

European reading of NSS dynamics, cyber posture, and market effects

For discussion – non-paper

Scope

This note provides an informal European strategic reading of current US National Security Strategy (NSS) dynamics and emerging cyber posture trends based on the National Cyber Security Policy (NCSP) Draft. It focuses on *cyber offensive capabilities*, *market-structuring effects*, and the fact that the current US strategic trajectory is *poorly received across Europe*, a reality that must now be treated as a strategic variable in its own right.

This is not a critique of US intentions nor EU position. It is an honest assessment of political reception, institutional sensitivity, and systemic consequences on the European side of the alliance of what we call **#TheReset strategy of the US**.

- Europe can afford a reset, it cannot accept a reboot

Europe can afford a reset. It cannot accept a reboot. Recent reporting by Bloomberg News, including access to a draft of the forthcoming US cyber strategy, confirms a doctrinal and operational shift regarding the role of the private sector in cyber offensive capabilities.

This shift opens a moral and political debate that Europe will not be able to avoid. It raises fundamental questions about *the legitimacy of the use of force in cyberspace*, *the delegation of this responsibility to private actors*, and *the boundary between* what is technically possible and what is politically and democratically acceptable.

From a European perspective, this issue is extremely sensitive. While certain capabilities exist, and while some openness may be found in parts of the private sector, this remains a minority position. The dominant European doctrine continues to hold that defence and security fall primarily under the responsibility and monopoly of the State, a position to which this note explicitly aligns.

Seen from Europe, the emerging weaponisation of the private sector is clearly disruptive, and likely unacceptable without strong public control, political accountability, and democratic oversight.

- Strategic implication for the transatlantic relationship

The issue is not alliance compatibility. It is calibration, sovereignty, and honesty.

The transatlantic relationship remains central. But as cyber posture, private-sector weaponisation, and market integration deepen, poor reception in Europe risks becoming self-reinforcing if left unaddressed. The danger is not open rupture.

It is progressive, silent misalignment.

EUROPEAN READING OF NSS DYNAMICS, CYBER POSTURE, AND MARKET EFFECTS

Executive Summary

Key message : Europe can afford a reset, It cannot accept a reboot of its political, legal, and democratic foundations. The current US strategic trajectory, as reflected in the NSS and emerging cyber doctrine, is poorly received across Europe. This reception is not a misunderstanding or a semantic issue, but a negative political response that has now become a strategic variable in itself.

1. NSS as a power-structuring framework : While still often read in Europe as a rhetorical or ideological document, the NSS increasingly functions as a power-structuring framework. It confirms the integration of technology, economy, and security, the redefinition of alliances as conditional ecosystems, and the normalization of persistent competition, particularly in cyberspace. This reading remains insufficiently internalized at political and regulatory level in Europe.

2. Shift toward permanent cyber posture : US cyber doctrine is evolving from exceptional use toward a permanent posture, with increasing integration of private-sector actors into national cyber capabilities. The boundaries between defence, offence, and economic security are blurring. While framed as efficiency and scale, this shift generates significant political, legal, and governance consequences for Europe.

3. Private-sector weaponisation and OCAAS : The normalization of cyber offensive capabilities leads to models resembling Offensive Capacities As A Service (OCAAS). This raises European concerns regarding legitimacy, delegation of sovereign responsibilities, political control, legal accountability, and escalation management. From a European standpoint, defence and security remain primarily a State responsibility, making private-sector weaponisation highly sensitive without strong public control.

4. Market structuring and #Market5% : Beyond doctrine, the NSS contributes to market structuring. Cyber and defence capabilities are increasingly bundled into integrated service stacks dominated by US-embedded actors. The push toward a 5% spending target risks creating a de facto captive market for US technologies under NATO standards, reflecting a commercial strategy as much as a security one.

5. Russia and China as strategic levers : China acts as a systemic accelerator, justifying expanded cyber posture and lowered thresholds, while challenging European norms. Russia functions as a functional and economic catalyst. By being framed as more “manageable”, strategic pressure on Europe increases mechanically, reinforcing the imperative for European defence spending and procurement.

Strategic implication : The transatlantic relationship remains central. The issue is not alliance compatibility, but calibration, sovereignty, and honesty. If Europe’s negative reception is ignored, it risks becoming self-reinforcing, leading not to rupture but to progressive, silent misalignment.

Bottom line - This note does not question US intentions. It highlights a political reality: the US strategy is poorly received in Europe, and that reception now shapes outcomes. Addressed early, this tension can be managed. Ignored, it becomes structural

1. The NSS: between rhetoric and power structuring

From a European strategic standpoint, the NSS is still largely read as a rhetorical or ideological document. Only a limited number of actors currently interpret it as a power-structuring framework with concrete consequences for allies.

Yet the NSS confirms three major evolutions.

First, the full integration of technology, economy, and security. Cyber, cloud, AI, data, semiconductors, and digital infrastructure are no longer adjacent to national security. They are treated as core instruments of power.

Second, the redefinition of alliances as conditional ecosystems. Allies are increasingly assessed through operational contribution, interoperability, speed of execution, and capacity absorption, rather than political alignment alone.

Third, the normalisation of persistent competition, particularly in cyberspace. Conflict is no longer episodic. It is continuous, distributed, and embedded within economic and technological systems.

In Europe, this reading exists, but it is far from being fully internalised at political and regulatory level.

2. Cyber posture evolution: permanence over exception

Ongoing US cyber policy work and doctrinal discussions point to a clear shift. Cyber is no longer framed as an exceptional capability activated in crisis. It is becoming a baseline, permanent posture, integrated across military, intelligence, economic, and diplomatic layers.

Three dynamics are particularly visible:

- the move toward persistent cyber presence,
- the growing functional integration of the private sector (cloud providers, cybersecurity firms, data platforms) as de facto components of national cyber posture,
- the progressive blurring of boundaries between cyber defence, cyber offence, and economic security.

Internally, this evolution is framed in terms of efficiency and scale.

Externally, it generates significant political, legal, and market consequences for allies.

Two key takeaways from this page

- The NSS signals a shift from values-based alignment to power-based alliances, where contribution, speed, and operational capacity now define partnership credibility.
- US cyber strategy is moving from episodic response to permanent posture, embedding cyber, private actors, and economic security into a continuous competition framework with direct consequences for allies.

3. Market-structuring effects and the emergence of OCAAS

The normalisation of cyber offensive posture produces direct market-structuring effects. Cyber capabilities are increasingly bundled into integrated service stacks combining cloud infrastructure, AI-driven analytics, threat intelligence, security operations, and resilience and recovery services.

This leads de facto to models akin to Offensive Capacities As A Service (OCAAS), even if the term itself is not formally used. The effects are structural:

- concentration around actors embedded in US security ecosystems,
- strong path dependency for allies,
- reduced contestability for non-aligned or late-entry actors,
- progressive normalisation of US technical standards as operational defaults.

From a European perspective, this is first and foremost a political issue related to values and legitimacy, which is likely to translate rapidly into a strategic economic and sovereignty issue. The prospect of such capabilities being offered to allied or partner governments raises central questions of political control, legal responsibility, escalation management, and democratic legitimacy.

4. The 5% Market, the blind spot of the debate

The core dynamic likely lies here. By pushing Europeans toward a 5% defence spending target, the United States contributes to the creation of a de facto captive market for its defence and technology industries, increasingly presented as NATO standards.

This is a commercial strategy as much as a security one. Budgetary pressure becomes an instrument coherent with America First, at a time of supply-chain reconfiguration and intensified global competition.

This reading does not negate political or civilisational dimensions. It completes them by revealing the silent architecture of a new transactional order.

If Russia were to enter Estonia tomorrow, Europeans and Americans would stand together. That reality must not be denied. But strategic analysis requires looking beyond the immediate.

The issue is also these 5%, and the market they create.

Two key takeaways from this page

- The normalization of cyber offensive posture is quietly structuring a new market, where offensive capabilities are bundled as services (OCAAS), concentrating power, standards, and dependency.
- The 5% defence spending target is not only a security issue but a market-creation mechanism shaping a de facto captive transatlantic market under NATO standards, and already anticipated and targeted by US private sector.

5. Key European perception signal: hostility as a strategic variable

Regardless of stated intentions, current NSS-driven dynamics are increasingly perceived across Europe as hostile.

This perception does not stem from anti-American sentiment. It results from the lived experience of structural effects that are seen as:

- constraining,
- asymmetrical,
- and difficult to reverse once embedded.

This is particularly acute in cyber, cloud, market structuring, and normative space. In political reality, intention matters less than effect. When effects are experienced as a reduction of strategic room for manoeuvre, perception shifts from cooperation to coercion, even if coercion is not intended. This perception has become a political and regulatory variable in its own right, shaping debates, legislative reflexes, and alliance narratives.

Ignoring it increases systemic risk.

Acknowledging it enables policy management.

6. Values and domestic constraints: the core friction point

European systems operate under constitutional and political constraints that differ structurally from those of the United States. These include:

- strong proportionality requirements,
- separation between civilian, military, and intelligence functions,
- protection of encryption,
- accountability and judicial oversight,
- limits on the normalisation of permanent surveillance.

As cyber conflict becomes persistent, *tension grows between US operational logic and European domestic acceptability*. This is not framed in Europe as a moral critique of US choices.

It is experienced as a governance stress test, with direct implications for policy sustainability and democratic legitimacy. If unmanaged, this tension risks producing silent divergence at implementation level, rather than explicit political disagreement.

Two key takeaways from this page

- The European perception of the US strategy as hostile has become a strategic variable in its own right, regardless of US intentions.
- The core transatlantic friction lies in European legal and democratic constraints, rather than in a moral or ideological disagreement.

7. China as an accelerator of posture and thresholds

China functions as a systemic accelerator.

As a competitor combining scale, state integration, and technological depth, it serves both as:

- a strategic benchmark,
- and a justification for expanded cyber posture and lowered thresholds.

From Europe, this logic is largely understood. However, it also creates a risk of alignment by contrast, whereby thresholds justified through comparison with China progressively reshape acceptable norms, even within systems that explicitly reject the Chinese model.

This generates internal political pressure that EU institutions cannot ignore.

8. Russia as a functional catalyst and economic lever

Russia plays a different, but equally central role.

In cyber terms, it functions as a persistent, credible, yet economically non-competitive adversary.

This makes it an effective catalyst for:

- sustained threat perception,
- budgetary justification,
- urgency framing,
- accelerated procurement and deployment.

More importantly, the NSS subtly attenuates the centrality of the Russian threat in discourse. This is not appeasement. It is a political move that reshapes the hierarchy of perceived risks.

By portraying Russia as “manageable” by Washington, strategic pressure on Europe increases mechanically. Russia has not changed its nature, but the way it is framed conditions European reactions, particularly on the Eastern flank.

Closing observation

This note is shared in the spirit of strategic honesty.

The NSS and emerging US cyber posture display internal coherence. They also generate second-order effects that are now politically salient and negatively received across Europe. That reception may be unintended. But it is real.

And in strategy, reception shapes outcomes. Addressed early, this tension can be managed. Ignored, it becomes structural.