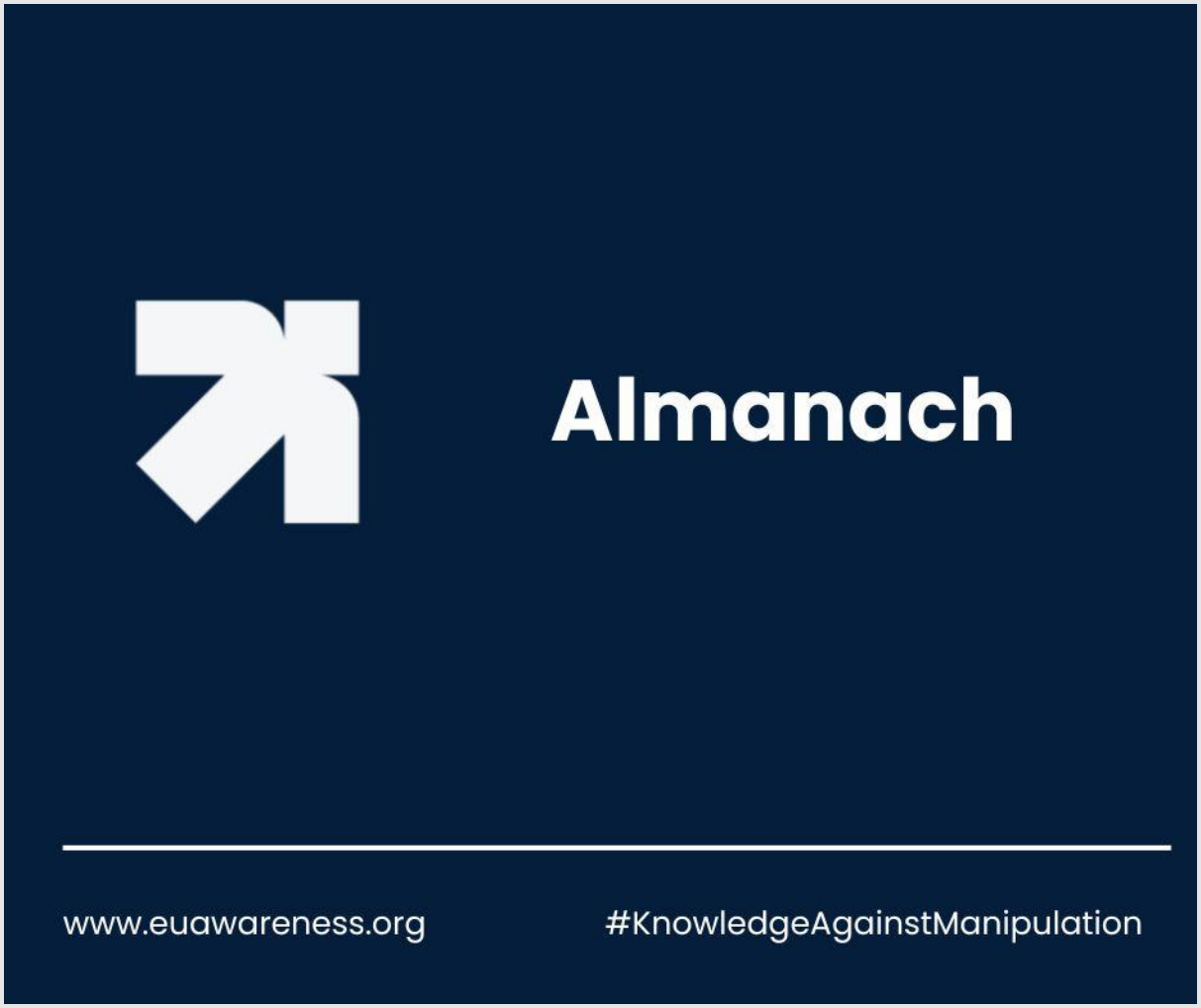


Almanach #19

Commentary by Andro Gotsiridze

Espionage Has Changed. What Must European Security Protect?

How intelligence, foreign influence and human vulnerabilities are reshaping European security

The opinions and conclusions expressed are those of the author and do not necessarily reflect the views of the EU Awareness Centre.

© [2026] EU Awareness Centre. All rights reserved.

18 November 2026

Espionage Has Changed. What Must European Security Protect?

How intelligence, foreign influence and human vulnerabilities are reshaping European security

Allegations involving Nvidia's former chief executive Jensen Huang have drawn attention. On 11 November 2026, Nvidia's board accepted his resignation, three days after announcing an independent investigation into reports of a possible foreign intelligence operation. The company confirmed his departure in a regulatory filing. The company has said it has no reason to believe its secrets or US national security were compromised. The espionage allegations remain unproven, and no official reason for his departure has been given.

Whatever the investigation establishes, the case raises a wider question: how should Europe protect strategic companies and their decisions from foreign intelligence and influence?

Strategic technologies, critical infrastructure and political institutions face espionage, disruption and foreign influence. A target's value may lie not only in the information it possesses, but also in the decisions it can make or influence.

The Changing Security Environment

The past three decades have transformed the environment in which intelligence services operate. As Sir Alex Younger, the former Chief of MI6, recalled, three assumptions shaped intelligence work in the early post-Cold War era. Democracy seemed to have triumphed after the Soviet Union's collapse; secrecy could be maintained through convincing cover, assumed identities, and cash transactions; and a recognisable, if imperfect, distinction between peace and war existed.

None has survived intact. Renewed confrontation with authoritarian powers has sharpened the importance of intelligence. Hybrid conflict has blurred not only the boundary between peace and war, but also the traditional distinctions between corporate, human and national security.

Much of the critical infrastructure on which societies depend is owned or operated by private companies. Disruption of energy, healthcare, transport or communications can therefore extend beyond commercial losses to affect people's safety, livelihoods and confidence in public institutions.

Digitalisation has introduced another dimension. We now operate in a world of ubiquitous digital traces. The 2018 Salisbury poisoning investigation demonstrated how passport records, travel data and other digital traces could expose even experienced Russian intelligence operatives. For corporate executives and other strategic figures, similar information can reveal personal relationships, routines and vulnerabilities that may be exploited for coercion, blackmail or the preparation of targeted operations, including sabotage.

A private company's vulnerability can therefore threaten human security and, through wider economic, societal and cognitive consequences, become a national security concern.

Europe's Expanding Security Vulnerabilities

Nvidia illustrates this strategic exposure. Its chips are central to artificial intelligence, economic competition, defence and intelligence. Decisions about technology transfers, partnerships and access to advanced computing can have geopolitical consequences.

Europe faces similar vulnerabilities. In 2019, Dutch semiconductor equipment manufacturer ASML disclosed the theft of intellectual property from its US subsidiary. Although Chinese state involvement was not established, the case demonstrated the strategic value of proprietary technology and specialist knowledge. Such assets have commercial and national security significance.

Political institutions are also exposed. In September 2025, a German court convicted Jian Guo, a former European Parliament assistant, of spying for China. He had collected information on parliamentary activities and monitored Chinese dissidents in Europe. The case illustrates the intelligence value of institutional access and relationships.

The investigation into alleged corruption involving Huawei-related lobbying in the European Parliament raised another concern. In March 2025, Belgian prosecutors charged five individuals in connection with alleged bribery involving payments and benefits intended to influence political positions. Huawei said it has zero tolerance for corruption and would cooperate with the investigation. These allegations do not establish a state-directed intelligence operation, but raise concerns about improper influence on political decisions.

Strategic exposure is not limited to technology giants. Small suppliers, laboratories or software providers may possess assets far more important than their size suggests. Russia's sabotage operations across Europe, including attacks on logistics and facilities linked to support for Ukraine, demonstrate another form of pressure on business.

In 2024, Western intelligence reportedly uncovered a Russian plot to assassinate Armin Papperger, chief executive of Rheinmetall, a major supplier of military equipment to Ukraine; a NATO official publicly acknowledged the threat in January 2025. In 2026, German media reported suspected Russian-linked surveillance of Stefan Thumann, head of drone manufacturer Donaustahl, and concerns about a possible assassination plot, also examined in a Die Zeit investigation. The arrest warrants concerned suspected espionage, not attempted murder. These cases illustrate how strategic competition can expose corporate leaders themselves to threats of physical violence.

Although these cases differ in method and evidentiary status, together they show how access, personal relationships and decision-making authority can expose businesses and political institutions to exploitation.

In an increasingly sensor-rich world, digitalisation and artificial intelligence also make it easier to combine leaked information with open-source data. Such analysis can help adversaries identify vulnerabilities, map relationships and plan operations intended to influence strategic decisions—even without obtaining new classified information.

From Espionage to Influence and Cognitive Confrontation

Intelligence operations need not aim solely at stealing classified information. Collection seeks to establish what an adversary intends to do; influence seeks to affect the eventual decision. It can exploit personal trust, professional relationships or access without direct coercion.

The same logic extends beyond individuals and corporate decisions. Foreign actors may seek to shape political perceptions, exploit social divisions, undermine institutional confidence and influence collective decisions. This is where traditional intelligence and influence operations intersect with Foreign Information Manipulation and Interference (FIMI) and the broader concept of cognitive warfare.

These activities differ in method, but their strategic objectives can converge. Cognitive operations may target the perceptions and trust on which collective decisions depend, influencing how capabilities are understood, prioritised or employed.

This is particularly important in understanding the subversive objectives of hybrid operations. Disruption of critical infrastructure, for example, may cause immediate economic damage and undermine human security. But its wider strategic value may lie in the uncertainty and dissatisfaction it generates. When such consequences are exploited through information manipulation, the objective may be to weaken confidence in institutions, increase pressure on governments and influence their political choices. A temporary disruption may thus be intended to produce enduring political and cognitive consequences.

Foreign actors may seek to shape how Europeans perceive threats and decide how to respond. Russia's information manipulation campaigns provide an example. The European External Action Service's fourth report on FIMI threats, published in March 2026, documents campaigns including efforts to reduce international support for Ukraine by portraying assistance as wasteful and European leaders as prolonging the war. The strategic objective is to influence political choices without necessarily resorting to overt military force. Whether such campaigns achieve their intended effects requires separate assessment.

The Enduring Human Factor

But knowing more about someone is not the same as understanding them. Technology may reveal where a person goes or whom they meet. Explaining why they act, what they fear, or how they might respond to pressure is another matter. Love, loyalty, vanity, ambition and disappointment shape decisions; sometimes people cannot fully explain their own motives.

Human intelligence, HUMINT, therefore remains indispensable. Its fundamental challenge remains crossing cultural, political, and personal barriers, establishing trust, and persuading people to provide information or take action. Digital analysis can help prepare an approach; it cannot secure loyalty or replace the judgement needed to distinguish a genuine source from deception.

These relationships impose obligations. Sources may risk their freedom or lives by cooperating. Protecting them is an enduring professional responsibility that continues long after the intelligence is delivered. Earning trust requires emotional intelligence, patience, and optimism. Intelligence officers routinely face the difficult task of persuading people to act against deeply established loyalties.

Yet the emotions that make trust possible can also be exploited. A person can be sincerely in love while someone else seeks to exploit the relationship. Traditional recruitment motives include money, ideology, coercion, compromise and ego; emotional attachment can intersect with any of them. Wealth may reduce the attraction of money without removing the need for affection or the fear of exposure.

These vulnerabilities are not confined to intelligence recruitment. Political leaders, corporate executives and other decision-makers remain susceptible to personal trust, emotional attachment and misplaced confidence. When individuals have strategic access or authority, exploiting their relationships can have consequences far beyond the individuals involved. A compromised executive may be pressured not only to disclose information, but also to influence a commercial decision, facilitate access or circumvent an established safeguard. The challenge is to prevent such exploitation from undermining independent decisions.

Intelligence and Political Judgement

Better collection is insufficient if leaders ignore intelligence warnings. The relationship between intelligence and political leadership is therefore as important as collection itself.

At a televised Russian Security Council meeting in February 2022, Sergei Naryshkin, the head of Russia's Foreign Intelligence Service, initially suggested giving diplomacy another chance, provoking a sharp reaction from President Vladimir Putin. The exchange illustrates a fundamental risk: when political leaders discourage dissent, intelligence professionals may struggle to present assessments their superiors don't want to hear. Russia's subsequent miscalculation of Ukraine's resistance makes this lesson particularly significant. Intelligence leadership requires the professional courage to deliver unwelcome truths—and political leadership must be willing to hear them.

The intelligence failures preceding Hamas's attack on Israel on 7 October 2023 offer a different lesson. Israeli intelligence had obtained a detailed outline of the attack, known as the Jericho Wall plan, but its significance was underestimated, and warnings were not adequately acted upon. Excessive confidence in technological surveillance and sophisticated border defences also contributed to a false sense of security. The case shows that advanced intelligence capabilities cannot prevent strategic surprise when technological confidence replaces critical judgement.

A more recent controversy raises a related question. According to reporting based on sources familiar with the matter, President Donald Trump was briefed aboard Air Force One in May 2026 on intelligence concerns involving Nvidia's then-chief executive, Jensen Huang, and suspected links to Chinese intelligence. Trump later said he was not aware of the allegations. These conflicting accounts raise questions about how sensitive intelligence is communicated, assessed and used at the highest political level, without establishing what the president actually knew.

Although different in nature, these cases underline a common principle: the strategic value of intelligence depends not only on what is collected, but also on independent assessment, institutional safeguards and the willingness of decision-makers to act on credible information.

Implications for European Security

The response must go beyond protecting information or warning executives about suspicious relationships. Consequential decisions need safeguards too, in government and business alike, because vulnerabilities can be exploited through both technical access and human relationships.

First, treat identity and decision-making authority as strategic assets. Cyber operators compromise credentials or impersonate trusted users to gain access; human intelligence operations may exploit personal trust and emotional dependence. Both can exploit the gap between apparent trust and actual authority. Protect privileged identities, verify consequential requests independently and investigate unusual changes in access or approval patterns.

Second, map decision pathways, not only technical attack surfaces. Who can authorise technology transfers, change suppliers, influence export-control decisions or override safeguards? Separation of duties and independent review can protect critical decisions from manipulation that involves no conventional security breach. Governments also need protected channels for independent intelligence assessment: corroboration matters, but dismissing credible analysis because it contradicts political expectations can prove costly.

Third, combine technical indicators with human context. Patterns-of-life analysis and cyber threat intelligence can reveal anomalies, but they can't establish hostile intent. Intelligence and corporate

security teams need corroboration, proportionate escalation procedures and respect for private lives. The aim is proportionate response, not permanent scrutiny.

Finally, extend this approach through strategic supply chains and integrate geopolitical threats into corporate risk management. Companies with unique intellectual property, essential technology or critical infrastructure may be strategically important regardless of size. Executive protection, business continuity, supply-chain resilience and cooperation with public authorities are as necessary as conventional cybersecurity.

Yet businesses alone cannot address these challenges. Companies must protect essential services and strategic decisions; national governments must assess hostile intentions and coordinate security responses; and European institutions must facilitate cooperation across borders, supply chains and critical sectors.

Europe already has important instruments to address these risks. The EU's Economic Security Strategy addresses strategic dependencies, technology leakage and economic coercion, while foreign investment screening, the NIS2 Directive and the Critical Entities Resilience Directive provide complementary mechanisms for protecting strategic assets, managing cyber risks and strengthening essential services.

Yet these frameworks do not, by themselves, address covert influence on human judgement. The EU's response to FIMI focuses on information manipulation, not on influence exercised through personal relationships. Cooperation among intelligence services, public authorities, businesses and civil society remains necessary, with safeguards for privacy, independent judgement and democratic debate.

The challenge is not simply to protect what Europe possesses, but also to safeguard how Europe decides.

Conclusion

Sound intelligence judgement requires keeping suspicion distinct from evidence. The broader lessons do not depend on the outcome of the Nvidia investigation. Technology has transformed collection and influence, but not the importance of trust, motivation and professional judgement.

For Europe, hybrid conflict has exposed the interdependence of corporate, human and national security. Protecting Europe against hostile influence therefore requires more than technical resilience. Institutional safeguards and independent intelligence assessment are essential, but their effectiveness ultimately depends on the people who apply them. Intelligence remains a human profession, dependent on trust, responsibility and understanding motivation.

The operating environment of espionage has changed radically. Human nature has not.



Andro Gotsiridze *is a Georgian intelligence and cybersecurity expert with extensive experience in intelligence operations, national security, and corporate security.*