orange™ Cyberdefense

Caught in the Cloud

Europe's cyber dilemma in a shifting world

Table of Contents

1. Introduction

The long peace

Security is an emotional state. It's the feeling we have – as people, businesses and societies – that we are safe. Safe to live our lives, raise our children, conduct our business and pursue our dreams.

The relative safety, peace and prosperity that much of the world has enjoyed since 1945 was not accidental. It emerged from the ashes of two world wars and the deliberate construction of a new global order. The United States, emboldened by victory and uniquely unscathed by war on its soil, set the terms of this new world.

Under the Marshall Plan, the U.S. financed the reconstruction of Europe, not only to prevent the spread of communism but to build reliable markets and allies. The Truman Doctrine pledged American support for free nations resisting subjugation, effectively laying the ideological foundation for containment and the West's post-war alliances. Together, these doctrines crystallized in the "Pax Americana": a U.S.-led global system of security, open trade, and technology leadership.

NATO, the Bretton Woods institutions, and a web of treaties and informal norms ensured that global trade routes stayed open, allies were protected, and American technology - military, economic, and digital - formed the spine of international progress. Trust in the system rested on the predictability of American power and the perception of shared interest.

This architecture was imperfect and often asymmetrical. But for many - including Europe - it delivered security, growth, and a sense of geopolitical certainty. For nearly eight decades, the U.S. guaranteed the sea lanes, policed the digital commons, and deterred hostile states.

Today's global efforts to counter cybersecurity threats are also largely built on the state of relative peace, global norms, open markets, stability and security that the Pax Americana created.

At the heart of this state of relative safety we have been benefiting from is an infrastructure of trust. For people to feel safe, they need to trust each other and trust the systems, processes and structures they depend on for their work and daily lives. It's obvious really. Nobody would feel safe in a car if they didn't trust the brakes, nobody would feel safe with an elected government if they didn't trust the election systems, and nobody will engage with digital platforms if they don't trust the security of the web. Digital systems run on trust.

The loss of trust in any essential system is like a cancer that spreads and will kill that system as surely as a bullet to the head. Trust is the sinew that glues any complex system together. Every security failure leads to a little bit of trust dying. Slowly, silently, but ever so surely, a system rots when security fails, and trust is allowed to die.

The long peace under Pax Americana provided a stable foundation, but that foundation is shifting. Europe's deep strategic dependence on U.S. cybersecurity capabilities - from intelligence and infrastructure to frameworks and funding - is now being tested by changing American priorities and a more volatile global landscape.

This paper discusses how those tectonic geopolitical changes are undermining trust, threatening the state of safety, and compelling European institutions to rethink national security architectures and approaches at every level.

The paper argues a moment of uncertainty is also a moment of opportunity: cybersecurity leaders in Europe can choose to retreat inward, or it can lead outward - by embracing interdependence not as a weakness, but as a mature and deliberate strategy for global security. This journey requires tactical resilience, strategic sovereignty, and a firm commitment to collaboration.

As elements in a global system, businesses worldwide are confronting the same threats and opportunities. Safety is an essential attribute of any functional system, and trust is the infrastructure on which safe systems must be built. Trust is a function of certainty, and certainty emerges from resilience. During uncertain times such as these, this fundamental calculus must influence business leaders in their risk assessments just as much as political leaders.

2. A fragile pillar: The CVE program and its funding crisis

In April 2025, the cybersecurity community was reminded of the fragility inherent in global reliance on U.S.-centric infrastructure. The Common Vulnerabilities and Exposures (CVE) program, managed by MITRE and funded by the U.S. government, came perilously close to shut down due to a lapse in contract renewal by the Cybersecurity and Infrastructure Security Agency (CISA)[1].

The CVE program is foundational to global cybersecurity, providing standardized identifiers for publicly known software vulnerabilities. Its sudden jeopardy sent shockwaves through the industry, acutely illustrating the risk of over-dependence on a single nation's resources for critical cybersecurity functions.

In response to the crisis, potential alternatives are emerging. The European Union Agency for Cybersecurity (ENISA) accelerated the development of the European Vulnerability Database (EUVD)[2], aiming to provide a regional counterpart to the CVE. Simultaneously, the CVE Foundation was announced, seeking to establish a globally governed vulnerability identification system less susceptible to national funding fluctuations[3]. The Global CVE Allocation System (GCVE) has also been suggested as a decentralized approach to vulnerability identification and numbering[4]. GCVE empowers independent GCVE Numbering Authorities (GNAs) to assign identifiers autonomously, enhancing flexibility and scalability while maintaining compatibility with the traditional CVE system. Eventually GCVE thus hopes to reduce reliance on centralized structures and promote a more distributed, resilient framework for vulnerability tracking.

Meanwhile we remain reliant on CVE and potential further disruptions. And even if the current CVE "crisis" is resolved, it's more than just a speedbump for the cybersecurity industry. Instead, it must be understood as only the most recent example of a broader, systemic erosion of the historical geopolitical status quo, with direct implications for trust within the cyber domain.

In the current era this deterioration in trust was most visibly illustrated when Edward Snowden disclosed extensive information about the National Security Agency's (NSA) global surveillance programs in 2013[5]. The revelations exposed the depth of US government surveillance and the involvement of major tech companies, leading to a significant erosion of public trust in both governmental and private sector data handling practices.

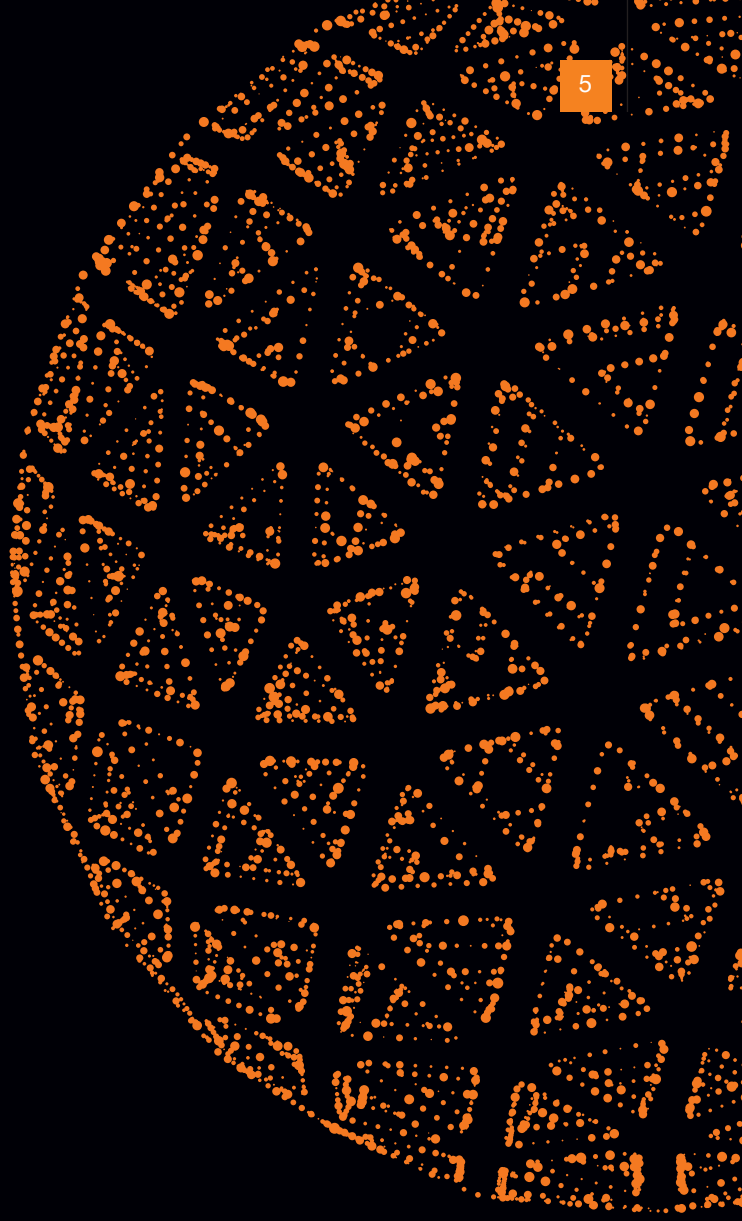
More fundamentally, however, Section 702 of the US Foreign Intelligence Surveillance Act (FISA) had already been enacted in 2008[6]. This provision authorizes the U.S. government to collect foreign intelligence without a warrant by targeting non-U.S. persons reasonably believed to be located outside the United States. The terrorist attacks on September 11 2001 had exposed significant gaps in U.S. intelligence capabilities, prompting the Bush administration to initiate the President's Surveillance Program (PSP), which authorized warrantless surveillance of international communications involving suspected terrorists. Following concerns about the legality and potential abuse of the PSP, congress passed the FISA Amendments Act[7]. Consequently, US agencies such as the NSA can potentially collect foreign intelligence by targeting non-U.S. persons by accessing data stored on U.S.-based cloud service providers, even if the data is stored on servers located in Europe.

Despite extensive critique and debate, the US Congress recently passed the "Reforming Intelligence and Securing America Act", which reauthorized Section 702 for a further two years, extending its validity until April 2026[8].

In 2018, the "Clarifying Lawful Overseas Use of Data (CLOUD) Act" technically allowed U.S. law enforcement to access data stored by U.S.-based companies, regardless of where the data is physically located (although it did also provide mechanisms for appeal)[9]. This extraterritorial reach has exacerbated concerns among international partners, particularly in the European Union, about conflicts with local data protection laws and the potential for unauthorized access to sensitive information.

The broad surveillance powers granted to US agencies have long been a point of contention in EU-U.S. data transfer agreements. Citing concerns over U.S. surveillance practices and the lack of adequate legal remedies for EU citizens, the European Court of Justice invalidated the Privacy Shield framework in 2020 (Schrems II)[10]. The EU-U.S. Data Privacy Framework was adopted in 2023 to address these issues, but some still argue that it may not fully resolve the underlying conflicts between U.S. surveillance laws and EU data protection standards. Further concerns about the definition of entities subject to surveillance, potentially including a wider range of service providers with access to communication data, have raised further concerns about the extent of U.S. surveillance and its impact on European data sovereignty[11].

In recent years the foundations of trust that cemented the US-led global order have begun to crack. Since there can be no safety without trust, repairing or replacing an infrastructure of trust must be a key concern for business leaders.



3. A shifting tide: Retrenchment and the Zeihan hypothesis

Peter Zeihan is an American analyst and geopolitical strategist. He argues (somewhat contentiously) that globalization - enabled and underwritten by U.S. security guarantees - is entering a period of systemic collapse[12]. According to Zeihan, America's shifting demographics, declining dependence on foreign trade, and political fatigue from costly overseas commitments, have been pushing the country toward isolation.

Under President Donald Trump these trends have become policy. The "America First" doctrine has led to the questioning of alliances, withdrawal from international agreements, tariffs on historic allies, and diminished enthusiasm for NATO. Mr Trump's reported ambivalence toward Ukraine[13], public skepticism of NATO's value[14], and praise for autocratic leaders like Vladimir Putin[15] have sent shockwaves through traditional alliance structures.

The implications go beyond rhetoric. Critical structures like intelligence-sharing have been strained, transatlantic digital policy coordination has become politicized, trade negotiations have grown hostile, and key U.S.-led norms around data privacy, surveillance, and platform governance now diverge sharply from European values.

The global order that Europe once depended on no longer seems reliable. As America signals a reduced appetite to serve as global guarantor, Europe finds itself reckoning with the reality of decreased access to military, economic, technological, and intelligence support.

4. The world we face: Fractures, isolation, and cyber balkanization

This geopolitical chilling between the US and Europe is unfolding in a world that is already fundamentally reshaping. As the U.S., China, and Russia jostle for dominance, smaller nations increasingly find themselves clustering around major powers for security, trade, and technological support, which has ideological and technical consequences.

In cybersecurity, we see a form of "cyber balkanization" - a digital landscape splintered by competing norms, standards, platforms, and alliances. Cyber balkanisation is the geopolitical fragmentation of the internet - once envisioned as an open, borderless network - into national or bloc-aligned cyber domains, driven by technology dependencies, security imperatives, and political influence, echoing Cold War-era divides.

China pushes its model of digital sovereignty and censorship. Russia supports asymmetric cyber operations and proxies. The U.S. and Europe also differ on surveillance, privacy, and platform regulation.

As dependencies harden and trust erodes, powerful nations begin requiring partners to adopt their regulatory regimes, data standards, and technology stacks. The result is a fragmented world where technological and security alliances often drive or are driven by political forces. If U.S. commitment to European security continues to wane, this trend may intensify. European states may align more closely with each other, and possibly with emerging powers like India or the UK, U.S. adversaries may feel emboldened, and target European systems with greater intensity, and global responses to cyber threats may fracture, with fewer shared frameworks and slower coordinated action.

Europe, in this context, risks becoming isolated.

5. Tactical implications of U.S. withdrawal: A shifting cybersecurity threat landscape

As the United States signals a potential reduction in its global security commitments, Europe faces an immediate transformation of the cybersecurity threat environment. The implications of this shift are multifaceted:

Escalation of Threats Due to Reduced U.S. Engagement

The U.S. has historically been instrumental in identifying and countering cyber threats through initiatives like the indictment of state-sponsored actors from Iran, China, and Russia, and the disruption of cyber extortion operations such as LockBit[16]. These efforts have been pivotal in maintaining a level of deterrence against malicious cyber activities.

European nations, particularly the UK, have relied heavily on U.S. cyber intelligence to monitor advanced cyber threats from adversaries like Russia, China, Iran, and North Korea. U.S. cyber and intelligence capabilities have provided critical insights into zero-day vulnerabilities, ransomware groups, and state-backed cyber espionage that directly impact European interests. A decrease in U.S. proactive cyber-defense measures and intelligence sharing could embolden threat actors, leading to intensified operations targeting European entities. This scenario may compel European organizations to increase cybersecurity budgets and develop more self-reliant defense mechanisms.

Emergence of a cyber threat intelligence (CTI) void

The U.S. has been a cornerstone in global cyber threat intelligence, supporting resources like the National Vulnerability Database (NVD), Known Exploited Vulnerabilities (KEV) catalog, Exploit Prediction Scoring System (EPSS), and the MITRE ATT&CK framework. These tools are integral to the cybersecurity operations of many European organizations. A potential reduction in the availability or support of these resources could create a significant intelligence gap, challenging European entities to find or develop alternative sources of reliable CTI, as we've already observed happening with the EUVD. This void presents both a threat to current cybersecurity postures and an opportunity for European businesses to invest in indigenous intelligence capabilities.

Increased skepticism toward U.S. technology providers

The evolving political landscape and shifting U.S. attitudes toward Europe and Ukraine have led to growing distrust of U.S.-based technology providers. Waning trust is exacerbated by incidents like the one that occurred during February 2025 negotiations between U.S. President Trump and Ukrainian President Zelensky, in which Trump advisor Elon Musk purportedly invoked a threat to withdraw the commercial Starlink satellite system from Ukraine[17], a move which would prove devastating to the Ukrainian war efforts. In a more recent June 2025 incident it was alleged that Microsoft "cancelled" the email address of the International Criminal Court (ICC) chief prosecutor Karim Khan who had been previously targeted by a President Donald Trump, who claimed the court had "engaged in illegitimate and baseless actions" against the U.S. and Israel[18]. While Microsoft has denied these allegations (as Musk did also) the incidents sparked widespread concerns in Europe.

Microsoft has apparently taken note of these concerns and responded with an intensive campaign apparently designed to assuage European businesses anxieties. In April 2025 company Vice President Brad Smith announced five new "Digital Commitments" to Europe[19], followed an announcement of a new "European Security Program" in by a June 2025[20]. Nevertheless, concerns about foreign government influence over technology companies have prompted some European organizations to prioritize digital sovereignty. If trust in U.S. technologies continues to wane, European demand for homegrown cybersecurity solutions is likely to rise, fostering a more autonomous and secure digital ecosystem.

Potential economic measures impacting cybersecurity collaboration

In recent times, the U.S. has increasingly utilized economic tools, such as sanctions and tariffs, to assert its economic policies. The imposition of tariffs on exports from Europe could prompt reciprocal tariffs on technology and cybersecurity from the U.S., thus disrupting existing collaborations and supply chains.

In a recent example of this dynamic, in March 2025 the European Union announced retaliatory tariffs after the Trump Administration began imposing 25% tariffs on all steel and aluminum imports[21]. Such economic risks may incentivize European businesses to diversify their technology suppliers, reducing reliance on U.S. products and encouraging the development of local alternatives. This shift could in turn accelerate Europe's journey toward digital sovereignty and thus help reshape the global cybersecurity landscape.

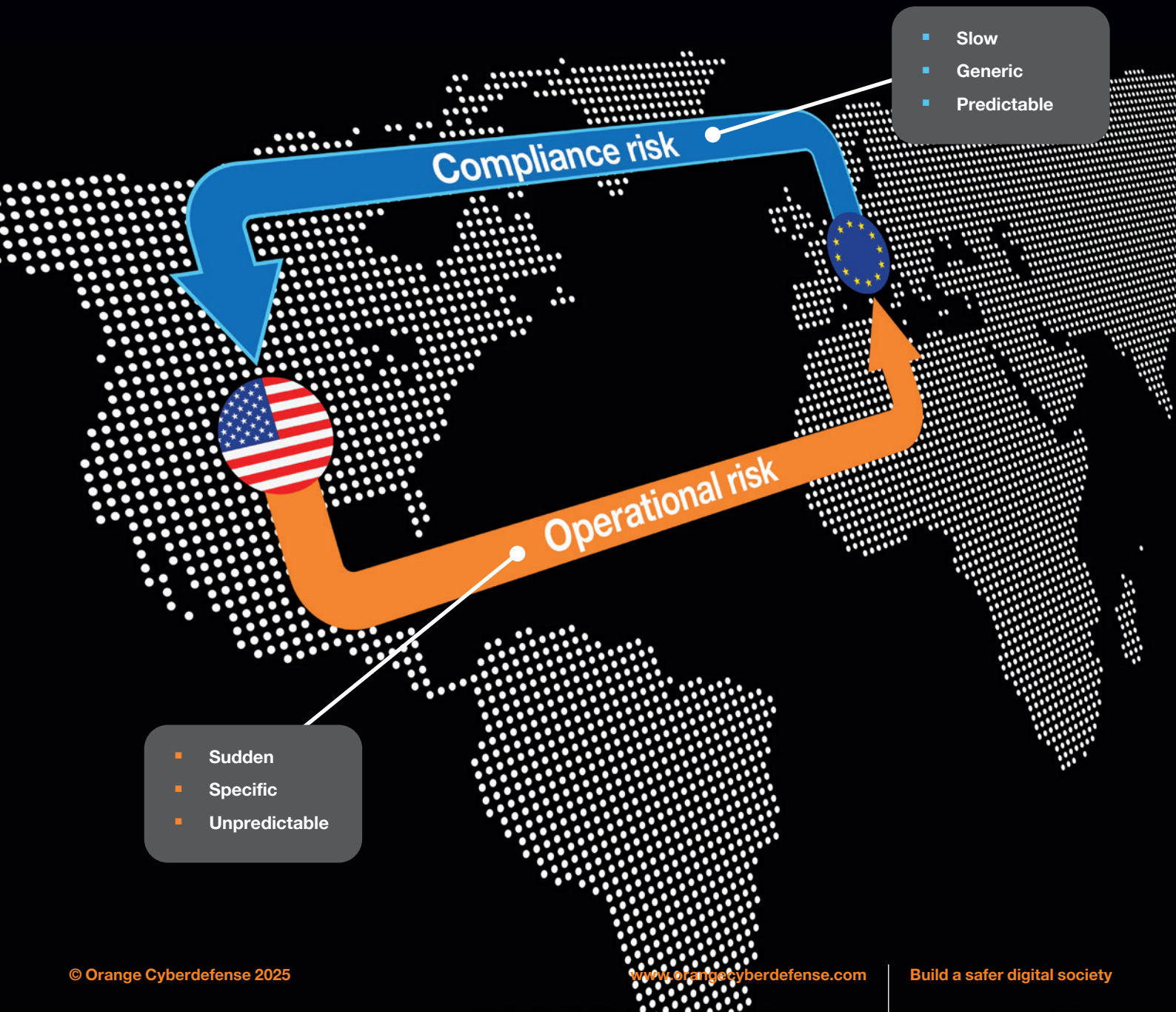
From a risk perspective, these economic measures can be broadly viewed through two lenses:

Compliance risk

Compliance risk arises from the E.U.'s assessment of US assurances that they can comply with E.U. regulations regarding issues like privacy. The risk is that E.U. data may no longer be lawfully stored or processed by U.S. companies. This is a legislative process, which is transparent to the public. It will impact the whole Union in the same way and will develop over a reasonable timespan.

Operational risk

Operational risk arises from U.S. technology companies being compelled to enforce U.S. government sanctions, for example by denying services to sanctioned entities. The allegations that Microsoft denied email access to the ICC's chief prosecutors illustrates this risk. The sanctions against the ICC are non-judicial, as they emerge from US national security mechanisms and are thus not subject to senate or judicial approval. Sanctions can be very specific (to the level of individual employees), happen very quickly, and are not subject to public transparency, so they are impossible to predict.



6. Europe's digital dependency: A critical assessment

The EuroStack project is a strategic pan European initiative aimed at establishing a sovereign and integrated digital infrastructure to bolster Europe's technological autonomy. Originated from a parliamentary event in 2024 and commissioned by the Bertelsmann Stiftung, its flagship report was supported by institutions like CEPS, and the Mercator Foundation[22].

According the Eurostack report, over 80% of Europe's digital technologies are imported. U.S. companies dominate foundational tools, with Microsoft, Apple, and Google controlling over 90% of the European market for operating systems. Just three U.S.-based firms—Amazon, Microsoft, and Google—account for nearly 70% of Europe's cloud infrastructure market and 70% of foundational AI models have been developed in the United States, with another 15% in China. Meanwhile, China controls approximately 90% of the world's rare earth refining capacity—crucial for the production of everything from smartphones to wind turbines. And in terms of digital innovation investment, EU firms represent only 7% of global R&D spending in software and internet technologies, compared to 71% by U.S. firms and 15% by Chinese firms.

This technological dependency extends acutely into the cyber security realm also.

Europe's digital infrastructure and cybersecurity posture have long benefited from extensive, if often underappreciated, collaboration with the United States. Through a vast network of government agencies, standards bodies, nonprofit initiatives, and public-private partnerships, the U.S. supports a substantial portion of the threat intelligence, technical standards, and incident response capabilities that European organizations rely on to operate securely.

Government bodies like the U.S. Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) routinely provide legal, investigatory, and tactical support to European allies. The DOJ's Computer Crime and Intellectual Property Section (CCIPS) conducts legal training and prosecutorial cooperation with European counterparts, while the FBI's Cyber Action Team (CAT) and the Internet Crime Complaint Center (IC3) share vital incident data and intelligence.

Meanwhile, the Cybersecurity and Infrastructure Security Agency (CISA) leads global coordination of cyber threat bulletins and maintains public resources like the Known Exploited Vulnerabilities (KEV) catalog and U.S.-CERT advisories that European defenders regularly consume.

The U.S. National Institute of Standards and Technology (NIST) plays a foundational role through its Cybersecurity Framework (NIST CSF), widely used across Europe as a model for risk management and regulatory alignment. This influence is further reinforced by tools and frameworks developed by U.S. nonprofit institutions.

For example:

MITRE's Common Vulnerabilities and Exposures (CVE) program, which provides standardized identifiers and structured vulnerability data essential for global risk prioritization and remediation.

MITRE ATT&CK, a knowledge base of adversary tactics and techniques, now deeply embedded in threat intelligence platforms and red/blue team strategies across European enterprises.

Center for Internet Security (CIS), which publishes globally adopted configuration baselines and security controls used to harden systems across industries.

FIRST (Forum of Incident Response and Security Teams), which fosters cross-border collaboration among CSIRTs and response teams and includes many prominent European members.

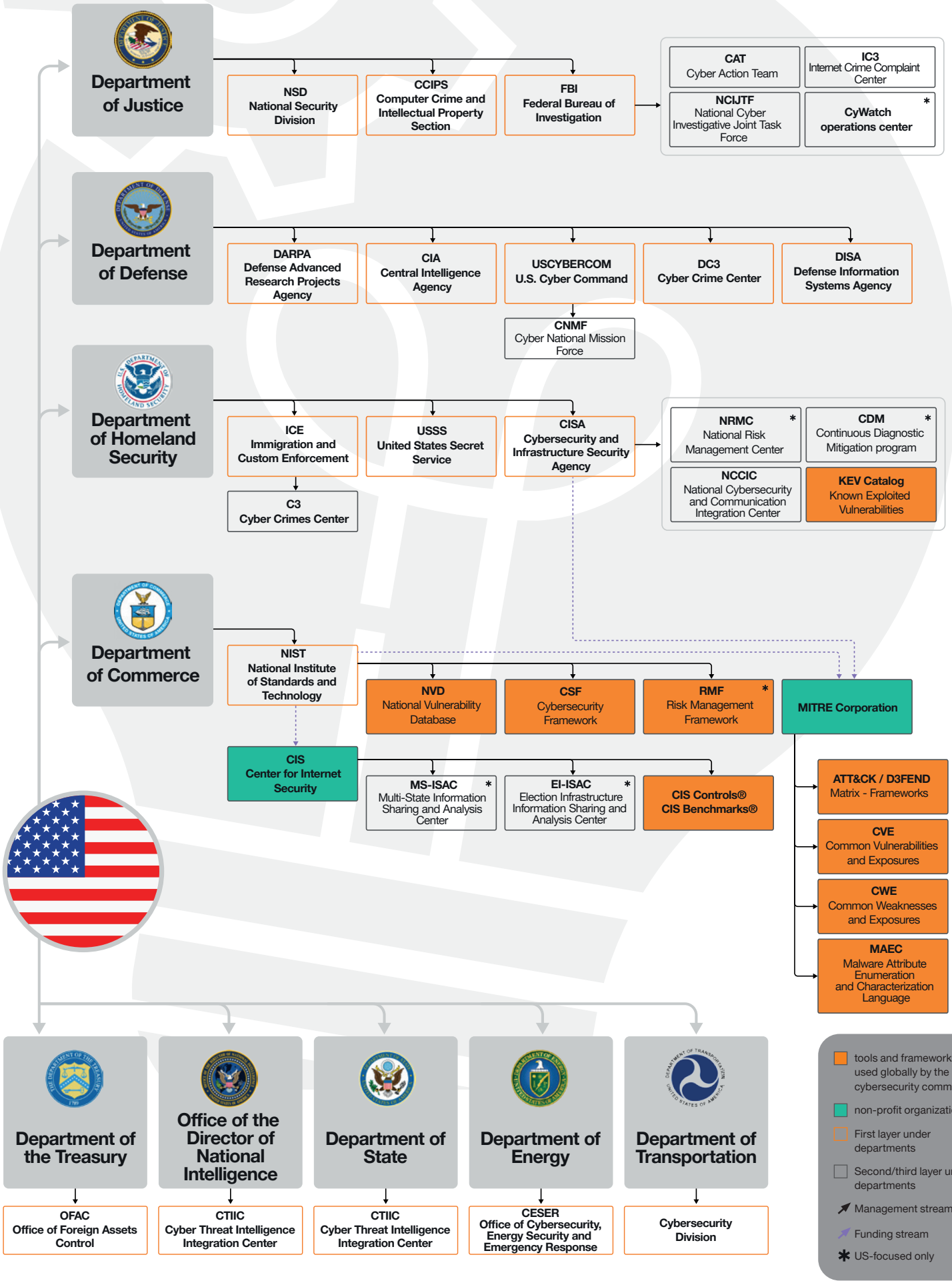
Global Cyber Alliance (GCA), which develops free tools to reduce systemic cyber risks and collaborates directly with European municipalities, SMEs, and nonprofits.

Additionally, the **Office of Foreign Assets Control (OFAC)** under the U.S. Treasury Department imposes targeted sanctions against cybercriminals and state-aligned threat actors. These sanctions, often coordinated with international partners, hinder ransomware and other criminal groups by limiting their access to global financial systems—providing indirect protection to European companies at risk of extortion or fraud.

An important proactive aspect of this support comes from the US Cyber National Mission Force (CNMF), which conducts "hunt-forward" defensive cyber deployments at the request of allies. Since 2023 there have reportedly been 22 missions to 17 countries, including European nations and Ukraine[23]. In Ukraine, for example, U.S. "Hunt Forward" teams reportedly worked alongside local cyber defenders to uncover and neutralize threats before they impact critical infrastructure – a model of active, international cyber defense that benefits the broader European digital ecosystem. These contributions illustrate the highly asymmetric - but deeply integrated - dependency on U.S. resources, intelligence, and strategic support. While they significantly enhance European resilience, they also illustrate the risks of overreliance.

A shift in U.S. posture - whether political or logistical - could dramatically impact the availability of these tools and capabilities, while relying on them also sacrifices sovereignty. By inviting unregulated access by U.S. authorities into sovereign European data and systems, and by developing a critical dependency on U.S. technology and services during times of vulnerability, European institutions may also cede control to U.S. and thus develop new vulnerabilities.

For Europe, this obviously suggests the need to cultivate its own capacities.



7. From dependency to strategic interdependence: A new European cybersecurity trajectory

The security community's response to shifting global dynamics cannot be to sever international ties or retreat into its own isolated nationalism. Cybersecurity, by its very nature, is a global problem that demands global solutions. Threat actors operate transnationally, exploit common technologies, and frequently target global supply chains. When security fails at one place, the implications frequently reverberate globally. Resilience in this environment can only come through coordinated effort, shared intelligence, and mutual trust.

However, the current imbalance - defined by Europe's deep reliance on U.S. technology, intelligence, operational capabilities, and leadership - poses a strategic threat. It is increasingly clear that European organizations must chart a new course toward a more balanced and durable state of strategic interdependence, in which power, knowledge, and capabilities are more evenly distributed, and alliances are chosen deliberately, not enforced by a stronger power.

To reach this end-state of balanced interdependence, cybersecurity leaders must first take two preparatory steps:

Tactical resilience: Harden what you can control

In the short term, European security leaders must work with the realities they face. Achieving sovereignty is a long-term project, but building tactical resilience needs to start now. This involves focusing on areas where immediate control is possible:

Assess procurement risk

European buyers should assess their exposure to suppliers and technologies that may introduce geopolitical risk, avoid unnecessary complexity, and assess potential overreliance on foreign entities. Procurement is not just a cost decision; it is a strategic security decision. Engaging trusted European service providers and integrators not only diversifies operational dependence, but also strengthens local talent, reinforces regional resilience, and supports the long-term viability of a European cybersecurity ecosystem.

Reduce attack surface

The fastest and most effective way to improve security is to reduce the number of exposed systems. Simplify infrastructure, eliminate redundant services, and shield internal assets from external exposure. There is a prevailing narrative that cybersecurity requires perpetually adding security technology to the stack. This approach is questionable at many levels, however, and more so now that every technology acquisition can also exacerbate strategic vulnerability. In the current context, perhaps more than ever, less can be more.

Appropriate cyber intelligence

As with security technology, more intelligence is not always better. What matters is intelligence that is timely, actionable, relevant, and trustworthy. While U.S.-based feeds have long dominated, alternative sources - European providers, international partners, and industry ISACs - offer viable and often underutilized options.

The intelligence generated by an enterprise's own security operations is similarly essential and often under-exploited. Europe's apparent dependence on U.S. intelligence feeds should catalyze a somber re-assessment of how, and why, we use cyber threat intelligence.

Beyond tactical resilience, the cybersecurity community must turn its attention to the pursuit of strategic sovereignty - the development of an autonomous foundation for its digital future. This does not imply isolation or duplicating every U.S. capability but rather ensuring that Europe can choose its alliances freely and from a position of strength.

Strategic Sovereignty: The Strength to Choose Alliances

The EuroStack initiative describes a vision for a technologically resilient Europe, presenting a comprehensive strategy to establish Europe's digital sovereignty. It advocates for the development of a federated digital infrastructure encompassing cloud services, data governance, and artificial intelligence, rooted in European values and legal standards.

Key components of EuroStack include:

Federated Cloud Infrastructure

Developing interconnected cloud services that ensure data remains within EU jurisdictions. This approach aims to reduce dependency on non-European cloud providers and enhance data sovereignty.

Open-Source Platforms

Promoting the use of open-source software to enhance transparency, reduce vendor lock-in, and foster innovation. As of a few years ago, Europe had over 3 million open-source contributors, reportedly surpassing the United States in active participation[24]. By leveraging Europe's strength in open-source communities, EuroStack proposes to build a resilient and collaborative digital ecosystem.

Investment in R&D

Allocating resources to research and development to drive innovation within the continent. The initiative calls for substantial investment, including the establishment of a European Sovereign Tech Fund to support homegrown technologies and reduce reliance on foreign solutions.

EuroStack describes a path via which Europe may begin to transition from a position of dependency to one of strategic autonomy. This shift would enable the continent to safeguard its democratic values, enhance cybersecurity, and ensure that its digital infrastructure aligns with its economic and societal objectives.

As of May 2025, EuroStack has support from key EU member states like Germany and France[25], and appears to be transitioning from conceptualization to early-stage implementation. Yet tangible progress varies across its components. Securing the proposed €300 billion required to fund the program remains a significant challenge, while estimates are that an additional €150 billion in investment will be needed between 2025 and 2030[26]. Experts worry that current EU funding instruments are inadequate or misaligned for EuroStack's specific goals, and complain that projects are too slow to evaluate and assign, with funds misdirected or captured by special interests[27].

Cloud is a particular area of concern. European providers reportedly hold less than a 10% share of the cloud infrastructure market, with most European data centers owned or rented by hyperscalers like AWS, Microsoft Azure, and Google Cloud. This poses a significant obstacle to EuroStack's goal of reducing dependency on non-European tech giants.

The Gaia-X initiative, launched by Germany and France in 2019, aimed to establish a federated, secure, and transparent digital ecosystem to enhance Europe's digital sovereignty[28]. Its objectives included fostering innovation, ensuring data control, and reducing dependency on non-European cloud providers. But Gaia-X has faced significant challenges. Critics argue that early inclusion of non-European stakeholders diluted its sovereignty goals. US companies and major U.S. cloud providers quickly became involved, leading to concerns about the project's direction, and ultimately casting a shadow over the initiative.

In contrast, France's SecNumCloud, established by the National Agency for the Security of Information Systems (ANSSI), offers a stringent cloud security qualification[29]. It mandates that certified providers localize data within the EU and remain free from non-EU legal obligations, such as the U.S. CLOUD Act.

This framework has successfully certified providers like OVHcloud and is considered a benchmark for trusted cloud services in France.

At the European level, the EU Cybersecurity Certification Scheme for Cloud Services (EUCS) seeks to harmonize cloud security standards[30]. Initially, EUCS included sovereignty requirements similar to SecNumCloud, but recent drafts have removed these provisions, sparking debate[31][32]. Some argue that the removal fosters inclusivity and market competitiveness, while others express concerns over potential foreign access to sensitive data.

The divergence between national initiatives like SecNumCloud and broader EU efforts like EUCS highlights persistent obstacles to achieving a unified approach to digital sovereignty. While Gaia-X set out with ambitious goals, its impact has been limited by governance challenges and external influences.

Ultimately, businesses need to proceed from the understanding that the cloud is a borderless space, and that the geographic location of the data matters little if access is not fundamentally controllable.

8. Leading to interdependence: Europe's role in a new digital order

As the global digital landscape becomes increasingly fragmented, Europe stands at a pivotal juncture. With its unique blend of regulatory foresight, commitment to democratic values, and experience with collaboration, Europe is well-positioned to champion a model of healthy and sustainable interdependence in cybersecurity.

As Stephen Covey famously described in his "Maturity Continuum," the evolution from dependency through independence to interdependence marks a higher form of operating in the world[33]. Applied to cybersecurity, interdependence is not a sign of weakness - it is a deliberate and mature strategy that recognizes the complex, contagious nature of modern digital risk. No organization, company, or nation can stand entirely alone in cyberspace. The systems we defend are interconnected; the vulnerabilities we face are shared. So too must be the response. By viewing interdependence as a positive state, European businesses can turn shared risk into collective resilience and lead the world by example. This approach involves:

1. Setting global standards

Europe's regulatory frameworks, notably the General Data Protection Regulation (GDPR)[34], have set benchmarks for data protection worldwide. The GDPR's emphasis on user consent, data minimization, and transparency has influenced data protection laws in numerous countries, demonstrating Europe's capacity to shape global digital norms.

2. Promoting ethical tech development

The European Union's approach to digital transformation is rooted in protecting fundamental rights, sustainability, ethics, and fairness[35]. With this human-centric vision of the digital economy and society, technology developers should aim to ensure that technological advancements align with human rights and democratic values.

3. Fostering inclusive innovation

European leaders recognize the importance of inclusive innovation in driving holistic growth. Initiatives like the Digital Europe Programme aim to enhance digital skills across the continent, ensuring that diverse populations can participate in and benefit from technological advancements[36]. By investing in education and training globally, Europe businesses can help bridge the digital divide and foster a more inclusive digital economy.

4. Coordinating defense in an interconnected threat environment

Cybersecurity threats often propagate through shared platforms, third-party services, and cross-border supply chains. In this environment, failure in one node often impacts many others. This reality calls for a coordinated defense posture: one in which threat intelligence is shared, attack surface reductions are standardized, and proactive threat hunting is conducted across national and institutional boundaries.

5. Institutionalizing digital cooperation mechanisms

Effective interdependence requires structured and sustained collaboration. The United Nations' report, **The Age of Digital Interdependence**, emphasizes the need for enhanced digital cooperation to address the societal, ethical, legal, and economic impacts of digital technologies[37]. European cyber professionals can lead by establishing and participating in multistakeholder platforms that facilitate dialogue among governments, private sector entities, civil society, and technical communities. Such platforms can harmonize efforts, share best practices, and develop interoperable solutions to common cybersecurity challenges.

6. Enhancing cybersecurity capacity building

Addressing cybersecurity effectively necessitates building capacities across all sectors and member states. The European Union's cybersecurity policies highlight the importance of skills and awareness in promoting cyber resilience[38]. Cybersecurity leaders can invest in education and training programs – especially within their own supply chain and local ecosystem - to develop a skilled cybersecurity workforce, thus helping to ensure that organizations across the union have the necessary expertise to manage and mitigate cyber risks.

7. Promoting transparency and trust in digital infrastructure

Trust is foundational to interdependence. Ensuring transparency in digital infrastructure, including clear communication about cybersecurity practices and incidents, fosters trust among stakeholders. The European Union's emphasis on data protection and privacy, as seen in its regulatory frameworks, serve as solid frameworks for promoting transparency and building trust in digital systems.

8. Encouraging public-private partnerships

Cybersecurity is a shared responsibility that benefits from public-private collaboration[39]. TThe European Union's cybersecurity strategies advocate for partnerships between governmental bodies and private sector organizations to enhance cyber resilience. By fostering such partnerships, cybersecurity leaders can leverage the strengths of both sectors to develop innovative solutions and share critical threat intelligence.

Europe's strength lies in its ability to balance sovereignty with collaboration. With this advantage, the European cybersecurity community has the opportunity and responsibility to guide the global community toward a new era of deliberate, secure, and principled interdependence.

Conclusion

Toward a secure and interdependent future

As the world contemplates the dawn of the A.I. revolution, few doubt that successful adoption will bring economic prosperity and geopolitical leverage. But therein lies the catch. Like any powerful technology, A.I. can just as easily result in ceding power as gaining it[40]. Decisions to adopt foreign-built models, tools, or services risk deepening dependency and inviting external influence. At the current pace of change, Europe's political relevance may depend not on how fast it acts—but on how wisely it chooses to adopt technologies that align with its values and long-term vision.

The world is shifting, and the stakes are high. As Europe treads the line between innovation and sovereignty, it stands at a crucial crossroads.

Yet uncertainty also presents opportunity. Cybersecurity has never been merely a technical field; it reflects our geopolitical choices, economic structures, and willingness to collaborate in a fractured world. As the era of relative peace and global order begins to waver, cybersecurity professionals must decide: retreat inward, or lead outward. By treating interdependence not as vulnerability, but as a mature and strategic choice, it can chart a new path for digital security and governance.

This journey demands tactical resilience, strategic sovereignty, and an unshakable commitment to collaboration. Having shown it can balance sovereignty with openness and power with principle, Europe is well positioned to guide the world toward a digital future that is secure, equitable, and enduring.

Authors

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Bjørn Kristian Rasmussen
CTO Norway
Orange Cyberdefense

Disclaimer

Sources

[1] https://www.cisa.gov/news-events/news/statement-matt-hartman-cve-program

[2] https://euvd.enisa.europa.eu

[3] https://www.thecvefoundation.org

[4] https://gcve.eu

[5] https://www.wired.com/2014/01/how-the-us-almost-killed-the-internet

[6] https://www.csis.org/analysis/reforming-section-702-foreign-intelligence-surveillance-act-digital-landscape

[7] https://en.wikipedia.org/wiki/FISA_of_1978_Amendments_Act_of_2008

[8] https://www.lawfaremedia.org/article/fisa-section-702-reauthorized-for-two-years

[9] https://en.wikipedia.org/wiki/CLOUD_Act

[10] https://cdt.org/insights/fisa-702-expansion-impact-on-the-eu-u-s-data-privacy-framework/

[11] https://www.itic.org/news-events/techwonk-blog/expansion-of-fisa-electronic-communications-service-provider-definition-must-be-removed

[12] https://zeihan.com

[13] https://www.reuters.com/world/europe/trump-halts-all-us-military-aid-ukraine-white-house-official-says-2025-03-04/

[14] https://www.brookings.edu/articles/trump-remains-a-nato-skeptic/

[15] https://en.wikipedia.org/wiki/Foreign_policy_of_the_first_Donald_Trump_administration

[16] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[17] https://kyivindependent.com/us-threatens-to-shut-off-starlink-if-ukraine-wont-sign-minerals-deal-sources-tell-reuters/

[18] https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/

[19] https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/

[20] https://blogs.microsoft.com/on-the-issues/2025/06/04/microsoft-launches-new-european-security-program/

[21] https://abcnews.go.com/International/eu-announces-28-billion-countermeasures-trumps-steel-tariffs/

[22] https://www.euro-stack.info/docs/EuroStack_2025.pdf

[23] https://therecord.media/cyber-command-hunt-forward-missions-2023-haugh-senate

[24] https://www.linuxfoundation.org/blog/whats-the-state-of-open-source-in-europe-and-why-does-it-matter-now

[25] https://www.cascadeadvisory.co/post/european-digital-sovereignty

[26] https://www.reframetech.de/wp-content/uploads/sites/23/2025/02/EuroStack-_2025_final-Sec3.pdf

[27] https://www.reframetech.de/en/2025/02/13/eurostack-shaping-europes-digital-future/

[28] https://fr.wikipedia.org/wiki/Gaia-X

[29] https://scalingo.com/blog/secnumcloud-qualification-anssi-guide

[30] https://www.rstreet.org/research/cybersecurity-score-european-cybersecurity-certification-scheme-for-cloud-services-eucs/

[31] https://www.reuters.com/technology/deutsche-telekom-airbus-slam-plan-allowing-big-tech-access-eu-cloud-data-2024-04-10/

[32] https://www.reuters.com/technology/cybersecurity/industry-groups-urge-quick-adoption-eu-cybersecurity-label-that-favours-big-tech-2025-02-28

[33] https://www.ryandelaney.co/blog/maturity-continuum

[34] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[35] https://profiletree.com/digital-single-market/?utm_source

[36] https://ncpflanders.be/digital-europe-programme

[37] https://digitallibrary.un.org/record/3865925

[38] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies #ecl-inpage-skills-and-awareness

[39] https://industrialcyber.co/regulation-standards-and-compliance/european-commission-rolls-out-protecteu-strategy-to-boost-internal-security-resilience-against-hybrid-threats/

[40] https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=1062&context=jgi_research

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 15 CyberSOCs and CERTs distributed across 11 location in the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors.

We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences, including Infosec, RSA, 44Con, BlackHat and DefCon.

www.orangecyberdefense.com