CSC 2.0

Strengthening NATO Through Military Mobility and Critical Infrastructure Cybersecurity

By Jiwon Ma

Executive Summary

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. 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.

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.