

LESSONS FROM SPAIN

European Resilience: Cyber, Defense & Cloud as Strategic Infrastructure

Jacobo Ramos Folch

Aspen Institute España | Madrid Roundtable, 30 September 2026

INTERNATIONAL PARTNERS
aspen institute

aspen institute españa

Aspen Institute Germany

aspen institute central europe

About the Project

The resilience of modern states increasingly rests on the interplay between cyber capabilities, defense, and cloud infrastructure. These domains can no longer be viewed in isolation: secure digital systems underpin military readiness, trusted cloud services enable both government and business, and cyber resilience has become a prerequisite for economic competitiveness.

Against this background, three members of the Aspen International Partners network — Aspen Institute Central Europe, Aspen Institute Germany, and Aspen Institute España — with the support of Microsoft and in collaboration with Aspen Institute Romania, launched a cross-border initiative aimed at examining and strengthening European resilience across the interconnected domains of cyber, defense, and cloud infrastructure.

As part of the project, four European Resilience Roundtables were convened in Warsaw, Berlin, Madrid, and Brussels, bringing together senior representatives from government, defense institutions, industry, and the broader policy community in each country to examine national resilience challenges and identify lessons relevant at the European level. The insights generated across the four roundtables are captured in a series of European Resilience Reports presented to key EU stakeholders.

The Madrid roundtable, organized by Aspen Institute España on September 30, 2026, with the support of Microsoft, explored the changing relationship between technology, cybersecurity and conflict, alongside the industrial capabilities required to strengthen European security and defense. This report captures the reflections and conclusions developed during the roundtable, with the intent to inform both Spanish national policy discussions and the broader European Resilience report series.

LESSONS FROM SPAIN

European Resilience: Cyber, Defense & Cloud as Strategic Infrastructure

Jacobo Ramos Folch

Aspen Institute España | Madrid Roundtable, 30 September 2026

Executive Summary

The Spanish European Resilience Roundtable examined how Europe can protect its security, prosperity and democratic institutions amid accelerating technological change and geopolitical uncertainty.

Held in Madrid on 30 September 2026 and organized by Aspen Institute España and supported by Microsoft, the discussion brought together perspectives from government, industry, academia and the wider policy community. It considered cybersecurity, digital infrastructure and defense capabilities as interconnected foundations of technological resilience and strategic autonomy, with particular attention to the institutions and partnerships needed to translate strategic ambition into tangible results.

A central concern was the gap between Europe's recognition of its vulnerabilities and its capacity to address them. Regulatory frameworks and industrial programs must adapt to technological developments and evolving threats. Although assessments of Europe's capacity differed, the implementation challenge was clear: legislation must translate into effective policy, investment commitments must produce operational capabilities, and cooperation must deliver results beyond declarations.

Sovereignty and interdependence are closely connected. Access to secure international infrastructure and trusted partnerships can strengthen resilience by providing flexibility and continuity during crises. The challenge is to determine which dependencies Europe should accept, which it should reduce, and how these choices should balance economic costs and security requirements.



Defense modernization added an industrial dimension to the debate. Digital technologies, civilian innovation and military capabilities are increasingly converging, while defense platforms operate as parts of interconnected systems. These developments require faster program delivery, broader coordination across government and closer European cooperation. However, national industrial priorities, differing institutional cultures and concerns about sharing sovereignty in defense continue to shape the scope and pace of that cooperation.

Resilience also depends on public trust. Promoting secure and resilient cyber, defense and cloud infrastructure requires effective institutions. Their ability to deliver tangible results helps sustain confidence in democratic governance. Strengthening European resilience therefore means delivering security and technological progress while preserving trust in institutions and the values they are intended to protect.

Table of Contents

About the Project 2

Executive Summary 4

1. Introduction: Spain's Experience in the European Context 7

Technological Change in an Environment of Conflict 7

2. Resilience of Cyberspace 8

Emerging Technologies and Evolving Cyber Threats 8
Cybersecurity Beyond Governments and Large Companies 8
Regulatory Quality and Implementation 8

3. Resilience of Defense Digital Infrastructure and Defense Modernization 9

Industrial Capacity and Integrated Defense Systems 9
Strategic Innovation 9
Accelerating Programs and Broadening Implementation 9
Sharing Capabilities and Balancing Strategic Priorities 10
National Priorities and Innovation Cultures 10
The Human Consequences of Technological Development 10

4. Resilience of Cloud Infrastructure 11

Managing Dependencies and Strengthening Interdependence 11
Digital Infrastructure, Control and Continuity 11
Verifiable Commitments and Transparency 11
AI Safety and Predictable Regulation 12

5. Lessons Learned for European Coordination 13

Annex 15

1 Introduction: Spain's Experience in the European Context

The roundtable began with introductory remarks by Lisa Mónaco, President of Global Affairs at Microsoft. José Pardo de Santayana, retired Colonel of the Spanish Army, and Raül Blanco, Chief Executive Officer at SAPA, then opened the discussion. The session was moderated by Salomé Santos, lawyer, independent board member and Aspen España Fellow.

Spain's experience provided concrete reference points. The April 2025 power outage across the country and the September cybersecurity incident affecting Renfe, Spain's national rail operator, and Adif, its railway infrastructure manager, illustrated the importance of infrastructure reliability and data protection. Although distinct, these events brought the resilience of essential systems into public focus. Spain's military deployments abroad further highlighted its role in addressing shared security threats and contributing to European and allied defense.

These Spanish examples placed technological resilience within the broader context of Europe's industrial capabilities, governance and strategic autonomy. Regulatory quality, industrial capacity, public-private relationships and institutional credibility all affect preparedness. Europe's ability to shape its technological and security environment depends in part on whether its decision-making processes can keep pace with the developments they seek to govern.

Technological Change in an Environment of Conflict

Technological development is a constant feature of human history, but the expansion of digital technologies is increasing both the speed of transformation and the vulnerabilities societies must manage. As economic activity, public services and everyday life become more dependent on digital systems, resilience becomes increasingly important, even in a peaceful international environment.

Major conflicts intensify this process in three ways. First, war accelerates technological development and its application to military purposes, as illustrated by the growing militarization of space. Second, the priority given to winning a war makes international dialogue and agreement on technological safeguards more difficult. Third, cyberattacks become more frequent and technologically sophisticated, increasing pressure on the systems that support government, business and society.

The prospect of prolonged conflict in Ukraine and the Middle East reinforces the need for sustained preparedness. Europe faces an environment in which technological capabilities develop rapidly while the conditions for cooperation and collective restraint deteriorate.

2 Resilience of Cyberspace

Emerging Technologies and Evolving Cyber Threats

Cybersecurity preparedness must look beyond AI to quantum technologies and their implications for business, communications and relations between countries. Their development raises questions about governance and the future security of data.

Alongside these emerging challenges, the incident affecting Adif and Renfe reinforced the need to protect existing servers, systems and citizens' data. Agentic AI raises concerns about more capable cyber attacks, increasing the importance of transparency from technology companies about these risks and the safeguards available to public entities and private organizations. Non-state actors with access to advanced technologies but operating outside established regulatory frameworks present a further challenge.

Cybersecurity Beyond Governments and Large Companies

Even a small security gap in an interconnected system can have wider consequences. A phishing attack directed at an assistant rather than an organization's leadership illustrates how less protected individuals can expose wider systems. Preparedness must therefore extend beyond governments and large companies to society, SMEs and entrepreneurs.

Smaller actors are also sources of innovation, as illustrated by entrepreneurs developing drones in Ukraine. Their contribution raises questions about who should take responsibility for their preparedness and how they can be incorporated into a broader approach to security and defense.

Regulatory Quality and Implementation

Assessments of Europe's regulatory role differed. Regulation remains a European strength, but implementation speed and practical guidance on frameworks such as the AI Act remain concerns. Europe's capacity to retain influence over international rules was also questioned amid con-cerns about its geopolitical and technological position. China's capacity to innovate through state-directed initiatives challenged the assumption that regulatory leadership alone could sustain Europe's influence.

Regulatory quality depends on whether economic, budgetary and impact assessments meaningfully inform legislation and whether public authorities understand the practical conditions facing the private sector. Publishing a law is distinct from implementing public policy and verifying its results. The ambition to be a regulatory superpower, including expectations surrounding the 'Brussels effect', must therefore be assessed against implementation and outcomes.

Regulation should establish the rules of the game, while bureaucracy can obstruct their practical application. The active role played by governments in the United States and China also places public intervention within a wider international context. The challenge is to improve public-private relations and regulatory design while supporting innovation and competitiveness.

3 Resilience of Defense Digital Infrastructure and Defense Modernization

Industrial Capacity and Integrated Defense Systems

The war in Ukraine and changes in transatlantic relations have increased the urgency of strengthening Europe's capacity to provide for its security and defense. A strong, technologically advanced industrial base is essential to protecting Europe's prosperity, values and way of life. Strengthening defense serves to safeguard these foundations rather than promote a culture of violence.

Technologies are increasingly dual-use, moving rapidly from civilian applications into military capabilities. Drones illustrate this trend across air, land and sea, while the convergence of physical and digital domains makes AI, cybersecurity and communications central to defense policy. Defense modernization therefore requires thinking in terms of systems: frigates and future combat aircraft must connect with other capabilities on land, at sea, in the air and in space.

Strategic Innovation

Strategic innovation, involving major investments in AI and digital infrastructure, differs from tactical innovation developed in response to battlefield requirements. Ukraine illustrates the importance of flexibility and rapid adaptation. The effectiveness of European defense investment depends on how resources are used and whether investment reflects strategic assessments of threats, alongside the overall level of spending.

Defense investment also functions as industrial policy. National industrial approaches can intensify competition between states as well as companies, complicating European cooperation. Aligning industrial objectives with shared security requirements therefore remains a central challenge.

Accelerating Programs and Broadening Implementation

Common European industrial and technological programs, alongside national defense strategies, need faster implementation. Announcements and budgetary planning must translate into signed contracts and deployed capabilities. Long design, administrative and production cycles raise questions about whether traditional defense modernization programs remain fit for purpose in an environment of accelerating technological change.

Implementation cannot be left to a single ministry acting in isolation. The scale of resources and the breadth of technological requirements call for coordination across defense, industry, science and other areas of government. Spain's Strategic Projects for Economic Recovery and Transformation (PERTE) provided an example of coordination across government and the private sector for broader industrial and technological initiatives. Investment in AI, cybersecurity, communications and drones should contribute both to defense and to a more productive, technologically advanced economy, with social and regional benefits.

Sharing Capabilities and Balancing Strategic Priorities

Sharing defense competences at the European level offers an approach to cooperation without transferring them entirely. The shift from efficiency and globalization towards security and resilience can increase costs. Industrial policy must therefore consider broader strategic objectives alongside the competitiveness of individual companies and sectors.

European cooperation becomes necessary where technological requirements exceed national capabilities. Pooling resources and expertise can help countries develop capabilities they could not achieve individually. Spain was described as supportive of sharing competences and drawing on European funding to advance these priorities.

National Priorities and Innovation Cultures

Cultural differences and institutional continuity help explain Europe's defense fragmentation. The role of domestic defense industries in supplying national armed forces illustrates why countries retain their own capabilities even while participating in international partnerships. European defense companies remain competitors, and cooperation must accommodate the strategic purposes for which they exist.

Innovation also depends on institutional and cultural conditions. Silicon Valley cannot simply be replicated in Europe, where attitudes towards risk, failure and innovation differ. Likewise, proposals that work within the US Department of Defense may not translate directly to Spain's Ministry of Defense. Industrial and technological policy must account for the institutions and cultures through which ideas become capabilities.

The Human Consequences of Technological Development

The implications of technological change extend to freedom, truth, employment and human agency. The encyclical *Magnifica Humanitas* by Pope Leo XIV, included in the preparatory readings, provided a reference point for concerns about the potential dehumanization of society in the era of AI. Its appeal for demilitarization stood in tension with the growing emphasis on developing technologies to secure military advantage.

Remote warfare makes this tension particularly visible. Greater distance from an adversary can make the human consequences of violence less visible to those using force. The discussion drew on research on drone operators working from bases in the United States to examine the contrast between conducting operations remotely and operating in a conflict zone.

Reducing the exposure of a country's own personnel could also weaken an important restraint on decisions to wage war. Conducting operations with fewer soldiers at risk does not necessarily mean that warfare becomes less dangerous. Technological protection for those deploying force may coexist with greater risks for those exposed to it.

Increasing destructive capacity brings greater responsibility and a stronger need for regulation. Yet the incentives created by conflict can work against this objective: governments and other actors concentrate on how technology can help them prevail, while efforts to establish limits become harder to pursue. Henry Kissinger's call for dialogue between the major powers on artificial intelligence underscored the importance of addressing technological risks before they become more difficult to control.

4 Resilience of Cloud Infrastructure

Managing Dependencies and Strengthening Interdependence

Cloud infrastructure and international technology partnerships bring the relationship between sovereignty and interdependence into focus. Europe must assess which dependencies should be reduced, which can be accepted and what costs those choices entail. Greater control over critical capabilities must be considered alongside access to technologies, infrastructure and expertise that support competitiveness and preparedness.

These relationships are reciprocal. European reliance on US technology exists within wider patterns of investment, trade and commercial activity that also connect American companies to European markets. Interdependence can therefore provide a basis for cooperation and shared interests, while maintaining alliances remains important to the security of both sides.

International technology partnerships can also strengthen domestic capabilities. Investment in digital infrastructure can support developers, businesses, educators and students, enabling them to build products and retain economic value locally. Participation in international ecosystems can therefore contribute to Europe's technological capacity and ability to act.

The challenge is to distinguish dependencies that constrain Europe's choices from relationships that expand its capabilities. Resilience requires an assessment of where external reliance creates vulnerabilities, alongside an understanding of how trusted partnerships and shared infrastructure can help address them.

Digital Infrastructure, Control and Continuity

These relationships also depend on trust in technology providers and the control needed to sustain essential services during crises. Sovereignty encompasses control, choice and self-determination. Managing risk according to data sensitivity offers an alternative to assuming that isolation of data and systems necessarily provides greater security.

Access to secure global infrastructure can provide threat intelligence and continuity. The evacuation of Ukrainian government data to cloud infrastructure elsewhere in Europe illustrated how cross-border capabilities can help sustain services when physical assets are threatened. Cloud infrastructure therefore forms part of a country's capacity to act during crises.

Verifiable Commitments and Transparency

Reliance on digital infrastructure makes it necessary for technology providers to demonstrate that their commitments are being met. Alliances, common values, principles and actions must be supported by verifiable commitments across all layers of digital infrastructure. The Trusted Technology Alliance provided a reference point for transparent governance, secure supply chains, privacy and respect for the rule of law.

Translating these commitments into trust requires clarity about who verifies compliance and who oversees that verification. Transparency reports and information on AI

governance and safety practices provide a starting point. Depending on the circumstances, verification could involve self-attestation or regulatory obligations. Technology providers should be assessed against their demonstrable commitments and practices, rather than solely by their national origin.

AI Safety and Predictable Regulation

Verification also connects trust in technology providers with the regulation of AI safety. Regulation and innovation need not be mutually exclusive. High-risk AI uses require safeguards, and companies should test and improve products they believe unsafe before bringing them to market. These safeguards help establish the trust needed for adoption.

For these safeguards to support both safety and innovation, businesses also need clear and predictable requirements to plan investment, engineering and product development. The EU's right to regulate was recognized, while differing implementation timelines across its 27 member states remained a concern. The General Data Protection Regulation (Regulation (EU) 2016/679) provided a reference point for discussing common European requirements and their implications for technology providers. The broader challenge is to establish safeguards that build trust while giving businesses the clarity needed to innovate and invest.



5 Lessons Learned for European Coordination

From Diagnosis to Action

Across cybersecurity, defense and cloud infrastructure, the central implementation challenge is to translate Europe's understanding of its vulnerabilities into the institutional capacity to address them. While institutions debate and regulate, companies and other actors are making technological choices. Urgent action is needed to preserve Europe's ability to shape its technological future. Otherwise, it risks having to accept rules and systems established by others.

Europe's capacity to respond during crises, particularly the pandemic and vaccine deployment, provides grounds for optimism. The Letta and Draghi reports offered reference points for diagnosing Europe's challenges, while joint research, funding and industrial programs marked progress towards greater European cooperation in a historically national defense sector. The concern remains, however, whether implementation can keep pace with geopolitical events and technological developments.

Better regulatory assessments, faster contracting and more agile industrial programs are practical priorities. The relevant measure of progress is whether institutions can translate policy and resources into capabilities at the pace required by technological and geopolitical change.



Institutional Credibility and Coordinated Governance

The gap between regulation and delivery affects trust in institutions and the credibility of democratic governance. Ineffective implementation risks strengthening the appeal of alternative models that do not offer the same protection of civic freedoms. China's strategic planning, its position in critical-mineral supply chains and its ambitions in physical AI illustrate the pressure on Europe to translate policy into capabilities.

Governance structures must also address the interaction between technologies. Treating developments in blockchain, tokenization and financial markets separately from AI can leave their growing connections insufficiently understood. An overarching analytical perspective is needed to assess whether European and international governance structures can address the risks generated by competition between companies and countries.

The growing role of multinational companies raises further questions about the extent to which governments and societies should rely on private actors to address strategic vulnerabilities. Clear responsibilities are needed across national authorities, European institutions, NATO and the private sector.

Coordination must also reflect the connections between technologies and the distribution of capabilities across government, industry and society. This means addressing governance silos, strengthening preparedness among smaller actors and aligning public-private cooperation with security objectives. European programs offer opportunities to share costs and expertise but must accommodate national defense priorities and institutional cultures.

Effective policy delivery is ultimately linked to institutional trust. Europe's ability to protect its infrastructure, develop technological capabilities and establish credible oversight will shape confidence in its institutions. What is at stake is Europe's capacity to strengthen resilience at the pace required to protect its security and sustain trust in democratic governance.



Annex

List of Speakers

The following speakers participated in the Madrid roundtable on September 30, 2026:

José Pardo de Santayana
Colonel (ret.) of the Spanish Army

Raül Blanco
Chief Executive Officer, SAPA

Salomé Santos
Of Counsel, Regula; Aspen España Fellow

Lisa Mónaco
President of Global Affairs, Microsoft

About the European Resilience Project

In a joint effort, three members of the Aspen International Partners network — Aspen Institute Central Europe, Aspen Institute Germany, and Aspen Institute España — with the support of Microsoft and in collaboration with Aspen Institute Romania, launched a cross-border initiative aimed at examining and strengthening European resilience across the interconnected domains of cyber, defense, and cloud infrastructure. As part of the project, four European Resilience Roundtables were convened in Warsaw, Berlin, Madrid, and Brussels, bringing together senior representatives from government, defense institutions, industry, and the broader policy community in each country to examine national resilience challenges and identify lessons relevant at the European level. The insights generated across the four roundtables are captured in a series of European Resilience Reports presented to key EU stakeholders.

About the Aspen Institute España

Aspen Institute España is a non-partisan foundation, dedicated to promoting values-based leadership and dialogues on critical issues for the future of our society. The Institute offers a plural and balanced forum to debate issues of general interest among participants who aim to turn their ideas into action. Its activities are developed through programs, seminars and conferences on leadership, values and public policies.

More information about the Aspen Institute España:
https://aspeninstitute.es/en/

More information about the Aspen Institute International Partners:
https://www.aspeninstitute.org/programs/international-partners

Imprint

Publishers:
Aspen Institute España
Calle Princesa 18
28008, Madrid
Spain

The Aspen Institute
2300 N St NW, Suite 700
Washington, DC 20037
USA

Authors:
Jacobo Ramos Folch | International Policy Advisor & Visiting Professor (IE University; University of Navarra)

International Project Lead: Florentina Dumitru
Domestic Project Lead: Santiago Liniers

Design and Layout: Logan Richman | The Aspen Institute

Publication: November 2026

The Aspen Institute International Partners and Aspen Institute España wish to thank Microsoft for its support and partnership in this project.

The findings included in this report are drawn from the roundtable and expert discussions and do not necessarily reflect the official views of the Institute. All content was reviewed and verified by the project team. Event photography captured by Rodrigo Gilsanz Tejedor for Aspen España. Other report photography sourced via Unsplash.

INTERNATIONAL PARTNERS
aspen institute

aspen institute españa

Microsoft