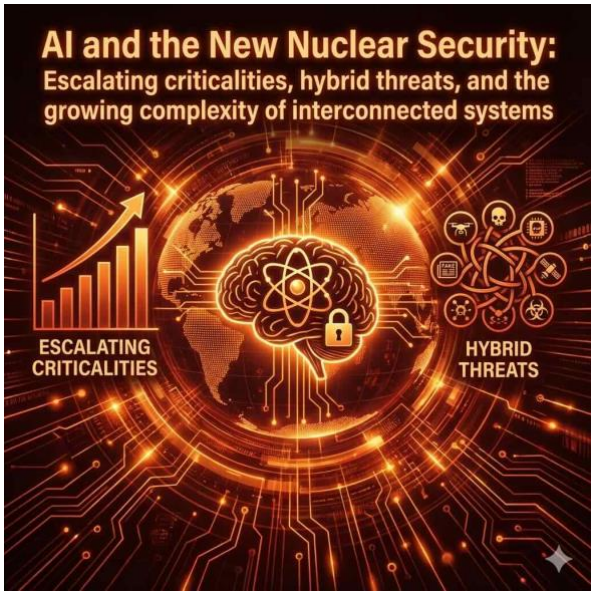
AI and the New Nuclear Security

Escalating criticalities, hybrid threats, and the growing complexity of interconnected systems

*To compete with Chinese and American dominance, Europe must complete its transition towards **industrialized nuclear power**. The security lessons emerging from 2024 are unambiguous: **there can be no digital sovereignty—particularly in AI—without energy sovereignty**. Protecting critical infrastructure through intelligent digitalization, reducing excessive bureaucracy, and investing in an independent European supply chain are no longer policy options, but strategic necessities. Only by doing so can nuclear energy continue to illuminate—and power—the future of the continent. –*

By Dr. Gustavo Scotti di Uccio[1]

1 A Strategic Choice for Europe 2
2 Energy as the New Currency of Power 2
3 Security in a Hyper-Connected World 2
4 Europe's "New Nuclear" and the Global Race 2
5 Real-World Incidents Highlighting Systemic Risks 2
5.1 Conflict-Driven Attacks on Nuclear Sites 3
5.2 Military Pressure on Supporting Infrastructure 3
5.3 Armed Activity Near Nuclear Sites 3
5.4 Cyber and Information Security Threats 3
5.5 Security Compliance Failures and Internal Vulnerabilities 3
6.1 The Strategic Advantages of Digitalisation 4
6.2 Growing Complexity and New Vulnerabilities 4
6.3 AI Autonomy and the Non-Negotiable Role of Humans 5
6.4 Avoiding the "Illusion of Digital Safety" 5
7 Critical Infrastructure and the Cybersecurity Dilemma 5



[1] *Gustavo Scotti di Uccio, Ph.D. in Nuclear Physics, was an executive in the Finmeccanica/Leonardo group for over 30 years, working in the fields of defence, security, and critical infrastructures. For the past 15 years, he has been the President and General Manager of AOS (Atlantic Organization for Security), a security and defence engineering & program management firm based in Belgium.*

1 A Strategic Choice for Europe

As AI accelerates and energy systems grow more complex, nuclear power sits at the intersection of technology, security, and sovereignty. Europe's challenge is not simply to produce more electricity, but to do so within a framework that is secure, resilient, and strategically autonomous. In an era of hybrid threats and systemic interdependence, **the future of nuclear energy is inseparable from the future of Europe's digital and geopolitical autonomy**.

2 Energy as the New Currency of Power

By the mid-2020s, computing power has overtaken traditional indicators as a key measure of geopolitical strength. The rapid expansion of Artificial Intelligence has transformed data centers from background IT assets into **energy-intensive infrastructures**. By 2030, electricity demand linked to AI is expected to triple, creating an urgent need for power sources that are at once abundant, continuous (baseload), and carbon-free.

In this scenario, nuclear energy is no longer merely a low-carbon solution; it has become a **strategic pillar**. The United States is capitalizing on private-sector dynamism, with initiatives such as Microsoft's restart of Three Mile Island and Amazon's acquisition of data centres near existing nuclear plants. China, by contrast, is advancing through centralised planning, with over 150 new reactors projected in the next 15 years. Europe's response is more structural: a strategy focused on **industrial standardisation and technological leadership**, particularly in Small Modular Reactors (SMRs).

3 Security in a Hyper-Connected World

The main challenge today is no longer confined to managing the reactor core itself, but to securing an increasingly interconnected ecosystem. A clear paradox has emerged: just as European nuclear output returns to historic highs, the overall system becomes more complex—and more exposed.

Digitalisation has dramatically expanded the threat landscape. Nuclear facilities are now vulnerable not only to conventional cyber intrusions, but also to **hybrid attacks** that blend cyber, physical, and organisational weaknesses. Security can no longer be an afterthought; it must be *native*, embedded from the earliest design stages through a "security by design" approach. An attack on the control systems of a plant connected to a critical data center could trigger cascading disruptions across the wider digital economy.

At the same time, new technologies are introducing unexpected risks. The widespread use of portable digital devices has led to incidents such as lithium-battery fires in controlled areas, highlighting how innovation can outpace existing physical-security protocols and force their rapid revision.

4 Europe's "New Nuclear" and the Global Race

To counter Sino-American leadership, Europe is betting on innovation combined with sovereignty over the full value chain.

A flagship example is **NUWARD**, the French-led SMR programme supported by a broad European alliance, including Italy's Ansaldo Nucleare. Designed as a fully digital, modular reactor, NUWARD benefits from more than €300 million in state-aid-backed research funding and represents Europe's answer to China's speed-driven construction model.

Alongside SMRs, large-scale projects such as **EPR2 and Hinkley Point C** remain essential to Europe's industrial strength. France's decision to repurchase the Arabelle turbines—previously owned by General Electric—signals a clear intent to keep critical technologies under European control and to reduce strategic dependence on non-European suppliers.

5 Real-World Incidents Highlighting Systemic Risks

Europe's ambition to build sovereign nuclear capabilities — from **NUWARD SMRs** to *EPR2* and *Hinkley Point C* — is not happening in a vacuum. The global nuclear landscape is increasingly shaped by **incidents that underscore how hybrid threats, conventional attacks, and systemic complexity compound one another**.

Among others, in the recent years there were examples illustrating the kinds of challenges Europe's strategy must address in its future process. These real-world cases — from conventional strikes on nuclear infrastructure in war zones to cyber campaigns and internal compliance failures — demonstrate that:

- **Nuclear systems no longer exist in secure, isolated bubbles**: They are part of larger grids and networks that are susceptible to hybrid threats.

- **Threat surfaces are expanding**: Wars, drones, grid disruptions, digital attacks and supply chain vulnerabilities all intersect with nuclear operations.
- **System complexity magnifies risk**: As nuclear plants integrate with AI, digital controls, and data centres, the room for hybrid attacks grows.

Europe's "New Nuclear" ambitions — in SMRs, EPR technology, and digitalised operations — must therefore be matched with a **security strategy that is as multi-layered and adaptive as the threats themselves**: blending physical security, cyber-resilience, conflict-aware planning, and regulatory compliance into one cohesive framework.

5.1 Conflict-Driven Attacks on Nuclear Sites

In **June 2025**, military operations in the Middle East escalated dramatically when Israeli and U.S. forces targeted multiple Iranian nuclear facilities. Three key sites — including *Natanz*, *Isfahan*, and *Fordo* — were struck by precision ordinance, resulting in significant infrastructure damage. According to the IAEA, while there was *no detected increase in radioactivity outside the plants*, **radiological and chemical contamination occurred within the facilities** themselves. These events demonstrate how conflicts can directly affect nuclear installations, creating not only physical destruction but also complex radiological hazards that require sophisticated containment and monitoring strategies[2].

5.2 Military Pressure on Supporting Infrastructure

Even when nuclear plants are not themselves struck, **attacks on supporting energy infrastructure** can destabilise operations. In **Ukraine**, for example, intense targeting of the national electric grid by Russian forces — including drone strikes, missiles, and other weapons — has repeatedly interrupted power supplies needed to safely run reactors at *Zaporizhzhia*, *Rivne* and *Khmelnytskyy*. These disruptions force reactors to reduce output or shift to backup systems, compounding the risk of operational faults or safety system failures. International observers have noted that *prolonged instability in grid connections directly undermines nuclear safety standards*[3].

5.3 Armed Activity Near Nuclear Sites

Similarly, the Russian nuclear plant near *Kursk* experienced a **drone-caused fire** after a military-related attack damaged a transformer. Although there was no critical radiological release, this incident vividly shows how conventional weapons and unmanned systems can affect nuclear infrastructure components, especially in conflict zones close to industrial assets[4].

5.4 Cyber and Information Security Threats

Beyond kinetic attacks, nuclear systems face **digital threats** that exploit the interconnectedness of modern industrial environments.

In the **United States**, hostile hackers reportedly compromised IT systems at the *Kansas City National Security Campus*, a facility integral to nuclear weapons component production, using vulnerabilities in widely used software platforms. Even though this was not a power reactor, it illustrates how critical nuclear-related infrastructure can be targeted via digital attack vectors — and how vulnerabilities in general-purpose systems can have wider implications for safety and supply chains[5].

In **Iran**, government reports from late 2024 described *massive cyberattacks* that hit segments of the nuclear industry's networks, alongside broader governmental systems, resulting in data theft and increased exposure to potential sabotage. Although precise details remain limited, this incident highlights how non-state and state-affiliated actors are increasingly probing nuclear-related digital environments[6].

5.5 Security Compliance Failures and Internal Vulnerabilities

Even in non-conflict settings, systemic weaknesses can pose risks. The UK's *Sellafield* nuclear site, one of the world's largest nuclear waste facilities, was fined for significant **cybersecurity failings** — including unpatched vulnerabilities and failure to follow regulatory

[2] Euronews: (The attacks have raised fears about nuclear contamination that could raise health risks. 19/06/25)

[3] Il Fatto Quotidiano: (Ukraine, raids on energy infrastructure: "Nuclear power plant output reduced" – 23/12/2025)

[4] Greenreport: (Attacco con droni alla centrale nucleare russa di Kursk – 25/08/2025)

[5] Red Hot Cyber: (Criminal Hackers Breach US Nuclear Weapon Production Facility – 27/10/25)

[6] TGCOM24: (Iran: colpiti da massiccio cyberattacco, di mira anche gli impianti nucleari – 12/10/2024)

standards. While no attack was publicly confirmed, the unresolved weaknesses created the potential for serious breaches, showing that **internal governance and system resilience are as critical as external defence**[7].

Broader data from UK nuclear regulators also reveal an **uptick in security breaches**, including unauthorised access and malware threats across civil nuclear sites. This trend underscores the fact that **as nuclear power expansion accelerates, security challenges are growing in volume and diversity**[8].

6 Digital Transformation: The Nervous System of Modern Nuclear

Digital transformation has become the **nervous system of modern nuclear power**. It connects sensors, control rooms, maintenance teams, supply chains, regulators and, increasingly, data centres and AI-driven applications. Properly implemented, it enhances safety, efficiency and competitiveness. Poorly governed, however, it introduces new layers of complexity and risk that can undermine the very resilience it is meant to deliver.

Digital transformation is indispensable for the future of nuclear energy. Without it, nuclear power cannot scale, compete, or integrate with AI-driven economies. With it, however, comes a profound responsibility: **to manage complexity without surrendering control**.

The nuclear systems of the future will be partly algorithmic—but they must remain fundamentally human-governed. In an era of hybrid threats, interconnected infrastructures and autonomous technologies, the strength of modern nuclear power will lie not only in smarter machines, but in the **wisdom with which humans choose to use them**.

Digital twins are already in operation at sites such as Hinkley Point C, where every pipe and cable has a virtual counterpart. These models allow operators to simulate maintenance activities, minimise downtime, and significantly reduce the risk of human error.

Advanced tools like **CADOR software** enhance radiological protection by predicting radiation doses with millimetre-level accuracy, improving worker safety during inspections. Meanwhile, AI-driven predictive maintenance systems analyse vast streams of sensor data to detect early signs of degradation—such as stress corrosion—long before they evolve into critical failures.

6.1 The Strategic Advantages of Digitalisation

At its best, digital transformation radically improves how nuclear facilities are designed, operated and secured.

Digital twins are one of the most powerful examples. In plants such as Hinkley Point C, every physical component—from major systems down to individual pipes and cables—has a virtual replica. These models allow operators to simulate maintenance activities, test operational scenarios, and anticipate failure modes without touching the real plant. The result is shorter outages, lower costs, and a significant reduction in human error.

Advanced **radiological protection tools**, such as CADOR software, further illustrate the benefits. By modelling radiation fields with millimetre-level precision, these systems allow work to be planned in ways that minimise exposure, improving worker safety while maintaining operational efficiency.

Perhaps the most transformative application is **predictive maintenance**. AI systems analyse vast streams of sensor data—vibrations, temperatures, pressures, chemical signatures—to detect weak signals of degradation such as stress corrosion or material fatigue. Problems that once emerged suddenly can now be identified months in advance, shifting nuclear safety from a reactive to a preventive paradigm.

Together, these tools increase availability, reduce costs, and strengthen safety margins—key factors if nuclear energy is to remain competitive in an AI-driven, electrified economy.

6.2 Growing Complexity and New Vulnerabilities

Digitalisation also **increases systemic complexity**, and with it, new vulnerabilities.

As nuclear plants become software-defined infrastructures, they inherit many of the risks typical of large digital systems: software bugs, configuration errors, dependency on updates, and exposure to cyber and hybrid threats. The integration of nuclear facilities with external systems—electric grids, cloud platforms, data

[7] Red Hot Cyber: (La Sicurezza dei sistemi Nucleari è imprescindibile! – 05/10/2024)

[8] The Ferret: *(Security breaches at UK nuclear police reach eight year high – 04/03/2023)*

centres—means that failures or attacks can propagate across sectors.

There is also a growing **technological dependency risk**. Highly digitalised plants rely on specialised software, proprietary algorithms, and long supply chains for hardware and updates. This raises questions of sovereignty, long-term maintainability, and resilience in crisis scenarios where access to vendors or digital services may be disrupted.

Another often overlooked issue is **operational overload**. Excessive digital interfaces, alarms, and procedural layers can overwhelm operators, especially in abnormal situations. Instead of simplifying decision-making, poorly designed digital systems may obscure critical information at the very moment it is most needed.

6.3 AI Autonomy and the Non-Negotiable Role of Humans

The most sensitive issue concerns the **autonomy of AI systems**.

AI excels at pattern recognition, optimisation, and early warning. However, it operates on probabilistic logic and historical data. In nuclear safety, where rare and unforeseen events matter most, this creates a fundamental limitation. An AI system may optimise for efficiency or likelihood, but struggle with **black swan scenarios**, ethical judgement, or conflicting safety priorities.

For this reason, **human control must remain non-negotiable**. AI in nuclear systems should operate under a strict *human-in-the-loop* or *human-on-the-loop* model:

- Humans must retain ultimate authority over safety-critical decisions.
- AI recommendations must be explainable, traceable, and challengeable.
- Operators must be trained not only to use AI systems, but to recognise when to override or ignore them.

The risk is not that AI will "take control", but that humans may **over-trust automated systems**, especially under stress. History in other sectors—from aviation to finance—shows that excessive reliance on automation can degrade human skills and situational awareness over time.

In nuclear operations, maintaining **human competence, intuition, and responsibility** is as important as deploying advanced algorithms.

6.4 Avoiding the "Illusion of Digital Safety"

There is also a broader governance challenge. Digital transformation can create an **illusion of safety**, where compliance with digital procedures replaces real understanding of physical systems. Regulators and operators alike risk focusing on dashboards, metrics, and documentation, while losing sight of hands-on expertise and practical experience.

True nuclear safety does not emerge from software alone. It depends on a balanced ecosystem where:

- Digital tools enhance, rather than replace, human judgement.
- Automation supports operators without deskilling them.
- Security is designed holistically, integrating cyber, physical, organisational and human factors.

7 Critical Infrastructure and the Cybersecurity Dilemma

The increasing integration of nuclear power plants with data centres and digital industrial platforms—often described as the **E-Factory model**—has fundamentally altered the security landscape of nuclear energy. Facilities that were once designed as largely self-contained, analogue systems are now deeply interconnected nodes within global digital networks. This shift has expanded the **attack surface** well beyond the physical perimeter of the plant, exposing nuclear operations to cyber, hybrid, and systemic risks that were previously marginal or non-existent.

From an operational perspective, this integration delivers clear benefits. Digital connectivity enables real-time monitoring, advanced diagnostics, remote maintenance, and tighter coupling between energy production and high-demand digital consumers such as AI-driven data centres. However, the same connectivity also introduces **new forms of fragility**. Vulnerabilities in external networks, supply-chain software, or shared digital services can propagate rapidly into safety-critical environments. In such a context, a cyber incident does not need to directly target a reactor to have serious consequences; disruptions to auxiliary systems, data integrity, or decision-support tools may be sufficient to compromise safe operations.

The **IGSNR has cautioned against the "bureaucratisation of security"**[9], a phenomenon in which security becomes dominated by procedures, compliance checklists, and digital reporting rather than by real operational understanding. As systems grow more complex, there is a risk that security is perceived as a matter of documentation rather than of competence. Excessive reliance on automated controls, dashboards, and formal processes can unintentionally erode hands-on expertise, slow down decision-making in crisis situations, and reduce the operator's ability to recognise weak or atypical signals.

True resilience in critical nuclear infrastructure therefore depends on achieving a **delicate balance between automation and human agency**. Algorithmic tools and cybersecurity technologies are indispensable for managing complexity at scale, detecting anomalies, and responding rapidly to known threat patterns. Yet they must be designed to support, not replace, human judgement. Operators need clear, intelligible information—not opaque "black box" outputs—so they can understand system behaviour, question automated recommendations, and intervene decisively when conditions deviate from expected scenarios.

Equally important is the **human and organisational dimension of security**. Psychological safety—the ability of personnel to raise concerns, report anomalies, and challenge decisions without fear of blame—is a critical enabler of early risk detection. Continuous training is essential to ensure that skills keep pace with evolving technologies and threat vectors, particularly in environments where digital and physical systems are tightly coupled. Transparency, both within organisations and towards regulators, helps prevent the accumulation of latent vulnerabilities that often precede major incidents.

In this sense, cybersecurity in the nuclear domain cannot be reduced to firewalls, encryption, or intrusion-detection systems alone. It is a **socio-technical challenge**, where technical defences, organisational culture, and human competence must reinforce one another. As nuclear infrastructure becomes ever more digital and interconnected, the central dilemma is not whether to embrace digitalisation, but how to do so without sacrificing the depth of expertise, situational awareness, and human responsibility upon which nuclear safety ultimately depends.

[9] See https://www.aofs.org/2025/04/01/the-new-frontier-of-european-nuclear-energy/