SPECIAL REPORT · NATO / RUSSIA / EUROPEAN SECURITY

NATO's New Defence Investment Baseline and the Security Implications for Europe-Linked Organisations

Author: Benjamin Traunecker / SF Custos Global · **Reviewed to:** 2026-07-06

NATO's New Defence Investment Baseline and the Security Implications for Europe-Linked Organisations

Executive summary

NATO's 2025 Hague Summit changed the baseline for European security planning. The Alliance did not simply restate the older 2% defence-spending target. Heads of State and Government committed Allies to invest 5% of GDP annually by 2035, split between 3.5% for core defence requirements and up to 1.5% for defence- and security-related expenditure such as critical infrastructure protection, network defence, civil preparedness, resilience, innovation and defence industrial capacity.

For organisations with exposure to Europe, this is more than a military budget issue. NATO is signalling that Russia remains a long-term threat to Euro-Atlantic security and that deterrence now depends on forces, readiness, infrastructure, industrial output and resilience. Companies should expect a more defence-oriented operating environment across parts of Europe: more military mobility, more host-nation support activity, stronger cyber and infrastructure protection requirements, higher political attention to supply chains, and tighter scrutiny around strategic industries.

The 2025 Hague Declaration also points toward the next NATO meeting in Türkiye in 2026. That matters because the period between The Hague and Türkiye is likely to be treated by Allies, analysts and industry as an implementation window. The question will not be whether NATO leaders agreed a new target; that is now on record. The question will be whether national plans, budget paths, infrastructure upgrades and industrial capacity can move quickly enough to match the threat picture.

Russia remains the main driver behind this shift. NATO's 2024 Washington Summit Declaration described Russia as the most significant and direct threat to Allied security. The Hague Declaration narrowed the summit message but reinforced the same direction: Russia is treated as a long-term Euro-Atlantic challenge, not a short crisis that can be waited out. That has implications for organisations operating near the Alliance's eastern flank, in defence-adjacent sectors, in logistics, energy, cyber, transport, aviation, maritime services and executive travel.

The Middle East and Iran are not the centre of the Hague text, but they remain part of the wider strategic picture. NATO's 2024 declaration stated that instability in Africa and the Middle East directly affects Allied security and that Iran's destabilising actions affect Euro-Atlantic security. For companies, that means European security planning cannot be separated from pressure on air routes, maritime corridors, energy costs, cyber threats and diplomatic risk linked to wider geopolitical competition.

SF Custos Global assessment: The main risk for companies is not an immediate NATO-related crisis. It is a structural shift in the European operating environment. Defence spending, critical infrastructure protection, cyber resilience and civil

preparedness are moving from policy background to business-relevant planning factors. Organisations should treat the period before the 2026 Türkiye meeting as a useful window to review travel exposure, supply chains, crisis thresholds and executive movement planning in Europe and adjacent regions.

What matters now

- **The spending baseline has changed.** NATO's 5% commitment by 2035 creates a new benchmark for national defence planning, industrial capacity and infrastructure readiness. Companies should expect defence and resilience to remain high on the European policy agenda.
- **The 5% figure is broader than military procurement.** The Hague Declaration separates 3.5% for core defence requirements from up to 1.5% for defence- and security-related expenditure, including critical infrastructure, network defence, civil preparedness and resilience. This brings corporate operating environments closer to national security planning.
- **Russia remains the organising threat.** NATO's official language treats Russia as a long-term security challenge. This supports continued attention to the eastern flank, high-readiness forces, air and missile defence, logistics, reinforcement routes and resilience against hybrid activity.
- **The 2026 Türkiye meeting becomes an implementation checkpoint.** The Hague text says Allies look forward to their next meeting in Türkiye in 2026. That creates a natural review point for whether defence-spending plans, industry commitments and resilience measures are moving from declaration to execution.
- **Expert commentary reinforces the pressure on implementation.** Public defence-policy discussion around the summit has focused less on the existence of the threat and more on whether Allies can meet the new spending, readiness and industrial requirements. That commentary should be treated as analytical context, not as a substitute for official NATO sources.

Current operating picture

The Hague Summit took place on 24–25 June 2025 in the Netherlands. NATO described the summit purpose as addressing challenges facing the Alliance and further strengthening deterrence and defence. The official declaration reaffirmed Article 5, the transatlantic bond and the need to protect the Alliance's population, freedom and democracy.

The key shift was financial and structural. Allies committed to invest 5% of GDP annually by 2035 on core defence requirements and defence- and security-related spending. The declaration states that this investment is intended to provide the forces, capabilities, resources, infrastructure, warfighting readiness and resilience needed to deter and defend. It also requires Allies to submit annual plans showing a credible incremental path toward the 3.5% core-defence component.

That structure matters. The 3.5% component is tied to NATO's agreed definition of defence expenditure and Capability Targets. The additional 1.5% category is wider: critical infrastructure, network defence, civil preparedness, resilience, innovation and defence industrial base. This makes the commitment more relevant to companies than a conventional military-budget figure. It points toward ports, railways, airports, energy infrastructure, data networks, procurement chains, industrial facilities, cybersecurity and civil contingency systems.

The 2024 Washington Summit Declaration gives the wider background. NATO then stated that Russia's full-scale invasion of Ukraine had shattered peace and stability in the Euro-Atlantic area and that Russia remained the most significant and direct threat to Allied security. It also highlighted terrorism, instability in Africa and the Middle East, Iran's destabilising actions, China's coercive policies, the Russia-China strategic partnership, and hybrid, cyber and space threats.

The Hague Declaration is shorter, but it sits on top of that threat picture. It names the long-term threat posed by Russia and the persistent threat of terrorism. It also reiterates enduring support to Ukraine and allows direct contributions to Ukraine's defence and defence industry to count toward Allies' defence spending. That creates a link between national budget pathways, Ukraine support, defence industrial output and NATO's future readiness.

For organisations, the practical issue is exposure. A company does not need to be part of the defence sector to be affected. A logistics provider may face more military movement across road, rail or port networks. An energy company may see stronger state attention to resilience and redundancy. A technology company may be pulled into network-defence or critical-infrastructure expectations. A firm moving executives through eastern Europe may see more frequent changes in airport, route or local security conditions when tensions rise.

The 2026 Türkiye meeting is therefore not just a diplomatic date. It is a visible marker for implementation. By then, governments will face questions about annual plans, budget credibility, industrial capacity, support to Ukraine and whether resilience measures are moving at the speed implied by the Hague commitment.

Key risk mechanisms

1. Defence spending becomes an operating-environment issue

The new spending commitment will shape procurement, industrial demand and political expectations. Defence-related sectors may benefit from sustained demand, but they may also face tighter compliance, export-control, sanctions and supply-chain scrutiny. Non-defence companies can still be affected if they operate infrastructure, logistics, energy, telecommunications, transport or technology assets that national authorities classify as relevant to resilience.

2. Eastern Europe remains a higher-attention environment

NATO's focus on Russia and reinforcement of collective defence keeps the eastern flank politically and militarily relevant. The main company-level risk is not a single uniform threat across the region. It is a combination of military activity, cyber pressure, information operations, airspace sensitivity, border restrictions and local security posture changes that can affect travel, site access and contingency planning.

3. Critical infrastructure and cyber resilience move closer together

The Hague text explicitly places critical infrastructure protection and network defence inside the 1.5% defence- and security-related category. That is a strong signal. Cybersecurity, physical security, industrial continuity and civil preparedness are no longer separate management lanes in a crisis. For companies, the useful question is whether one disruption could affect data, movement, power, fuel, personnel and communications at the same time.

4. Defence industrial capacity becomes a strategic bottleneck

NATO's declaration commits Allies to expand transatlantic defence industrial cooperation, eliminate defence trade barriers and strengthen the defence industrial base. This reflects a wider problem: deterrence depends not only on political commitments but also on production capacity, munitions, repair cycles, transport, skilled labour and reliable supply chains. Companies in dual-use or adjacent sectors may be drawn closer to national security priorities.

5. Middle East pressure remains a second-order European risk

Iran and the Middle East are not the centre of the Hague Declaration, but NATO's 2024 official language makes clear that instability in the Middle East and Iran's actions affect Euro-Atlantic security. For organisations, this appears through energy exposure, maritime risk, air-route changes, diplomatic tension, cyber activity and personnel risk in regional hubs. European security planning should therefore not treat Russia and the Middle East as completely separate files.

Implications for organisations

Companies operating in Europe: The practical task is to identify where NATO's defence and resilience agenda intersects with business operations. That may include logistics nodes, rail corridors, port access, aviation routes, energy supply, data centres, cloud dependencies, subcontractors, staff movement and executive travel.

Defence-adjacent and dual-use suppliers: Companies supplying transport, communications, cyber, energy, engineering, manufacturing or logistics services may face stronger public-sector demand and stronger scrutiny at the same time. Contracting, export controls, security clearances, sanctions exposure and supply-chain transparency should be reviewed before new demand accelerates.

Organisations with eastern-flank exposure: Travel and site-visit planning should be more sensitive to military exercises, border measures, cyber incidents, demonstrations linked to the war in Ukraine, and diplomatic advisories. The risk is not constant across Poland, the Baltic states, Romania, Bulgaria, Slovakia or Finland, but the region will remain closer to NATO's deterrence posture than western European business hubs.

Boards and risk owners: NATO's 5% commitment is a strategic signal that Europe is planning for a harder security environment. Boards should not read it only as a government budget story. It affects resilience expectations, insurance questions, procurement priorities, cyber posture and the credibility of crisis plans.

Executive protection and travel teams: Senior movement into defence-policy events, government districts, energy sites, cyber conferences, logistics nodes or eastern-flank locations should be planned with a more political risk-aware lens. The most useful triggers are not only protests or violent incidents, but also sudden government advisories, airspace changes, cyber warnings, diplomatic escalation and military movement restrictions.

Watch indicators

- National budget plans showing whether Allies can move credibly toward the 3.5% core-defence component and the wider 5% annual commitment by 2035.
- NATO or national guidance on what will count under the 1.5% defence- and security-related category, especially for critical infrastructure, cyber and civil preparedness.
- Announcements on military mobility, port, rail, road, airbase and logistics upgrades in eastern and northern Europe.
- New procurement, industrial cooperation or defence-trade measures linked to NATO capability targets and Ukraine support.
- Russian military, cyber or hybrid activity that targets eastern-flank states, defence industry, undersea infrastructure, energy networks or transport systems.
- Middle East escalation affecting energy pricing, air routes, maritime corridors, diplomatic facilities or cyber threat levels in Europe-linked business environments.
- The agenda and preparatory statements ahead of NATO's 2026 meeting in Türkiye.

Recommended actions

Within 30 days: Map company exposure to NATO-linked operating environments: eastern-flank travel, logistics routes, energy dependency, strategic suppliers, critical infrastructure, cyber networks and executive movement to political or defence-related events.

Within 60 days: Review whether crisis thresholds are specific enough. A useful threshold should say who can delay travel, reroute personnel, suspend site visits, escalate cyber monitoring, notify leadership or activate alternative logistics when a

NATO-related or Russia-linked indicator changes.

Within 90 days: Reassess supplier and infrastructure dependencies that could be affected by defence spending, sanctions, procurement pressure, cyber risk or military mobility. This is especially relevant for companies with transport, technology, energy, manufacturing, communications or logistics exposure.

Selected sources

- NATO, *The Hague Summit Declaration*, 25 June 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration
- NATO, *Defence investment and NATO's 5% commitment*. https://www.nato.int/en/what-we-do/introduction-to-nato/defence-expenditures-and-natos-5-commitment
- NATO, *2025 NATO Summit in The Hague – Overview*. https://www.nato.int/en/news-and-events/events/2025/6/overview---2025-nato-summit-in-the-hague
- NATO, *Washington Summit Declaration*, 10 July 2024. https://www.nato.int/cps/en/natohq/official_texts_227678.htm
- Foundation for Defense of Democracies public expert commentary by RADM (Ret.) Mark Montgomery and associated guests on NATO summit issues, reviewed as analytical context only.

Method note

This report is based on official NATO source material reviewed up to 6 July 2026 and analytical assessment by SF Custos Global. Public expert commentary was used only as context for the policy debate and was not treated as an independent factual source. This report does not replace legal, insurance, sanctions, travel-security or country-specific professional advice.