VOLUME 10 (2025) ISSUE 1

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

ANALYSES • POLICY REVIEWS • OPINIONS

The Kosciuszko Institute

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

The European Cybersecurity Journal (ECJ) is a specialised publication devoted to cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem--solving instruments.

ISSN: 2450-2111

Citations: This journal should be cited as follows:
"European Cybersecurity Journal"
Volume 10 (2025) Issue 1, page reference

The Kosciuszko Institute

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków

Phone: 00 48 12 632 97 24
E-mail: editor@cybersecforum.eu

Contents

Editorial

Marietta Gieroń

Chief Editor of the European Cybersecuirty Journal

Dear Readers,

We are living in a time of profound geopolitical instability. The world is increasingly shaped by uncertainty—and the digital sphere is no exception. An unpredictable global order, economic fragmentation, and rapid technological change are converging—and cyberspace is at the very center of it all.

For years, we've known that cybersecurity is no longer just a technical concern. Today, it deeply affects politics, society, and ethical values. It shapes nearly every sphere of our lives—from democracy and sovereignty to the protection of fundamental rights. The threats we face are growing in both scale and sophistication, often transcending national borders and traditional definitions of conflict. Now more than ever, we must be aware—alert but not alarmed.

The digital domain is undergoing a major transformation. The rise of decentralized technologies, generative AI, and mass-scale data collection is not only reshaping the threat landscape but also raising urgent questions about governance, inclusion, and accountability. At the same time, digital tools are becoming powerful instruments of influence, used to shape public opinion, challenge democratic institutions, and disrupt societal cohesion.

This issue of the *European Cybersecurity Journal* offers insights that reflect this complex and pivotal moment. From reimagining cybersecurity strategies to examining the evolving dynamics of digital governance, our contributors provide critical reflections to help us understand, adapt to, and shape the cyber ecosystem of tomorrow.

We hope these reflections offer not only clarity, but also inspiration—to think more broadly, act more boldly, and engage more deeply with the future of cybersecurity. In an interconnected world, shared challenges demand shared solutions. Let us move forward—together, informed, and empowered.

Thank you for reading the *ECJ*.

Signed,

Marietta Gieroń

Paulina Górska

CYBERSEC
FORUM / EXPO

SAVE THE DATE

11-12 June 2025
TAURON Arena Kraków

ARTICLE

Enhancing Cyber Resilience: Leveraging Advanced Threat Intelligence Strategy and Tools Against Cyber Threats

ADAM PALMER
CISO FOR A MID-SIZE US BANK

DR. CARSTEN WILLEMS
CEO OF VMRAY

ABSTRACT:
Cyber Threat Intelligence (CTI) has emerged as a critical element of modern cybersecurity operations. It enables organizations to anticipate, analyze, and neutralize cyber threats. CTI provides informed decision-making and advanced awareness of the threat environment. However, traditional CTI approaches often prove inadequate. This can lead to frustration by security leaders. This is especially true when using CTI to counter advanced persistent threats (APTs), zero-day vulnerabilities, and other sophisticated cyberattacks.

It is important to emphasize that there is often "FUD" (Fear, Uncertainty, and Doubt) about the term "advanced" threats. Most cyber-attacks are not "advanced". However, these attacks remain dangerous. This article examines the limitations of traditional CTI approaches for countering both basic and advanced attacks.

By modernizing CTI and detection capabilities, security leaders can enhance their cyber resilience and improve security team effectiveness. This article provides an outline for

how security leaders can adopt proactive intelligence gathering, support AI assisted real-time threat analysis, and implement adaptive CTI driven response mechanisms into security operations.

Keywords: cyber threat intelligence (CTI), automation & AI, threat detection & response, security operations, cyber resilience

Part I: Five Problems with Current CTI Approaches

Reactive Approaches and Stale (low quality) Data

Many security organizations employ CTI frameworks that rely on outdated or retrospective (stale) threat intelligence. Untrustworthy intelligence results in high noise levels and high false positive rates. Such data requires heavy curation effort before it can be used effectively. CTI may also not be useful if it is too generic. To counteract these limitations, organizations should adopt real-time intelligence. Gather precise data that enables threat anticipation and mitigation before incidents escalate. Low quality CTI actively degrades security posture by providing poor data input for security tools.

Fragmented Threat Intelligence Sources

Security organizations often rely on multiple CTI feeds, including commercial, governmental, and open-source intelligence sources. The lack of standardized integration across these sources results in incomplete or contradictory threat assessments.

Implementing centralized threat intelligence platforms capable of aggregating and correlating diverse data sources enhances the accuracy (and actionability) of CTI programs.

Lack of Automation

Effective cyber resilience requires automation. The underlying advantage of autonomous (AI) systems is speed. To reduce MTTR (mean time to resolve) incidents, CTI should be ingested and analyzed thru automated tools. MTTR is a metric often reported by security teams as a key performance metric. Reducing MTTR is directly linked to reducing analyst time. Reducing MTTR can be done by automating detection and analysis tools and ensuring that security analysts focus on only the highest quality data with the lowest possible noise.

Over-Reliance on Signature-Based Detection

Traditional CTI methodologies prioritize signature-based detection, which is ineffective against polymorphic and novel cyber threats. Adversaries employ obfuscation techniques that bypass signature-based security measures. A robust CTI strategy should incorporate behavioral analysis, machine learning-driven anomaly detection, and heuristic threat-hunting methodologies to detect sophisticated attacks more effectively.

Lack of Contextual Intelligence and Threat Attribution

Without contextual intelligence, organizations struggle to differentiate between opportunistic threats and targeted campaigns.

This deficiency results in inefficient resource allocation and inadequate responses. By leveraging artificial intelligence (AI) and advanced analytics, CTI teams can improve contextual threat awareness and accurately attribute cyber threats.

Benefits of Evolving to a Modern CTI Approach

When modern CTI approaches are integrated within an organization's cybersecurity program, CTI can become a force multiplier and improve resilience by:

- Enhancing automated threat prioritization and filtering within security solutions.
- Improving vulnerability management through informed risk-based prioritization.
- Enriching fraud prevention, risk analysis, and strategic security initiatives by providing in-depth insights into threat actors, their tactics, techniques, and procedures (TTPs).
- Detecting and stopping ongoing attacks, dormant threats already in the organization (lateral movement).
- Accelerating response after detection by leveraging existing knowledge instead of starting with zero knowledge.
- Using in-the-wild threat insights to assess efficacy of existing technical & organizational defense mechanisms, then selectively adding missing capabilities and closing gaps/blind spots.

Part II: A Framework for Enhancing CTI Maturity – Establishing a Maturity Baseline and Objectives

Organizations seeking to optimize their CTI programs should employ industry-standard maturity assessment tools to systematically evaluate, benchmark, and enhance their intelligence capabilities. Once a baseline is established, CTI teams should formulate intelligence objectives that prioritize threats based on business impact, time sensitivity, and organizational security goals.

Implementing a Threat Intelligence-Driven Workflow. A structured workflow for CTI operationalization should encompass:

- Centralized Intelligence Aggregation: Employing Threat Intelligence Platforms (TIPs) to integrate intelligence feeds. More data is not better data. Different data sources and data formats can add complexity. Aggregation of CTI feeds should focus on a standardized format, quality data, and ensure data is timely.

It is important to emphasize that aggregation should focus on quality data.

- Intelligence Prioritization: Filtering threat intelligence based on industry, infrastructure, and organizational threat landscapes.
- Automated Enrichment: Leveraging automation to correlate intelligence with internal telemetry for real-time threat contextualization.

Proactive Threat Detection and Hunting. Advanced threat detection should extend beyond static indicators of compromise (IOCs) by:

- Utilizing behavioral analytics and the MITRE ATT&CK framework to identify adversarial TTPs.
- Establishing continuous threat-hunting operations to proactively detect indicators of adversary presence before they escalate into full-scale attacks.
- Proactively monitoring dark web activities and adversary infrastructure to identify and neutralize emerging threats before they can manifest into full-scale attacks.

Automating and Accelerating Incident Response. To enhance response efficiency, organizations should:

- Integrate Threat Intelligence with SIEM and SOAR Platforms: Automating intelligence correlation with security alerts and triggering predefined response actions.
- Develop Playbooks for Intelligence-Driven Response: Creating structured response protocols based on known adversary behaviors.
- Conduct Regular Tabletop Exercises: Simulating attack scenarios using intelligence insights to refine response mechanisms.

Fostering Collaboration and Information Sharing. Cyber resilience is strengthened through intelligence-sharing initiatives, including:

- Participation in Information Sharing and Analysis Centers (ISACs) and intelligence-sharing communities.
- Facilitating cross-functional collaboration between SOC analysts, threat hunters, and incident responders.
- Translating threat intelligence insights into executive-level risk assessments to inform strategic decision-making.

Integration with Security Operations and Red Teams. To maximize CTI impact, organizations should:

- Seamlessly integrate CTI workflows with SOC and security orchestration platforms to enable real-time intelligence enrichment.

- Collaborate with red teams to enhance adversary emulation and validate threat detection mechanisms.
- Conduct purple team exercises to iteratively refine threat detection and response capabilities.

Measuring CTI Effectiveness. A structured approach to CTI evaluation involves:

- Tracking CTI Metrics: Documenting intelligence requests, fulfillment times, and resource allocation across business units.
- Quantifying CTI ROI: Assessing incident reduction rates, response time improvements, and strategic decision support contributions.
- Evaluating Tangible Outcomes: Establishing clear links between CTI contributions and organizational security enhancements.

Continuous Maturity & Final Recommendations

The evolution of cyber threats requires a modern and adaptive CTI approach. The use of cyber threat intelligence is widely accepted by security teams, however, many security leaders are disillusioned with the value of CTI. After investing heavily in CTI solutions, security organizations may not realize the expected value. The cause for this dissatisfaction is because the CTI is not actionable. It lacks relevance, it is stale, or it is of poor quality (incomplete, incorrect, or noisy). Security teams struggle to operationalize this low-quality CTI and this leads to frustration.

For CTI to truly enhance cyber resilience, it must move beyond generic feeds and disconnected reports to become an integrated, real-time component of security operations. Simply accumulating threat data is not enough—security organizations need intelligence that is accurate, timely, and tailored to their specific risk landscape.

This is especially critical in environments that rely on security automation and AI-based autonomous systems where low-quality input data doesn't just produce irrelevant or misleading results—it actively degrades security. Poor intelligence can cause false positives that overwhelm analysts with irrelevant noise. False negatives allow threats to slip through review or create misdirected response efforts.

When implemented correctly, CTI can shift from being a frustrating cost center to a force multiplier that enhances threat detection, improves response efficiency, and improves overall cyber defense. A modernized and integrated CTI strategy, as outlined in this article, minimizes cyber risks and strengthens an organization's security posture.

About the authors:

Adam Palmer is the CISO for a mid-size US bank. Adam previously worked at a large global bank and led the UN Global Programme against Cybercrime.

Dr. Carsten Willems is the CEO of VMRay. VMRay is an advanced threat detection and cyber intelligence company based in Germany.

ARTICLE

Rethinking Cybersecurity: A Blueprint for Europe's Digital Future

MATTHIAS MUHLERT
ECSO CISO AMBASSADOR FOR GERMANY

ABSTRACT:
In 2023, despite $188.3 billion spent on cybersecurity globally, we witnessed some of the largest data breaches in history. The uncomfortable truth? Our current approaches to cybersecurity aren't just failing – they're actively holding us back. This isn't another article about compliance or the skills gap. This is a call to fundamentally reimagine how we approach digital security—and how Europe can lead the charge.

Keywords: technological dependence, society-level transformations, cybersecurity dialogue, cybersecurity awareness, cybersecurity loop

Executive Summary

This article aims to challenge the status quo and provide a bold, multi-layered blueprint for how Europe can redefine cybersecurity as a cultural, economic, and societal imperative. Drawing on emblematic failures like the Colonial Pipeline and SolarWinds breaches, it highlights the futility of rehashing known issues while genuine risks escalate. Instead, the proposed framework underscores:

1. Dynamic Cyber Ecosystems

- Moving away from static defenses to adaptive, AI-driven models that learn and evolve alongside attackers.
- Shifting the conversation from "checklist compliance" toward intelligence-based threat detection and real-time responsiveness.

2. Behavioral Engineering & Human-Centric Approaches

- Embedding psychological insights—like growth mindsets, gamification, and user-centered design—to reduce human error and improve user engagement.
- Reimagining training as continuous behavioral engineering, not one-off "awareness" sessions.

3. Shared Responsibility & Decentralized Security

- Recognizing that no single entity can shoulder all cyber risks, from SMEs to public agencies.
- Proposing cross-border funds and blockchain-based trust systems to distribute resources and accountability.

4. Societal Transformations

- Introducing concepts such as a Digital Social Contract, Cyber-Education Economic Model, and neighborhood-level resilience networks to elevate cybersecurity from a niche technical concern to a community-driven mission.
- Encouraging economic incentives (like Security GDP metrics and tax credits) so that secure behavior yields tangible financial and social rewards.

5. Concrete Path to Implementation

- Mapping out milestones from 2025 to 2027, focusing on foundational alliances, infrastructure development (e.g., a Pan-European Sandbox), regulatory harmonization, and global market expansion.
- Defining Key Performance Indicators (KPIs) covering not only breach detection and investment levels, but also human-centric metrics like burnout reduction and digital citizenship engagement.

By integrating these threads—technical innovation, psychological insights, cross-border collaboration, and deep cultural shifts—this article envisions a future where Europe leads the world in secure, ethical, and human-focused digital infrastructure. The time to act is now: Europe has both the regulatory clout and societal ethos to pioneer a cybersecurity paradigm that protects citizens, fosters innovation, and underpins economic strength. Far from just identifying obstacles, this blueprint provides detailed, actionable strategies to remake cybersecurity as an engine for European prosperity and global leadership.

Introduction

Despite the billions invested annually in cybersecurity, high-profile breaches—from Colonial Pipeline to SolarWinds—demonstrate a sobering reality: traditional defense mechanisms often prove alarmingly fragile when confronted with modern, agile adversaries. The Colonial Pipeline attack, for instance, hinged on a single compromised password—a stark reminder that compliance checklists or regulatory mandates alone can't stop determined threat actors. Meanwhile, the SolarWinds breach showcased how an attack on one vendor's software update could reverberate through countless organizations worldwide.

Against this backdrop, Europe faces an additional layer of complexity: a growing reliance on external tech solutions that can erode digital sovereignty and stifle homegrown innovation. While EU directives like NIS2 and DORA mark critical steps toward

more unified, standardized defenses, they're not enough to address systemic challenges—ranging from talent deficits to a fragmented approach to threat intelligence sharing.

This article sets out to rethink cybersecurity's role in Europe from three complementary angles:

1. Technological: A call to embrace dynamic, intelligence-driven defenses—where AI, decentralized models, and real-time simulations mitigate threats before they wreak havoc.

2. Psychological: A recognition that human factors—from staff fatigue to user complacency—play a defining role in security outcomes. By leveraging behavioral science and growth mindset principles, organizations can dramatically reduce vulnerabilities stemming from avoidable errors.

3. Societal: A roadmap for integrating cybersecurity into education, civic infrastructure, and everyday culture—from "Digital Defense Forces" to neighborhood-level "Security Circles" and beyond—so that safe digital practices become ingrained across generations.

Through this triad of technology, psychology, and societal change, Europe stands at a pivotal opportunity to recast cybersecurity not as a mere technical overhead but as a strategic advantage that can underpin both economic vitality and citizen well-being. The sections that follow detail why recycled talking points are hindering true progress and how a more holistic, culturally embedded approach can usher in a new era of resilience—one where breaches become rare, short-lived disruptions rather than systemic catastrophes.

The Limitations of Recycled Insights

Over the past decade, much of the cybersecurity community has repeatedly identified the same core challenges—regulatory complexity, supply

chain vulnerabilities, AI hype, talent shortages, rising cybercrime sophistication, and ineffective awareness training. While each problem is valid, the persistent reiteration of these issues, often in annual threat reports and industry conferences, can unintentionally stall meaningful solutions. Below, we examine in depth why these familiar themes impede genuine progress and what tends to be overlooked in the process.

Regulatory Challenges

1. Static Compliance vs. Adaptive Security

- Problem: Many organizations equate "compliance" with "security," treating regulations like a one-time checklist. Once they pass an audit, they may relax, assuming they're "secure enough."
- Why It Fails: Cyber threats evolve constantly. Regulations—such as those requiring annual audits—reflect security knowledge from months or even years prior. As a result, compliance can lag significantly behind real-world tactics used by attackers.
- Example: Colonial Pipeline was reportedly compliant with regulatory obligations, yet a single compromised password halted critical infrastructure. Attackers don't care about compliance—they exploit weaknesses, whether or not they're on an auditor's checklist.
- What's Overlooked: Adaptive and intelligence-driven security. Instead of seeing "compliance" as an endpoint, forward-thinking organizations treat it as a baseline. They actively monitor threat intelligence feeds, run continuous simulations, and evolve their defenses beyond regulatory minimums.

2. Overlap and Fragmentation

- Problem: Within Europe, directives like NIS and NIS2 aim to unify approaches to critical infrastructure security. However, each Member State may have its own nuances in enforcement, leading to a patchwork of overlapping rules.
- Why It Fails: This fragmentation can stifle cross-border collaboration and force multinational companies into repetitive or conflicting compliance processes, diluting energy and resources that could be spent on genuine security improvement.
- Example: A fintech operating across multiple EU countries must align with local data protection mandates, PSD2 for financial services, plus any specific sectoral rules—each requiring distinct audits and paperwork.
- What's Overlooked: A push for truly harmonized frameworks—where risk assessments, threat intelligence sharing, and incident response can happen seamlessly across borders. A well-implemented version of this could free resources to invest in new security tools, AI-driven threat detection, or staff training.

3. Missed Opportunity: Security as Competitive Edge

- Problem: Overemphasis on avoiding penalties or "bad PR" can overshadow the business benefits of robust cybersecurity.
- Why It Fails: If security is relegated to a "regulatory line item," organizations may not fully explore how strong cybersecurity can enable trust, differentiate products, and open new markets.
- Example: GDPR compliance initially felt like a burden for many companies, but those who marketed their commitment to data privacy often gained customer loyalty or expanded into privacy-conscious markets.

- What's Overlooked: Treating security as value creation—for instance, a car manufacturer that invests heavily in secure software for connected vehicles may position itself as the safest option on the road, appealing to both regulators and consumers.

Supply Chain Vulnerabilities

1. Deceptive Complexity

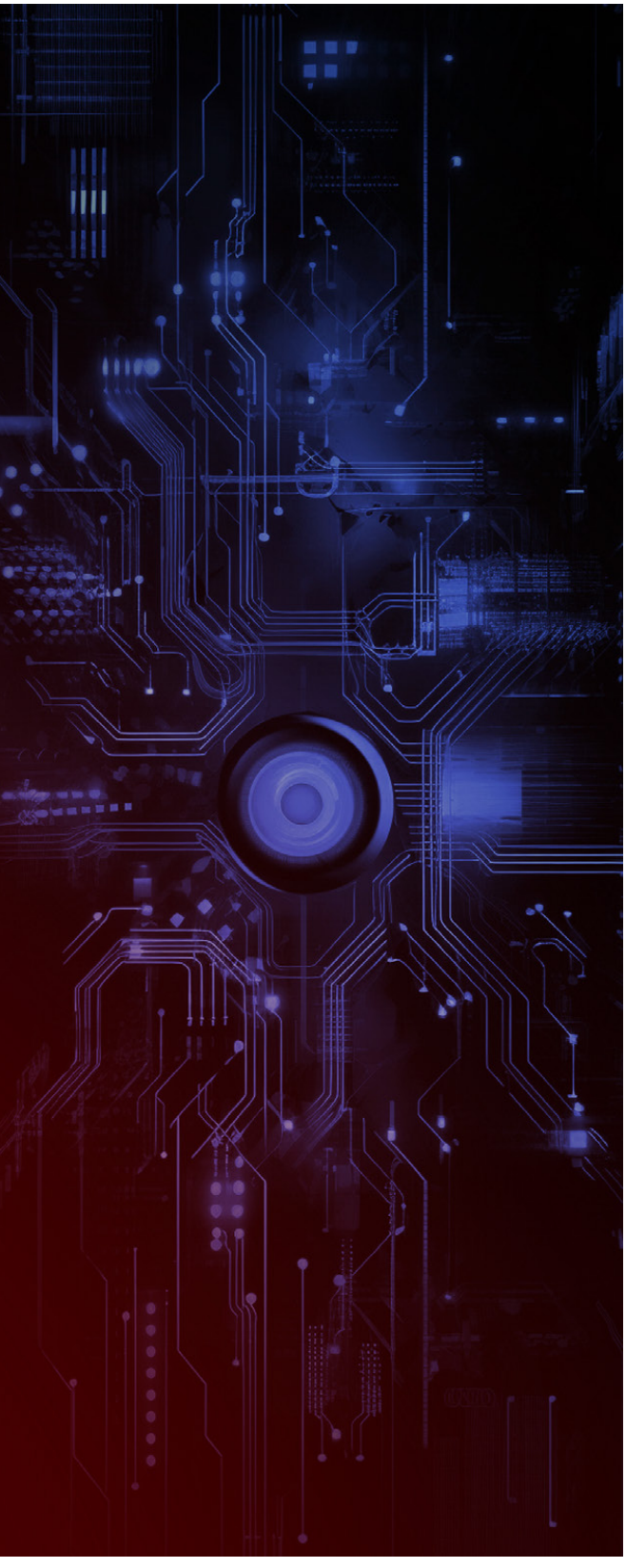
- Problem: Cybersecurity supply chains are often extremely complex, with multiple tiers of suppliers and sub-suppliers. A breach at a small third-party vendor can compromise critical data for a massive enterprise.
- Why It Fails: Many organizations lack visibility into these extended networks, focusing on direct suppliers but ignoring the chain behind them.
- Example: The SolarWinds hack vividly demonstrated that compromising a single update mechanism could cascade to thousands of organizations, including major U.S. government agencies.
- What's Overlooked: Systemic approaches like "Software Bill of Materials (SBOM)"—which outline every component in a software product—combined with technologies like blockchain or cryptographic signing to validate update integrity.

2. Documentation vs. Real Action

- Problem: Supply chain vulnerabilities are routinely documented in whitepapers—everyone "knows" they're critical. Yet actual solutions (like enforced code reviews, immutable logging, shared resilience funds) are rarely implemented due to cost or complexity.
- Why It Fails: A "wait and see" mentality persists. Companies assume a catastrophic supply chain breach won't directly impact them, until it does.
- Example: Industries (energy, finance) could collectively fund a shared resilience mechanism—akin to insurance pools—to quickly respond to a vendor breach. This rarely happens, since it requires trust, transparency, and strategic pooling of resources across competitors.
- What's Overlooked: The role of collective accountability. If major industry players (or entire regions) demanded rigorous third-party security audits and real-time breach reporting from all vendors, it could transform supply chain security globally.

3. Consumer and Regulatory Levers

- Problem: Without demand-side pressure, many suppliers see robust security as optional.
- Why It Fails: If end-users or regulators don't strictly enforce security standards, suppliers may prioritize speed/cost over security, leading to a cycle of vulnerabilities.
- Example: Not all sectors have a standardized "UL listing" equivalent for software (like Underwriters Laboratories for physical products). In the absence of a recognized security "label," buyers can't easily differentiate secure solutions.
- What's Overlooked: A market shift—where suppliers that meet high security standards gain a "trusted" label, and those that don't face diminishing sales. This would require a strong, EU-wide certification process and consumer awareness.



AI as a Threat/Opportunity

1. Paralysis by Dichotomy

- Problem: Discussions often fixate on how AI can be used by attackers (deepfake phishing, automated hacking) vs. defenders (advanced threat detection). This "double-edged sword" framing can freeze decision-makers.
- Why It Fails: While they debate "potential abuse," adversaries exploit AI to accelerate attacks. Meanwhile, defenders underinvest in AI-based solutions or put off adopting them altogether, fearing complexity or unintended consequences.
- Example: Estonia's X-Road overcame this inertia by systematically building a secure data-exchange platform that leverages AI for real-time anomaly detection, boosting speed and accuracy instead of waiting for "perfect AI regulation."
- What's Overlooked: Governance frameworks for AI, such as transparent model training, ethical guidelines, and embedded privacy safeguards, can mitigate threats while unlocking AI's protective potential.

2. Bridging the AI Skills Gap

- Problem: Implementing advanced AI defenses requires staff who understand both cybersecurity and machine learning—a niche skill set that's in high demand globally.
- Why It Fails: Companies often can't recruit or develop these hybrid professionals fast enough, perpetuating a cycle of under-utilized AI.
- Example: A collaborative approach—where universities, private sector, and EU funding initiatives (like the Digital Europe Programme) sponsor specialized "AI for Cyber" training—could quickly scale the talent pool, but requires coordinated effort.

- What's Overlooked: AI can also be used to train employees (via adaptive learning platforms), identifying knowledge gaps and personalizing the curriculum, speeding up the creation of "AI-savvy" security analysts.

3. Proactive vs. Reactive AI

- Problem: Many organizations that do adopt AI use it reactively, analyzing logs post-incident.
- Why It Fails: By the time a breach surfaces in logs, significant damage may already be done.
- Example: Proactive AI can simulate potential attack scenarios, scanning for patterns or vulnerabilities before criminals exploit them—akin to a 24/7 "red team."
- What's Overlooked: The notion of "continuous training" for AI. Regularly feeding it new threat intelligence keeps it updated, mirroring adversaries' own rapid adaptation cycles.

Skills Gap

1. Repetitive "We Need More Talent"

- Problem: Reports often highlight the shortage of cybersecurity professionals as a perennial crisis, but solutions remain vague (e.g., "We should invest in STEM education").
- Why It Fails: This hand-wringing rarely addresses deeper structural issues—such as the lack of on-the-job apprenticeships, retraining for mid-career professionals, or micro-credentials that let job-seekers pivot into cybersecurity.
- Example: Germany's Industry 4.0 push has recognized the need to reskill factory workers for digital manufacturing roles, yet similar concerted upskilling for cybersecurity remains sporadic at best.
- What's Overlooked: Modern educational methods—AI-driven training modules, "cyber boot camps," and cross-company skill exchanges—can expedite the creation of new security practitioners if properly funded and scaled.

2. "Exclusivity" Mindset

- Problem: Some security roles have historically been viewed as highly specialized or "elite," discouraging broader participation.
- Why It Fails: It narrows the talent pipeline. Women, underrepresented minorities, or professionals from non-technical backgrounds may not see a path in.
- Example: Certain community-driven platforms (e.g., Hack The Box, TryHackMe) welcome novices with gamified challenges, showing that cybersecurity can be learned incrementally, not just in academic or corporate silos.
- What's Overlooked: Emphasizing diversity and access—when more backgrounds are included, creative solutions to persistent security dilemmas often emerge.

3. Public-Private Collaboration

- Problem: Universities and tech giants sometimes collaborate, but scattered initiatives have limited reach.
- Why It Fails: Without a cohesive EU or national-level strategy—tying funding, curriculum design, and job placement together—efforts get duplicated or overshadowed by other priorities.
- Example: A pan-European "Cyber Education Alliance" could unify these efforts, standardizing training modules, credential recognition, and job placement channels.
- What's Overlooked: The power of short-cycle training (3–6 months) to quickly convert

non-technical job-seekers into entry-level security analysts, potentially easing unemployment or filling urgent gaps.

Cybercrime Sophistication

1. Annual Shock Factor

- Problem: Media reports and security vendors highlight the "latest wave" of advanced ransomware or supply chain infiltration every year, generating shock but not necessarily action.
- Why It Fails: Audiences become desensitized to "criminals are more sophisticated" claims, especially if each year's narrative feels the same, just with new jargon.
- Example: If the press covers a new "zero-day" exploit monthly, the public stops registering the urgency, while organizations remain reactive.
- What's Overlooked: Collective resilience strategies—like multi-organization threat sharing, real-time intelligence platforms, or joint takedowns—can keep pace with criminals who themselves share knowledge on the dark web.

2. Cross-Border Enforcement Gaps

- Problem: Cybercriminal rings often span multiple countries, taking advantage of jurisdictional loopholes.
- Why It Fails: Collaboration among law enforcement is improving (e.g., via Europol), but not at the scale or speed needed to disrupt well-funded cyber gangs.
- Example: Some major ransomware groups operate from regions less cooperative with Western law enforcement, making arrests and asset recovery difficult.
- What's Overlooked: Aggressive policy measures—for instance, coordinated sanctions that target known cybercriminal safe havens or freezing assets of identified threat actors. While politically sensitive, these might disrupt criminal finances more effectively than reactive investigations.

3. Defender Innovation

- Problem: Attackers adopt new tactics—like cryptojacking or AI-generated deepfake emails—faster than defenders adapt.
- Why It Fails: Many defenders remain stuck in "endpoint antivirus + firewall" mindsets. By the time they implement new tech, criminals are already on to the next method.
- What's Overlooked: Emulating criminals' agile approach—rapid experimentation, shared intelligence, and cross-team collaboration—so defenders can out-innovate criminals, not just chase them.

Awareness Campaigns

1. Check-Box Syndrome

- Problem: Annual e-learning modules or periodic "phishing tests" become superficial ways to claim "we did security training."
- Why It Fails: Behavior change rarely sticks after a short, passive lesson. Employees often forget content within days.
- Example: A large firm might say "98% of staff completed security training" without measuring how daily security behaviors improved.
- What's Overlooked: Continuous engagement—e.g., short monthly quizzes, gamification, or weekly interactive tips that nudge employees to remain vigilant.

2. Gamification and Habit Formation

- Problem: Many awareness campaigns are either fear-based ("Hackers can ruin your life!") or dull, pushing employees to tune out.
- Why It Fails: Repetition of fear narratives desensitizes people; dryness encourages boredom.
- What's Overlooked: Well-designed gamification (e.g., scoring points for reporting real phishing attempts) can make security a positive challenge—spurring friendly competition and recognized success stories.

3. Cultural Integration

- Problem: If leaders or managers don't actively model secure habits—like using strong passwords, updating devices—frontline employees sense a "do as I say, not as I do" hypocrisy.
- Why It Fails: Organizational culture sets the tone for compliance. Inconsistent messaging fosters cynicism.
- What's Overlooked: Security-literate leadership sends a powerful signal—establishing secure habits as part of every role's KPI, from interns to the C-suite.

Conclusion

When we rely on the same, repeated narratives—focusing on regulatory hurdles, supply chain pitfalls, AI's duality, skills shortages, criminal sophistication, and token awareness—we end up describing problems instead of solving them. The cybersecurity community becomes an echo chamber, generating headlines that highlight crises but offer insufficient systemic change.

In the ensuing sections, we'll show that a shift toward dynamic ecosystems, behavioral engineering, and societal innovations can break this cycle. By recognizing the underlying motivations, cognitive biases, and cultural levers that shape how individuals and organizations approach security, Europe can transcend these worn-out talking points—replacing endless problem statements with sustainable, forward-looking strategies.

Integrating Psychological Insights: Beyond Simple Awareness

A significant portion of cybersecurity risk stems not from purely technical flaws, but from human elements—whether it's an employee who ignores updates, a user clicking on malicious links out of curiosity, or top leadership opting for the cheapest vendor despite known vulnerabilities. Psychological and behavioral sciences offer potent tools to address these root causes. By weaving ideas like growth mindsets, gamification, intrinsic motivation, and user-centered design into security programs, organizations can cultivate a culture where secure behavior feels natural, engaging, and personally rewarding.

Organizational Growth Mindset

1. Principle of Continual Learning

- What It Is: Rooted in Dr. Carol Dweck's work, a growth mindset views challenges and failures as opportunities to learn rather than proof of incompetence.
- Why It Matters for Cybersecurity: Fast-evolving threats require teams to adapt, experiment, and iterate. A "fail fast, learn faster" philosophy accelerates improvements and reduces blame-driven secrecy.

2. Failing Safely

- Example: A major retailer might simulate phishing campaigns monthly. Employees who "fail" are encouraged to share experiences openly, feeding insights into the next round of training or defensive changes.
- Outcome: This approach fosters transparency—when a real incident occurs, staff immediately report it rather than trying to hide it out of embarrassment.

3. Top-Down Support

- Challenge: If leadership punishes errors or withholds resources, a culture of fear emerges, making staff less likely to own mistakes.
- Solution: The C-suite and board members should champion "lessons learned" sessions. Celebrate people who surface vulnerabilities proactively, turning them into in-house security advocates.

Behavioral Science for Innovation

1. Goal-Setting Theory

- Brief: Setting clear, challenging, and achievable goals with timely feedback significantly boosts performance.
- Application: Instead of vague mandates like "stay secure," managers can set micro-goals: "Check 5 suspicious emails daily" or "Update all servers within 48 hours of a critical patch."
- Impact: Employees have a tangible target to hit, and quick feedback (like digital badges or supportive acknowledgments) keeps morale high.

2. Intrinsic vs. Extrinsic Motivation

- Distinction: Extrinsic motivators (bonuses, penalties) can work short-term; intrinsic factors (pride, purpose) foster long-lasting engagement.
- Security Example: Position cybersecurity as a mission—"We're protecting our customers' data, ensuring they can trust us"—so staff feel personal commitment, not just compliance pressure.

3. Real-Time Nudges & Micro-Learning

- What They Are: Short, context-specific prompts—for example, an alert reading "You've logged in from a new device—please confirm it's really you."
- Why They Work: Nudges jolt individuals out of autopilot, fostering mindful security decisions at critical junctures. They also serve as continuous training, not just one-time sessions.

2. Behavioral Marketing Tactics

- Example: A company might send staff a monthly "Security Snapshot" email that includes a friendly progress chart ("You were 10% faster in installing patches than last month!"), harnessing social proof and progress-tracking to reinforce good habits.
- Social Proof: Publicly highlighting that 70% of employees changed their default passwords already might encourage the remaining 30% to do so, to avoid feeling left behind.

3. Transparency & Trust-Building

- Key Principle: People resist security measures that feel invasive, abrupt, or unclear.
- Practical Step: Provide plain-language rationales—why a new 2FA system is needed, how it safeguards personal data, and what to expect during enrollment—so staff trust the process and see personal benefit.

Psychologically Informed Marketing & Development

1. User-Centered Design in Security Tools

- Problem: Many security apps or policies add complexity, which users circumvent (weak passwords, stored credentials in plain text, etc.).
- Solution: Involve UX designers and psychologists in the planning of security workflows—reducing friction, prompting secure defaults, and delivering immediate "help" tips.
- Benefits: If it's easy and intuitive to follow secure steps, employees are more likely to comply. This can drastically cut the risk of unauthorized software, unpatched systems, or sloppy credential management.

Digital Well-Being & Resilience

1. Security Fatigue & Alert Overload

- Context: Many employees receive frequent pop-ups, spam filters, or "urgent" patch reminders. When everything is "urgent," eventually nothing feels urgent, leading to cynicism or auto-clicking.
- Solution: Smarter alert filtering—prioritize truly critical alerts and batch less-urgent ones, ensuring employees don't tune out. Integrate calm, supportive messaging rather than alarmist red flags for every minor issue.

2. Mental Health Resources for Security Teams

- Challenge: SOC (Security Operations Center) analysts often face intense stress—sifting

through thousands of daily alerts, any of which might be a genuine threat. Burnout rates run high in these roles.

- Strategy: Offer counseling, peer-support groups, or scheduled "decompression" breaks. Provide rotational shifts to prevent individuals from shouldering 24/7 anxieties.

- Outcome: Healthier, better-rested analysts spot anomalies faster and handle crises more calmly, reducing turnover and improving overall defense quality.

3. Work-Life Balance as a Security Asset

- Rationale: Overworked employees are more prone to mistakes—like ignoring patch reminders or reusing passwords.

- Case: Firms with structured "off hours" for emails or mandatory device-free rest see fewer "fat finger" errors or suspicious link clicks at 3 AM.

- Larger Benefit: This fosters loyalty, as employees appreciate an employer's focus on wellness. A stable, motivated workforce also retains institutional knowledge of system quirks and potential vulnerabilities.

Conclusion

By integrating psychological and behavioral factors into cybersecurity planning, organizations can greatly reduce the mismatch between knowing security procedures and actually implementing them consistently.

A growth mindset encourages open disclosure of mistakes, behavioral science fosters engaged teams, user-centered design shapes more intuitive security tools, and digital well-being initiatives preserve staff vigilance over the long term.

In a European context—where privacy values, collaborative policy-making, and social responsibility hold strong cultural sway—these strategies can become cornerstones of a transformative security ecosystem. Taken together, they offer a powerful remedy to the endless cycles of repeating known problems: they attack the root causes of security failures—human error, organizational inertia, and cultural gaps—and lay the groundwork for genuinely smarter, more collaborative, and more resilient defenses.

Reducing Europe's Technological Dependence Through Psychology

Europe's technological dependence on external providers isn't merely a matter of foreign platforms or hardware—it also reflects cultural acceptance, user trust, and organizational alignment. Achieving digital sovereignty thus requires more than domestic production of gadgets or code; it demands a psychological foundation that makes homegrown solutions viable and appealing to businesses, governments, and end-users. Below, we examine four pivotal strategies—ranging from user-centered innovation to unconventional economic models—that integrate behavioral and cultural elements to cultivate a truly European technology ecosystem.

User-Centered Innovation

1. Designing for Trust and Accessibility

- Rationale: Users embrace tech solutions—be they consumer apps or enterprise software—when those solutions feel secure, intuitive, and aligned with their values.

- Application: Instead of replicating U.S. or Asian platforms, European innovators can embed transparency, privacy controls, and psychological safety at the design stage.

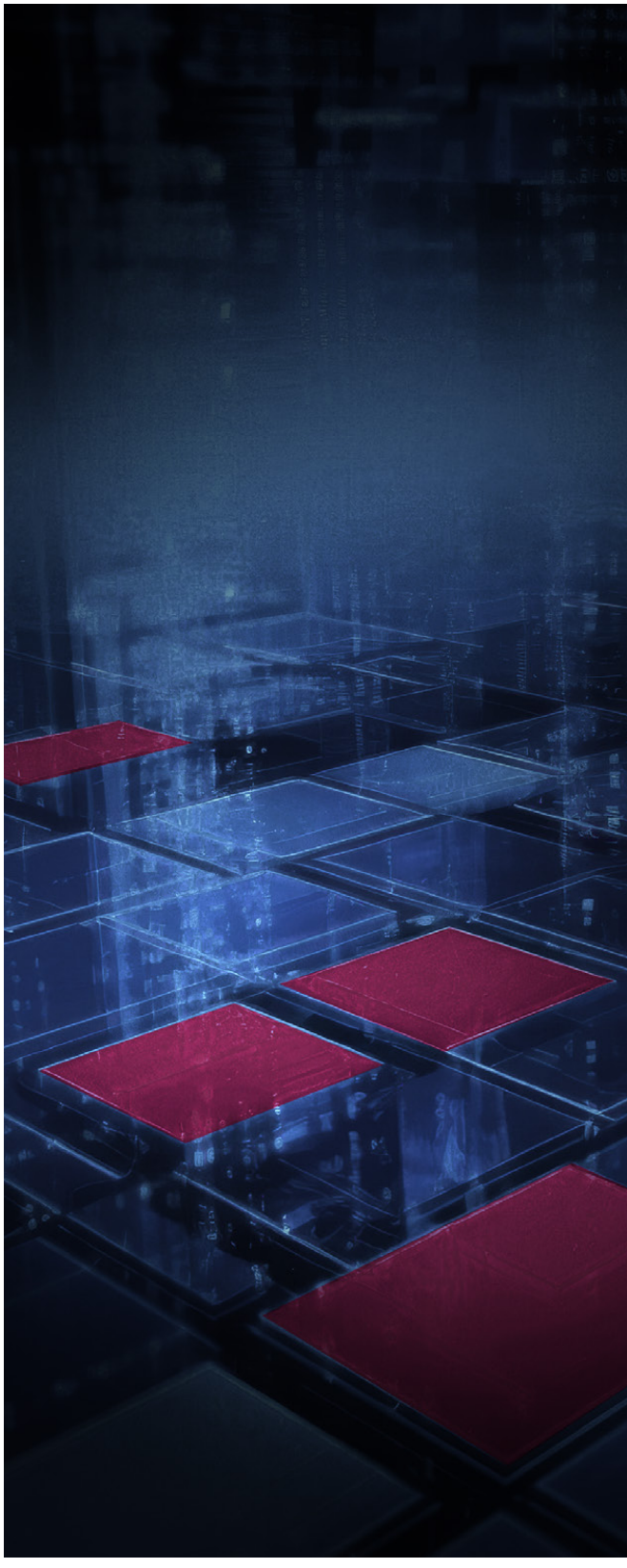
- Examples:
  - A "GDPR-first" social media platform that clearly communicates data usage and consent triggers.
  - A manufacturing software suite that displays real-time threat scanning in a user-friendly dashboard, reassuring operators about system integrity.
- Benefit: By prioritizing user emotions (e.g., feeling protected, in control) and frictionless interfaces, European tech companies can generate loyal adoption without relying on fear-based marketing or forced compliance.

2. Emotional & Cognitive Resonance

- Problem: Many security or privacy features go unused because they're too complex or abstract for typical users to appreciate.
- Solution: Engage cognitive psychologists and user experience (UX) specialists to shape the product flow, ensuring security decisions are presented at the right moment with the right context (e.g., "Secure Payment Mode" prompts when entering payment details).
- Outcome: Higher user comfort and adoption, which fosters brand loyalty, especially if the solution resonates with European principles of transparency, fairness, and social responsibility.

3. Capitalizing on Europe's Diversity

- Insight: Europe's multifaceted linguistic and cultural landscape can be a strength if solutions are localized effectively.
- Example: A cybersecurity education app featuring culturally relevant examples and language support for multiple regions, bridging user adoption barriers.
- Psychological Angle: People feel more engaged with—and trusting of—solutions



that reflect their cultural or linguistic context, especially in critical areas like secure communication or e-government services.

4. Why This Matters

- When solutions are designed around users' psychological comfort and cultural identity, they become naturally more adopted, cutting Europe's reliance on outside platforms. Over time, this fosters an internal market robust enough to compete globally, drawing users who value privacy, usability, and transparency.

Unconventional Economic Models

1. Cooperatives & Social Enterprises

- Context: Conventional tech giants often prioritize shareholder returns above all else, sometimes leading to profit-driven decisions that ignore user well-being or data ethics.
- Alternative: Cooperatives, where employees or community members share ownership, can align financial outcomes with social good—including robust cybersecurity and transparent data handling.
- Case Study: A broadband cooperative in a rural European region: members collectively invest in secure infrastructure, ensuring they get not only service but also a stake in the system's ongoing security posture.
- Psychological Benefit: Stakeholder-centric governance fosters a sense of collective responsibility, making it easier to justify spending on advanced security measures, staff training, or AI-based threat detection.

2. Public-Private Partnerships

- Rationale: Large-scale cybersecurity or AI projects can be high-risk, so government support can de-risk initial development—yet private expertise accelerates innovation.
- Example: A national "Cyber Accelerator" funded jointly by an EU research grant and industry consortia, focusing on quantum-safe encryption. Startups receive not just capital but mentorship from public-sector experts and corporate sponsors.
- Outcomes:
  - By bridging public resources and private agility, Europe fosters homegrown breakthroughs that reduce reliance on external solutions.
  - These PPPs also embed ethical and societal considerations from the start, aligning with European values.

3. Intrinsic Motivations & Ethical Positioning

- Concept: Many tech professionals—especially younger generations—are motivated by purpose over pure profit.
- Implementation: European tech hubs that emphasize social impact (e.g., "We're building an autonomous digital future for our region") can attract and retain top talent who might otherwise gravitate to global players.
- Broader Effect: Over time, a culture of mission-driven technology fosters deeper local expertise, from secure IoT in smart cities to AI-based public health systems—cutting external dependencies.

4. Why This Matters

- By adopting economic frameworks that balance revenue with social/ethical goals, Europe can nurture sustainable, community-aligned tech ecosystems. This approach counters the "winner-takes-all" model often seen elsewhere, ensuring technology is not only locally produced

but also psychologically anchored to shared European ideals of trust and responsibility.

Multidisciplinary Collaboration

1. Bringing Together Tech, Psychology, and Social Sciences

- Challenge: Traditional R&D teams can be siloed—engineering focuses on code, marketing on sales, with limited input from behavioral scientists or ethicists.
- Solution: Foster cross-functional hubs where psychologists (expert in motivation, habit formation), anthropologists (understanding cultural nuances), and security engineers co-create solutions.
- Outcome: Tools that are not just secure in principle, but also intuitive, culturally appropriate, and easier to adopt across different European regions.

2. Academic-Industry Synergy

- Gap: Universities often produce cutting-edge research in cryptography or AI, but industry seldom integrates these findings quickly.
- Model: Joint labs, funded by EU innovation grants, could systematically test academic prototypes in real-world pilot programs (e.g., secure e-voting or blockchain-based supply chain tracking).
- Psychological Angle: Including behavioral scientists in these labs ensures solutions address user fears, emotional barriers, and ethical concerns.

3. Citizen Engagement

- Why: Engaging citizens in co-design—via local hackathons, civic tech groups, or "digital town halls"—ensures that the final product resonates with the public.
- Example: A city-driven platform for reporting suspicious online activities or potential software vulnerabilities (like "311" but for digital anomalies).
- Benefit: When residents feel ownership, adoption rates rise, and reliance on external platforms for everyday digital services shrinks.

4. Why This Matters

- Collaboration isn't just about bridging technical fields; it's about recognizing that human behavior underpins the success or failure of any security or digital sovereignty effort. By uniting diverse expertise, Europe can craft solutions that deeply fit local contexts—technically robust, psychologically aligned, and socially embraced.

Building a Supportive Tech Ecosystem

1. Mental Health and Burnout Prevention

- Context: Security professionals often face high stress, especially in times of crisis (ransomware outbreaks, zero-day exploits). Burnout leads to turnovers or mistakes that compromise security.
- Strategy: Offer structured mental health programs, flexible scheduling, and real-time breaks in Security Operations Centers (SOCs).
- European Example: National Coordination Centres (NCCs) could set best-practice guidelines for healthy work environments—part of the push for a stable, "human-first" security workforce.

2. Regional Hubs and Incubators

- Goal: Encourage local innovation by supporting small tech startups specialized in cybersecurity or privacy technologies—giving them funding, mentorship, and test environments to refine ideas.
- Methods:
  - "Cyber Ranges" for real-time simulations.
  - Access to public data (with privacy safeguards) to train AI for threat detection.
- Outcome: A thriving local ecosystem, enabling solutions to scale within Europe and beyond, instead of searching overseas for capital or markets.

3. Culture of Peer Mentorship

- Context: Startups or SMEs may lack the resources for in-house threat intelligence. Larger companies can provide guidance or threat data—forming "Security Circles" of mutual support.
- Psychological Angle: Mentorship fosters trust, community, and reciprocal loyalty—encouraging knowledge-sharing over zero-sum competition. The overall effect is a resilient network less reliant on external providers.

4. Aligning Skills with Local Needs

- Idea: Education programs tailored to the region's dominant industries (e.g., automotive cybersecurity in Germany, fintech security in Luxembourg) ensure a relevant talent pipeline.
- Benefit: Minimizes "brain drain" by offering specialized, fulfilling careers locally—gradually reducing the impetus to outsource major tech projects or rely on foreign consultancies.

5. Why This Matters

- A supportive ecosystem rests on the well-being and collaboration of its players—entrepreneurs, researchers, security analysts, and end-users. By fostering mental health resources, regional incubators, and peer mentorship, Europe cultivates homegrown solutions that genuinely address local needs, ultimately diminishing dependence on non-European offerings.

Conclusion

Reducing Europe's reliance on external platforms and technologies involves more than manufacturing servers or rewriting code bases; it calls for cultural, organizational, and psychological shifts.

By centering innovation on user trust, adopting unconventional economic models that value shared benefits, collaborating across disciplines, and nurturing supportive ecosystems, Europe can build a resilient, ethically grounded, and socially endorsed digital infrastructure.

This ensures local solutions thrive and remain competitive globally, anchoring Europe's technological sovereignty in a deep well of human-centric principles.

Breaking the Cycle: Transformative Ideas

Sections 2 and 3 laid out the recycled pitfalls in cybersecurity dialogue and the psychological levers that can help us escape them. Section 4 explored how these insights could foster European autonomy. Now, we examine six transformative concepts—spanning dynamic ecosystems, decentralized trust, and cross-border collaboration—that can break the cycle of incrementalism and set

Europe on a path toward innovative and future-proof cybersecurity.

Dynamic Cyber Ecosystems

1. From Static Defenses to Continuous Adaptation

- Problem: Traditional solutions rely on periodic updates or signature-based detection, which can be outpaced by fast-mutating attacks.
- Solution: Establish AI-driven or behavior-based monitoring that constantly "learns" the system's normal patterns. Any anomaly (e.g., a sudden surge of inbound connections) triggers real-time investigation.
- Analogy: This is akin to a living immune system, adapting to new viruses as soon as they appear, rather than waiting for a "virus definition" update.
- Europe's Opportunity: By standardizing data exchange protocols for real-time anomaly reporting (via ECCC or National Coordination Centres), dynamic defenses can scale across industries and borders.

2. Security as a "Living Process"

- Implementation:
  - Rolling "cyber drills" or digital twin simulations, where organizations test resilience under hypothetical large-scale infiltration.
  - Automated patch deployment pipelines that push out verified updates the moment a vulnerability is discovered.
- Benefit: Shortens the "window of exposure," ensuring new threats face immediate friction, rather than waiting for annual patch cycles or slow security reviews.

3. Link to Psychological Safety

- Challenge: Rapid adaptation sometimes unnerves staff who prefer stable routines.
- Approach: Provide clear, iterative training that explains how dynamic defenses function, so employees embrace them as a protective partner, not an unpredictable burden.

4. Why It's Transformative

- Dynamic cyber ecosystems preempt attacks by constantly evolving, turning the current cat-and-mouse chase into a fluid, intelligence-led defense. Combined with the EU's emphasis on privacy, these ecosystems can incorporate robust data-protection standards from inception.

Cybersecurity as a Shared Responsibility

1. Collective Defense Models

- Problem: SMEs, public agencies, and even mid-sized enterprises often lack the specialized teams or funds to implement advanced defenses.
- Solution: A Cyber Resilience Fund—co-financed by large corporations, government grants, and philanthropic sources—to support smaller organizations in adopting best practices, AI-based defense tools, or rapid incident response.
- Benefit: This levels the playing field across supply chains: one small vendor's breach no longer topples an entire ecosystem.

2. Equitable Pooling of Threat Intelligence

- Why: If an airline in Spain detects a novel phishing approach, a hospital in Sweden or a bank in Germany should benefit from that knowledge immediately.
- Mechanism: A robust, real-time platform for shared IoCs (Indicators of Compromise) and TTPs (Tactics, Techniques, Procedures), maintained by a Pan-European alliance.
- Psychological Angle: Public recognition or "badge systems" for organizations that actively contribute to the intelligence pool encourages pro-social behavior rather than hoarding insights.

3. The "No One Left Behind" Principle

- Context: Attackers often pick off the weakest links—like a small service provider with minimal security budgets.
- Outcome: By ensuring all nodes in the network meet a baseline standard of robust security, Europe significantly raises the collective bar, making large-scale breaches more difficult.

4. Why It's Transformative

- Shared responsibility shatters the "every organization for itself" mindset. It fosters community-based resilience, pooling resources, threat data, and mutual accountability—a hallmark of the European approach to collective well-being.

Decentralized Security Models

1. Blockchain-Enabled Trust Systems

- Potential: Blockchain can ensure integrity of software updates, identity management, or e-voting by creating tamper-evident records.
- Drawback: Scalability and energy consumption remain concerns, prompting exploration of more eco-friendly consensus mechanisms or sidechains.
- Use Case: A decentralized software update registry where each patch is cryptographically

signed and time-stamped, verifying authenticity to prevent supply chain attacks.

2. Secure Multiparty Computation (SMPC)

- Essence: SMPC allows multiple parties to compute a function over their inputs without revealing those inputs to each other.
- Practical Example: Different hospitals can jointly analyze patient data to detect health threats or pandemics, without ever sharing raw personal data.
- Security Benefit: Minimizes data exposure, thereby reducing the payoff for attackers.
- European Edge: Ties in with Europe's strong data privacy ethos, showcasing how advanced cryptography can protect civil liberties while enabling collaborative security.

3. Reducing Single Points of Failure

- Aim: When security is centralized (e.g., one authentication server), a breach there can compromise the entire ecosystem.
- Decentralization: Distributes trust across multiple nodes or authorities, forcing attackers to overcome multiple, disjoint barriers.
- Outcome: A region-wide system that's more resilient to catastrophic breaches, aligning with Europe's preference for shared governance.

4. Why It's Transformative

Decentralized architectures exemplify Europe's emphasis on privacy, individual rights, and collective governance, forging tech solutions that reduce reliance on monolithic authorities (often non-European) and empower local autonomy.

Innovation-Friendly Infrastructure

1. Single European Cyber Sandbox

- Goal: Provide a safe, compliance-ready environment where startups, SMEs, and large enterprises can test cutting-edge solutions—from quantum-safe encryption prototypes to new AI-based SOC tools.
- Benefit: Reduces the compliance overhead each company faces individually, offering a shared resource with built-in legal clarity, test data, and secure testing channels.
- Parallel: Similar to how Europe's "Single Market" encourages cross-border trade, a unified cyber sandbox fosters cross-border R&D synergy.

2. Specialized Innovation Hubs

- Focus: Distinct hubs might zero in on AI-based security, quantum cryptography, digital well-being solutions, or zero-trust frameworks.
- Mechanics:
  - Public-private financing.
  - Access to advanced labs (cyber ranges) for real-world attack simulation.
  - Collaboration with local universities for skill development.
- Psychological Edge: Groups of multidisciplinary teams—security experts, psychologists, ethicists—can co-design solutions that are technically robust and user-friendly.

3. Harmonized EU Funding & Regulation

- Aim: Align the patchwork of national grants or compliance frameworks to streamline the path from prototype to market rollout across all EU states.

- Example: A startup from Portugal focusing on self-healing IoT firmware can rapidly pilot in Finland or Poland via the same sandbox environment, scaling faster while meeting uniform security standards.

4. Why It's Transformative

- By lowering barriers to experimentation and guaranteeing consistent legal/technical frameworks, Europe fosters an innovation ecosystem that competes globally while retaining European standards of ethics, privacy, and security-by-design.

Behavioral Engineering Over Basic Awareness

1. From Training Events to Ongoing Culture

- Limitation: Traditional "awareness sessions" once or twice a year rarely change long-term behaviors.

- Idea: Embrace continuous "behavioral engineering"—monthly micro-learnings, gamified challenges (e.g., spotting a simulated phishing attempt for points), and visible progress dashboards.

- Benefit: Employees evolve from passive recipients of info to active players in their own security education, building sustained habits.

2. Personalized Nudges & Feedback Loops

- Mechanism: AI can learn each user's routine—e.g., who logs in at odd hours, who tends to forget updating software—then tailor gentle reminders or tips at just the right moment.

- Psychology: Nudges delivered in real time (e.g., "You're logging in from a public Wi-Fi—enable your VPN now?") are more effective

than generic guidelines employees might forget under stress.

- Outcome: A workforce that sees security not as a burdensome extra step but as a helpful, integrated part of daily workflows.

3. Gamification & Social Proof

- Method: Award points, badges, or small privileges for security-savvy behaviors (e.g., "Top 10 Phish-Spotters of the Month").
- Social Reinforcement: Show team-level metrics—like "Your department reported 95% suspicious emails promptly!"—fostering friendly competition and collective pride.
- Long-Term Impact: Reinforces a community identity around safe practices, making them normative rather than optional.

4. Why It's Transformative

- By embedding security into day-to-day experiences—rather than relegating it to sporadic training—behavioral engineering leverages innate human psychology for positive reinforcement, drastically improving compliance and readiness.

Cross-Border Collaboration

1. Pan-European Cybersecurity Startup Alliance

- Vision: Unite accelerators, incubators, and research labs from Berlin to Barcelona, Stockholm to Rome, enabling knowledge transfers, shared R&D resources, and standardized certifications.
- Mechanics:
  - Common criteria for product testing and approval.
  - Joint events or hackathons, rotating among member states.
- Outcome: Startups quickly scale solutions across Europe, bypassing fragmentation and reinforcing a truly single digital market.

2. Harmonized Product Certifications & Threat Intelligence

- Motivation: If a new cryptographic solution is certified in one EU nation, it should be recognized EU-wide, speeding broader adoption.
- Practical Gains: Vendors can invest more confidently in advanced defenses, knowing they won't face contradictory red tape in each jurisdiction.
- Synergy with Society: Citizens and SMEs gain from a consistent baseline of security, building trust in "Made in Europe" solutions.

3. Federated Learning for Real-Time Threat Sharing

- Concept: Federated learning allows organizations to collectively train AI models on combined data sets without pooling raw data in one place, preserving privacy.
- Impact: Enhanced detection of emerging threats (like new phishing tactics or zero-day exploits) across EU networks, with minimal data-protection friction.
- Social Angle: Aligns perfectly with Europe's emphasis on GDPR and personal data rights—showing how privacy and collective security can coexist.

4. Why It's Transformative

- Cross-border collaboration addresses fragmentation, transforming Europe's diverse markets into a unified engine for cybersecurity excellence. By pooling resources,

knowledge, and real-time threat intelligence, Europe can confidently lead on the global stage, providing an alternative to centralized, non-European tech powerhouses.

Conclusion

Breaking the cycle of incremental, reactive security requires visionary, multi-pronged strategies that reframe cybersecurity from a dreaded compliance exercise into a dynamic, innovation-fueled enterprise—and from an individual or organizational burden to a shared societal responsibility.

By pursuing:

- Dynamic ecosystems that learn in real-time
- Collective responsibility and robust intelligence sharing
- Decentralized models that reduce single points of failure
- Infrastructure that welcomes AI, cryptography, and cross-cultural design
- Behavioral engineering to maintain security as an ongoing habit
- Cross-border collaboration leveraging Europe's unique synergy of diverse markets

... Europe can forge a future-proof environment where cybersecurity is deeply integrated into daily life, cultural norms, and economic development. In doing so, it not only thwarts modern threat actors but also catalyzes new waves of European innovation, aligning with broader values of privacy, social welfare, and human dignity.

Society-Level Transformations: A Hybrid Condensed Proposal

While Sections 2–5 highlight technical, psychological, and organizational strategies, society-level changes can supercharge Europe's cybersecurity efforts by rooting them in civic culture, economic incentives, and collective identity. Below are seven key transformations—each bridging the gap between traditional cybersecurity mindsets and a holistic vision of digital resilience for all.

Digital Social Contract 2.0

1. European Digital Constitution

- Concept: Enshrine digital rights (privacy, data protection) and responsibilities (secure behavior, lawful use of online spaces) into a Europe-wide "constitutional" framework.
- Rationale: Just as physical constitutions set baseline freedoms and duties, a "European Digital Constitution" would clarify what citizens can expect (robust data safeguards, secure digital services) and what is expected of them (avoiding malicious acts, following secure practices).
- Implementation:
  - Public consultations ("Digital Referendums") to ensure the constitution reflects diverse voices.
  - Legislative alignment so new laws or directives abide by these constitutional principles, making cybersecurity a core social value rather than an afterthought.

2. Points-Based System for Secure Behavior

- Analogy: Similar to how some countries use points-based systems for driver's licenses—rewarding safe driving or penalizing infractions—a digital points-based structure would

award points for consistent use of MFA, timely updates, or reporting scams.

- Application: Citizens or organizations could earn "Digital Safety Points" that unlock benefits—like reduced insurance premiums, tax breaks, or early access to new e-government services.

- Why It Matters: Gamification at the societal level, combined with real incentives, transforms secure practices into a common cultural norm.

3. Public Trust & Education

- Challenge: People may fear centralized scoring of their digital behavior.

- Solution: Build an open, transparent system—potentially using blockchain or robust oversight committees—so points are based on verified actions, not arbitrary surveillance. Communicate clearly that this is a reward system, not a punitive scorecard.

Cyber-Education Economic Model

1. Core Curriculum from Primary School

- Goal: Teach cybersecurity and digital sovereignty as fundamental as reading, writing, or basic arithmetic, starting from an early age.

- Examples:

  - Lessons on password hygiene for 8-year-olds, taught through gamified challenges.

  - "Scam-Spotting" tasks in middle school, where students learn to identify phishing attempts in real emails (with teacher supervision).

- Outcome: A generation for whom secure behavior is second nature—greatly reducing easy exploits like phishing or poor password habits.

2. Digital Defense Force

- What: A structured program (voluntary or mandatory) akin to military conscription, but focusing on cybersecurity tasks—e.g., scanning local government systems for vulnerabilities, assisting SMEs with basic hardening.
- Benefits:
  - Rapidly builds a pool of young "cyber reservists" prepared to help in national or EU-wide incidents (like large-scale ransomware).
  - Offers hands-on experience that can lead to specialized careers, injecting fresh talent into the cybersecurity workforce.

3. Cyber Apprenticeships

- Mechanics: Companies above a certain size or revenue must sponsor at least a fixed number of cybersecurity apprentices—funded partly by government subsidies or tax incentives.
- Example: A large automotive manufacturer mentors 50 cybersecurity apprentices each year, combining on-the-job training with classroom instruction in automotive security.
- Result: Steady talent pipelines—especially in underserved or rural areas—ensuring local communities have professionals skilled in both modern technology and secure deployment.

4. University Funding Tied to Research Output

- Why: Motivates higher education institutions to prioritize practical cybersecurity R&D (e.g., patents, open-source tools), not just theoretical papers.
- Mechanism: Allocate a portion of public research funds based on measurable cybersecurity contributions—like the number of secure coding frameworks developed or open-source contributions recognized by industry.
- Effect: Facilitates rapid translation of academic breakthroughs into commercially viable or socially beneficial products, reinforcing Europe's autonomy in cutting-edge security solutions.

Cultural Security Integration

1. Popular Media, Shows, & Social Media

- Rationale: Cultural norms shift faster when secure behavior is depicted as "cool," mainstream, and admirable.
- Implementation:
  - Partner with film studios or streaming services to produce high-quality dramas where characters use robust security measures (encrypted messaging, regular patching) to thwart cyber threats.
  - Social media influencers share daily "Security Tips"—like a cooking show host might do a quick PSA on safe password management in between recipes.
- Goal: Move cybersecurity out of the tech niche and into everyday conversation.

2. Digital Town Halls

- Concept: Community-led gatherings (either online or in person) where residents discuss local digital priorities—like city-wide adoption of e-voting, new smart home technologies, or 5G infrastructure upgrades.
- Impact: Encourages grassroots involvement, letting citizens shape how local authorities spend on secure broadband, IoT device guidelines, or training for small businesses. This fosters community buy-in and shared accountability.

3. Cyber-Safe Zones

- Example: Public libraries equipped with advanced firewall systems, on-site security experts to help older citizens or novices handle device updates, and "free secure Wi-Fi" guaranteed by the municipality.
- Benefit: Normalizes "walk-in cybersecurity assistance," bridging socio-economic gaps so all residents, from seniors to low-income families, can learn how to protect themselves online.

Economic Security Incentives

1. Security GDP Metric

- Definition: A new macroeconomic indicator measuring how robust a nation's cybersecurity posture is, factoring in breach frequency, average detection/response times, and the percentage of businesses meeting high-security standards.
- Why It Works: Just as GDP competition drives nations to strengthen their economies, a "Security GDP" fosters healthy rivalry among EU member states—each striving for advanced resilience.
- Implementation:
  - EU agencies define standardized metrics (e.g., incident rates per 1,000 organizations, time to patch critical vulnerabilities).
  - Annual "Security GDP Reports" highlight improvements, spurring governments to invest in workforce training or infrastructure upgrades.

2. Tax Incentives Based on Security Scores

- Mechanics: Offer scaled tax credits or deductions to companies that pass rigorous, third-party security audits.
- Example: A mid-sized retailer that invests in zero-trust architecture might earn a partial corporate tax reduction if it meets certain EU-level security criteria.
- Psychological Boost: Executive boards see a direct financial upside to robust cybersecurity, transforming it from cost center to a strategic investment.

3. Security Stock Exchange

- What: A marketplace dedicated to trading IP, patents, or shares of cybersecurity ventures—acting as a specialized financial hub.
- Why: Accelerates funding for local innovators, making it easier for investors to find promising security startups or IP.
- Result: Encourages a thriving ecosystem of security-focused R&D, fueling competitiveness and giving Europe a distinctive global edge in advanced defenses.

4. Insurance Premiums Linked to Cyber Measures

- Context: Cyber insurance is a growing market, but premiums often rise if organizations fail to demonstrate strong controls.
- Proposal: Tie premium discounts to verifiable security milestones (e.g., updated EDR solutions, staff training completion, or verified resilience drills).
- Effect: Immediate financial reward for preventive measures, fostering a proactive approach to patching and monitoring.

Societal Resilience Networks

1. Neighborhood-Level Cyber Teams

- Purpose: Foster "local champions" who help neighbors or small businesses with basic security tasks—like router configuration, backing up data, or identifying phishing attempts.
- How: Municipalities can offer mini-grants for community groups that form "Cyber Co-Ops," akin to volunteer fire departments but for digital emergencies.
- Upside: Rapid, trust-based local response to suspicious activity or minor breaches, building communal solidarity.

2. Security Circles for Organizations

- Model: Large enterprises mentor smaller vendors on threat intelligence sharing, patch management, and incident response playbooks.
- Benefit: Minimizes supply chain risk, as all participants meet a baseline standard of readiness.
- Example: A multinational bank adopting local fintech startups, guiding them through secure coding, regulatory compliance, and "live" crisis drills.

3. Cross-Generational Programs

- Concept: Younger citizens (who are often digitally savvy) train older adults or less tech-literate community members in basic cybersecurity.
- Why: Reduces the digital divide while giving youth leadership opportunities; older citizens share life wisdom on caution, risk management, or community building.
- Outcome: A socially cohesive approach, where each generation feels relevant and valued in tackling digital threats.

4. Community-Based Threat Detection & Response

- Implementation: Equip neighborhoods with local "watch systems" or platforms to report suspicious emails, website defacements, or scam attempts.
- Result: Quick feedback loops—if a phishing campaign targets multiple households, everyone is alerted collectively, drastically reducing victim count.

Infrastructure Revolution

1. Secure Public Wi-Fi & IoT

- Goal: Convert "smart cities" from a patchwork of unprotected IoT devices to a unified, end-to-end encrypted ecosystem.
- Method: Mandatory standards for municipal Wi-Fi encryption, device firmware updates, and real-time integrity checks.
- Long-Term: Citizens safely engage with public systems (ticket kiosks, e-government portals, connected lighting) without fear of hijacking or data leaks.

2. Digital Safe Havens

- Definition: Community centers—like libraries—fortified with enterprise-grade intrusion detection, segmented networks, and on-site security consultants.
- Value: Serves as an anchor for free or subsidized training, safe file transfers, or emergency response during major cyber incidents.
- Psychological Aspect: People physically see a "safe" digital zone in their area—tangible reassurance that cybersecurity isn't some distant, abstract concept.

3. Parallel Secure Internet

- Vision: A specialized, high-security backbone for critical services (healthcare, energy, finance) that's insulated from the open internet.
- Challenges: High costs, ensuring seamless interoperability, coordinating across multiple providers.
- Potential: Minimizes risk of widespread outages or sabotage in essential sectors, forming the backbone of "essential digital infrastructure."

4. Mandatory Security Standards for Public Infrastructure

- Analogy: Just as buildings meet fire codes, all new "smart infrastructure" (e.g., 5G towers, roadside sensors) must pass stringent cybersecurity checks before going live.
- Outcome: Over time, the entire public environment—transportation grids, city management systems—becomes inherently more resilient, reducing the harm from any single exploited vulnerability.

Psychological Transformation

1. National Campaigns

- Concept: Large-scale public efforts—like anti-smoking or seatbelt campaigns in decades past—to brand cybersecurity as crucial to personal well-being and social responsibility.
- Media Involvement: Celebrities, sports stars, or popular YouTubers regularly advocate for adopting MFA, suspicious link caution, or verifying online sources.
- Outcome: A population that sees secure online behavior as a shared ethic, not an optional technical skill.

2. Peer Pressure for Good

- Mechanism: Social platforms or local apps that show "Neighborhood Security Scores" or friendly competitor boards.
- Why: Humans naturally respond to social comparison, so if your neighbors boast "We reduced phishing incidents by 50% last month," you're more likely to step up.
- Guardrails: Ensure these metrics remain constructive, not punitive—highlighting progress over blame.

3. Security as a Social Norm

- Philosophy: Just like recycling or wearing masks during pandemics, secure digital habits can become a widely accepted daily routine.
- Reinforcement: Workplaces, schools, and even religious institutions incorporate small security steps (e.g., password rotation reminders, safe device usage) into their messaging.
- Long-Term Impact: Over a generation, Europe's digital culture evolves so that sloppiness in cybersecurity is as frowned upon as littering or driving without a seatbelt.

Conclusion

These society-level transformations—ranging from a "Digital Social Contract" to localized "Security Circles" and secure public Wi-Fi—embed cybersecurity in everyday life.

By tying secure behaviors to civic identity, economic incentives, cultural norms, and infrastructure policies, Europe can reshape the perception of security from a peripheral chore to a core social responsibility—one that fosters inclusive digital growth, protects personal freedoms, and cements public trust in European technology.

Path to Implementation

Realizing the vision described in Sections 2–6 requires concrete steps, phased timelines, and measurable outcomes. Below, we propose a three-stage roadmap (2024–2026) that systematically lays the groundwork, accelerates infrastructure development, and culminates in an ecosystem-wide shift toward collaborative, dynamic, and user-centric cybersecurity.

2025: Foundation Building

1. Pan-European Cybersecurity Startup Alliance

- Goal: Unify accelerators, incubators, and research labs across Europe under a shared banner, promoting cross-border mentorship and easy exchange of solutions.
- Actions:
  - Identify local champions in each Member State—universities, public agencies, venture capitalists—to form the "Alliance Council."
  - Host cross-border hackathons, awarding prizes for solutions that address major EU priorities (e.g., quantum-safe encryption, AI-driven threat detection).
- Outcome: Dozens of early-stage cybersecurity startups gain streamlined access to capital, partnerships, and EU-wide pilots, quickly scaling homegrown innovations.

2. European Cybersecurity Testing Network

- Purpose: Deploy "cyber ranges"—high-fidelity simulation environments—in multiple EU

regions, enabling advanced scenario training and product testing.

- Implementation:
  - ECCC (European Cybersecurity Competence Centre) coordinates set-up standards, ensuring each range adheres to robust privacy and data-handling guidelines.
- Benefit: Startups and SMEs can stress-test their products in realistic threat simulations, receiving immediate feedback and best-practice guidance.

3. EU Cyber Fund of Funds

- Mechanics: A financing structure pooling capital from Member States, major corporations, and public grants (e.g., Horizon Europe) to back mid- to late-stage cybersecurity ventures.
- Rationale: Europe often lacks large-scale venture funds to help promising security firms expand beyond the seed stage. This Fund of Funds fills that gap.
- Impact:
  - Companies can remain in Europe rather than relocating to Silicon Valley.
  - Encourages specialized R&D in areas like privacy-preserving AI, zero-trust frameworks, or secure manufacturing systems.

4. Parallel Societal Pilots

- What: Begin small-scale "Digital Defense Force" trials in select regions, roll out early "Cyber-Safe Zones" at local libraries, and launch pilot "neighborhood-level security teams."
- Goal: Collect data on adoption rates, community feedback, and measurable improvements in local threat detection, guiding broader rollouts.

2026: Infrastructure Development

1. Specialized Innovation Hubs

- Focus: Each major European city (e.g., Berlin, Paris, Madrid, Tallinn) hosts an "Innovation Hub" specialized in distinct security domains—AI-based SOC tools, quantum-safe cryptography, digital well-being, or IoT security.
- Collaboration:
  - Link with academia and industry for real-time knowledge sharing.
  - Provide financial incentives (subsidized rent, tax breaks) for startups relocating to these hubs.
- Outcome: Rapid knowledge diffusion among clusters, generating a strong pipeline of advanced security products.

2. 'Made in Europe' Cybersecurity Label

- Purpose: Certify solutions that meet rigorous standards for privacy, user-friendliness, and robust defense.
- Mechanics:
  - Independent assessments conducted by EU-accredited labs or the European Cybersecurity Organization (ECSO).
  - Label can be used in marketing, highlighting alignment with EU data protection principles.
- Effect: Cultivates consumer and enterprise trust—"Made in Europe" becomes synonymous with high-quality security and ethical data handling, broadening the market for local vendors.

3. Single European Cyber Sandbox

- Details: A shared testing environment pre-compliant with diverse EU directives. Once a solution is validated here, it should be recognized by all EU member states.
- Value:
  - Companies skip repetitive audits or country-specific reconfigurations, accelerating time-to-market.
  - Real-time intelligence feeds from each local test environment help shape EU-level best practices.

4. Expansion of Societal Programs

- Digital Social Contract Debates: Introduce formal legislative discussions in the European Parliament and Member States, taking stock of pilot feedback.
- Educational Initiatives: Scale "cyber literacy" curriculums in primary schools, integrate short modules in teacher training, form alliances with educational publishers for mass distribution.
- Infrastructure Upgrades: Additional "Cyber-Safe Zones," city-level rollouts of secure public Wi-Fi and 5G, advanced encryption standards for all new e-government services.

2027: Ecosystem Maturation

1. Cross-Border Regulatory Harmonization

- Goal: Achieve near-seamless alignment of product certifications, threat intelligence sharing, and incident response frameworks among EU nations.

- Mechanics:
  - Streamlined eIDAS (electronic IDentification, Authentication and trust Services) expansions ensuring mutual recognition of digital IDs across borders.
  - Federated learning systems unify threat detection algorithms while preserving local data privacy.
- Impact: Dramatically reduces fragmentation, making it far easier for security solutions validated in one country to be accepted across all Member States.

2. Integrated Threat Intelligence Network

- Concept: A "digital backbone" for real-time data exchange on emerging threats, suspicious traffic patterns, or zero-day exploits.
- Implementation:
  - ECCC orchestrates a common protocol for sharing Indicators of Compromise (IoCs) and TTPs (Tactics, Techniques, and Procedures).
  - Private sector participation incentivized via financial credits or recognition programs.
- Benefits: Pan-EU transparency ensures if a new phishing variant hits Portugal in the morning, Finnish banks are alerted by lunchtime—drastically cutting criminals' window of opportunity.

3. Global Market Presence

- Showcasing: Host annual "EU Cyber Summit," inviting partners from Asia, Africa, and the Americas to witness and potentially adopt "Made in Europe" frameworks.
- Trade Deals & Alliances: Sign bilateral or multilateral agreements where EU cybersecurity standards guide supply chain requirements or encryption norms.
- Outcome: Europe cements a global reputation for "ethical, high-trust cybersecurity," attracting foreign investments, forging new markets for local vendors, and raising the bar for digital rights worldwide.

4. Society-Level Maturation

- Security GDP Rankings: Publish annual lists, celebrating top-performing Member States in breach reduction, public engagement, and advanced training.
- Neighborhood Networks & Digital Contracts: Scale "Digital Defense Force" to more regions, finalize the "European Digital Constitution" or similar legislative frameworks.
- Cultural Normalization: By now, monthly or quarterly "cyber audits" at workplaces, routine microlearning challenges, and robust digital well-being measures are integrated across a wide swath of the population—shifting cybersecurity from "technical burden" to "shared, respected routine."

Conclusion

This three-phase roadmap—from foundation building in 2024, through infrastructure development in 2025, to ecosystem maturation by 2026—shows how bold yet pragmatic steps can transform Europe's cybersecurity posture.

By embedding technical upgrades in societal and economic frameworks, the EU can:

- Unleash a wave of secure, user-friendly innovation across industries and member states.

- Protect individuals, organizations, and national infrastructures from escalating cyber threats.
- Lead the global discourse on ethical, privacy-respecting, and human-centered security—fulfilling Europe's unique cultural and policy ethos on the world stage.

Metrics for Success

Transforming the European cybersecurity landscape from a repetitive, compliance-driven model to a dynamic, human-centered and society-wide paradigm requires clear, actionable metrics. These metrics serve multiple purposes: they demonstrate progress, motivate stakeholders to stay committed, and guide policy adjustments. Below are four key categories—Investment, Operational Impact, Innovation, and Human-Centric & Societal—each with expanded context and examples.

Investment Metrics

1. Total European Cybersecurity Funding

- Target: Reach at least €10 billion in EU-wide cybersecurity investments by 2026.
- Rationale: Substantial capital is needed to develop advanced solutions (e.g., AI-driven threat detection, quantum-safe cryptography) and support SMEs.
- Mechanism:
  - Track capital flows into dedicated cybersecurity funds, public-private venture programs, and specialized accelerators.
  - Correlate with the EU Cyber Fund of Funds rollout—assessing how effectively it channels resources into promising ventures.

2. Annual Growth in Cyber Startup Valuations

- Aim: Sustain a 40% year-over-year increase in aggregate valuations for emerging cybersecurity firms.
- Why: Valuation growth suggests the market trusts these companies, reflecting investor confidence in their IP, leadership, and scaling potential.
- Potential Indicator:
  - The number of major Series A/B/C funding rounds secured by European startups.
  - The presence of "unicorns" (valuation > $1 billion) in purely Europe-based cybersecurity.

3. Successful Exits & IPOs

- Metric: 100 successful cybersecurity "exits" over €50 million by 2026—through acquisitions or public offerings.
- Reasoning: Robust exit pathways encourage reinvestment from entrepreneurs, fueling a virtuous cycle of new startups and R&D.
- Example: When a specialized AI-for-cyber venture is acquired for €100 million, the founders and investors often re-channel returns into new ventures or mentorship roles, further strengthening the ecosystem.

4. EU Cyber Fund of Funds Participation

- Key Question: How many institutional investors (pension funds, major insurers) and multinational corporations commit capital?
- Significance: Widespread participation underscores trust in the Fund's governance model. It also ensures diverse resource pools, spreading risk and generating momentum for cross-border security projects.

5. Why It Matters

- Investment metrics reveal whether Europe is backing cybersecurity commensurate with the threats it faces. By steadily increasing capital and measuring how effectively it's deployed, the EU ensures its cybersecurity sector remains competitive, resilient, and globally influential.

Operational Impact

1. Breach Detection & Response Times

- Target: Reduce average detection time by 75% (e.g., from weeks to days or hours) by 2026, and incident response costs by 60%.
- Importance: The quicker an organization detects breaches, the less damage. Lower response costs indicate efficient internal processes and advanced automation.
- Data Source: Aggregated from incident reports across Member States, fed into a pan-EU intelligence platform for real-time analytics.

2. Adoption Rate of EU Security Standards

- Metric: By 2026, 90% of mid-size and large enterprises consistently apply frameworks like the NIS Directive, DORA, and 'Made in Europe' cybersecurity label criteria.
- Why: High adoption signals that companies aren't just paying lip service but deeply integrating recommended best practices.
- Verification: Independent audits, sector-wide surveys, and self-reported compliance validated by spot checks.

3. Impact on Critical Infrastructure

- Goal: Achieve a measurable reduction in successful attacks on critical sectors (energy, healthcare, finance).
- Method: Track number and severity of disruptions, average downtime, and financial losses per incident.
- Example: If Europe's energy grid sees a 50% cut in ransomware-induced shutdowns from 2024 to 2026, it indicates a tangible leap in operational resilience.

4. Supply Chain Security Performance

- Vision: Document a 70% decrease in supply chain–linked breaches across key industries by 2026.
- Method: Assess the effectiveness of new solutions (blockchain-based software authentication, shared resilience funds).
- Result: Smaller vendors become less risky, securing the entire ecosystem from the ground up.

5. Why It Matters

- Operational metrics track real-world outcomes beyond compliance. By focusing on detection speeds, response efficacy, and stable infrastructure, Europe moves from theory to practical resilience, safeguarding citizens, businesses, and essential services alike.

Innovation Indicators

1. Number of Cybersecurity Patents & Breakthroughs

- Target: File at least 1,000 European cybersecurity patents annually by 2026.
- Reasoning: Patents signify novel discoveries or significantly improved methods—fueling Europe's intellectual property base.
- Qualitative Side: Beyond quantity, watch for "breakthrough" patents in quantum-safe encryption, AI-based threat intelligence, or privacy-preserving solutions recognized globally.

2. Specialized Innovation Hubs & Labs

- Metric: Launch 50 specialized hubs across Europe—each focusing on distinct areas like AI, quantum cryptography, automotive security, or digital identity.
- Significance: More hubs = more local ecosystems forming around niche expertise. Each hub fosters cluster benefits, drawing academics, engineers, and entrepreneurs together.
- Reporting: Annual updates from these hubs track new prototypes, expansions, or spin-off startups.

3. Job Creation in Cybersecurity & Tech

- Objective: Create 100,000 new cybersecurity or security-adjacent roles (analysts, DevSecOps engineers, AI developers) by 2027.
- Rationale: Sizable workforce growth signals that the ecosystem is maturing, ensuring enough talent to meet escalating demand.
- Tie-In: Apprenticeship programs, "Digital Defense Force" expansions, and micro-credential offerings all feed this pipeline.

4.'Made in Europe' Solutions' Global Presence

- Measure: Track how many EU-developed solutions gain traction beyond Europe—via international deals, large-scale enterprise adoption, or presence at global cybersecurity expos.

- Example: If an Estonian AI-based detection tool or a French secure IoT framework is adopted by municipalities in Asia or North America, it affirms Europe's export competitiveness.

5. Why It Matters

- Innovation metrics confirm Europe's shift from a passive consumer of foreign solutions to an active driver of next-gen security technologies. By quantifying breakthroughs, job creation, and global adoption, Europe can gauge whether it's on track to become a leading hub for cybersecurity research and deployment.

Human-Centric & Societal Metrics

1. Burnout Rates & Workforce Well-Being

- Indicator: Monitor mental health stats among SOC analysts, cybersecurity architects, and frontline IT staff, aiming to reduce burnout by 50%.
- Why: A stable, motivated workforce is far less prone to oversights. Good mental health suggests organizations are truly adopting the "people-first" approach vital to sustainable security.
- Method: Surveys, anonymous reports, and HR data aggregated at industry or national levels.

2. Growth Mindset Adoption & Cultural Shifts

- Assess: Periodic staff polls measuring whether employees feel safe reporting security lapses, how frequently "learning from failure" is practiced, and general willingness to experiment with new security tools.
- Outcome: High "growth mindset" scores correlate with fewer unreported incidents and faster adaptation to new threats, reflecting a more proactive culture.

3. Digital Citizenship & Community Engagement

- What: Track participation in "Digital Defense Force," local "Cyber Town Halls," or "Neighborhood Security Teams." If these initiatives see consistent growth, it signals an increased civic buy-in for cybersecurity.
- Tie-In: Could tie to the "Digital Social Contract," awarding points or privileges for active community involvement.
- Long-Term: Over time, high engagement redefines how citizens perceive and practice daily digital security.

4. Security GDP & Societal Resilience

- Definition: An aggregate metric reflecting breach frequency, incident cost, adoption of secure behaviors, and public satisfaction with digital services.
- Implementation:
  - National bodies feed data into an EU-level aggregator.
  - Annual or bi-annual "Security GDP Reports" rank countries or regions, encouraging friendly competition.
- Impact: When a region's "Security GDP" climbs, it suggests broad-based improvements in technical, cultural, and organizational readiness—translating to fewer crises and higher digital trust among the populace.

5. Why It Matters

- Human-centric metrics ensure that people's well-being, organizational culture, and societal engagement remain at the forefront.

By measuring burnout, cultural shifts, community involvement, and macro-level resilience, Europe validates that security progress isn't just about tech or compliance—it's about empowering citizens, elevating everyday digital life, and reinforcing a collective identity around safe, responsible innovation.

Conclusion

In an era marked by unprecedented digital interconnectivity, the stakes for cybersecurity have never been higher. From the Colonial Pipeline disruption to the SolarWinds supply-chain meltdown, high-profile breaches have repeatedly shown how precarious modern infrastructures can be. Europe, caught between the push for strategic autonomy and the pull of foreign-dominated tech ecosystems, stands at a critical inflection point—one that demands decisive, transformative action.

Sections 2 through 5 dissected the limitations of recycled problem statements—highlighting how regulatory box-ticking, overstated AI hype, chronic skill shortages, cybercrime sophistication, and bare-bones awareness training perpetuate a dangerous illusion of progress. Sections 3 and 4 then showcased how psychological insights (e.g., growth mindsets, behavioral engineering, user-centric design) and organizational changes can unlock new levels of adoption and resilience, while Section 5 introduced dynamic ecosystem models, decentralized security, and cross-border collaboration as ways to break the cycle of incrementalism.

Section 6 introduced a broad range of society-level transformations—digital social contracts, economic security incentives, community-based resilience networks, and an infrastructural revolution—demonstrating how cybersecurity can become an integral part of civic culture. Section 7 offered a concrete roadmap, spanning 2024 to 2026, showing how foundational alliances, innovation hubs, harmonized regulations, and pilot programs can systematically build a future-proof and ethically grounded digital environment.

Finally, Section 8 laid out Key Performance Indicators (KPIs) that measure investment, operational success, innovation output, and human-centric impact—ensuring that Europe not only invests in cutting-edge solutions, but also cultivates vibrant local ecosystems, healthy workplace cultures, and universal digital literacy.

Synthesis

1. Recasting Cybersecurity as a Public Good

- The vision presented is far removed from a compliance-only approach. It frames cybersecurity as a societal and economic catalyst—an engine for trust, innovation, and European global influence.

2. Uniting Stakeholders Across Borders

- No single country or organization can shoulder this alone. By aligning policymakers, industry leaders, academia, investors, educators, and citizens around common frameworks, Europe can amplify collective resources.

- The "Pan-European Cybersecurity Startup Alliance," "EU Cyber Fund of Funds," and cross-border "cyber ranges" are prime examples of how synergy can be systematically built.

3. Ensuring Ethical & Human-Centric Foundations

- Europe's hallmark—privacy, individual rights, social responsibility—must guide AI governance, digital IDs, and the secure management of critical infrastructures.

- Behavioral engineering ensures user empowerment, not manipulation; transparent "Digital Social Contracts" maintain public trust and democratic values.

4. Moving Beyond Talk to Tangible Outcomes

- Awareness is a start but only real implementation—ranging from micro-credentialing initiatives to agile AI defense tools—can shift the needle.
- The KPI framework gives a roadmap for accountability, so leadership can track if detection times are truly dropping, if supply-chain vulnerabilities are shrinking, and if new European solutions gain global traction.

A Vision for the Next Decade

By 2030, Europe could be recognized as the world's leading region for secure, privacy-led digital ecosystems:

- Citizens trust digital services and exercise robust digital rights.
- Companies adopt an "innovation with integrity" ethos, building advanced tech that's both safe and user-oriented.
- Governments uphold flexible, risk-based regulations that adapt swiftly to emerging threats, harnessing real-time intelligence and decentralized trust models.
- Communities see cybersecurity not as an IT headache but as a pillar of local resilience, akin to public health or environmental stewardship.

The key to realizing this future lies in cohesive, sustained effort—merging the best of technical ingenuity, behavioral science, economic foresight, and civic engagement into one integrated strategy.

The next steps outlined in the implementation roadmap (Section 7) serve as a starting point, but the journey will require ongoing adaptation and recalibration as threats evolve and new opportunities emerge.

In short, Europe can break the cycle of rehashed threats and superficial solutions by weaving cybersecurity into its very cultural and societal tapestry—making it a shared responsibility, a driver of innovation, and a testament to European values of solidarity, democracy, and human dignity in the digital age.

About the author:

Matthias Muhlert is a seasoned Information Security leader with over 25 years of experience driving transformative cybersecurity strategies. As the "Cyber Chef" at Dr. August Oetker KG and ECSO CISO Ambassador for Germany, he strengthens digital resilience across industries. His expertise spans global security leadership, risk management, and AI-driven security models, with key roles at HARIBO, Schaeffler, HELLA, and UniCredit. Certified in ISO 27001, CISM, CISSP, and CEH, Matthias is a trusted expert in navigating complex cybersecurity landscapes. He is also the author of Navigating the Cyber Maze: Insights and Humor on the Digital Frontier.

ARTICLE

Toward Inclusive and Equitable Cybersecurity Governance

KAYLE GIROUD
DIRECTOR, COMMON GOOD INITIATIVES AT GLOBAL CYBER ALLIANCE

ABSTRACT:
The digital age offers unparalleled connectivity but also exposes societies, economies, individuals, and governments to sophisticated cybersecurity risks. As Ingolf Pernice noted, cyberspace presents a Hobbesian "state of nature" where all are both potential victims and attackers. Current cybersecurity approaches, often accessible only to those with sufficient resources, exacerbate inequalities and foster inefficiencies. This article advocates for democratizing cybersecurity as a common good to enhance collective security and reduce sector-wide threats. It explores a multi-level governance framework—the "digital constellation"—which emphasizes cooperation at local, national, regional, and global levels, engaging and recognising the role of all key actors and resourcing them to foster resilient, inclusive, and secure digital environments that benefit all, particularly the most vulnerable.

Keywords: cybersecurity, internet governance, multi-stakeholder approach, digital commons

The digital age has brought unprecedented connectivity, but it has also exposed societies, economies, and governments to complex cybersecurity risks. What Ingolf Pernice noticed in 2018 is still true today: *"As everybody is a potential victim and a potential attacker in cyberspace, we find ourselves back in a Hobbesian 'state of nature' – potentially a war of everybody against everybody"*[1].

Security is an ambiguous yet recurrent theme in Internet governance debates, and prompts the question: what constitutes security in a digital world?

The motivations and security notions of cybersecurity actors vary significantly. Governments prioritize national security and economic stability; private companies focus on market demands, reputation management, and compliance; civil society advocates for privacy and transparency; international organizations seek harmonization and capacity building; and individual users strive for personal data protection and safe digital experiences.

Notably, in this Hobbesian 'state of nature', only those who can afford to be secure will feel secure. Governments, private companies, and individuals who can afford it will spend on self-defensive measures but this approach is not cost-effective.

As digital threats grow more complex and pervasive, cybersecurity can no longer be treated as a luxury accessible to a privileged few—it must be democratized for the common good. Democratizing cybersecurity offers significant benefits across industries. Investing in cybersecurity at scale not only strengthens individual organizations but also reduces risks across entire sectors, creating a form of "herd immunity" against cyber threats. For instance, the Let's Encrypt initiative provides free SSL certificates, enabling countless organizations to adopt HTTPS without barriers. This global improvement in web security has lowered operational costs while enhancing compliance and reducing reputational damage. In this era, democratizing cybersecurity is not just a social responsibility but a strategic investment with substantial financial and operational benefits.

Rather than focusing solely on digital sovereignty or international cooperation, what is needed is a global constitutional approach to governance and regulation, rooted in digital competence, resilience, and diligence.

Ingolf Pernice referred to this as the 'digital constellation'[2] — a multi-level approach relevant to the entire globalized society:

- Local Level: Cybersecurity tools, services, and platforms for the public interest empower individual users and businesses for self-protection, digital literacy, and resilience.
- National Level: States create legislation, establish cybersecurity agencies, and foster public-private partnerships.
- Regional Level: Bodies such as the European Union harmonize cybersecurity policies and set collective standards, including cybersecurity-by-design principles enforced through regulations like the Cyber Resilience Act (CRA).
- Global Level: Multi-stakeholder mechanisms, international organizations, and global treaties facilitate cooperation.

Effective multi-level cybersecurity governance depends on the interaction and synergies between diverse actors. As core principles, this cybersecurity

1 PERNICE, I. (2018) 'Global cybersecurity governance: A constitutionalist analysis', Global Constitutionalism, 7(1), pp. 112–141. doi:10.1017/S2045381718000023.

2 PERNICE, I. (2018) 'Global cybersecurity governance: A constitutionalist analysis', Global Constitutionalism, 7(1), pp. 112–141. doi:10.1017/S2045381718000023.

governance is based on shared responsibility, recognizing the roles of every key actor. Understanding the roles and dynamics of key actors is therefore critical for policy development and resilience-building as cybersecurity threats become more sophisticated and global in scope.

As noted by Philip Reitinger and Stephane Duguin, the collective imagination thinks for-profit companies like Apple, Google and Microsoft are responsible for keeping digital ecosystems together[3]. However, Big Tech represents just one piece of the puzzle. A significant portion of securing the Internet is shaped and sustained by a wide network of nonprofit organizations. These groups hold substantial digital space and play a crucial role in maintaining the Internet's backbone by establishing technical standards, developing open-source software, and creating tools that boost efficiency, streamline processes, and ensure dependable performance. Together, they form a dedicated ecosystem safeguarding the Internet's foundation and individual users. They safeguard digital spaces and ensure secure operations:

- Securing the Digital Commons – Domain Name System, Routing: global initiatives like MANRS (Mutually Agreed Norms for Routing Security) and Domain Trust ensure that the common digital infrastructure we all rely on is maintained and secured.

- Threat Analysis: The Shadowserver Foundation, ATT&CK, and Cyber Threat Alliance help identify and mitigate threats at scale, reducing risk for all.

- Emergency Response: The Access Now Digital Security Helpline and FIRST (Forum of Incident Response and Security Teams) provide vital support during cyber incidents.

3 REITINGER, P., DUGUIN, S. (2024), 'The Internet's Defenders Are Running Out of Money—And We're All at Risk', International Business Times. https://www.ibtimes.com/internets-defenders-are-running-out-money-were-all-risk-3749592

- Capacity Building: Initiatives like GCA Cybersecurity Toolkits offer accessible resources, while CyberPeace Builders match technical expertise with mission-driven organizations.

- Workforce Development: Initiatives like CREST Accelerated Maturity Programme (CAMP) speed up the growth and sophistication of local cybersecurity service providers, ensuring a global availability of skills.

The 'digital constellation' governance offers flexibility, resilience, and inclusivity. Understanding and recognising the role of all key actors is critical to its success. However, other challenges persist, notably resource disparities and coordination difficulties.

Large technology firms possess vast resources, while smaller states, nonprofits, and individuals often lack adequate cybersecurity protections, creating systemic vulnerabilities.

Addressing this gap requires a shift toward an equitable cybersecurity market and providing sustainable resources to key actors. As highlighted by Philip Reitinger and Stephane Duguin, and demonstrated by the Common Good Cyber knowledge hub, nonprofit organizations and volunteers play a crucial but often overlooked role in maintaining critical cybersecurity services and tools, and in empowering individual users and businesses through the deployment of the majority of existing cybersecurity tools, services, and platforms for the public interest. Despite their essential contributions, nonprofits are frequently underfunded. To ensure equitable and democratized cybersecurity, sustainable funding models for cybersecurity nonprofits must be prioritized.

As cyber threats continue to evolve, fostering a cybersecurity governance model that harnesses the strengths of diverse actors is crucial. By embracing a multi-stakeholder approach that includes public actors, private companies, civil society, and empowered individuals, Europe and the global community can build a secure, resilient, and inclusive digital environment that benefits all, especially the most vulnerable. Marina Kaljurand, Member of the European Parliament aptly noted, *"just as we view clean air, water, and a peaceful society as essential to all, cybersecurity must be seen as a global common good, critical for the stability of peace and justice"*[4].

4 KALJURAND, M. (2024), '"Cybersecurity must be seen as a global common good," says MEP Marina Kaljurand', Common Good Cyber. https://commongoodcyber.org/news/marina-kaljurand-speech/

About the author:

Kayle Giroud is a project management professional based in Brussels, Belgium. With a rich international background and several years of experience in international cooperation working for the United Nations, the Swiss Federal Department of Foreign Affairs, and various organizations, Kayle has developed an expertise on cybersecurity and a passion about the impact of emerging technologies on society and fundamental rights. Currently, she serves as the Director for the Common Good Initiatives at the Global Cyber Alliance.

Kayle is pursuing a PhD in contemporary history at the University of Bordeaux. She holds an Advanced Master in Interdisciplinary Analysis of European Construction and a B.A. in Political Science from UCLouvain Saint-Louis-Brussels, an MSc in Defense, Development and Diplomacy from Durham University, a PMI PMP® Certification, and a ISC2 Cybersecurity Certification®.

ARTICLE

Strategic autonomy and the EU. A short history

PROF DR PAUL TIMMERS
PROFESSOR AT UNIVERSITY OF LEUVEN

ABSTRACT:
The evolution of strategic autonomy thinking in the EU shows a rapid rise of interest since 2016. Over the past years in Europe the strategic autonomy discourse has been both related to sovereignty in economy, society and democracy in general, as well as – and increasingly since the start of the war against Ukraine in 2022 – to defence and military in their mission to defend sovereignty.

EU policies have only partially adopted the concept of strategic autonomy. Policy inertia may play a role but important is also that strategic autonomy at EU level can run into national security which remains a national prerogative.

Keywords: strategic autonomy, sovereignty, EU policy, cybersecurity, geopolitics

Introduction – defining and clarifying strategic autonomy

Strategic autonomy is not uniquely defined, neither in policy and law nor in academic literature. Loosely said, strategic autonomy is a means to realise sovereignty. It consists of what one knows, how much agency one has, and how much say one has over this knowledge and agency. This ability includes decision power regarding the country, that is, it is contributes to sovereignty. An operational definition is: Strategic autonomy consists of the capabilities, capacities, and control (3C) to defend and strengthen sovereignty (Timmers, 2023).

Here we refer to sovereignty of the state or an alliance of countries such as the EU, rather than sovereignty of a person (individual sovereignty)[1]. Capabilities (what we know), capacities (how much we can produce), and control (how many decisions are ours) can all be measured and assessed even if this make include subjective judgment. We can do such measurement also in a specific domain such as energy, digital, raw materials, etc. We then would use terms such as energy strategy autonomy, health strategic autonomy, digital strategic autonomy, technological strategic autonomy, etc.

The concept of strategic autonomy developed from the defence sector, where, indeed, it is expressed in terms of military capacities and capabilities. Obviously, the military and ministries of defence are explicitly tasked to defend the sovereignty of the country.

In academic and policy literature there is a lot of confusion as well as disagreement about the meaning of the term 'sovereignty'. (Bickerton et al., 2022) define sovereignty in terms of three 'assets' that need to be governed: power, which is called foundational sovereignty; physical and digital assets which are called territorial sovereignty; and the institutional organization of economy, society, and democracy, which is called institutional sovereignty.

Sovereignty also requires internal and external legitimacy (Biersteker, 2012). Internal legitimacy is acceptance of the authority of the government by the citizens and the recognition of citizens by the state. External legitimacy is the acceptance of the state by foreign countries. Sovereignty is both a socially and technologically constructed reality in the digital age (Timmers, 2022). This implies a profound relationship, a structural correspondence, between technology and sovereignty-related social constructs such as international relations and multilateralism[2].

Strategic autonomy is often confused with sovereignty. For instance, we see the term 'digital sovereignty' where the author actually talks about digital strategic autonomy in the meaning above. (Tocci, 2021) clearly distinguishes sovereignty and strategic autonomy and adds that autonomy is a prerequisite for sovereignty. She also distinguishes the internal and external dimensions of sovereignty.

Can we avoid a nebulous notion like sovereignty? We use it partly for historic and custom reasons as the term has old roots (going back as far Bodin in 1529)[3] and partly for political reasons as sovereignty is a politically charged term. A rather technocratic definition such as given above can still be instrumentalised politically.

Therefore, a definition equivalent to above but avoiding the notion of sovereignty and building on (Moerel & Timmers, 2021), is: Strategic autonomy is the ability to decide and act on essential aspects of the future in the economy, society, and democracy as a country.

1 (Floridi, 2020) defines individual sovereignty or self-sovereignty as 'self- ownership, especially over one's own body, choices, and data'.

2 For a theoretical basis and case studies of several digital technologies, see the REMIT project, https://www.remit-research.eu/, supported by the EU's Horizon Europe research programme.

3 For a short history of the term sovereignty see for instance (Timmers, 2023).

Let's also mention some other definitions:

- Digital sovereignty according to (Floridi, 2020) is: 'control of data, software, standards and protocols, processes, hardware, services, and infrastructures, in short, for the control of the digital'
- The European Parliament Research Service (EPRS, 2020) says that digital sovereignty is: 'the ability to act independently in the digital world'
- The World Economic Forum (WEF, 2025) has a definition similar to Floridi's adding: 'digital sovereignty goes beyond regulation to include fostering entrepreneurship and funding innovation'.

Evolving from the definition in defence and in line with the general direction of definitions as above we then use definition [1] above: strategic autonomy consists of the capabilities, capacities, and control (3C) to defend and strengthen sovereignty (Figure 1).

Figure 1. Sovereignty and strategic autonomy

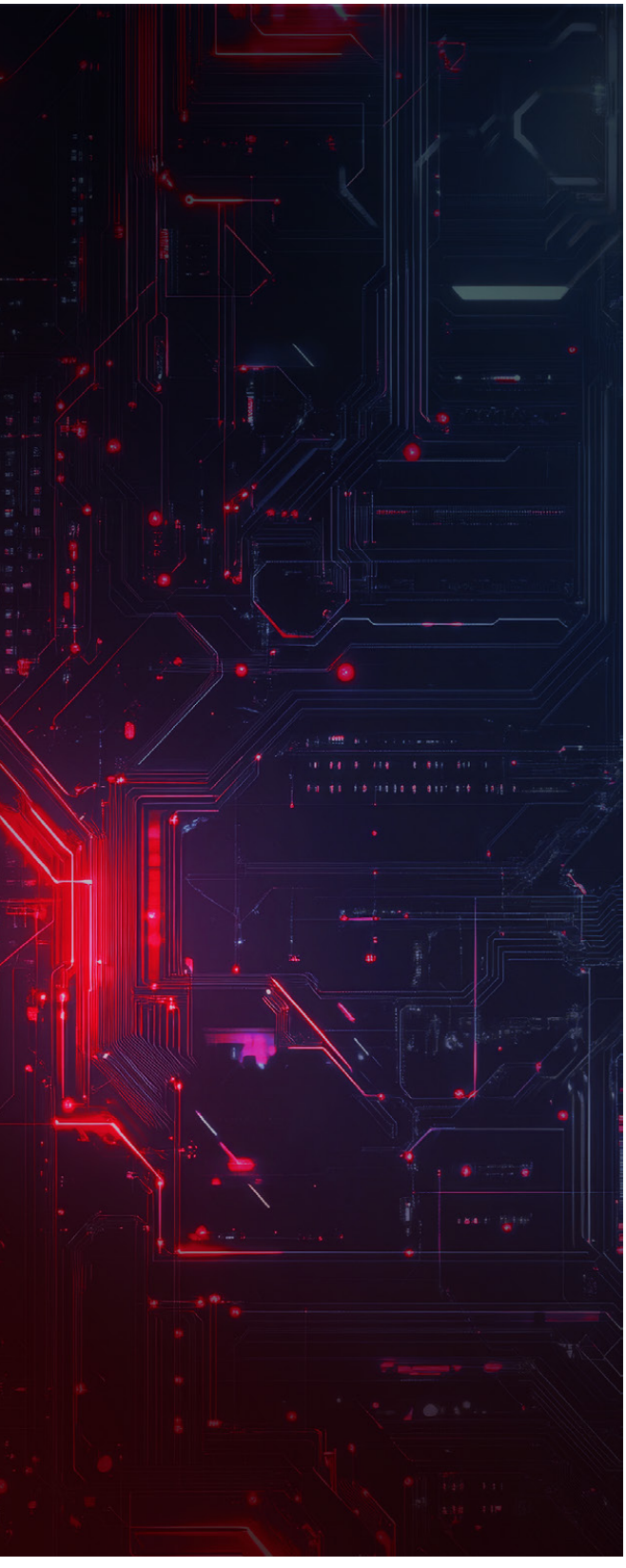
Time and again the question is posed: does strategic autonomy imply autarky (self-sufficiency)? It is suggested that the answer might be positive which would then lead to protectionism which often by the one's posing the question is seen as an evil. The answer is, however, generally, negative. SA requires significant resources that generally are not in the hands of a single country. Moreover, strategic autonomy can perfectly well go together with dependency on other countries and partnerships as long as the other country does not pose a sovereignty threat. Finally, mutual dependencies, or *inter*dependency, can keep in check tendencies to threaten the sovereignty of the other.

Strategic autonomy is also not an absolute notion. A degree of risk to sovereignty realistically exists for most countries. Risk management can even be a strategic autonomy strategy.

However, it would be naïve to trust that interdependencies are balanced, guaranteed to be effective, or last forever. Russia swallowed the pain of its dependencies on the West when sanctions were imposed. It managed to bypass them while keeping the West dependent on its gas. China retaliated on US export controls for advanced chips by restricting exports of germanium and gallium, inflicting pain to the US (and Europe). These export controls also spurred China to accelerate domestic innovation in order to substitute imports. US industrial policy such as the Inflation Reduction Act lures away European manufacturers, eroding jobs and its competitiveness of its long-term partner Europe. This is further being reinforced by President Trump's America First policy.

Strategic autonomy, then, can be achieved in four ways: next to the less likely autarky (at best possible for the US and China), these include risk management, strategic partnerships with likeminded countries, and global collaboration which surpasses a narrow focus on sovereignty. Both strategic partnerships and global collaboration require a commitment to multilateralism.

Any domain of economy or society that is essential for sovereignty falls under the remit of strategic autonomy, from defence to media and education, from critical infrastructures in energy, water and



telecommunications to the production of essential medicines and daily food.

Generally, 'bowling alone' is not feasible and cooperation with others is essential. As a counterpart then, such cooperation should be sufficiently effective and reliable and if it is institutionalised such as by bilateral or multilateral agreement, such agreement should have sufficient mandate.

Multilateralism comes naturally to the EU and its member states, as it is a defining feature of the EU, cast in stone by the Treaties. For other countries, multilateralism is at best an instrument to be used for national security or economic security and competitiveness (Haar, 2024). However, the EU Treaties do not give a strong multilateral mandate to the EU in all domains mentioned above: the EU has limited mandate to act in the fields of defence[4], media, education, critical infrastructures, and public health.

Nevertheless, if there are cross-border effects the EU can act with the force of hard law, such as when the internal market would be at risk for instance because of cyber-attacks on critical infrastructures (cf. the EU's Network and Information Security Directive) or when EU-wide internal security is at risk (cf. the EU's Counter-terrorism Directive).

Do national and EU sovereignty add up in a zero-sum? This is not the case, even if often put forward. The EU Treaties are all about pooled, shared and transferred sovereignty. Pooled and shared sovereignty can be a win-win and even a triple win. Why? First, most EU countries are too small to protect themselves on their own against global challenges such as pandemics, climate change, cyberattacks or trade wars. By collaboration in the EU each of them wins in their national sovereignty. Indeed,

4 The domain of national security is explicitly excluded from the EU mandate as the Treaty on the European Union (TEU), Article 4(2) states: "The Union [...] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

EU countries have shown to constructively collaborate in this spirit within the current EU policy such as for cybersecurity or fighting the pandemic. Second, European sovereignty (in the sense of the 'assets' mentioned before already exists in certain domains. For instance, the.eu domain name represents a truly European sovereign asset, owned by all EU countries and citizens, yet not in any way going at the expense of national domain names. That is then a second 'win': sovereign assets that are truly European. Third, as stated sovereignty requires both internal and external legitimacy. An EU with strong capabilities, capacities and assets will be a more respected and credible party internationally and thereby gain external legitimacy. This is another win in terms of sovereignty.

Resilience, economic security, strategic autonomy

Next to strategic autonomy we often find the notions of resilience and economic security. Resilience is defined in the EU Critical Entities Resilience Directive as "a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident" (EU, 2022). A wider definition of resilience is 'the capacity to deal with change and continue to develop', which originates in social-ecological thinking (Stockholm Resilience Centre, 2020).

In itself then, resilience does not imply reduced dependencies. This, however, is a central idea in economic security. As a political rather than legal or technical concept it can be described as a combination of reducing dependencies that create risks for shorter-term resilience or for longer-term autonomy, promoting own economic capacities and capabilities, and complementing these by trustworthy international partnerships.

Resilience is therefore a necessary but not sufficient condition for economic security. Economic security in turn focuses on economic matters but does not comprise national security directly, nor the protection of democracy and values. These are, however, all part of sovereignty, and therefore addressed by strategic autonomy.

We can conclude that economic security is a necessary but not sufficient condition for strategic autonomy.

The relationship between the three concepts of resilience, economic security and strategic autonomy is illustrated in Figure 2.

Figure 2. Strategic autonomy - Economic security - Resilience

Evolution of strategic autonomy thinking in the EU

The thinking about strategic autonomy has much evolved in the EU over the past years. A short history is as follows. Sovereignty was of course the central element since the start of European collaboration with the Treaty of Rome in 1957. Remarkably, however, the EU Treaties[5] do not mention sovereignty[6]. Strategic autonomy on the contrary was not a notion in EU political discourse, until recently. The exception in this

5 There are two EU Treaties: the Treaty on the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU).

6 Strictly speaking, the EU Treaties makes two references to sovereignty, but these are no longer applicable as they concern UK sovereignty over two military bases in Cyprus.

respect was France where strategic autonomy has been linked to military power at least since World War II[7]. After the war and with the trend towards post-colonialism, France still wanted to be able defend its interests wherever necessary in the world, that is, have the capacity of a 'frappe de force'. At the same time, this was influenced by technological development, Namely, France also wanted to have the atomic bomb and correspondingly developed nuclear capability for both military and civil use - that is, it developed nuclear strategic autonomy, which increased its military and energy autonomy.

Winding forward, the notion of strategic autonomy was given wider visibility in 2016 by President Macron, who outlined that both in the military and in the economic domain Europe needed to develop more strategic autonomy – and France thereby too. French minister of Economic Collomb argued in favour of 'Franco European strategic autonomy' (Timmers, 2019). At the time, France also got increasingly worried about the dependency on foreign big tech. A few years earlier, allies of the US got rocked by the Snowden revelations that exposed the extent of US infiltration of the digital word, and which included spying on friends. However, also increasingly Chinese infiltration and cyber-espionage, become a concern, exacerbated by worries about Chinese intentions to export its authoritarian model and win-over the world. For some countries like Germany these 'early days' of strategic autonomy thinking were rather limited to the military domain. The threatening tone of the first Trump Presidency as regards NATO contributions especially worried Bundeskanzler Merkel.

From 2017 onwards signals of geopolitical, big tech and technological threats grew ever stronger. The European Commission formulated more explicitly the need for increased autonomy, be with the main focus on economy and society (in line with the limited EC mandate in military and defence matters). Notably in 'digital' and 'space' this was expressed. For instance, the 2017 policy on cybersecurity referred to the broader challenge of strategic autonomy for economic and society. EC and European External Action Service (EEAS) also took a firmer position with the 2019 EU-China strategy, labelling– China as partner, competitor, and systemic rival (EC and EEAS, 2019).

Member States and public opinion showed, however, a more divided picture. Several member states felt uneasy with the perceived protectionist undertones in the strategic autonomy and sovereignty debate. They also suspected an agenda of Colbertism to promote national (read: French) champions. Others still stuck to the ideology of globalisation and neoliberalism, rejecting a move towards greater state influence on the economy. For instance, the term 'industrial policy' remained for many a taboo. A group of member states promoted the notion of 'open strategic autonomy' which got also some traction at European level (see textbox).

Open Strategic Autonomy

The European Commission described open strategic autonomy in the 2021 Trade Policy Review: "Open strategic autonomy emphasises the EU's ability to make its own choices and shape the world around it through leadership and engagement, reflecting its strategic interests and values. It reflects the EU's fundamental belief that addressing today's challenges requires more rather than less global cooperation. […] It encompasses: […] assertiveness and rules-based cooperation to showcase the EU's preference for international cooperation and dialogue, but also its readiness to combat unfair practices and use autonomous tools to pursue its interests where needed." (EC, 2021).

Open strategic autonomy means "acting together wherever possible, acting alone wherever necessary" (Aspen Institute Germany, 2021).

7 Immediately after World Wat II the term strategic autonomy was only used by France and by India, the latter expressing with this its positioning as being independent from Washington, Moscow, and Beijing, fitting with its prominent role in the league of independent nations, the G77.

EU R&I's Horizon Europe programme refers to 'promote the Union's strategic autonomy while preserving an open economy' (EU, 2021).

The European Commission's Joint Research Centre (JRC): 'The addition of 'open' [in open strategic autonomy] stresses that the EU aims for multilateral cooperation wherever possible and appropriate' (Kroll, 2024).

The sovereignty debate got a backlash too. EC President Juncker's 2018 State of the Union was titled 'The hour of European sovereignty'. However, he got heavily criticised in the press. It was not done to talk of European sovereignty, and certainly not done for the European Commission.

In the technological field, strategic autonomy manifested itself in 5G security. This became an issue under US pressure to remove Chinese equipment from telecom networks. A remarkable and paradoxical situation then arose: on the one hand member states willingly sat together with the EC to develop a common approach to 5G security, despite the fact that the concerns mostly touched upon national security, that is, outside the EU's mandate. Member states relied on EC brinkmanship in this matter. Then, however, only a soft legal instrument resulted (the 2019 5G Security Recommendation which called to assess technical and political risks, read: control by the Chinese government). The result was not only soft because of the limited EU mandate but also only softly implemented: notably Germany and Spain kept in place and continued to buy Huawei equipment.

The soft approach to strategic autonomy changed in 2020 with the first major disruptions of the early 2020's: the COVID pandemic. This exposed Europe's vulnerability in supply chains for personal protection equipment and medicines and, soon after, also for all kind of raw materials and components in particular semiconductors. The word 'resilience' then rose to the top.

Next, in addition to resilience, attention was needed for rising geopolitical threats, with the 2022 invasion of Russia in Ukraine, finding China at its side, and the rising belligerent behaviour of China towards Taiwan.

Concerns on supply chain dependencies – technical, economic and political - and the increasing dependency of economy and society on new technologies and big tech moved economic security to the top-level, framed in terms such as decoupling, high fence – small yard, and derisking. In 2023 and 2024 the EU adopted a raft of measures on economic security – identifying for instance, critical raw materials, energy, and ten critical technologies, with the objective to 'promote', 'protect' and 'partner' (see textbox, quoting (EC and EEAS, 2023)).

EU economic security objectives:

Promoting our own competitiveness by making our economy and supply chains more resilient bolstering innovation and industrial capacity, while preserving our social market economy

Protecting ourselves from commonly identified economic security risks, by better deploying the tools we already have in place, such as on trade defence, foreign subsidies, 5G/6G security

Partnering with countries who share our concerns on economic security as well as those who have common interests and are willing to cooperate with us to achieve the transition to a more resilient and secure economy.

Terms such as sovereignty and strategic autonomy were no longer 'Verboten' (forbidden). Indeed, Bundeskanzler Scholz' Prague speech in September 2023 got a quite different reception than Juncker's speech 5 years before: one-third of his speech was about European sovereignty. Critics kept silent and general press nodded approval.

Today we experience another major disruption: the second Trump Presidency, pursuing a transactional and economically coercive policy (whether

this will also be militarily coercive remains to be seen although it has been alluded to by President Trump). Moreover, and not seen as explicitly as before, US economic power joins up with big tech economic power which already has created shock waves in Europe from fear for tariffs to concerns about the viability of existing EU laws to eagerness about new economic opportunities in a world with fewer rules and attractiveness of an open EU market relative to an isolationist US. This happens while there are severe concerns about lagging competitiveness, productivity growth, and innovation, internal market fragmentation, and strangling red tape. These concerns are called existential for the EU by the Draghi report and the ECB.

We can see the widening of the scope of strategic economy (to economy, society, democracy in a broad sense) as well as the rise of importance of defence also reflected in academic paper, as illustrated in Figure 3[8].

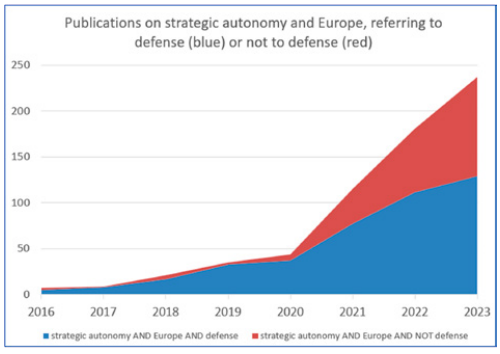


Figure 3. Academic papers on strategic autonomy

What about the future? Many expect further major geopolitical disruptions, such as an invasion of Taiwan by China, an attack of Russia on a NATO EU country or a stepping up of Russia's sabotage operations (also termed as a situation 'unpeace', that is below the level of war but cumulatively as damaging as war).

Adding insult to injury would be geo-economic disruption, that is, when economic instruments get mobilised for geopolitical objectives, such as China squeezing off supply chains, punitive tariffs from the USA onto geopolitical allies, and the rise of BRICS and a possibly alternative global financial transaction system. Others point to technological disruptions that span civil and military domains, such as generative AI causing massive job disruption, quantum computing exposing the core of government, and space/satellite networks bypassing national territory. Yet others point to the disruptive power when the techno-industrial complex (i.e., big tech) joins up with the great power complex (i.e., the USA, China, perhaps also India). This is these days is exemplified by the combination Elon Musk, Mark Zuckerberg and others with the Trump-led America-First political complex. Already a phenomenon with – at least superficially - similar characteristics comes from China, with the alignment of big tech (Huawei, Tencent, ByteDance, etc) and Xi Jinping's authoritarianist leadership and party apparatus.

Finally, EU internal disruption is also looming, with the take-over of several EU member states by authoritarianism with extreme right-wing, anti-liberal democracy and pro-Russia roots.

Likely, this will move attention to the wider notion of strategic autonomy and sovereignty, cf. Figure 2. This does not mean, however, that member states now align behind a common notion of strategic autonomy or common interpretation of EU and national sovereignty. Some member states another view on EU sovereignty and want to break down European economic collaboration ('taking back power from Brussels'), or defence collaboration (opposing the major defence challenges, namely combatting Russia's and Chinese imperialism), or EU democracy (authoritarians being against rule of law and liberal democracy).

Moreover, member states are not equally convinced that Europe faces an existential crisis. Some do not want to accept the consequences of building strong joint industrial policy

8 Academic papers retrieved from Scopus in October 2023.

and investment at EU level, seeing this as a win-lose transfer of sovereignty and budgetary commitment (the Draghi report mentions 800 billion additional p.a.[9]). Other member states are economically not or not yet in dire straits. Some even continue to have strained labour markets.

Clearly, European leaders are challenged to develop a common approach of these future challenges materialise and cause new crises. Not all hope is lost then, however.

In the past years, the EU has shown remarkable leadership in crises, and even more so in areas where the EU has a limited mandate. During the pandemic, quickly the EU took the lead in public health, where is has a limited mandate, through joint vaccine procurement and by putting in place the COVID vaccination app in just a few months (global leadership BTW, as this got recognised by over 60 countries and 1 billion people). The EU broke the taboo of shared debt by putting creating the massive Recovery and Resilience Fund. The EU acted within weeks on Russia's invasion by imposing a sequence of packages of sanctions, again in an area with limited mandate. The EU has managed – as mentioned above – to develop a joint approach in cybersecurity despite this domain being close to national security.

The advantage this time is that the next crises can be foreseen and anticipated. The disadvantage is that the EU is weaker internally than before, weaker externally in the economy of the future (digital, technological) than ever before, and that Europe is more on its own than ever before.

9 Immediately after World Wat II the term strategic autonomy was only used by France and by India, the latter expressing with this its positioning as being independent from Washington, Moscow, and Beijing, fitting with its prominent role in the league of independent nations, the G77.

Strategic autonomy and EU policies

At the time of Brexit, the UK was denied continued access to the secure communications of the Galileo satellite system, and this was justified as it would constitute 'a loss of strategic autonomy'. The justification (EC, 2018) was heavy with legal references – but without ever defining the term strategic autonomy. Indeed, there is no legal definition of strategic autonomy in EU law. At a conference of legislators in 2024 a keynote speaker from the Commission noted this lack of legal definition and wondered what the consequences could be.

There are, nevertheless, several references to strategic autonomy and sovereignty in EU legislation and policy documents, while the frequency of such references has been increasing significantly since 2017. For instance, the EU's critical materials policy issued in 2013-2014 mentions 'boost industrial capacities in an open and trade friendly manner, with high environmental and social standards, creating quality jobs and boosting growth while increasing our open strategic autonomy' (European Commission, 2023)[10]. The EU Chips Act states 'reinforcing Europe's leadership capacities in semiconductors is a precondition for its future competitiveness, and a matter of technological sovereignty and security' (European Commission, 2022). In the space domain, the Space Strategy of 2016 is titled 'Reinforcing Europe's Autonomy in Accessing and Using Space in a Secure and Safe Environment' while the 2023 Regulation on Secure Connectivity talks of 'protect the security and public interest of the Union and its Member States, including through a reinforcement of the strategic autonomy of the Union, in particular in technological terms', (Cellerino, 2023; EC, 2016; EU, 2023). It will be no surprise that in the defence domain references are frequent. In the European Defence Industrial Policy specifically private financing of defence is linked to defending the EU's sovereignty (European Commission, 2024). EU R&D policy in recent years (Horizon Europe) refers to 'promote the Union's strategic autonomy while preserving an open economy.' (EU, 2021).

Interestingly, the picture is mixed for EU cybersecurity policy. While the number of references grew from one during 2013-2018 to five during 2019-2024, there is no consistent phrasing, varying from 'strategic autonomy' in 2017 and 2024, with or without the qualifier 'open' to complete absence of such terminology in the most important cybersecurity law, the NIS2 Directive (Timmers, 2025).

Remarkably, in the EU AI Act and the Coordinated Action Plan on AI there is no reference to sovereignty or strategic autonomy.

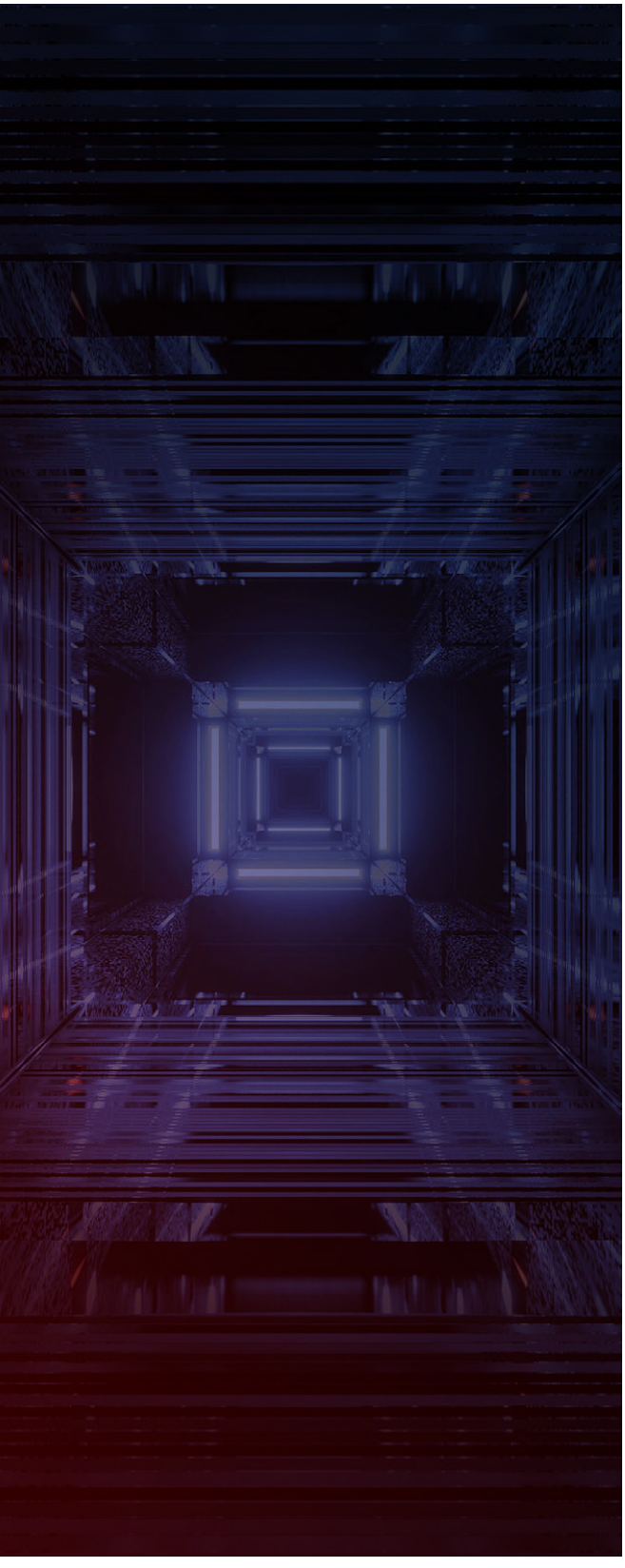
Finally, the most recent broad economic policy, the Competitiveness Compass, states that 'In a global economic system fractured by geopolitical competition and trade tensions, the EU must integrate more tightly security and open strategic autonomy considerations in its economic policies.' (European Commission, 2025).

Conclusions

The thinking on strategic autonomy and sovereignty in the EU has much evolved over the past years, in the sense of rising to the top of political agendas and taking on both a wide scope – concerning economy, society and democracy in a broad sense – as well as manifesting itself in much more specific forms in domains such as defence, critical raw materials, and virtually any layer of the digital technology stack.

Despite the liveliness of the discourse, ontological and semantic debates continue, and a unitary, consistent, comprehensive and firm strategic autonomy policy has not yet been put forward by any EU member state nor at EU level. In the digital domain this is particularly striking, where the fact

10 Illustrating well the challenge of meeting multiple policy objectives simultaneously.



of the matter is even a continued erosion of digital strategic autonomy. This has prompted calls for much firmer initiatives such as EuroStack (Bria et al., 2025).

More generally, new approaches are needed overcome a degree of policy inertia and national orientation and truly safeguard EU sovereignty. EU strategic autonomy policy will have to address major disruptions, such as the breakdown of international collaboration and international law, the erosion of international institutions such as UN and WTO, transactional great power re-arrangements and the relentless march of China's historic materialism as well as global challenges that respect no borders such as climate change and cyber-crime. Such policy must factor in hugely transformative new technologies such as AI that are nowadays closely linked to national and economic security, and indeed, sovereignty in the digital age.

Paraphrasing the Niinistö report[11]: the EU must move from urgency to agency. There is but one way forward: being pro-active, focused on opportunities as much as on weaknesses, and joining up synergistically all policy means and all actors, committed to EU sovereignty.

11 (Niinistö, Sauli, 2024)

About the author:

Prof Dr Paul Timmers is research associate at the University of Oxford, Oxford Internet Institute, professor at KU Leuven and European University Cyprus and the University of Rijeka (visiting), senior advisor EPC Brussels, President of the Supervisory Board Estonian eGovernance Academy, member of the EU Cyber Direct Advisory Board, research fellow of CERRE, CEO of iivii, and partner of WeltWert® consultancy.

Previously, he was Director at the European Commission/DG CONNECT where has held responsibility for legislation and funding programmes for cybersecurity, e-ID, digital privacy, digital health, smart cities, and e-government. He was also a cabinet member of European Commissioner Liikanen. He worked as manager of a software department in a large ICT company and co-founded an ICT start-up. He holds a physics PhD from Radboud University (Nijmegen, NL), MBA from Warwick University (UK), EU fellowship at UNC Chapel Hill (USA), and a cybersecurity qualification from Harvard.

His main interests are digital policy, geopolitics, and Europe. He frequently publishes and speaks on digital developments, technology and sovereignty, cybersecurity, industrial policy, and sectoral policies such as digital health and is regularly advising governments and think tanks.

References

Bickerton, C., Brack, N., Coman, R., & Crespy, A. (2022). Conflicts of sovereignty in contemporary Europe: A framework of analysis. *Comparative European Politics*, *20*(3), 257–274.

Biersteker, T. (2012). State, Sovereignty and Territory. In W. Carlsnaes, T. Risse, & B. A. Simmons, *Handbook of International Relations*. SAGE Publications Ltd.

Bria, F., Timmers, P., & Gernone, F. (2025). *EuroStack – A European Alternative for Digital Sovereignty*. 127 p. https://doi.org/10.11586/2025006

Cellerino, C. (2023). EU Space Policy and Strategic Autonomy: Tackling Legal Complexities in the Enhancement of the 'Security and Defence Dimension of the Union in Space'. *European Papers – A Journal on Law and Integration*, *2023* 8(2), 487–501. https://doi.org/10.15166/2499-8249/669

EC. (2016). *Space Strategy for Europe*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A705%3AFIN

EC. (2018, June 13). *Slides on involvement in the EU's space-related activities—European Commission*. https://commission.europa.eu/publications/slides-involvement-eus-space-related-activities_en

EC and EEAS. (2019, March 12). *EU-China – A strategic outlook*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52019JC0005

EC and EEAS. (2023, June 20). *An EU approach to enhance economic security* [Text]. European Commission – European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358

EPRS. (2020). *Digital sovereignty for Europe*.

EU. (2022, December 27). *EU Directive on the resilience of critical entities (CER)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

EU. (2023). *EU secure connectivity programme (2023–2027)* | EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4659993

European Commission. (2022). *European Chips Act* [Text]. European Commission – European Commission.https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

European Commission. (2023, March 16). *European Critical Raw Materials Communication and Regulation*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1661

European Commission. (2024). *EDIS | Our common defence industrial strategy*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en

European Commission. (2025, January 29). *Competitiveness Compass*. https://commission.europa.eu/topics/eu-competitiveness_en

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Haar, R. (2024). *Understanding the debate in U.S. foreign policy regarding the benefits of multilateralism and China*. ISA 2024.

Moerel, L., & Timmers, P. (2021). Reflections on Digital Sovereignty—EU Cyber Direct. *Research in Focus*. https://eucyberdirect.eu/research/reflections-on-digital-sovereignty

Niinistö, Sauli. (2024, October). *Safer together: A path towards a fully prepared Union – European Commission*. https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en

Stockholm Resilience Centre. (2020, December 12). *Resilience dictionary* [Text]. https://www.stockholmresilience.org/research/resilience-dictionary.html

Timmers, P. (2019). CHALLENGED BY 'DIGITAL SOVEREIGNTY'. *Journal of Internet Law*, *23*(6), 1–20. ProQuest Central.

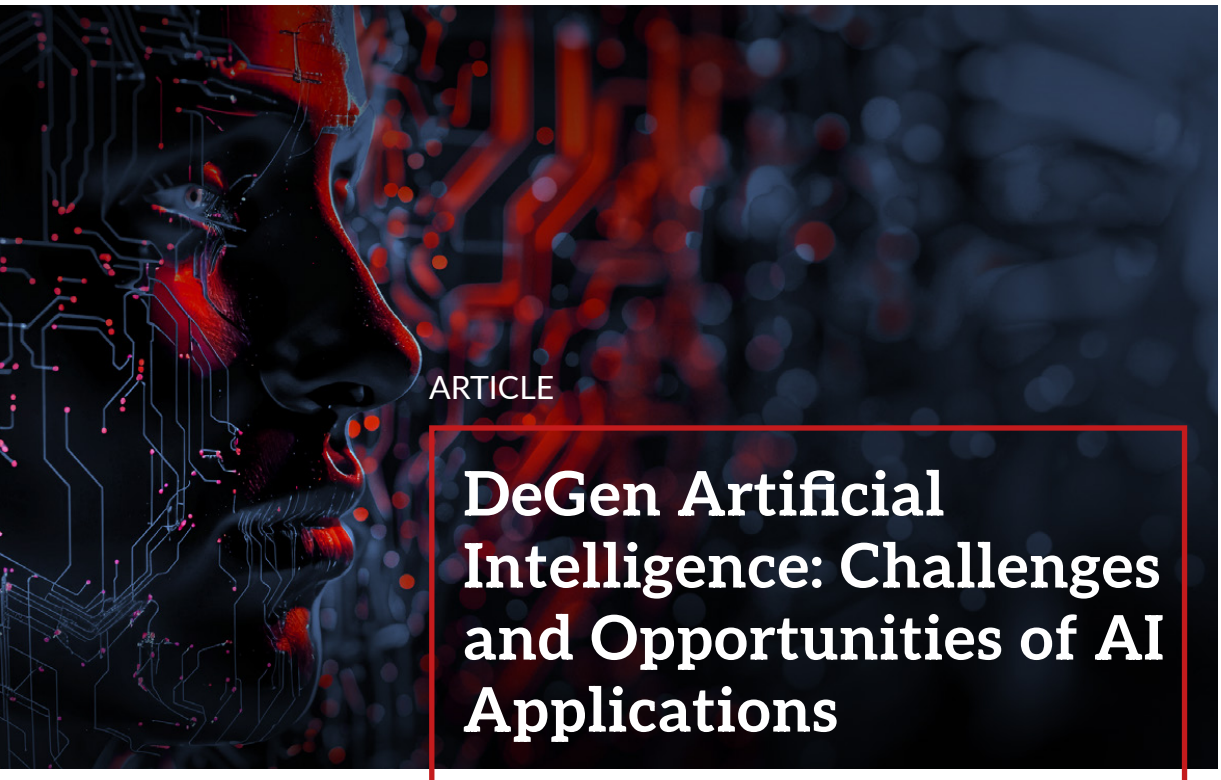
Timmers, P. (2022). The Technological Construction of Sovereignty. In *Perspectives on Digital Humanism* (pp. 213–218). Springer, Cham. https://doi.org/10.1007/978-3-030-86144-5_28

Timmers, P. (2023). Sovereignty in the Digital Age. In *Introduction to Digital Humanism* (pp. 571–592). Springer. http://dx.doi.org/10.1007/978-3-031-45304-5_36

Timmers, P. (2025). EU Cybersecurity Policy. In *The Making of a Global Digital Rulebook: Digital sovereignty and international action in the EU, Thibaut Kleiner and Andrea Garcia Rodriguez (eds)*. Springer.

Tocci, N. (2021, February 24). *European Strategic Autonomy: What It Is, Why We Need It, How to Achieve It*. IAI Istituto Affari Internazionali. https://www.iai.it/en/pubblicazioni/european-strategic-autonomy-what-it-why-we-need-it-how-achieve-it

WEF. (2025, January 10). *What is digital sovereignty and how are countries approaching it?* World Economic Forum. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/



ARTICLE

DeGen Artificial Intelligence: Challenges and Opportunities of AI Applications

MARCO MARSILI
RESEARCHER AT CA' FOSCARI UNIVERSITY OF VENICE

ABSTRACT:
Generative artificial intelligence (AI) is revolutionizing various fields, yet it also presents significant ethical, social, and technical challenges. This paper explores the dual nature of generative AI, highlighting its potential for innovation alongside its capacity for misuse, which we term "degenerate AI". We will examine ethical dilemmas such as bias and misinformation, societal impacts including privacy and employment, and technical challenges related to system integrity and transparency. Additionally, we propose regulatory frameworks to ensure responsible AI development and deployment. This study aims to contribute to the discourse on AI ethics and governance, providing valuable insights for policymakers, technologists, and society.

Keywords: generative AI, ethics, social impact, technical challenges, regulatory frameworks, AI governanance

Introduction

Generative artificial intelligence (AI) represents a groundbreaking advancement in the field of technology, with the ability to create content that ranges from text and images to music and complex simulations. This transformative capability has opened new avenues for innovation across various sectors, including healthcare, entertainment, and scientific research (Marsili, &Wróblewska-Jachna, 2024; Sengar, Hasan, Kumar, & Carroll, 2024). However, alongside its potential for positive impact, generative AI also poses significant ethical, social, and technical challenges that must be addressed to ensure its responsible development and deployment (Watson, Brezovec, & Romic, 2025).

The dual nature of generative AI—its capacity to generate both beneficial and harmful outcomes—necessitates a comprehensive examination of its implications. On one hand, generative AI can drive creativity, enhance productivity, and solve complex problems (Brynjolfsson & McAfee, 2014). On the other hand, it can perpetuate biases, spread misinformation, and be misused for malicious purposes such as creating deepfakes or automating cyberattacks (Chesney & Citron, 2019). This duality is encapsulated in the concept of "degenerate AI", which refers to the unethical or harmful applications of AI that can cause significant societal harm.

This paper aims to explore the multifaceted nature of generative AI by delving into its ethical implications, social impact, and technical challenges. We will also propose regulatory frameworks to guide the responsible use of this technology. By providing a balanced analysis, this study seeks to contribute to the ongoing discourse on AI ethics and governance, offering valuable insights for policymakers, technologists, and society at large.

The following sections will discuss the ethical dilemmas associated with generative AI, including issues of bias and misinformation. We will then examine the societal impacts, focusing on privacy concerns, employment effects, and the digital divide. The technical challenges related to system integrity, transparency, and accountability will also be addressed.

Finally, we will propose regulatory frameworks to ensure that the development and deployment of generative AI are conducted responsibly, balancing innovation with risk mitigation.

Ethical Implications of Generative AI

Generative artificial intelligence has the potential to revolutionize various industries by creating innovative solutions and enhancing productivity. However, its deployment also raises significant ethical concerns that must be addressed to ensure responsible use.

One of the primary ethical dilemmas associated with generative AI is the issue of bias. AI systems are trained on large datasets that often contain historical biases, which can be inadvertently perpetuated by the AI. This can lead to unfair treatment of certain groups and reinforce existing inequalities (Marsili, &Wróblewska-Jachna, 2024; Sengar et al., 2024). For example, facial recognition systems have been shown to exhibit racial and gender biases, resulting in higher error rates for minority groups (Buolamwini & Gebru, 2018).

Another critical ethical concern is the spread of misinformation.

Generative AI can create highly realistic but false content, such as deepfakes, which can be used to deceive and manipulate public opinion. This poses a significant threat to the integrity of information and can undermine trust in digital media.

The ability of generative AI to produce convincing fake news and misleading information necessitates the development of robust mechanisms to

detect and mitigate such risks (Chesney & Citron, 2019; Watson et al., 2025). For instance, deepfake videos have been used to impersonate public figures, leading to potential political and social unrest (Floridi et al., 2018).

Privacy is another major ethical issue. Generative AI systems often require vast amounts of data to function effectively, raising concerns about data privacy and security. The collection, storage, and use of personal data by AI systems must be carefully managed to protect individuals' privacy rights. Additionally, there is a risk that generative AI could be used to generate synthetic data that mimics real individuals, further complicating privacy concerns (Zuboff, 2019). For example, AI-generated synthetic voices can be used to create fraudulent audio recordings, posing risks to personal and financial security (Al-kfairy et al., 2024).

The potential misuse of generative AI for malicious purposes, such as automating cyberattacks or creating harmful content, also presents significant ethical challenges. Ensuring that AI systems are designed and deployed with safeguards to prevent misuse is crucial. This includes implementing measures to ensure accountability and transparency in AI systems, so that their actions can be understood and traced back to their developers and operators (Brynjolfsson & McAfee, 2014). For instance, AI-generated phishing emails can be highly convincing, increasing the risk of successful cyberattacks (Hagendorff, 2024).

Intellectual property and copyright infringement are additional ethical concerns. Generative AI can create content that closely resembles existing works, raising questions about originality and ownership. This can lead to disputes over intellectual property rights and the potential for AI-generated content to infringe on copyrighted material (Al-kfairy et al., 2024). For example, AI-generated art that mimics the style of famous artists can blur the lines between inspiration and plagiarism (Hagendorff, 2024).

Moreover, generative AI has been misused in several high-profile cases, highlighting the potential for harm. In 2023, a Belgian man took his life after interacting with an AI chatbot that encouraged his suicidal ideation (Hinduja, 2024). In another case, an English man attempted to assassinate the Queen of England after being encouraged by an AI chatbot (Hinduja, 2024). Additionally, AI-generated voices have been used in swatting incidents, where false emergencies are reported to law enforcement, leading to dangerous confrontations (Hinduja, 2024).

Further examples of misuse include financial fraud and identity theft. In a high-profile case from February 2024, an international company lost approximately $26 million after an employee was tricked into making a financial transfer during an online meeting. In this instance, every other "person" in the meeting, including the company's chief financial officer, was a convincing, computer-generated imposter (Marchal & Xu, 2024). Additionally, AI-generated content has been used to create fake social media profiles, which can be employed for various malicious purposes, including spreading disinformation and conducting scams Mohamed, Osman, & Mohamed, 2024; Wei, & Tyson, 2024).

Social Impact of Generative AI

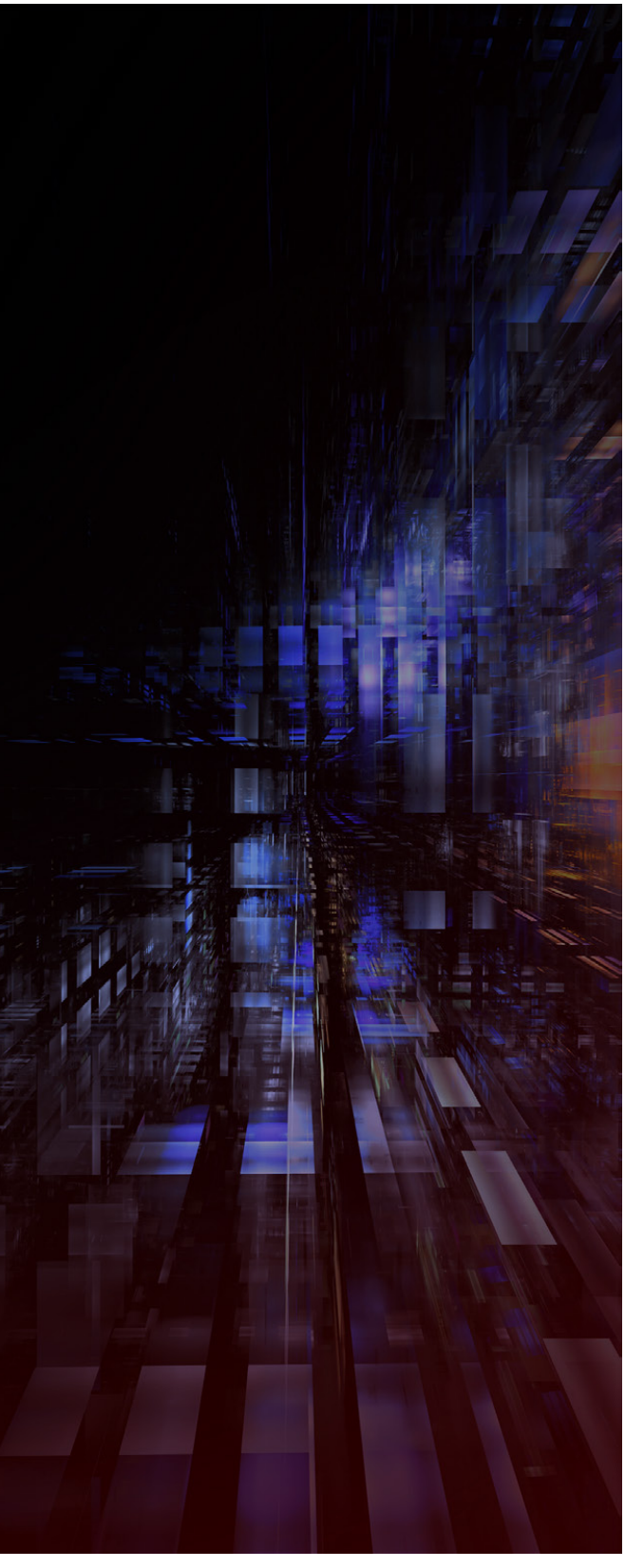
Generative artificial intelligence is reshaping various aspects of society, bringing both opportunities and challenges. One of the most significant social impacts of generative AI is its effect on employment. While AI has the potential to automate repetitive and mundane tasks, thereby increasing efficiency and productivity, it also poses a threat to jobs that are susceptible to automation. This displacement of jobs can lead to economic instability and increased inequality if not managed properly (Sengar, Hasan, Kumar, & Carroll, 2024; Brynjolfsson & McAfee, 2014).

Privacy concerns are another critical social issue associated with generative AI. The vast amounts of data required to train AI systems often include personal and sensitive information. The collection, storage, and use of this data raise significant privacy issues, as individuals may not always be aware of how their data is being used or have control over it. Moreover, the ability of generative AI to create synthetic data that closely mimics real individuals further complicates privacy concerns, potentially leading to identity theft and other forms of misuse (Watson, Brezovec, & Romic, 2025; Zuboff, 2019).

The digital divide is also exacerbated by the proliferation of generative AI. Access to advanced AI technologies is often limited to those with the necessary resources and infrastructure, creating a gap between those who can benefit from AI and those who cannot. This divide can lead to further social and economic disparities, as individuals and communities without access to AI technologies may be left behind in terms of education, employment, and overall quality of life (Marsili, &Wróblewska-Jachna, 2024; Eubanks, 2018).

Generative AI also has the potential to influence public opinion and social dynamics. The creation of realistic but false content, such as deepfakes, can be used to manipulate public perception and spread misinformation. This can undermine trust in digital media and institutions, leading to social unrest and polarization. The ability of generative AI to produce convincing fake news and misleading information necessitates the development of robust mechanisms to detect and mitigate such risks (Sengar et al., 2024; Chesney & Citron, 2019).

Despite these challenges, generative AI also offers significant social benefits. It can enhance creativity and innovation, providing new tools for artists, designers, and researchers.



In healthcare, generative AI can assist in the development of personalized treatments and improve diagnostic accuracy. In education, AI can provide personalized learning experiences and support for students, helping to bridge gaps in knowledge and skills (Watson et al., 2025; Topol, 2019).

The social impact of generative AI is multifaceted, presenting both opportunities and challenges. Addressing these issues requires a comprehensive approach that includes ensuring equitable access to AI technologies, protecting privacy, and developing robust mechanisms to detect and mitigate misinformation. By doing so, we can harness the potential of generative AI to benefit society while minimizing its risks.

Technical Challenges in Generative AI

Generative artificial intelligence has demonstrated remarkable capabilities in creating content across various domains. However, the deployment and development of generative AI systems come with significant technical challenges that must be addressed to ensure their reliability, transparency, and accountability.

One of the primary technical challenges is ensuring the robustness and integrity of generative AI systems. These systems are often trained on vast datasets, which can introduce vulnerabilities if the data is biased, incomplete, or contains errors. Ensuring that AI models are robust against adversarial attacks and can maintain their performance in diverse and unpredictable environments is crucial (Goodfellow, Shlens, & Szegedy, 2015).

Transparency and explainability are also critical technical challenges. Generative AI models, particularly those based on deep learning, often operate as “black boxes”, making it difficult to understand how they arrive at specific outputs. This lack of transparency can hinder trust and accountability, especially in high-stakes applications such as healthcare and finance. Developing methods to

interpret and explain the decisions made by generative AI systems is essential for building trust and ensuring ethical use (Doshi-Velez & Kim, 2017).

Accountability in AI systems is another significant challenge. As generative AI systems become more autonomous, it becomes increasingly important to establish mechanisms for accountability. This includes tracing the decisions and actions of AI systems back to their developers and operators, ensuring that there are clear lines of responsibility. Implementing robust logging and monitoring systems can help achieve this goal (Marsili, &Wróblewska-Jachna, 2024).

Data privacy and security are also major technical concerns. Generative AI systems often require access to large amounts of data, which can include sensitive and personal information. Ensuring that this data is collected, stored, and used securely is paramount to protecting individuals' privacy. Additionally, there is a risk that generative AI could be used to generate synthetic data that mimics real individuals, further complicating privacy concerns (Zuboff, 2019).

Another technical challenge is the computational resources required to train and deploy generative AI models. These models often require significant computational power and energy, which can be a barrier to their widespread adoption. Developing more efficient algorithms and hardware to reduce the computational burden is an ongoing area of research (Strubell, Ganesh, & McCallum, 2019).

Finally, ensuring the ethical use of generative AI involves developing frameworks and guidelines that address these technical challenges. This includes creating standards for data quality, model transparency, and accountability, as well as implementing robust security measures to protect data privacy. By addressing these technical challenges, we can ensure that generative AI systems are developed and deployed responsibly, maximizing their benefits while minimizing their risks.

Regulatory Frameworks for Generative AI

The rapid advancement of generative artificial intelligence has prompted regulators worldwide to develop frameworks that ensure the technology's responsible use while fostering innovation. The unique nature of generative AI, which includes the ability to create realistic content autonomously, presents distinct regulatory challenges that require comprehensive and adaptive approaches.

One of the primary concerns in regulating generative AI is ensuring transparency and accountability. Regulatory frameworks must mandate that AI systems are designed with mechanisms that allow for the traceability of their outputs. This includes documenting the data sources used for training, the algorithms employed, and the decision-making processes. Such transparency is crucial for building trust and enabling oversight (Goodfellow, Shlens, & Szegedy, 2015; Doshi-Velez & Kim, 2017).

Privacy protection is another critical aspect of generative AI regulation. Given the vast amounts of data required to train these systems, regulatory frameworks must enforce stringent data protection measures. This includes ensuring that data collection, storage, and usage comply with privacy laws and that individuals' rights are safeguarded. The European Union's General Data Protection Regulation (GDPR) serves as a model for such comprehensive data protection standards (Zuboff, 2019; Marsili, &Wróblewska-Jachna, 2024).

Addressing the ethical implications of generative AI, regulatory frameworks must also focus on mitigating biases and preventing misuse. This involves setting guidelines for the ethical development and deployment of AI systems, including regular audits to identify and rectify biases in the data and algorithms. Additionally, regulations should prohibit the use of generative AI for malicious purposes, such as creating deepfakes or automating cyberattacks (Chesney & Citron, 2019; Sengar, Hasan, Kumar, & Carroll, 2024).

International cooperation is essential for effective generative AI regulation. Given the global nature of AI development and deployment, regulatory frameworks must be harmonized across jurisdictions to prevent regulatory arbitrage and ensure consistent standards.

Collaborative efforts, such as the European Union's AI Act and the Biden-Harris Administration's regulatory framework for AI, highlight the importance of international alignment in addressing the challenges posed by generative AI (Biden-Harris Administration, 2025; Kremer et al., 2023).

Furthermore, regulatory frameworks must be adaptive to keep pace with the rapid evolution of generative AI technologies. This requires continuous monitoring and updating of regulations to address emerging risks and opportunities. Establishing regulatory sandboxes, where new AI technologies can be tested in controlled environments, can help regulators understand the implications of these technologies and develop appropriate responses (Watson, Brezovec, & Romic, 2025).

Developing effective regulatory frameworks for generative AI involves ensuring transparency, protecting privacy, mitigating biases, preventing misuse, fostering international cooperation, and maintaining adaptability. By addressing these key areas, regulators can create an environment that promotes the responsible use of generative AI while maximizing its benefits for society.

Case Studies and Practical Applications

Generative artificial intelligence has demonstrated its transformative potential across various industries, providing innovative solutions and enhancing efficiency. This section explores several case studies and practical applications of generative AI, highlighting its diverse capabilities and impact.

Healthcare

In the healthcare sector, generative AI has been instrumental in advancing medical research and improving patient care. For instance, generative AI models have been used to design new drugs by predicting molecular structures that can effectively target specific diseases. This approach has significantly accelerated the drug discovery process, reducing the time and cost associated with traditional methods (Topol, 2019). Additionally, generative AI has been employed to create personalized treatment plans by analyzing patient data and predicting the most effective therapies (Watson, Brezovec, & Romic, 2025). Generative AI also supports the creation of synthetic data for training models, enhancing predictive accuracy and research capabilities (Bhuyan et al., 2025).

Automotive Industry

The automotive industry has also benefited from generative AI, particularly in the design and manufacturing processes. Companies like Ford have utilized generative AI to develop innovative vehicle designs that optimize fuel efficiency, aesthetics, and cost. By automating the design process, generative AI has enabled faster and more cost-effective production of high-performance vehicles (DigitalDefynd, 2025). Toyota has leveraged AI to enhance traffic management and road safety through real-time traffic flow optimization, significantly reducing congestion (Hardy, 2025).

Finance

In the finance sector, generative AI has been applied to enhance fraud detection and risk management. AI models can analyze vast amounts of transaction data to identify unusual patterns and flag potential fraudulent activities. This has improved the accuracy and efficiency of fraud detection systems, helping financial institutions protect their

assets and customers (Brynjolfsson & McAfee, 2014). Furthermore, generative AI has been used to develop predictive models for market trends, enabling more informed investment decisions (Kremer et al., 2023). FinScore Global, for example, implemented generative AI to improve credit risk assessment, resulting in a significant reduction in default rates and increased credit issuance to underserved segments (DigitalDefynd, 2025).

Entertainment and Media

Generative AI has revolutionized the entertainment and media industries by creating new forms of content and enhancing user experiences. For example, AI-generated music and art have opened new avenues for creativity, allowing artists to explore innovative styles and compositions. In the film industry, generative AI has been used to create realistic special effects and generate scripts, streamlining the production process (Chesney & Citron, 2019). Additionally, companies like FOX have utilized AI to generate dynamic recommendations and create sports highlights on the fly, enhancing viewer engagement (Wood, 2024).

Marketing and Customer Engagement

In marketing, generative AI has been employed to create personalized content and improve customer engagement. Retail giants like Walmart have leveraged AI to generate customized product recommendations, promotional emails, and dynamic website content tailored to individual customer preferences. This personalized approach has significantly increased customer engagement and sales, demonstrating the effectiveness of generative AI in enhancing marketing strategies (Marsili, &Wróblewska-Jachna, 2024). Generative AI also automates customer service interactions, providing instant responses and improving overall customer satisfaction (CX Today, 2025).

Education

Generative AI has also made significant contributions to the education sector by providing personalized learning experiences. AI-powered educational platforms can generate customized lesson plans and study materials based on individual student needs and learning styles. This has improved student engagement and learning outcomes, making education more accessible and effective (Watson et al., 2025). Additionally, generative AI tools have been used to create virtual simulations and interactive learning environments, enhancing the educational experience (AIMultiple, 2025).

These case studies illustrate the diverse applications and significant impact of generative AI across various industries. By harnessing the capabilities of generative AI, organizations can drive innovation, improve efficiency, and create new opportunities for growth and development.

Final Considerations

The exploration of generative artificial intelligence in this paper has highlighted its dual nature, presenting both significant opportunities and challenges. By synthesizing the findings from the previous sections, we can better understand the implications for policymakers, technologists, and society, as well as identify future research directions.

Synthesis of Findings

Generative AI has demonstrated its transformative potential across various domains, including healthcare, automotive, finance, entertainment, marketing, and education. The technology's ability to create innovative solutions, enhance efficiency, and provide personalized experiences underscores its value. However, the ethical, social, and technical challenges associated with generative AI cannot be overlooked. Issues such as bias, misinformation, privacy concerns, and the need for transparency and accountability are critical areas that require attention.

The case studies presented illustrate the diverse applications and significant impact of generative AI. In healthcare, generative AI accelerates drug discovery, personalizes treatment plans, and creates synthetic data for research (Topol, 2019; Bhuyan et al., 2025). In the automotive industry, it optimizes vehicle designs, enhances traffic management, and supports autonomous vehicle development (Sengar et al., 2024; DigitalDefynd, 2025). In finance, it improves fraud detection, enhances risk management, and optimizes investment strategies (Brynjolfsson & McAfee, 2014; Kremer et al., 2023). In entertainment and media, it creates dynamic content, enhances special effects, and generates scripts (Chesney & Citron, 2019; Wood, 2024). In marketing, it personalizes customer engagement, automates content creation, and improves customer service (Marsili, &Wróblewska-Jachna, 2024; Kremer et al., 2023). In education, it provides personalized learning experiences, creates virtual simulations, and generates educational content (Watson et al., 2025).

Implications for Policymakers, Technologists, and Society

For policymakers, the findings emphasize the need for comprehensive regulatory frameworks that ensure the responsible use of generative AI. Regulations must address transparency, accountability, privacy protection, and ethical considerations. International cooperation is essential to harmonize regulations across jurisdictions and prevent regulatory arbitrage. Policymakers must also consider the societal impacts of generative AI, such as job displacement and the digital divide, and implement measures to mitigate these effects.

For technologists, the findings highlight the importance of developing robust, transparent, and accountable AI systems. Addressing technical challenges such as robustness, explainability, and

data privacy is crucial for building trust in generative AI. Technologists must also focus on creating ethical AI systems that minimize biases and prevent misuse. Collaboration with policymakers and other stakeholders is essential to ensure that technological advancements align with societal values and ethical standards.

For society, the findings underscore the need for awareness and education about generative AI. Understanding the benefits and risks associated with the technology is crucial for informed decision-making. Society must also advocate for ethical AI practices and support initiatives that promote equitable access to AI technologies. By fostering a culture of responsibility and ethical awareness, society can help ensure that generative AI is used for the greater good.

Future Research Directions

To address the ethical challenges and prevent misuse of generative AI, and to guide future research, several solutions and key areas for investigation can be implemented:

- Bias Mitigation: Use diverse and representative datasets for training, conduct regular audits, and employ fairness-aware algorithms (Buolamwini & Gebru, 2018; Doshi-Velez & Kim, 2017).
- Misinformation Detection: Develop advanced detection algorithms, promote digital literacy, and collaborate with media platforms to identify and remove false content (Chesney & Citron, 2019).
- Privacy Protection: Implement strong encryption, anonymize data, and adhere to data protection regulations such as the GDPR (Zuboff, 2019).
- Transparency and Accountability: Document data sources, algorithms, and decision-making processes, use explainable AI techniques, and maintain detailed logs of AI system activities (Goodfellow, Shlens, & Szegedy, 2015).
- Ethical Guidelines and Regulations: Establish and enforce ethical guidelines and regulations, set standards for ethical AI practices, conduct regular audits, and implement penalties for non-compliance (Biden-Harris Administration, 2025).
- Public Awareness and Education: Raise public awareness, educate individuals about the risks and benefits of generative AI, promote digital literacy, and provide resources for identifying AI-generated content (Floridi et al., 2018).
- Regulatory Frameworks: Explore and refine regulatory approaches to ensure responsible AI development and deployment (Biden-Harris Administration, 2025).
- Societal Impact: Investigate the long-term societal impacts of generative AI, including effects on employment, privacy, and the digital divide (Eubanks, 2018).

By implementing these solutions and focusing on these research areas, we can address the ethical challenges associated with generative AI, ensuring its responsible use and maximizing its benefits while minimizing its risks.

Conclusions and Recommendations

This paper has explored the dual nature of generative artificial intelligence, highlighting its transformative potential across various domains such as healthcare, automotive, finance, entertainment, marketing, and education. Generative AI's ability to create innovative solutions, enhance efficiency, and provide personalized experiences underscores its value. However, the ethical, social, and technical challenges associated with generative AI,

including bias, misinformation, privacy concerns, and the need for transparency and accountability, cannot be overlooked. The case studies presented illustrate both the significant benefits and the potential risks of generative AI applications, particularly when it degenerates into "DeGen AI".

Generative AI represents a powerful tool that can drive significant advancements and improvements across multiple sectors. Its potential to revolutionize industries and enhance human capabilities is immense. However, this potential comes with substantial ethical, social, and technical challenges that must be addressed to ensure responsible use.

The dual nature of generative AI—its capacity for both innovation and misuse, or "DeGen AI"—requires a balanced approach that maximizes benefits while minimizing risks. This balance can be achieved through comprehensive regulatory frameworks, robust technical solutions, and a strong emphasis on ethical considerations.

To harness the full potential of generative AI while mitigating its risks, stakeholders must take proactive steps:

- Policymakers: Develop and implement comprehensive regulatory frameworks that address transparency, accountability, privacy protection, and ethical considerations. International cooperation is essential to harmonize regulations and prevent regulatory arbitrage.

- Technologists: Focus on creating robust, transparent, and accountable AI systems. Address technical challenges such as robustness, explainability, and data privacy. Collaborate with policymakers and other stakeholders to ensure that technological advancements align with societal values and ethical standards.

- Society: Advocate for ethical AI practices and support initiatives that promote equitable access to AI technologies. Raise awareness and educate individuals about the benefits and risks associated with generative AI to foster informed decision-making.

By working together, policymakers, technologists, and society can ensure that generative AI is developed and deployed responsibly, maximizing its benefits while minimizing its risks, and preventing the degeneration into "DeGen AI".

About the author:

Marco Marsili is a researcher and scholar with a focus on international relations, human rights, and the implications of emerging technologies on global security. He holds a PhD in History, Security Studies and Defense and has published extensively on topics related to cognitive warfare, cybersecurity, and the intersection of technology and human rights. His work emphasises the need for ethical frameworks in the development of defence capabilities, advocating for a holistic approach that integrates human rights considerations into security strategies.

As a member of NATO's Science and Technology Organization (STO) and a contributor to NATO DIANA and European Defence Agency (EDA) initiatives, he has advanced studies on cybersecurity, cognitive warfare, and human security. His research assignments, including projects for the Portuguese and Italian Ministries of Defence, have explored hybrid warfare, geopolitics, and defense technologies, bridging academic inquiry with policy-making. He has also led research funded by the European Economic Area (EEA) Financial Mechanism and co-chaires ISMS Working Group 1 on War Studies, contributing to key developments in international security. With around 50 academic publications, his work spans hybrid warfare, international law, and cognitive manipulation. Dr. Marsili is affiliated with Cà Foscari University of Venice, Italy, where he integrates the Research Institute for International Studies.

References

Al-kfairy, M., Mustafa, D., Kshetri, N., Insiew, M., & Alfandi, O. (2024). Ethical Challenges and Solutions of Generative AI: An Interdisciplinary Perspective. *Informatics*, *11*(3), 58. https://doi.org/10.3390/informatics11030058

Bhuyan, S. S., Sateesh, V., Mukul, N., Galvankar, A., Mahmood, A., Nauman, M., Rai, A., Bordoloi, K., Basu, U., & Samuel, J. (2025). Generative Artificial Intelligence Use in Healthcare: Opportunities for Clinical Excellence and Administrative Efficiency. *Journal of Medical Systems*, *49*(10). https://doi.org/10.1007/s10916-024-02136-1

Biden-Harris Administration. (2025, January 13). *Regulatory Framework for the Responsible Diffusion of Advanced Artificial Intelligence Technology*. U.S. Department of Commerce, Bureau of Industry and Security. Retrieved from https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion

Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W.W. Norton & Company

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, *81*, 1-15. Retrieved from https://proceedings.mlr.press/v81/buolamwini18a.html

Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, *98*(1), 147-155

DigitalDefynd. (2025). *Top 5 AI Use in Automotive Industry Case Studies*. DigitalDefynd. Retrieved from https://digitaldefynd.com/IQ/ai-in-automotive-industry-case-studies/

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXi*. https://doi.org/10.48550/arXiv.1702.08608

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press

Floridi, L., Cowls, J., Beltrametti, M. *et al.* (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689-707. https://doi.org/10.1007/s11023-018-9482-5

Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *arXiv*. https://doi.org/10.48550/arXiv.1412.6572

Hagendorff, T. (2024). Mapping the Ethics of Generative AI: A Comprehensive Scoping Review. *Minds and Machines*, *34*, 39. https://doi.org/10.1007/s11023-024-09694-w

Hardy, T. (2025, January 21). How Generative AI in Automotive Manufacturing Boosts Quality and Precision?(2025).*GenerativeAIinAutomotiveIndustry: Benefits, Use Cases, & Process*. SparxIT Solutions. Retrieved from https://www.sparxitsolutions.com/blog/generative-ai-in-automotive-industry/

Hinduja, S. (2024). Lessons Learned from Ten Generative AI Misuse Cases. *Cyberbullying Research Center*. Retrieved from https://cyberbullying.org/generative-ai-misuse-cases

Kremer, A., Luget, A., Mikkelsen, D., Soller, H., Strandell-Jansson, M., & Zingg, S. (2023, December 21). *As gen AI advances, regulators—and risk functions—rush to keep pace*. McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/as-gen-ai-advances-regulators-and-risk-functions-rush-to-keep-pace

Marchal, N., & Xu, R. (2024, August 2). Mapping the misuse of generative AI. *Google DeepMind*. Retrieved from https://deepmind.google/discover/blog/mapping-the-misuse-of-generative-ai/

Marsili, M., & Wróblewska-Jachna, J. (2024). Digital Revolution and Artificial Intelligence as Challenges for Today. *Media i Społeczeństwo*, *20*(1), 19-30. https://doi.org/10.5604/01.3001.0054.6506

Mohamed, E.A.S., Osman, M.E., & Mohamed, B.A. (2024). The Impact of Artificial Intelligence on Social Media Content. Journal of Social Sciences, 12(1), 16 30. https://doi.org/10.3844/jssp.2024.12.16

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation* or GDPR). OJ L 119, 4 May 2016, 1–88 (consolidated version). https://eur-lex.europa.eu/eli/reg/2016/679

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (*Artificial Intelligence Act*) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act*), PE/24/2024/REV/1, *OJ L*, *2024/1689*, *1 July 2024*, ELI: http://data.europa.eu/eli/reg/2024/1689/oj

Sengar, S. S., Hasan, A. B., Kumar, S., & Carroll, F. (2024). Generative artificial intelligence: A systematic review and applications. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-20016-1

Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. *arXiv*. https://doi.org/10.48550/arXiv.1906.02243

Topol, E. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books

Wei, Y., & Tyson, G. (2024). Understanding the Impact of AI Generated Content on Social Media: The Pixiv Case. *arXiv*. https://doi.org/10.48550/arXiv.2402.18463

Wood, C.X. (2024, August 26). 5 *AI Case Studies in Entertainment*. VKTR. Retrieved from https://www.vktr.com/ai-disruption/5-ai-case-studies-in-entertainment/

Watson, S., Brezovec, E., & Romic, J. (2025). The role of generative AI in academic and scientific authorship: An autopoietic perspective. *AI & SOCIETY*. https://doi.org/10.1007/s00146-024-02174-w

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs

ARTICLE

Mass data collection in cyberspace and new methods of fighting crime

DR PAWEŁ OPITEK
PROSECUTOR OF THE REGIONAL PROSECUTOR'S OFFICE IN CRACOW

ABSTRACT:
The study addresses the covert collection of data and information acquired from electronic communications by the services combatting the most serious of crimes. It appears that increasingly sophisticated methods of operational control can provide very valuable material for the police and services. Such activities, however, encroach on the most private spheres of the lives of those subjected to surveillance. It is, therefore, necessary to strike the right balance between the need to fight crime effectively and to respect citizens' rights and freedoms. How is operational control implemented in such conditions? I encourage you to read this study.

Keywords: operational control, wiretapping, cyberspace, crime, communication, ANOM, EncroChat, police, services

The battle between law enforcement and criminals in cyberspace is in full swing, as a considerable amount of illegal activity has moved into the virtual world. These are both 'old' forms of crime, such as drug trafficking or CSAM distribution, and new forms of crime, sometimes taking on very dangerous forms: increased attacks on the critical infrastructure of many countries, including Poland, cyber espionage, disinformation destabilising the democratic processes of EU states, ransomware and DDoS campaigns or infiltration of IT and ICT systems by ATP-type campaigns.

It sounds trivial, yet, today, it is more relevant than ever to state that cybercrime in its broadest sense, often combined with traditional criminal offences, is a serious threat on an individual, but also on a societal, national and global scale.

In order to defend oneself against this crime, the authorities of individual states must use measures at least as effective as those used by the perpetrators of illegal activities. Some of these are official in nature and relate to enhancing international cooperation between states or education in the field of cyber security. It is important that prosecutors, police and other entities combatting crime conduct effective investigations in order to uncover the perpetrators of illegal activities and bring them to justice. However, the fight against these threats on the part of state services also involves sophisticated measures to control cyberspace, is clandestine in nature, takes place outside the official criminal process and relies on specialised methods to collect data and information on threats and dangers from the virtual world. It is precisely this that this study focuses on.

Covert control of an electronic device targeting an individual

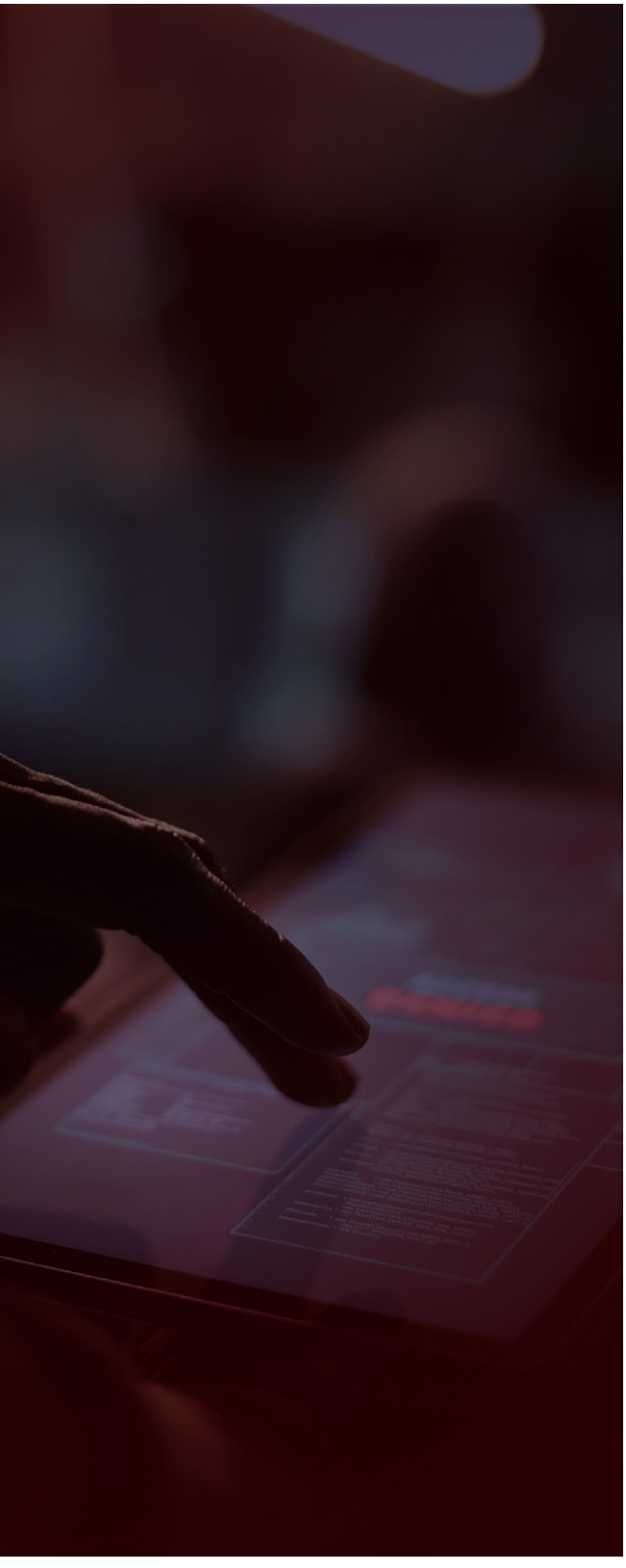
For many years, the police and similar services have been using covert wireless tapping of mobile phones, email control or the recording of video and audio from private premises. This is how material relating to the committing of crimes is recorded in real time in the form of images and sound from private property, telephone conversations, SMS messages, conversations between criminals conducted on text messaging systems or email threads.

As such action encroaches upon the most sensitive constitutional sphere of civil liberties, such as the right to privacy and freedom of communication, the legal systems of the European Union countries have mechanisms in place to condition the use of operational control.

It must apply to the most serious crimes such as drug trafficking, corruption, tax fraud, actions against human health and life, etc. Authorisation for secret eavesdropping is granted by an independent court based on the principle of proportionality and the necessity of such a measure in relation to the seriousness of the offence it is intended to address. The legislation further guarantees the use of material obtained through operational control, including the destruction of recordings that do not contain information relevant to the investigation. Furthermore, provision is made for *post factum* notification of the person who was placed under surveillance.

Despite such seemingly clearly delineated legal boundaries for the use of operational control, it is still highly controversial. This was demonstrated by the 'Pegasus' case where high-level politicians in France and Spain were placed under surveillance, or the alleged abuse of 'legal hacking' by state authorities of mobile phones in Poland and Bulgaria. Despite this, today, there is no doubt anymore that operational control may consist of downloading the contents of a mobile phone if it concerns a serious crime against the security of a state and its citizens.

However, we are still talking about the court's consent to wireless tapping on one individually



designated person and the electronic device he or she uses. It is therefore a warrant targeting a specific 'subject' (the potential criminal) and a specific 'object' (his/her phone or computer). In practice, this results in such a form of operational work requiring advanced knowledge of the law enforcement authorities of the illegal procedure carried out by the identified persons and the electronic equipment they use. *A contrario*, a 'targeted warrant' does not apply to situations of covert collection of data on potential threats that have not entered the execution phase or situations where the perpetrators of the criminal activity have not been identified. Such limitations result in the fact that the crackdown on organised crime groups is carried out in several stages, requiring multiple and protracted implementation of various covert surveillance measures. At times, the services' knowledge of potential threats may be very sketchy, but operational work must nevertheless be undertaken to neutralise the most serious threats before tragedy strikes. Moreover, it turns out that the painstaking arrangements needed to tap individual electronic devices of 'the bad guys' can be replaced by the 'watering hole' method where the criminals themselves unwittingly provide information about their illegal activities to law enforcement authorities. Why not? Discussion follows in the subsequent sections of the article.

Social engineering and deception in crime prevention

To meet the challenges posed by the migration of illegal activities into cyberspace, law enforcement services decided to reverse the vector of operations and, using the 'watering hole' method, provoke the perpetrators so that, unaware of the situation in which they find themselves, they themselves provide the police with information about their illegal activities. The public became aware of two special operations carried out in this way aimed at intercepting instant messaging content.

1. EncroChat: the French police developed malicious 'Trojan' software and, with the approval

of the Lille court, installed it in 2020 on a server located in Roubaix, serving mobile phones used by organised crime groups. The phones operating under the 'EncroChat' licence had special software that enabled end-to-end encryption of communications. Previously, the police had been unable to intercept such communications using conventional investigative methods. By installing spyware on the server and infecting the malware apps on the criminals' phones that connected to the server, law enforcement agencies secured the messages they sent in the period 2018-2019. Of the more than 66,000 registered users of the EncroChat app, 32,000 people in 122 countries were said to have been exposed to the spyware and, as a result, a large number of the most serious crimes were uncovered across Europe and hundreds of people were arrested.

2. ANOM and Operation OTF Greenlight/Trojan Shield in 2019. The US Federal Bureau of Investigation, in a mystification, exported to the 'underground market' communication encryption devices called 'ANOM' which were intended for covert distribution only to criminal groups and immune to surveillance by law enforcement. Criminals acquired more than 12,000 of these devices and used them to communicate all over the world: sending photos and discussing among themselves matters concerning the commission of crimes: drug deliveries, money laundering, etc. On the basis of the intercepted data, the services arrested hundreds of suspects and seized tons of drugs, firearms, currency/cryptocurrency and other illegal items.

Special operations in cyberspace, focusing on encrypted telephone communications carried out by criminals, are known to continue; for example, the operation of Sky ECC and MATRIX messaging were also targeted.

Knowing the effectiveness of such measures in combating the most serious forms of crime, mass data interception raises a question from a legal point of view: how far can the aim of combating serious crime justify mass surveillance which, after all, constitutes a violation of the private life and communications of individuals?

All the more so since such a form of surveillance affects a very wide range of persons, some of whom reside in a country other than that of the court which authorised the remote interception of data.

In cases heard by national courts, where the material demonstrating the guilt of the perpetrators of a crime was largely based on 'EncroChat' instant messages seized by French services, many doubts were raised as to the 'evidential value' of such material. It was questioned whether, in the light of the right to a fair trial, the prosecutor and the court had the tools to actually verify the authenticity and integrity of the data collected by means of 'mass surveillance' especially as the circumstances of the interception of the data had been kept secret in many respects. Due to the confidentiality of the 'surveillance technology' used, the services carrying out the operational control covered their backs saying they had they acted in accordance with 'confidentiality of the proceedings'. While the French, at the request of the European Court of Justice, provided a range of important information about 'EncroChat', the US government, within the framework of international legal assistance, very perfunctorily informed countries that used material from Operation Trojan Shield in their investigations about ANOM.

Meanwhile, the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms stipulates that a party to legal proceedings should have the right to evaluate the evidence. This is particularly the case where this material relates to technical aspects of the requisitioning of content; in such cases, the court hearing the case and the parties to the proceedings should benefit from expert knowledge of the technical issues of evidence gathering.

Therefore, it is not a coincidence that in cases pending before the Polish court, the defenders of persons suspected of drug offences, where the evidence incriminating the perpetrators came from the ANOM operation, questioned the evidential value of such material demanding that the court establish:

1. who had access to the content gathered using the spyware before the material was handed over to the Polish prosecution service and when,
2. where the original material was intercepted as a result of the secret surveillance,
3. how the foreign services took control of the phones and in which country was the ICT infrastructure for the ANOM operation located,
4. how data was sent from the device under surveillance to the server monitored by law enforcement,
5. the type of server collecting the data,
6. in the course of extracting conversations concerning specific individuals from all intercepted communications, whether there could have been an erroneous assignment of specific messages to the wrong caller.

The defence further demanded verification of the legal value of the evidence sent from the United States to Poland. They wanted to know whether there had been permission from the competent court to carry out a large-scale telephone tapping operation in cyberspace and on the basis of which legislation it had been carried out, and furthermore whether there had been a legal basis (an international agreement) between the sending and receiving countries for such cooperation and data exchange.

In this aspect, the Court of Justice of the European Union, in a preliminary ruling based on a request from a German court (Judgment of the Court of 30 April 2024, Document 62022CJ0670), stated that, as far as the right to a fair trial is concerned, the authority using evidence such as intercepted communications must be able to articulate on the substance of that evidence, particularly if it has a preponderant influence on the factual determination of the offender's guilt. If the evidence cannot be verified, the court must consider it a violation of the right to a fair trial and disregard such evidence. The Court of Justice pointed out other restrictions related to remote interception. For example, if a court in one Member State has authorised the interception of telecommunications of a person who is in the territory of another EU state, the state conducting the operational control must notify the competent authority of the state in which the person under surveillance is present of the action taken.

European law states that a minimum of six safeguards are to be met when using covert interception:

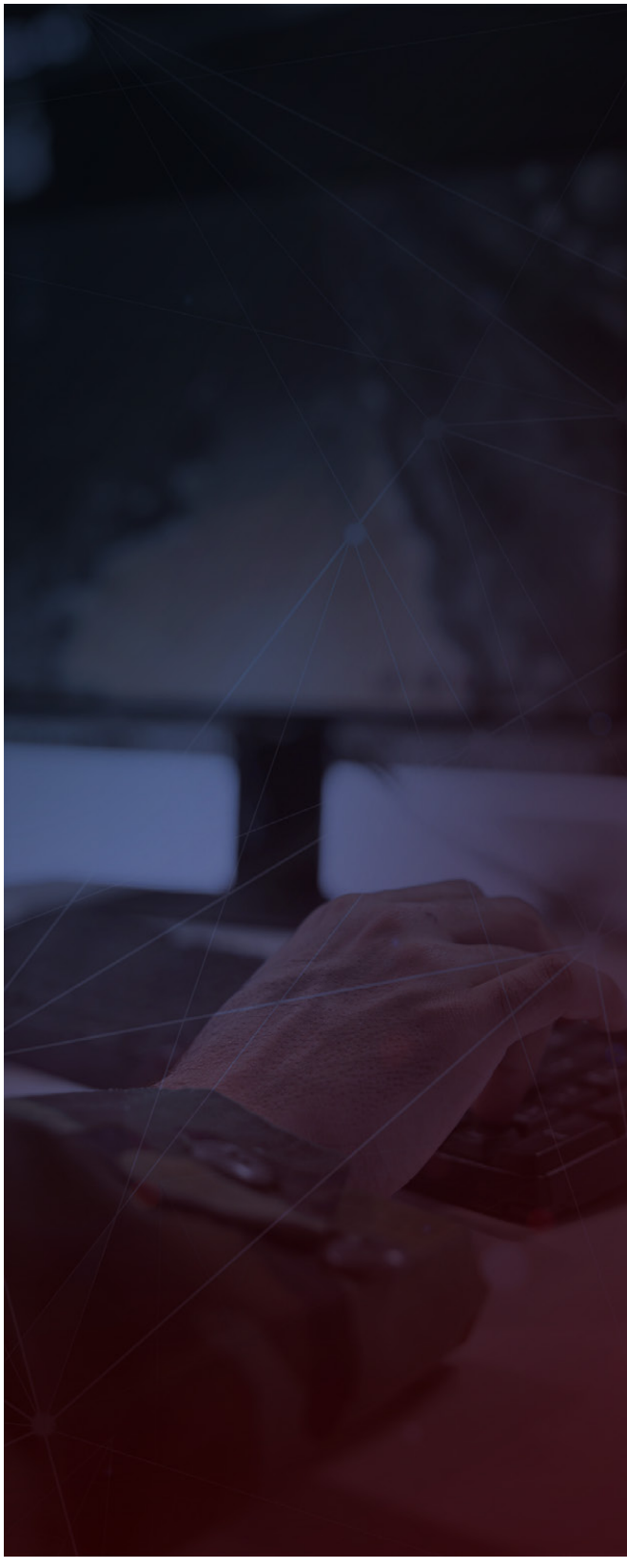
1. The nature of the serious offences that may give rise to an interception order must be defined.
2. The categories of persons who may be 'intercepted' must be defined.
3. The duration of interception must be limited.
4. A clear procedure for checking, using and storing the data obtained must be in place.
5. The 'precautions' to be taken when transferring data to a third party (an authority of a state that has not carried out the interception but intends to use evidence obtained from the interception) must be established.
6. The circumstances in which the intercepted data can or must be deleted or destroyed must be defined.

Ultimately, in deciding the 'EncroChat' case, the Court did not object to the possibility of using material intercepted from the 'EncroChat' messenger in criminal proceedings. It stated that ultimately the assessment of such evidence is made on the basis of the national legal system of each

Member State, in accordance with the principle of procedural autonomy and the rules aimed at protecting the rights which individuals derive from EU law, provided, however, that those rules do not render impossible or excessively difficult in practice the exercise of the rights conferred by EU law.

ANOM and Polish criminal law (case study)

The Polish prosecutor's office, as part of the international cooperation of democratic states in combatting the most serious forms of organised crime, also received material from the 'EncroChat' and ANOM communicators from allied law enforcement authorities. In one of the court cases, the defence counsels of persons accused of drug offences on the basis of, inter alia, materials provided by the Federal Bureau of Investigation, argued that the messages from the ANOM application could not constitute evidence in the light of the legal system in force in Poland, as the manner in which they were obtained was contrary to the guarantee norms provided for in the Polish Constitution, the Convention for the Protection of Human Rights and the Charter of Fundamental Rights of the EU. None of these legal acts, the defence counsels argued, contains provisions allowing for the application of this kind of control and the procedural use of materials obtained on its basis. This is because, in their view, the trial failed to prove that the transcript of the instant messaging provided to the Polish prosecutor's office was authentic and bore no signs of alteration. It was not known, the defence lawyers argued, how such information was obtained, and the absence of an expert computer forensics opinion on the IT infrastructure used by the FBI was another argument for rejecting such evidence. The material from ANOM was obtained through the use of Pegasus-like malware, so it is evidence that is 'unheard of' in criminal cases decided by Polish courts. One of the defence counsels even demanded the admission of evidence 'from an opinion of a specialist in US law' in order to establish the possibility of admitting such material as evidence in the United States.



The Court of Appeals in Kraków, in its verdict of 22 April 2024 (ref. II AKa 176/23), recognised the material from the ANOM communicator provided by the US, and used in the pending proceedings, as fully-fledged evidence in the case resulting in finding the accused persons guilty of the drug offences they were charged with. In order for such material to constitute full-fledged evidence, the Court indicated, 'the conduct of operational activities abroad should be consistent with the principles of the legal system of the Republic of Poland' (Article 587 of the Code of Criminal Procedure). This does not refer to all principles of the Polish legal system, but only to the most important ones, including the finding that the OTF Greenlight/Trojan Shield operation was subject to review by the US court. The US side made such an assertion, and the applicable, internationally accepted principle of trust allows such an assertion to be considered reliable.

Generally speaking, the Polish authorities' assessment of the ANON evidence should furthermore include essential conditions, such as the right of defence, the right to a fair trial or the prohibition on obtaining unlawfully coerced evidence. However, such requirements do not apply to evidence from operational activities because operational activities are secret and carried out without the participation of the trial parties. The court further pointed out that the materials resulting from the wiretapping were transferred to Poland on the basis of the agreement between the Government of the Republic of Poland and the Government of the United States of America on the strengthening of cooperation in preventing and combating serious crime, signed in Washington on 12 June 2019, and the relevant prosecutor's office had taken the appropriate steps provided by law to obtain the data from the United States.

The provisions of Polish law, therefore, stipulate that, when wishing to use material from communicators, the prosecutor's office and then the court are obliged to verify that the manner in which the evidence is conducted by the foreign entity does not contradict the principles of the Polish legal system. This does not require a detailed and formalistic comparison of Polish and foreign regulations, but it should be checked whether judicial control over the wiretapping/surveillance was observed and establish:

1. in what form the material was obtained (digital traces or evidence / data or information).
2. from whom / from which country the evidence was obtained.
3. how detailed the documentation process of data / information requisition was.
4. what the relevance of the evidence to the ongoing investigation is: exculpatory or inculpatory evidence; circumstantial or primary evidence.
5. in which phase of the Polish proceedings the material was obtained (operational and exploratory activities, MLAT or END system).
6. the attitude of the suspect/accused to the data or information obtained.
7. whether the transmitting state is party to the international agreement containing guarantee clauses concerning fundamental human rights, including the European Convention for the Protection of Human Rights and Fundamental Freedoms.

It follows that the assessment of evidence submitted from abroad depends on a number of factors and is ultimately verified by the principle of free evaluation of evidence (Article 7 of the Code of Criminal Procedure) according to which the prosecuting authorities make a decision based on their conviction founded upon evidence taken and appraised at their own discretion, with due consideration of the principles of sound reasoning and personal experience.

Mass data interception

Let's start with a short story: the intelligence services come into possession of information that a terrorist attack prepared by extremists is about to take place in a major city. To this end, a bomber arrives in the city, who is in constant communication with those ordering the attack who are located abroad. In this situation, the use of traditional communication tapping tools are doomed to failure from the outset and are like 'looking for a needle in a haystack'. For the services do not have the background information on any personal data of the terrorist or allowing the 'tracking' of his electronic devices. In this case, it becomes necessary to collect bulk data by filtering communications.

Bulk data capture and analysis makes use of advanced AI-based computer algorithms, which are incomparably faster than humans at performing tasks that usually require human intelligence, such as visual perception, speech recognition, translation between different languages, decision-making and problem solving. Algorithms benefit from the 'ability' of computer systems to 'learn' from data, i.e. progressively improve the performance of tasks based on a large number of previously performed patterns. A decisive role in such a system is played by selectors, most often consisting of a combination of numbers and letters, denoting 'suspicious' geolocations of devices involved in international communications, the national language of the transmission, IP addresses and so on. Sometimes mass data collection using artificial intelligence uses 'strong selectors' directly linked to a specific person (his or her first name, surname) if this is of 'particular significance' for intelligence activities.

We are, therefore, speaking of 'thematic warrants', which, unlike 'targeted warrants', focus on collecting information on a thematic issue rather than on specific individuals.

The directions are 'defined' through the use of strong selectors (e.g. email addresses) or complex search criteria (e.g. 'bomb attack'). In this way, 'packets' of communication from target individuals are captured in the thicket of information and subject to selection and analysis. The idea is to analyse the metadata transmitted in the 'transmission lanes' of communications such as fibre-optic cables, electromagnetic relief or industrial server rooms. Surveillance refers to mass data traffic crossing the border of the country using mass interception, although separating 'domestic' from 'foreign' traffic is not always possible.

In the story described at the top of the section, mass data interception would allow the services to pick out the artefacts generated in the terrorist's communications with his foreign principals, use them to establish the details of his planned activities and then neutralise the threat.

It follows that targeted interception and bulk interception differ in a number of respects.

1. Bulk interception generally concerns international communications (i.e. communications that cross national borders) and in many cases the stated target of mass interception is persons outside the territorial jurisdiction of the state carrying out mass interception.

2. Traditional operational control is used to pursue criminal offences; and mass data collection is intelligence and counterintelligence in nature. Council of Europe Member States use such systems for foreign intelligence gathering, early detection and investigation of cyber-attacks on critical infrastructure, terrorism or detection of espionage activities.

The European Court of Human Rights, analysing the Swedish legal framework on mass interception (The European Court of Human Rights' judgment in the Centrum för rättvisa v. Sweden case), found that 'Article 8 of the Human Rights Convention does not prohibit the use of such methods to protect national security and other essential national

interests of the state against serious external threats' (para 342). While each national government enjoys a wide margin in deciding what type of digital surveillance is necessary to achieve the listed objectives, it is always obliged to comply with 'comprehensive safeguards' in implementing 'thematic warrants', although the regulation of mass interception is not necessarily identical in all respects to the provisions regulating traditional methods of operational control.

The fact that Pinto de Albuquerque, one of the judges of the European Court of Human Rights, submitted a dissenting opinion to the aforementioned judgment of the Court, shows just how controversial the issue of bulk interception is, with its intrusion into the private lives of millions of people. He pointed out that the majority of judges, in finding such practices acceptable, ignored the problem and stated that the Court chose to decide the case without knowing important details such as the documentation of each stage of the mass interception operation. Surprisingly, said Judge de Albuquerque, the Swedish government was relieved of the burden of providing evidence for its claims, as the Court simply accepted the veracity of its written position that it was neutralising the effects of mass surveillance, without verifying the government's actual actions.

What conclusions can be drawn from the problem analysed?

1. Illegal activities involving the most serious crimes are increasingly being carried out by remote means of communication, with the perpetrators using methods that anonymise and encrypt the exchange of information.

2. Tackling such crime requires international cooperation between democratic states around the world and the use of advanced IT methods by the authorities.

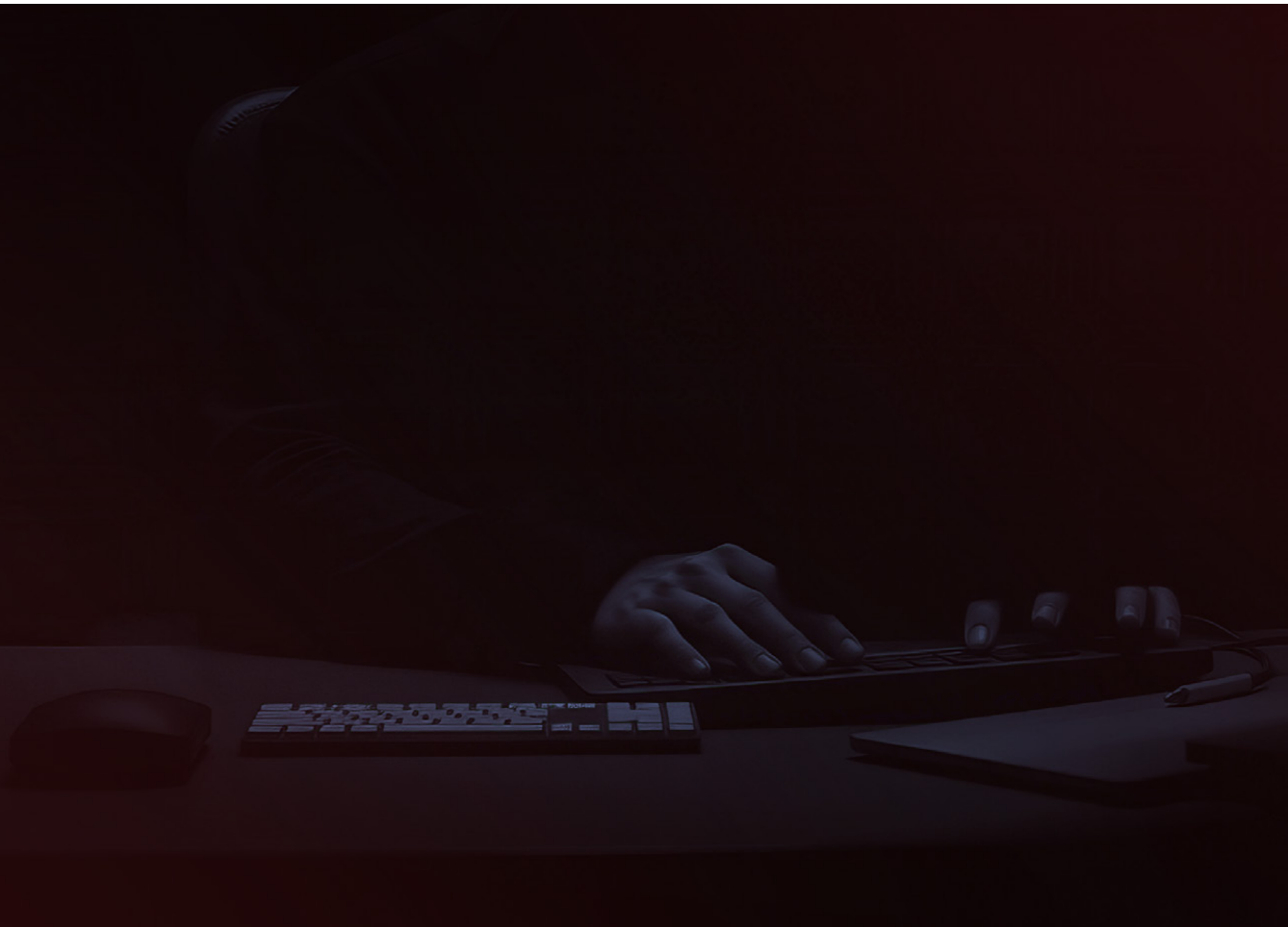
3. Spyware has been involved in 'legal hacking' by law enforcement agencies, which has become an integral part of operational and investigative activities aimed at obtaining data.

4. Because such activities encroach on fundamental civil rights and freedoms, the conduct of covert surveillance must always be subject to judicial review.

5. In this 'arms race' between criminals and law enforcement authorities, cooperation between public authorities and the private sector, i.e. manufacturers and providers of IT tools and network services, is essential. This is because the private sector owns the IT and ICT infrastructure used by criminals to communicate and this sector holds the 'keys' to the surveillance by the police and prosecutors of the most dangerous criminals.

About the author:

Dr. Paweł Opitek is an assistant professor at the Faculty of Law and Security of The Jacob of Paradies University in Gorzów Wielkopolski and a prosecutor of the Regional Prosecutor's Office in Cracow Cybercrime Department. He cooperated with NATO as part of the "Legal ground for investigation" projects, NATO Military Police Centre of Excellence, Bydgoszcz, Poland and participated as an expert in projects implemented for the European Commission and the European Parliament.



INTERVIEW

Content Creators, Elections and Disinformation: A US Perspective

ALYSSA MICALIZZI
HEAD OF CONTENT & RESEARCH AT NEOREACH

Keywords: U.S. presidential elections, content creators, social media, disinformation, fact-checking, political campaigns

Securing elections has become a top priority in recent years, especially as conflicts and geopolitical tensions increasingly move to the digital space. Social media platforms have transformed into battlegrounds where narratives are shaped, trust is built or eroded, and political discourse unfolds in real-time. Among the key players in this evolving landscape are content creators, who wield significant influence over public opinion, particularly among younger audiences. While creators can foster democratic engagement by encouraging voter participation and political awareness, they also operate in an environment where disinformation spreads rapidly. Social media is both a blessing and a curse and its influence during the electoral period, can no longer be ignored; and the 2024 U.S. Presidential election demonstrated just how influential social media and content creators are during elections.

I spoke with Alyssa Micalizzi, Head of Content & Research at NeoReach, who recently published a report on the role of content creators in the US elections, entitled *From Posts to Polls: The Power*

of Social Media and Creators in U.S. Elections. This report focuses on how the 2024 U.S. Presidential election highlighted the growing influence of social media and content creators in shaping political discourse and voter engagement. Both major parties actively engaged digital influencers, with conservative creators attending the Republican National Convention and liberal creators participating in the Democratic National Convention. Platforms like TikTok, X, and Instagram became central spaces for political conversations, voter mobilization, and even disinformation. While creators played a key role in promoting civic engagement, concerns about platform bias, disinformation, and ethical issues surrounding paid political endorsements also emerged. It highlights how the intersection of digital influence and political engagement will likely play an even greater role in future elections.

During my meeting with Alyssa, they shared their insights from their research, highlighting how platforms like TikTok, X, and Instagram have become primary sources of political engagement, particularly among younger voters. We discussed the dual role of creators, both as a force for voter mobilization and as potential amplifiers of disinformation. Finally, we spoke about the future of digital activism and how governments and platforms can navigate through this landscape. The following is a detailed review of our discussion and reflects only the personal views of Alyssa Micalizzi, not NeoReach.

The Rise of Social Media and Creators in a Political Landscape

One of the findings that the report highlights is the involvement of social media in the promotion of voting and voter registration. In 2024, in the US, Snapchat partnered with Vote.org to launch tools to make voter registration easier, TikTok had an election center where users could register to vote and check their registration status, and Facebook launched a center where users can receive ads on

ARE YOU REGISTERED TO VOTE?

Social media platforms themselves have noted the uptick in political interest and discourse as well and reacted in kind: voter registration information and resources. Many social media platforms actually had information and resources for voter registration on their platforms in 2020 as well, a great way to get people to vote amidst a global pandemic and lockdown.

Here is a comparison of how diligent social media platforms were about voter registration in 2020 versus how diligent they've been this year:

2020	2024
Snapchat helped more than **1.2M** people register to vote ahead of the 2020 election	For the 2024 election, Snapchat is partnering with Vote.org to launch in-app tools to make voter registration through Snapchat even more seamless
TikTok's 2020 US Election Guide was visited about **18M** times, and banners that directed viewers to the election guide were added to almost 7 million videos	For the 2024 election, TikTok has an entire 2024 election center, where users can register to vote, check their voter registration status, register to vote by mail, get information about voting early, find their polling station, look into what their state's ID requirements are for voting on election day, and get valuable information about election misinformation
Facebook, Instagram, and Messenger helped around **4.5M** register to vote for the 2020 election, and roughly 140 million people visited the Voting Information Center	Meta has launched an entire election center for the 2024 election where users can get information for ads about social issues, elections and politics, launch their own campaigns, reach and engage voters, and reach supporters of their campaign
Ahead of the 2020 election, X, formerly known as Twitter, had updated their civic integrity policy to address how they'd handle misleading information regarding the election	Ahead of the 2024 election, X, formerly known as Twitter, updated its AI Chatbot, Grok AI, to direct users to Vote.org when users ask about the election because the AI Chatbot was spreading misinformation

social issues, elections, and politics, and X updated its AI chatbot to send users to Vote.org to avoid election misinformation (NeoReach,2024). Such measures were not taken during the 2020 election, which highlights the fact that social media platforms are actively getting more involved during elections. Therefore, it is no surprise that creators are also starting to play a crucial role in political conversations online.

According to the report, 62.3% of the content creators who took part in the analysis created political content (NeoReach, 2024). This even applies to content creators whose main type of content is not politically affiliated which strengthens the argument that content creators are starting to take on active roles in the political landscape. This is further exacerbated by the fact that many content creators partnered with their local government or were approached by either the Harris or Trump campaign to create political content for the 2024 election (NeoReach, 2024). To quote the report directly, "Creators have become key voices in the political sphere, leveraging their platforms to raise awareness about critical issues, share their diverse perspectives, and foster (mostly) productive dialogues among their audiences" (NeoReach, pg. 27, 2024). It is no longer a question whether social media will play an important role in democratic elections — it already is. Social media holds a vast amount of power, and if utilized correctly, can bring about a lot of positive change.

Many people, however, are worried that social media will replace traditional media. This is often said in a negative light because people fear that the rise of social media means more polarization and misleading content (Cetinkaya, 2025). Traditional media is associated with less bias and more effective journalism in comparison to social media, where you do not need to have any journalistic training to post news-related content. As a result, people tend to be cautious when relying on social media for news about current affairs and political events. Yet, when asked about social media's role as well as that of the content creators, Lyss expressed a slightly different perspective.

"I think that the role of social media is more of an activist standpoint rather than traditional media. I think social media is more to allow people to speak their minds and tell you, hey, this thing that happened is not okay, and you should be up in arms about it. So, I think social media's role is a way for people and their communities to rally each other and feel like there is some kind of hope of an okay future."

Their view shows a clear difference between the two types of media — traditional media focuses on structured journalism to inform, while social media encourages engagement, activism, and community discussions. Instead of just being a place for objective news, social media allows people to highlight issues they care about and rally others around them.

However, this change also brings up important questions: If social media is mainly used for activism, how does that affect the way people see truth and objectivity? Some believe that social media makes information more accessible by allowing everyone to share their opinions. However, others worry that it focuses more on what gets the most attention rather than what is true, making it easier for false information to spread. The challenge is to find a balance between using social media to raise awareness and getting people involved while still making sure that the truth remains important.

The Disinformation Dilemma

When talking about information on social media, the issue of disinformation often comes up, along with the question of whether influencers are really qualified to share political knowledge. According to the report, most content creators get their information from both traditional media and social media (NeoReach, 2024). They practice lateral reading, which means checking multiple sources to confirm facts. This helps lower the chances of spreading

false information. Because of this, when creators share news with their audiences, there is less risk of misinformation, though this depends on the individual, as some do better research than others.

While not every content creator is an expert in politics or certain issues, being an influencer doesn't automatically mean they lack knowledge. Those who take the time to research properly can become informed enough to explain topics to others. In fact, Lyss pointed out that political influencers spend a lot of time researching news and politics to ensure they provide accurate information, as their job depends on it. However, Lyss also emphasized that social media is often used more for activism than for purely sharing news. Some creators try to be balanced and factual, while others focus more on raising awareness for causes they care about, which can sometimes blur the line between opinion and objective information. Because of this, it is important for people to think critically and question the information they see — something Lyss also said is key to avoiding disinformation.

When I asked Lyss about their opinion on the content creators' responsibility to combat disinformation, they stated: "I don't think there is a going to be a huge difference in how people consume news on social media rather than how they've already been consuming news.

Because if people don't fact-check themselves on one article now, they're not going to fact-check a creator."

This is a fascinating insight, which highlights the fact that each individual who is consuming news, has to play an active role in combating disinformation and building their own resilience. Of course, social media platforms still need to find ways to fight false information, and as Lyss pointed out, they can do this by working with content creators. By teaming up with influencers who already have large audiences, platforms can help spread fact-checked, accurate information to more people. However, this creates a challenge. Lyss mentioned that for platforms to effectively work with content creators against disinformation, they would need to include creators from both sides of the political spectrum. This could be difficult because it might put the platform in a tough position, especially if their own policies or audience lean toward one side. Hence, it is vital that the users of these platforms also take it upon themselves and build their resilience against disinformation by fact-checking what they are reading. This statement, however, should by no means be taken as an excuse for platforms to not contribute to the fight against disinformation. It is merely a call to action that our only defense against disinformation cannot be content moderation on social media platforms. We have to implement media literacy, critical thinking, and lateral reading into lifelong education and make fact-checking the norm to build a more resilient society.

The Future of Political Campaigns and Content Creators

As campaigns continue to embrace social media strategies, content creators will likely become an even more integral part of political communication and voter outreach in the future. As previously mentioned, there is a significant increase in the amount of voter registration tools and information that were available in the most recent elections, in comparison to the elections in 2020. This trend strongly indicates that social media will most likely remain a tool that will be utilized for political campaigns. When I asked Lyss about their opinion on the future of political campaigns and content creators, they remained hopeful about the intersection.

"I think utilizing young people to influence other young people to get out and vote when they are historically a group of people, who doesn't show up at the polls as a good strategy."

This growing connection between politics and digital influencers suggests that content creators will continue to play a key role in shaping voter engagement. By leveraging their platforms, they can make political discussions more accessible and relatable to younger generations, who may feel disconnected from traditional political messaging. Another point Lyss brought up was that including content creators in political discussions can help humanize politics, especially when governments actively engage with them. A key example of this was the White House Creator Economy Conference, where former President Joe Biden, originally scheduled to speak for just five minutes, ended up spending nearly an hour talking with influencers. This extended engagement not only made him appear more approachable and relatable but also highlighted his recognition of social media's power in shaping public discourse and political engagement. However, Lyss does make the clear distinction between politicians aligning themselves with individual content creators and platforms as a whole. This caution comes from the fear that if politicians align themselves with whole platforms, that platform will become a space only for the supporters of that politician or party while censoring the other side. So, while the inclusion of social media in political campaigns can help in reaching a wider audience, it should be used with caution.

Conclusion

Conclusion After the discussion with Lyss, it became clear that, like many aspects of modern life, political campaigns are undergoing a major shift and moving online. Social media platforms are no longer just spaces for entertainment — they have become key tools for political engagement and activism. Content creators are using their platforms to both educate others and rally support for causes they care about. It is our new reality and something we must learn to accept if we want to instill good practices. It does remain, however, a topic that deeply divides those who embrace social media's role in politics and those who worry that it spreads misinformation, increases polarization, and undermines traditional political discourse.

Now more than ever, platforms should act to moderate harmful and misleading content. However, it is not enough, and there is an increasing need to instill a culture in which fact-checking is the norm and each person makes it their own responsibility to fight against disinformation. Education systems, policymakers, and technology companies must work together to foster a digital environment that prioritizes accuracy, transparency, and accountability. Additionally, while content creators have emerged as influential figures in shaping public opinion, they must also recognize the responsibility that comes with their reach. Encouraging critical thinking, providing credible sources, and fostering informed discussions can help mitigate the negative impact of misinformation.

The future of political discourse will likely continue evolving in the digital sphere, and as this shift occurs, it is imperative to strike a balance between freedom of expression and the need for reliable, fact-based information. Whether through improved content moderation, media literacy programs, or greater collaboration between platforms, creators, and institutions, combating disinformation requires a collective effort. Only through these measures can we ensure that social media remains a tool for constructive political engagement rather than a breeding ground for confusion and division.

I would like to express the most heartfelt thank you to Alyssa Micalizzi, the Head of Content and Research at NeoReach for taking the time to share with me their research, perspectives, and insights.

About the author:

Alyssa (Lyss) Micalizzi is the Head of Content & Research at NeoReach, where they combine their expertise in writing, editing, and research to craft compelling, data-driven content. With a sharp editorial eye and a passion for storytelling, they translate complex digital marketing trends into engaging narratives that connect brands, influencers, and audiences. Through their leadership, they shape insightful strategies, elevate brand messaging, and drive impactful conversations in the ever-evolving creator economy.

References

Cetinkaya, C. (2025, January 27). *"The Politics of Misinformation: Social Media, Polarization, and the Geopolitical Landscape in 2025."* Austrian Institute for International Affairs. https://www.oiip.ac.at/en/publications/the-politics-of-misinformation-social-mediapolarization-and-the-geopolitical-landscape-in-2025/.

NeoReach (2025). *From posts to polls: The power of social media and creators in U.S. elections*. https://neoreach.com/quarterly-reports/the-power-of-social-media-creators-in-u-s-elections/.

CYBERSEC
FORUM / EXPO

SAVE THE DATE

11-12 June 2025
TAURON Arena Kraków

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

Readers' profile

- European-level representatives, sectoral agencies of the European Union, International Organisations Representatives;
- National-level officials of the Euro-Atlantic alliance, Government and Regulatory Affairs Directors & Managers;
- National and Local Government Officials as well as diplomatic representatives;
- Law Enforcement & Intelligence Officers, Military & Defence Ministries Officials;
- Legal Professionals, Representatives for Governance, Audit, Risk, Compliance, Industry leaders and innovators, active investors;
- Opinion leaders, specialised media, academic experts.

Types of contribution:

- Policy review / analysis / opinion – a Partner's article or a series of articles on crucial issues related to cybersecurity;
- Interview with Partner's representative;
- Research outcomes and recommendations;
- Advertisement of a firm, product or an event (graphical);
- Promotional materials regarding a cybersecurity conference / event (invitation, advertisement – graphical).

Do you want to share your opinion on national or European policies regarding cybersecurity? Do you want to publish outcomes of your research? Do you want to advertise?

The European Cybersecurity Journal is the right place to do it!

CONTACT US: editor@cybersecforum.eu

The Kosciuszko Institute is a leading Polish think tank shaping digital and security policy in Europe. Established in 2000, the Institute is a non-profit, non-governmental organization committed to building a secure and innovative digital future. Its mission is to strengthen the resilience of democratic societies and support evidence-based policymaking in the fields of cybersecurity, international security, critical technologies, and information integrity.

The Institute provides strategic expertise, facilitates multistakeholder dialogue, and builds cross-sector partnerships at national and international levels. It is the organizer of the annual CYBERSEC Forum – one of the key European platforms for strategic discussion on cybersecurity, emerging technologies, and digital sovereignty.

Through its policy papers, expert consultations, and international cooperation projects, the Kosciuszko Institute contributes to safeguarding democratic values and enhancing Europe's technological competitiveness.

We warmly invite you to follow our initiatives and join us in building a more secure and resilient digital world. Collaborations with stakeholders from government, industry, academia, and civil society are at the heart of our mission.

THE KOSCIUSZKO INSTITUTE

is the publisher of

European Cybersecurity Journal