilience," *European Commission*, "October 26, 2022. (https://ec.europa.eu/newsroom/cipr/items/764849/en); "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs," *European Commission*, accessed August 21, 2026, (https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs); Cristina Criscuoli and Federico Toscani, "NIS2 Series Part 2 – What should in-scope organisations do now to prepare for NIS2 compliance?" *DLA Piper*, December 4, 2024. (https://www.dlapiper.com/en-us/insights/blogs/cortex-life-sciences-insights/2024/nis2-series-part-2); "Commission takes action to ensure complete and timely transposition of EU directives," *European Commission*, March 26, 2026. (https://ec.europa.eu/commission/presscorner/detail/en/inf_26_679)

10. "Critical infrastructure resilience at EU-level," *European Commission*, January 13, 2026. (https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en)

11. "NIS 2: Where are European countries in transposing the directive? [updated January 2026]," *Wavestone*, November 25, 2024. (https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive)

12. European Commission, Press Release, "Commission refers Ireland, Spain, France, and the Netherlands to the Court of Justice for failing to transpose the rules on cybersecurity," July 8, 2026. (https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules)

13. European Commission, Press Release, "Commission Decides to Refer Bulgaria, France, Luxembourg, the Netherlands, Poland, Spain and Sweden to the Court of Justice of the European Union for failing to transpose the Directive on critical entities resilience," April 28, 2026. (https://ec.europa.eu/commission/presscorner/detail/en/ip_26_910)

14. Council of the European Union, Press Release, "Cyber resilience act: Council adopts new law on security requirements for digital products," October 10, 2024. (https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products)

15. "Where the CRA Stands today," *Cyber Resilience Act*, accessed August 21, 2026. (https://www.cyberresilienceact.eu/state-of-play.html)

16. "Cyber Resilience Act," *European Commission*, accessed August 21, 2026. (https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)

17. "Cyber Resilience Act – Reporting obligations," *European Commission*, accessed September 18, 2026. (https://digital-strategy.ec.europa.eu/en/policies/cra-reporting); European Union Agency for Cybersecurity, Press Release, "The CRA Single Reporting Platform is launched," September 11, 2026. (https://www.enisa.europa.eu/news/the-cra-single-reporting-platform-is-launched)

18. "NATO Defence Planning Process," *North Atlantic Treaty Organization*, April 16, 2025. (https://www.nato.int/en/what-we-do/introduction-to-nato/nato-defence-planning-process)

19. European Union Agency for Cybersecurity, "NIS Investments 2025," December 8, 2025, pages 9 and 12. (https://www.enisa.europa.eu/sites/default/files/2026-02/NIS%20Investments%202025%20-%20Main%20report.pdf)

20. North Atlantic Treaty Organization, "The Hague Summit Declaration," June 25, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration)

21. "Commissioner Tzitzikostas' statement at the EP Plenary Session on the importance of trans-European transport infrastructure," *European Commission*, April 1, 2025. (https://ec.europa.eu/commission/presscorner/detail/en/speech_25_941); European Parliament resolution of 17 December 2025 on military mobility (2025/2090(INI)), *Official Journal of the European Union*. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025IP0335)

22. European Court of Auditors, "EU military mobility: Full speed not reached due to design weaknesses and obstacles en route," February 5, 2025, page 7. (https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf)

23. Élie Tenenbaum and Amélie Zima, "Return to the East: the Russian Threat and the French Pivot to Europe's Eastern Flank," *French Institute of International Relations*, June 13, 2024, page 59. (https://www.ifri.org/en/studies/return-east-russian-threat-and-french-pivot-europes-eastern-flank)

24. "DACIAN FALL 2025: soutenir un exercice d'envergure [DACIAN FALL 2025: to support a large-scale exercise]," *French Commissariat des armées*, November 24, 2025. (https://www.defense.gouv.fr/commissariat/actualites/dacian-fall-2025-soutenir-exercice-denvergure)

25. The Netherlands has approximately 448 wagons, and Germany has 343 flatbed wagons reserved through contracts with DB Cargo. See: Rudy Ruitenberg, "Dutch military adds railway steel to rush troops to NATO's east flank," *Defense News*, February 7, 2025. (https://www.defensenews.com/global/europe/2025/02/07/dutch-military-adds-railway-steel-to-rush-troops-to-natos-east-flank)

26. Marcin Zaborowski and Lt. Gen. Pavel Macko, "Roads to Readiness: Military Mobility Infrastructure on NATO's Eastern Flank," *GLOBSEC*, June 13, 2025, page 13. (https://www.globsec.org/what-we-do/publications/roads-readiness-military-mobility-infrastructure-natos-eastern-flank)

27. Ibid.

28. Konrad Wolfenstein, "Inland ports: Europe's Achilles heel and NATO's underestimated pillar for military mobility," *Xpert*, August 2, 2025. (https://xpert.digital/en/inland-ports-of-europe)

29. Costas Paris and Daniel Michaels, "Europe Sees Its Own Ports as Vulnerable in Standoff with Russia," *The Wall Street Journal*, June 20, 2025. (https://www.wsj.com/world/europe/europe-sees-its-own-ports-as-vulnerable-in-standoff-with-russia-d43ecac5)

30. Marcin Zaborowski and Lt. Gen. Pavel Macko, "Roads to Readiness: Military Mobility Infrastructure on NATO's Eastern Flank," *GLOBSEC*, June 13, 2025, page 16. (https://www.globsec.org/what-we-do/publications/roads-readiness-military-mobility-infrastructure-natos-eastern-flank)

31. Will Croxton, "Beyond the Eagle S: how Yi Peng 3 and Newnew Polar Bear wreaked havoc in the Baltic Sea," *CBS News*, September 28, 2025. (https://www.cbsnews.com/news/eagle-s-how-yi-peng-3-and-newnew-polar-bear-wreaked-havoc-in-baltic-sea-60-minutes); Karl Kivil and Aili Vahtla, "China admits container ship Newnew Polar Bear damaged undersea gas pipeline," *ERR*, August 12, 2024. (https://news.err.ee/1609422658/china-admits-container-ship-newnew-polar-bear-damaged-undersea-gas-pipeline)

32. Sophie Himka, "Baltic Sea Undersea Cable Security," *The Henry M. Jackson School of International Studies*, July 9, 2025. (https://jsis.washington.edu/news/baltic-sea-undersea-cable-security); Elisabeth Braw, "Suspected sabotage by a Chinese vessel in the Baltic Sea speaks to a wider threat," *Atlantic Council*, November 21, 2024. (https://www.atlanticcouncil.org/blogs/new-atlanticist/suspected-sabotage-by-a-chinese-vessel-in-the-baltic-sea-speaks-to-a-wider-threat); Johan Ahlander, Louise Rasmussen, and Terje Solsvik, "Chinese ship linked to Baltic Sea cable breach resumes voyage," *Reuters*, December 21, 2024. (https://www.reuters.com/world/chinese-ship-linked-baltic-sea-cable-breach-resumes-voyage-2024-12-21)

33. European Defence Agency, "Military Mobility," accessed August 21, 2026, page 1. (https://www.pesco.europa.eu/wp-content/uploads/2024/11/2024-NL-Military-Mobility-MiMob-Website-leaflet.pdf); "Permanent Structured Cooperation (PESCO)," European Parliament, accessed August 21, 2026. (https://www.pesco.europa.eu)

34. European Commission, "Joint Communication to the European Parliament, the European Council and the Council Preserving Peace – Defence Readiness Roadmap 2030," October 16, 2025. (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025JC0027); European Commission, "Joint Communication to the European Parliament, the European Council and the Council on Military Mobility," November 19, 2025. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0846); European Commission, "Commission Staff Working Document on Military Mobility," November 19, 2025, pages 19-22. (https://defence-industry-space.ec.europa.eu/document/download/d868bd58-3b88-47ff-8cfc-c2d0e7b5b75f_en?filename=Staff%20Working%20Document%20on%20Military%20Mobility%2C%20accompanying%20the%20Proposal_0.pdf)

35. European Commission, "Joint Communication to the European Parliament, the European Council and the Council Preserving Peace – Defence Readiness Roadmap 2030," October 16, 2025. (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025JC0027)

36. European Parliament, "(NL) Military Mobility (MilMob)," page 2. (https://www.pesco.europa.eu/wp-content/uploads/2025/10/2025-NL-Military-Mobility-MiMob-Website-leaflet.pdf); European Court of Auditors, "EU military mobility: Full speed not reached due to design weaknesses and obstacles en route," February 5, 2025, pages 20-22. (https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf)

37. "Connecting Europe Facility 2021-2027 adopted," *European Commission, European Climate, Infrastructure and Environment Executive Agency*, July 20, 2021. (https://cinea.ec.europa.eu/news-events/news/connecting-europe-facility-2021-2027-adopted-2021-07-20_en); "Military mobility: the EU supports strategic investments on dual-use transport infrastructure with €807 million," *European Commission, European Climate, Infrastructure and Environment Executive Agency*, January 24, 2024. (https://cinea.ec.europa.eu/news-events/news/military-mobility-eu-supports-strategic-investments-dual-use-transport-infrastructure-eu807-million-2024-01-24_en)

38. European Court of Auditors, "EU military mobility: Full speed not reached due to design weaknesses and obstacles en route," February 5, 2025, pages 28-29. (https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf)

39. European Court of Auditors, "EU military mobility: Full speed not reached due to design weaknesses and obstacles en route," February 5, 2025, page 29. (https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf)

40. European Court of Auditors, "EU military mobility: Full speed not reached due to design weaknesses and obstacles en route," February 5, 2025, pages 33, and 42-43. (https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf); Lorne Cook, "An EU fund to help troops move quickly is too small and poorly managed, auditors say," *Associated Press*, February 5, 2025. (https://apnews.com/article/eu-defense-ukraine-military-mobility-transport-7ca644d2f000b53c7f8b3f663ca7f1c5)

41. European Commission, "Joint Communication to the European Parliament, the European Council and the Council on Military Mobility," November 19, 2025. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0846); Sebastian Clapp, Monika Kiss, and Mathias Gullentops, "Military Mobility," *European Parliamentary Research Service*, July 4, 2025, page 1. (https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775860/EPRS_BRI(2025)775860_EN.pdf)

42. "Questions & Answers," European Commission, accessed August 21, 2026. (https://transport.ec.europa.eu/transport-themes/military-mobility/questions-answers_en)

43. Ibid.

44. European Commission, "Military Mobility Package," August 2026, page 1. (https://defence-industry-space.ec.europa.eu/document/download/297bdcb7-365b-4d98-8bb3-81578f91c528_en?filename=Factsheet%20Military%20Mobility%20Package.pdf)

45. "Military Mobility: One step closer to a Military Schengen," *European Commission*, accessed August 21, 2026. (https://defence-industry-space.ec.europa.eu/eu-defence-industry/military-mobility_en)

46. "Strengthening military mobility in the EU," *European Council*, July 1, 2026. (https://www.consilium.europa.eu/en/policies/military-mobility); Emanuele Bonini, "Military mobility: inter-institutional negotiations to begin on 16 July," *EUnews* (Italy), July 8, 2026. (https://www.eunews.it/en/2026/07/08/military-mobility-inter-institutional-negotiations-to-begin-on-16-july)

47. José Papí, "Investing in Transport in the new MFF," *European Parliament: Directorate-General for Cohesion, Agriculture and Social Policies*, April 28, 2026, page 43. (https://www.europarl.europa.eu/RegData/etudes/STUD/2026/783532/CASP_STU(2026)783532_EN.pdf)

48. "List of completed CEF Transport projects funded under the military mobility envelope," *European Commission, European Climate, Infrastructure and Environment Executive Agency*, November 19, 2025. (https://cinea.ec.europa.eu/news-events/news/list-completed-cef-transport-projects-funded-under-military-mobility-envelope-2025-11-19_en)

49. Paula Soler, "Kubilius: EU needs at least €70 billion to strengthen military mobility," *Euronews* (France), March 25, 2025. (https://www.euronews.com/my-europe/2025/03/25/defence-kubilius-eu-to-strengthen-military-mobility-troops-equipment); European Commission, "Joint Communication to the European Parliament and the Council on Military Mobility," November 19, 2025, page 8. (https://defence-industry-space.ec.europa.eu/document/download/c3d3067c-6d9a-4f95-9a69-4dd99c340188_en?filename=Action%20plan%20on%20military%20mobility%202.0.pdf); Sebastian Clapp and Darius Engel, "European defence readiness roadmap," *European Parliamentary Research Service*, January 14, 2026, page 5. (https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782589/EPRS_BRI(2026)782589_EN.pdf); European Commission, "Joint Communication to the European Parliament, the European Council and the Council Preserving Peace – Defence Readiness Roadmap 2030," October 16, 2025. (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025JC0027)

50. Sebastian Clapp, Monika Kiss, and Mathias Gullentops, "Military Mobility," *European Parliamentary Research Service*, July 4, 2025, page 10. (https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775860/EPRS_BRI(2025)775860_EN.pdf); Theo Maiziere, "EU unveils €2 Trillion Budget for 2028-2034," *techUK*, July 17, 2025. (https://www.techuk.org/resource/eu-unveils-2-trillion-budget-for-2028-2034.html)

51. Sam McNeil, "EU rolls out plan to make it easier to deploy tanks and troops at short notice," *PBS*, November 19, 2025. (https://www.pbs.org/newshour/world/eu-rolls-out-plan-to-make-it-easier-to-deploy-tanks-and-troops-at-short-notice)

52. Emanuele Bonini, "Military mobility: inter-institutional negotiations to begin on 16 July," *Eunews* (Italy), July 8, 2026. (https://www.eunews.it/en/2026/07/08/military-mobility-inter-institutional-negotiations-to-begin-on-16-july)

53. "SAFE Security Action for Europe," *European Commission*, accessed August 21, 2026. (https://defence-industry-space.ec.europa.eu/eu-defence-industry/safe-security-action-europe_en)

54. North Atlantic Treaty Organization, "Data Strategy for the Alliance," May 5, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance)

55. Ibid.

56. Jakub Prezetacznik and Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," *European Parliamentary Research Service*, June 8, 2022, page 2 (https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf); "KA-SAT Network cyber attack overview," *Viasat*, March 30, 2022. (https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview)

57. UK Government, Press Release, "Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion," May 10, 2022. (https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion)

58. European Union Agency for Cybersecurity, "NIS Investments: Cybersecurity Policy Assessment," November 16, 2023, page 4. (https://www.enisa.europa.eu/sites/default/files/publications/CSPA%20-%20NIS%20Investments%20-%202023.pdf)

59. European Union Agency for Cybersecurity, "ENISA NIS360: Latest Insights in the Cybersecurity Maturity and Criticality of NIS Sectors of High Criticality," May 28, 2026, page 9. (https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf)

60. European Union Agency for Cybersecurity, "ENISA NIS360: Latest Insights in the Cybersecurity Maturity and Criticality of NIS Sectors of High Criticality," May 28, 2026, page 26. (https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf)

61. Ibid.

62. "Hacker attack at Split St. Jerome Airport," *AvioRadar*, July 23, 2024. (https://avioradar.net/en/hacker-attack-at-split-st-jerome-airport)

63. Andrius Sytas, "Russia group claims hack of Lithuanian sites in retaliation for transit ban," *Reuters*, June 27, 2022. (https://www.reuters.com/technology/lithuania-hit-by-cyber-attack-government-agency-2022-06-27)

64. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024. page 11. (https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf); Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," March 25, 2025, page 19. (https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf); Office of the Director of National Intelligence, "2026 Annual Threat Assessment of the U.S. Intelligence Community," March 18, 2026, page 16. (https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf);

65. U.S. Department of Justice, Federal Bureau of Investigation, "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," April 18, 2024. (https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says)

66. Microsoft Threat Intelligence, "New 'Prestige' ransomware impacts organizations in Ukraine and Poland," October 14, 2022. (https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland)

67. Tim Starks, "After major Poland energy grid cyberattack, CISA issues warning to U.S. audience," *CyberScoop*, February 10, 2026. (https://cyberscoop.com/cisa-warning-russian-cyberattack-poland-power-grid); U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps," February 10, 2026. (https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps)

68. National Research Institute, CERT Polska, "Energy Sector Incident Report – 29 December 2025," January 30, 2026. (https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025)

69. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Russian GRU Targeting Western Logistics Entities and Technology Companies," April 17, 2026, pages 3-10. (https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF)

70. Sarah Rainsford, "Poland says blast on rail line to Ukraine 'unprecedented act of sabotage," *BBC* (UK), November 18, 2025. (https://www.bbc.com/news/articles/cp85g86x0zgo)

71. European Union Agency for Cybersecurity, "ENISA NIS360: Latest Insights in the Cybersecurity Maturity and Criticality of NIS Sectors of High Criticality," May 28, 2026, pages 25 and 41. (https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf)

72. "Finland and Estonia warn vessels in the Gulf of Finland of an increase in GNSS disruptions," *Finnish Transport and Communications Agency*, June 13, 2025. (https://traficom.fi/en/news/finland-and-estonia-warn-vessels-gulf-finland-increase-gnss-disruptions)

73. Swedish Maritime Administration, "Ufs notice register," April 22, 2026. (https://ufs.sjofartsverket.se/en/Current/NoticeDetails?from=register&notice=20041); Swedish Maritime Administration, "Ufs Notices to Mariners, SWEDEN," July 2, 2025, page 4. (https://ufs.sjofartsverket.se/pdf/2025/1074EN.pdf)

74. Emma Burrows, "What to know about Russia's GPS jamming of a European official's plane," *PBS*, September 2, 2025. (https://www.pbs.org/newshour/world/what-to-know-about-russias-gps-jamming-of-a-european-officials-plane)

75. European Parliament, "Answer given by High Representative/Vice-President Borrell i Fontelles on behalf of the European Commission," June 1, 2023, page 1. (https://www.europarl.europa.eu/RegData/questions/reponses_qe/2023/001213/P9_RE(2023)001213_EN.pdf)

76. European Parliament, "(DE) Cyber and Information Domain Coordination Center (CIDCC)," accessed August 21, 2026, page 1. (https://www.pesco.europa.eu/wp-content/uploads/2025/10/2025-DE-Cyber-and-Information-Domain-Coordination-Center-CIDCC-Website-leaflet.pdf)

77. North Atlantic Treaty Organization, "Cyber defence," July 30, 2024. (https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence); North Atlantic Treaty Organization, "Vilnius Summit Communiqué," July 11, 2023. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique); North Atlantic Treaty Organization, "Allies practice coordination of mutual cyber support through NATO," April 14, 2025. (https://www.nato.int/en/news-and-events/articles/news/2025/04/14/allies-practise-coordination-of-mutual-cyber-support-through-nato)

78. North Atlantic Treaty Organization, "Allies agree new NATO Integrated Cyber Defence Centre," July 10, 2024. (https://www.nato.int/en/news-and-events/articles/news/2024/07/10/allies-agree-new-nato-integrated-cyber-defence-centre)

79. Carley Welch, "NATO to launch new cyber center by 2028: Official," *Breaking Defense*, December 6, 2024. (https://breakingdefense.com/2024/12/nato-to-launch-new-cyber-center-by-2028-official)

80. James Austin, Maj. Andrii Davydiuk, Adam Dollimore, Aleksi Kajander, and Erik Kursetgjerde, "Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure," *North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence*, July 18, 2025, page 5. (https://ccdcoe.org/uploads/2025/07/CCDCOE_Policy_Brief.pdf); North Atlantic Treaty Organization, "Alliance Maritime Strategy," October 29, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/10/29/alliance-maritime-strategy)

81. North Atlantic Treaty Organization, "Alliance Maritime Strategy," October 29, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/10/29/alliance-maritime-strategy)

82. James Austin, Maj. Andrii Davydiuk, Adam Dollimore, Aleksi Kajander, and Erik Kursetgjerde, "Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure," *North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence*, July 18, 2025, page 1. (https://ccdcoe.org/uploads/2025/07/CCDCOE_Policy_Brief.pdf)

83. "Russia's Next-Generation Warfare: Ivana Stradner, "The Informational Front in Russia's War," *American Foreign Policy Council*, September 4, 2019, page 7. (https://www.afpc.org/uploads/documents/Defense_Dossier_-_December_2025_Final.pdf); Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies*, August 10, 2010, page 1. (https://www.tandfonline.com/doi/abs/10.1080/13518040490450529)

84. Frank Juris, "Security implications of China-Owned critical infrastructure in the European Union," *European Parliament, Directorate-General for External Policies of the Union*, June 23, 2023, page 18. (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf); Jeanne-May Desurmont, "The Geopolitics of Chinese-Owned Ports," *Bloomsbury Intelligence and Security Institute*, October 24, 2024. (https://bisi.org.uk/reports/the-geopolitics-of-chinese-owned-ports)

85. Frank Jüris, "Security implications of China-Owned critical infrastructure in the European Union," *European Parliament, Directorate-General for External Policies of the Union*, June 23, 2023, page 19. (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf)

86. Frank Jüris, "Security implications of China-Owned critical infrastructure in the European Union," *European Parliament, Directorate-General for External Policies of the Union*, June 23, 2023, page 18. (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf)

87. Linton Nightingale, "Strategic stakes: EU sharpens focus on Chinese port ownership," *Lloyd's List*, February 20, 2025. (https://www.lloydslist.com/LL1152631/Strategic-stakes-EU-sharpens-focus-on-Chinese-port-ownership)

88. Renee Maltezou, "Greece's Piraeus port not for sale, China tells US," *Reuters*, November 20, 2025. (https://www.reuters.com/world/china/greeces-piraeus-port-not-sale-china-tells-us-2025-11-20)

89. Siobhán Delaney, "China Reshapes Global Shipping Order, Secures Stakes in 129 Ports Worldwide," *The Economy*, July 22, 2025. (https://economy.ac/news/2025/07/20250760866)

90. "COSCO buys big stake in Italian terminal," *Xinhua* (China), August 30, 2019. (https://www.chinadaily.com.cn/a/201908/30/WS5d69014fa310cf3e35568e0b.html)

91. "HHLA and Cosco finalise stake buy in Hamburg terminal," *Kuehne+Nagel*, June 21, 2023. (https://mykn.kuehne-nagel.com/news/article/hhla-and-cosco-finalise-stake-buy-in-hamburg-21-Jun-2023)

92. Karin Smit Jacobs, "Chinese strategic interests in European ports," *European Parliament*, February 27, 2023, page 1. (https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739367/EPRS_ATA(2023)739367_EN.pdf)

93. "History," *Terminal Link*, accessed August 21, 2026. (https://www.terminal-link.com/about)

94. "Map of Network," *Terminal Link*, accessed August 21, 2026. (https://www.terminal-link.com/ports/network)

95. Sönke Maatsch and Leona Gáborová, "Ownership structure of major terminal operators in the EU," *Institute of Shipping Economics and Logistics*, February 26, 2026, page 9. (https://idw-online.de/de/attachmentdata122133)

96. Frank Jüris, "Security implications of China-Owned critical infrastructure in the European Union," *European Parliament, Directorate-General for External Policies of the Union*, June 23, 2023, page 15. (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf)

97. Laurens Groeneveld and Maria Pankowska, "NATO in deep water because of Chinese port investments," *The Investigative Desk*, October 18, 2022. (https://investigativedesk.com/nato-in-deep-water-because-of-chinese-port-investments)

98. Karin Smit Jacobs, "Chinese strategic interests in European ports," *European Parliament*, February 27, 2023, page 2. (https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739367/EPRS_ATA(2023)739367_EN.pdf); "Map of Network," *Terminal Link*, accessed August 21, 2026. (https://www.terminal-link.com/ports/network)

99. ESET, "Iran-Aligned Cyberattacks: Rise in Disruptive Operations," May 14, 2024, page 6. (https://web-assets.eset.com/fileadmin/ESET/IL/APT_Activity_Report_Q4_2023-Q1_2024.pdf)

100. Frank Jüris, "Security implications of China-Owned critical infrastructure in the European Union," *European Parliament, Directorate-General for External Policies of the Union*, June 23, 2023, page 15. (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf)

101. Holger Roonemaa, Mari Eesmaa, Inese Braže, Sabīne Bērziņa, and Naglis Navakas, "Chinese intelligence increasingly setting sights on Estonia," *Postimees* (Estonia), September 5, 2019. (https://news.postimees.ee/6771074/chinese-intelligence-increasingly-setting-sights-on-estonia); Frank Jüris, "Estonia's Evolving Threat Perception of China," *The Prospect Foundation*, April 28, 2022. (https://www.pf.org.tw/en/pfen/33-8318.html)

102. Frank Jüris, "Security implications of China-Owned critical infrastructure in the European Union," *European Parliament, Directorate-General for External Policies of the Union*, June 23, 2023, page 26. (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf)

103. Henrique Almeida and Anabela Reis, "Portugal Agrees to Sell REN Stake for 592 Million Euros," *Bloomberg*, February 2, 2012. (https://www.bloomberg.com/news/articles/2012-02-02/portugal-agrees-to-sell-ren-stake-for-592-million-euros-1-); REN, "Energy in balance," accessed August 21, 2026, page 385. (https://www.ren.pt/media/hkmms4rx/ren-integrated-report-2024.pdf)

104. REN, "Energy in balance," accessed August 21, 2026, pages 39-40, 107, and 472-473. (https://www.ren.pt/media/hkmms4rx/ren-integrated-report-2024.pdf)

105. Moody's Ratings, "EDP, S.A.," April 20, 2026, page 3. (https://edp.com/sites/default/files/document/2026-04/Credit_Opinion-EDP-SA-Update-to-credit-20Apr2026-PBC_1477552.pdf); Sergio Goncalves, "Portugal's EDP, China Three Gorges change partnership terms," *Reuters*, December 10, 2021. (https://www.reuters.com/markets/deals/portugals-edp-china-three-gorges-change-partnership-terms-2021-12-10)

106. E-Redes, "EDP Distribuição prepares rebranding as E-REDES," August 13, 2020. (https://www.e-redes.pt/en/news/2020/08/13/edp-distribuicao-prepares-rebranding-e-redes)

107. REN, "Energy in Balance," accessed August 21, 2026, page 385. (https://www.ren.pt/media/hkmms4rx/ren-integrated-report-2024.pdf)

108. Karin Smith Jacobs, "Chinese strategic interests in European ports," *European Parliament*, February 27, 2023, page 2. (https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739367/EPRS_ATA(2023)739367_EN.pdf)

109. Ibid.

110. North Atlantic Treaty Organization, "The Hague Summit Declaration," June 25, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration)

111. North Atlantic Treaty Organization, "Strengthening NATO's eastern flank," June 17, 2026. (https://www.nato.int/en/what-we-do/deterrence-and-defence/strengthening-natos-eastern-flank)

112. North Atlantic Treaty Organization, "The Hague Summit Declaration," June 25, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration)

113. European Court of Auditors, "EU military mobility: Full speed not reached due to design weaknesses and obstacles en route," February 5, 2025, page 28. (https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf)

114. North Atlantic Treaty Organization, "The Hague Summit Declaration," June 25, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration)

115. Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), *Official Journal of the European Union*. (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1707498295481&uri=CELEX%3A02022L2555-20221227)

116. European Commission, "Joint Communication to the European Parliament and the Council on Military Mobility," November 19, 2025, page 9. (https://defence-industry-space.ec.europa.eu/document/download/c3d3067c-6d9a-4f95-9a69-4dd99c340188_en?filename=Action%20plan%20on%20military%20mobility%202.0.pdf)

117. Hannah Ahamad Madatali and Lucia Torlai, "Revision of the EU Foreign Direct Investment Screening Regulation," *European Parliamentary Research Service*, July 22, 2024, page 1. (https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762844/EPRS_BRI(2024)762844_EN.pdf); Consolidated text: Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, *Official Journal of the European Union*. (https://eur-lex.europa.eu/eli/reg/2019/452/2021-12-23/eng)

118. Raphaël Glucksmann, "Revision of the foreign direct investment (FDI) screening regulation," *European Parliament, Legislative Train Schedule*, June 20, 2026. (https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-revision-of-the-fdi-screening-regulation)

119. Regulation (EU) 2026/1386 of the European Parliament and of the Council of 17 June 2026 on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452, *Official Journal of the European Union*. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1386)

120. Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), *Official Journal of the European Union*. (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1707498295481&uri=CELEX%3A02022L2555-20221227)

121. U.S. Department of Transportation, "Prohibited Platforms," accessed August 21, 2026. (https://www.transportation.gov/mission/office-secretary/office-chief-information-officer/prohibited-platforms)

122. North Atlantic Treaty Organization, Movement Coordination Centre Europe, "Movement Coordination Centre Europe: MCCE at a Glance," May 21, 2024, page 2. (https://mcce-mil.org/wp-content/uploads/2024/05/mcce-at-a-glance-0524.pdf)

123. Aubrey Irvin and Rhonda Pitt, "Surface Exchange of Services: Coalition building while multiplying transportation capabilities," *U.S. Army*, August 11, 2021. (https://www.army.mil/article/249277/surface_exchange_of_services_coalition_building_while_multiplying_transportation_capabilities)

124. North Atlantic Treaty Organization, Movement Coordination Centre Europe, "Movement Coordination Centre Europe: MCCE at a Glance," March 15, 2024, page 2. (https://mcce-mil.org/wp-content/uploads/2024/04/mcce-at-a-glance-0324.pdf)

125. "The EATC," *North Atlantic Treaty Organization, European Air Transport Command*, accessed July 8, 2025. (https://eatc-mil.com/who-we-are/the-eatc)

126. North Atlantic Treaty Organization, "Rapid Air Mobility," June 21, 2022. (https://www.nato.int/en/what-we-do/deterrence-and-defence/rapid-air-mobility)

127. Community of European Railway and Infrastructure Company, "Military Mobility on rail: ensuring security and defence readiness 2030 and beyond," accessed August 21, 2026, page 1. (https://www.cer.be/images/publications/facts-figures/251209_CER_Factsheet_Military_Mobility.pdf)

128. European Commission, "Commission Statement by Commissioner Kubilius during the plenary session of the European Parliament: 'Serious threats to aviation and maritime transport from Global Navigation Satellite System Interference: urgent need to build resilience against spoofing and jamming,'" September 9, 2025. (https://ec.europa.eu/commission/presscorner/detail/en/speech_25_2072)

129. "Baltic–Nordic report: Russian GNSS interference disrupted almost 123,000 flights in four months," *EU Today* (UK), September 8, 2025. (https://eutoday.net/russian-gnss-interference-disrupted-123000-flights)

130. European Commission, "Commission Statement by Commissioner Kubilius during the plenary session of the European Parliament: 'Serious threats to aviation and maritime transport from Global Navigation Satellite System Interference: urgent need to build resilience against spoofing and jamming,'" September 9, 2025. (https://ec.europa.eu/commission/presscorner/detail/en/speech_25_2072)

131. European Commission, "EU GOVSATCOM: Securing Europe, from ground to space," February 26, 2026. (https://defence-industry-space.ec.europa.eu/eu-govsatcom-securing-europe-ground-space-2026-02-26_en)

132. European Union Agency for Cybersecurity, Press Release, "Cyber Europe 2026: All Eyes on the EU's Collective Response and Resilience," June 11, 2026. (https://www.enisa.europa.eu/news/cyber-europe-2026-all-eyes-on-the-eus-collective-response-and-resilience)

133. "The State of the Cybersecurity Workforce," *ISC2*, October 23, 2024. (https://www.isc2.org/Insights/2024/10/Cybersecurity-Workforce-INSIGHTS-October-2024)

134. "Inside Europe's Cybersecurity Skill Shortage in 2026," *Netgroup*, accessed August 21, 2026. (https://netgroup.com/blog/cybersecurity-skill-shortage)

135. European Union Agency for Cybersecurity, "NIS Investments 2025," December 8, 2025, page 12. (https://www.enisa.europa.eu/sites/default/files/2026-02/NIS%20Investments%202025%20-%20Main%20report.pdf)

136. "Inside Europe's Cybersecurity Skill Shortage in 2026," *Netgroup*, accessed August 21, 2026. (https://netgroup.com/blog/cybersecurity-skill-shortage)

137. Kirsti Melesk, Eve Mägi, Kaupo Koppel, and Aleksandr Michelson, "Labour force and skills needs in cyber security in Estonia. Main conclusions," *Praxis*, accessed August 21, 2026, page 1. (https://www.praxis.ee/uploads/2018/04/Küberturbe-uuring.-Lühikokkuvõte_eng.pdf)

138. European Union Agency for Cybersecurity, "NIS Investments 2025," December 8, 2025, page 12. (https://www.enisa.europa.eu/sites/default/files/2026-02/NIS%20Investments%202025%20-%20Main%20report.pdf)

139. Ibid.

About the Author

Jiwon Ma is a senior policy analyst at FDD's Center on Cyber and Technology Innovation, where she contributes to the CSC 2.0 project. She is the lead author of CSC 2.0's annual assessment of the implementation of Cyberspace Solarium Commission recommendations. Jiwon received a master's degree in international affairs from Columbia University's School of International and Public Affairs and a B.A. in global studies and education from Lesley University.

ACKNOWLEDGEMENTS

The author would like to thank the experts from government, U.S. military, allied institutions, and the private sector who provided invaluable insights and feedback throughout the research and writing process. This report is stronger for their contributions, although any errors of fact or judgment are the author's alone. The author is also grateful to David Adesnik, Tzvi Kahn, Grant Wishard, and David May for their rigorous edits, and to Daniel Ackerman and Liz Sunshine for the design and production of this report.

Cover illustration by Liz Sunshine.

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Mike J. Gallagher, Former U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Tom Fanning, Former Chairman, President, and CEO of Southern Company

Chris Inglis, Former National Cyber Director

Jim Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

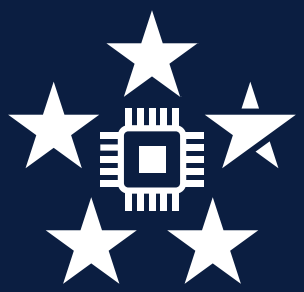
Samantha F. Ravich, Distinguished Fellow at the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Ben Sasse, Former U.S. Senator for Nebraska

Suzanne Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partners

FDD | CCTI | CMPP



CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission