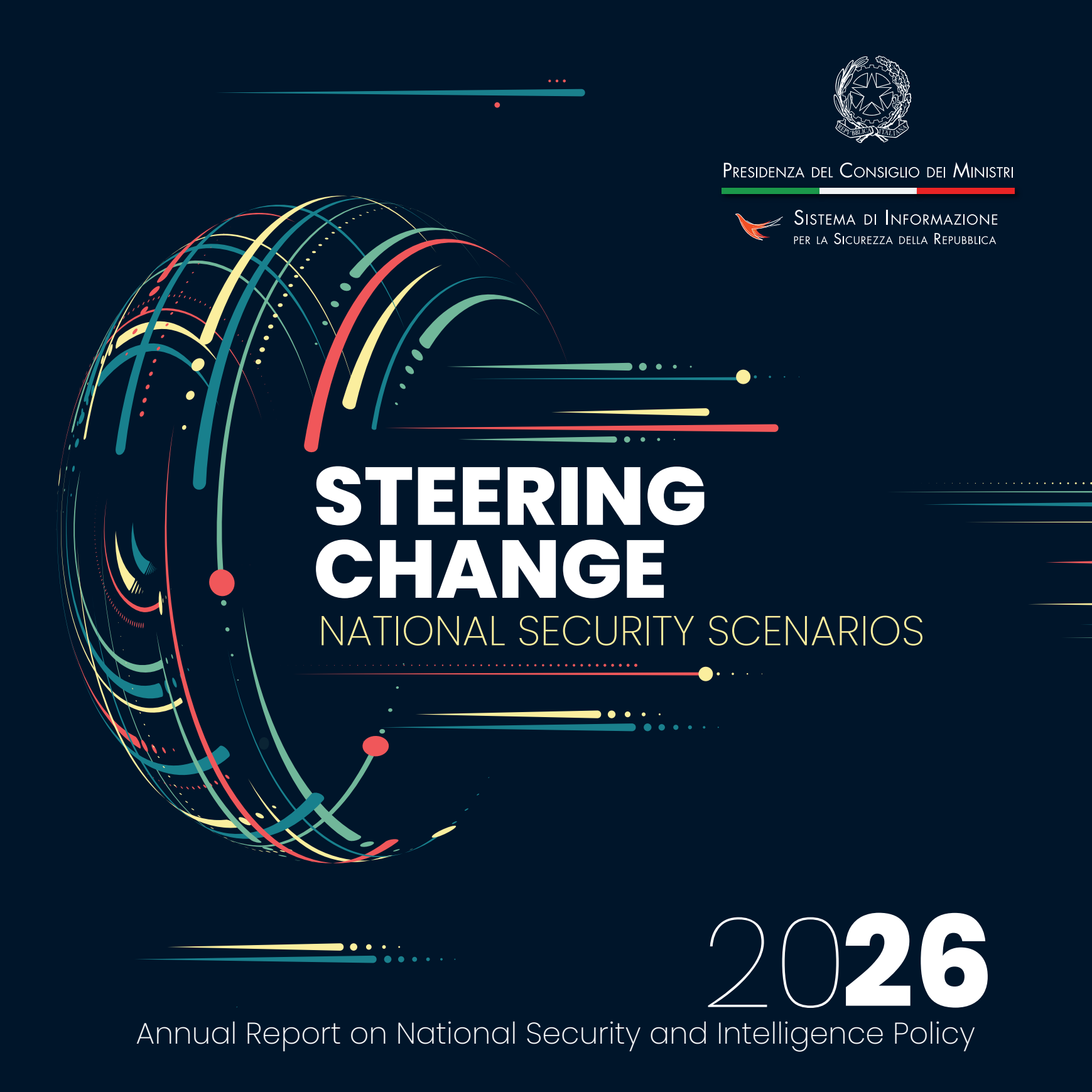


Presidenza del Consiglio dei Ministri

Sistema di Informazione per la Sicurezza della Repubblica

STEERING CHANGE

NATIONAL SECURITY SCENARIOS

2026

Annual Report on National Security and Intelligence Policy

The Annual Report for Parliament in digital version

TECHNOLOGY AS THE CATALYST FOR CHANGE

This Report is issued at a time when technology has gone beyond mere innovation to become the driving force of change and one of the main factors impacting our country's security. We stand at a historic juncture marked by deep and ongoing transformation, one that structurally alters strategic balances, economic stability, and social cohesion.

Technological innovation no longer merely follows change, it steers and accelerates it. It redefines how power is exercised, transforms the nature of threats, and influences the State's ability to anticipate and counter them. This raises new, complex legal issues on the boundaries of public action, respect for legality, and protection of fundamental rights enshrined in the Constitution.

Nowadays, the ongoing transformation has redefined threat itself. Threats no longer manifest only through visible events, but through continuous, pervasive, and often elusive dynamics. Today's threats operate in a multidimensional and multi-domain environment, extending beyond traditional domains into the cognitive, submarine, and intellectual property spheres. Consequently, risk no longer materializes through isolated, overtly hostile acts, but through cumulative processes. Such processes – embedded in coherent, long-term strategies – may affect institutional stability, public trust, as well as institutional decision-making capabilities. They do so while steadily operating below the armed conflict threshold, for example by compromising networks, manipulating information flows, or turning technology dependencies into leverage points.

New technological dynamics transcend geographical boundaries, economic sectors, and institutional domains, increasingly blurring the line between internal and external security while requiring an integrated analysis of different phenomena. Fully established technologies – such as pervasive digitalization and artificial intelligence – coexist with new scientific frontiers, including quantum technologies, which will introduce signi-

ficant disruptions in communications security and protection of sensitive information.

Hence, innovation has become the primary driver of systemic change, able to permeate every aspect of social, economic, political, and military structures. The speed of these changes frequently makes conventional tools to classify reality obsolete, complicating States' efforts to adopt suitable laws and measures to define constantly evolving phenomena. This heralds a transformation of legal systems themselves, with implications for the emergence of new rights and the need to protect individuals from frontier applications still lacking adequate regulatory frameworks.

The choice of the title "Steering Change" for this Annual Report holds that technological transformation provides the key to understanding today's security landscape. Rather than describing individual technologies or events, this Report offers a unified framework to understand threat evolution, detect system vulnerabilities, and strengthen prevention and risk management capabilities. This reflects the recognition that today security cannot rely only on reaction: it requires strategic foresight, accountability, and anticipatory capacity.

The 2026 Annual Report and Its Key Features

This Report, prepared for Parliament pursuant to Article 38 of Law No. 124 dated August 3rd, 2007 and pertaining to the national security and intelligence policy and the results achieved in 2025, features an innovative structure. In addition to the account of the activities carried out by the intelligence bodies – highlighted in specific, dedicated *boxes* – it offers a forward-looking perspective aimed at identifying evolutionary paths, emerging challenges, and development prospects.

The first chapter analyzes technology's impact across **eight strategically vital domains**. Each captures a distinct dimension of the same structural transformation. Alongside the core information, each chapter also features infographics designed to visualize summary overviews, facilitating the reading and understanding of the main topics covered. Namely the Report addresses the following areas:

1. Technological and Digital Sovereignty

A country's sovereignty is increasingly expressed through strategic autonomy, that is, the ability to manage its data, critical infrastructures, algorithms, and technology supply chains. Ungoverned dependencies may become structural pressure points, limiting a country's freedom of action. Therefore, the focus falls on opportunities and threats posed by the so-called *dual-use* technologies;

2. Geopolitical Shifts

Global paradigms have undeniably shifted and we

are witnessing a fundamental redefinition of the world order. This acceleration goes beyond technology, impacting international geopolitical and economic alignments and requiring a new strategic stance.

As geopolitical balances increasingly align along technological lines, control over emerging technologies, critical resources, and industrial *standards* directly affects power projection. This analysis covers key geopolitical *intelligence* priority regions: Europe, Africa, the Middle East, and the Indo-Pacific;

3. Economic-Financial Security

Economic-financial security faces a rising systemic risk. Digitalized markets, interconnected payment systems, cryptocurrencies, complex value chains, and new threats to critical infrastructures and high-competitiveness sectors (including energy and pharmaceuticals) magnify the effects of external *shocks*, hostile interference, and economic coercion, the hallmarks of *economic warfare*. Within this context, financial stability is no longer a merely macroeconomic issue, but a core pillar of national security;

4. Organized Crime Threat

Organized crime networks have evolved into technologically sophisticated actors. Cryptocurrencies, encrypted communications, digital platforms, and online anonymity enable unprecedented operational resilience, rapid adaptation, and evasion, while supporting the growth of illicit trade. The convergence of organized crime and technology poses a persistent, borderless threat; one that imposes a global vision requiring coordinated action, aiming *first* at targeting the digital ecosystems that channel illicit capital flows;

5. Internal Threat

The internal threat is also influenced by technology, although groups of radical extremists, resistant to technological progress, persist. In contrast, the online networks of the "international supremacist and accelerationist" far right embrace technology as a force multiplier for propaganda. In this regard, *online* radicalization, access to advanced digital tools, and remote action capabilities dramatically heighten the destructive potential of individual actors or groups;

6. Illegal Migration

Technology has become an increasingly vital tool to strengthen efforts in countering illegal migration flows. From a forward-looking perspective, such a threat may evolve into hybrid forms, serving as a possible leverage tool;

7. Terrorist Threat

Multiple international crises significantly shape the terrorist threat landscape, which has taken on an increasingly complex dimension. Within this context, the use of new technologies by individual actors, extremist and terrorist groups, represents a force multiplier for radicalization processes, propaganda dissemination, and the development of funding channels. Yet, AI remains a valuable tool to enhance prevention, counter-radicalization, and counter-terrorism efforts;

8. Hybrid Threat.

The hybrid threat embodies the operational synthesis of these dynamics. By coordinating technological, intelligence, economic, and political tools, adversaries can be struck without crossing the threshold of the use of force and armed conflict. Technology serves as the central enabler of such operations, making attribution, response, and deterrence more difficult. Information manipulation emerges as one of the most effective and pervasive instruments of this new threat vector, operating within the cognitive sphere, ultimately aimed at undermining the cornerstones of democratic societies.

Finally, this year's edition stands out for its innovative approach to both content and methodology. Besides **four dashboards** crafted exclusively through statistical methods and inserted within the chapters, the **Appendix** to this Report presents **five case-studies** developed via generative AI (GenAI) technologies, a new feature introduced in this edition.

They represent a methodological and scientific exercise aimed at showing – within the limits of public disclosure – the potential benefits of employing advanced tools to support analytical processes. Developed exclusively from open-source data and based on conventional computational capacity,[1] they explore scenarios of particular strategic interest linked to the thematic areas covered in the previous section, including: Russia-NATO conflict, space competition, Daesh in Syria, cryptocurrencies, and projections of migration flows.

The five case-studies were developed according to rigorous criteria and with an explicitly human-centered approach, conceiving AI as a support tool for analysts – able to train systems, effectively deploy applications, and validate results – while avoiding automation and any uncritical reliance on generated *outputs*. Indeed, analysts, OSINT operators, and technical staff worked in multidisciplinary teams, ensuring quality control at every stage: from setting intelligence questions to source selection, from interacting with the models to critically reviewing the results.

Conversely, the four *dashboards* aim at providing a methodological benchmark and enhancing understanding of the analyzed phenomena. These comprise strategic indicators dedicated to demography, climate, technology, and geopolitics: factors that reflect global *trends* and possess a cross-cutting nature, proving functional in representing the course and evolution of the phenomena under consideration.

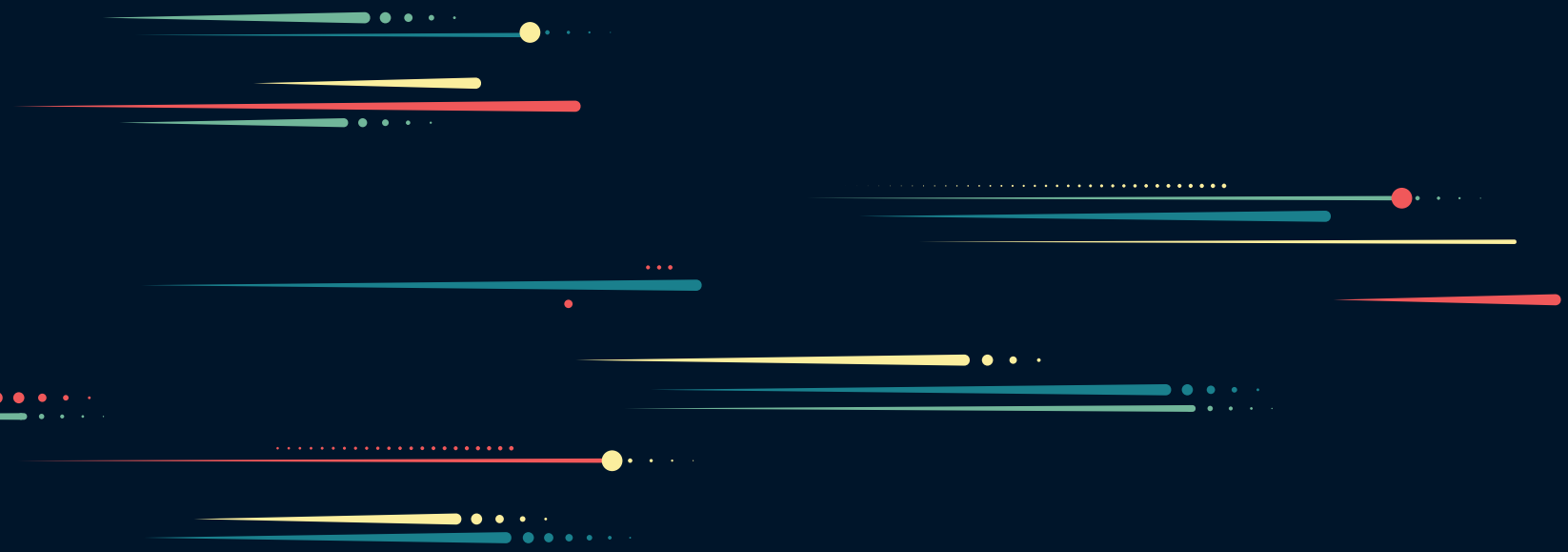
Overall, these purely technical case-studies aim at showing how the conscious integration of AI tech-

1. Commercial and open access applications were used, without relying on the greater computational and technological capabilities available within the intelligence system.

nologies – embedded within a rigorous methodological framework and under analysts' control – may enhance the wider quality of analysis, facilitate the emergence of patterns and trends, and ultimately support more informed and timely decision-making processes for the benefit of policymakers.

In line with the choice made last year, also this edition features a special **insert** dedicated to an advanced frontier of global competition. Particular focus has been placed on the advent of quantum technology, with the aim of exploring both its potential and the multiple implications arising from a national security perspective.

"Steering change" increasingly requires foresight capabilities to anticipate emerging phenomena and threats.



www.sicurezzanazionale.gov.it

#sicurezzanazionale