The Non-paper by Defense Minister Guido Crosetto: Italy Facing Hybrid Warfare (pdf)

Published on 19/11/2025

During the meeting of the Supreme Defense Council, the "Non-paper on countering hybrid warfare" drafted by **Defense Minister Guido Crosetto** was presented, a document that highlights how Italy is currently in a context characterized by multi-domain activities conducted by hostile actors in ways that do not exceed the threshold of traditional armed conflict.

The meeting was attended by **President of the Republic Sergio Mattarella**, **Prime Minister Giorgia Meloni**, **Minister of Foreign Affairs and International Cooperation Antonio Tajani**, **Minister of Enterprises and Made in Italy Adolfo Urso**, and **Chief of Defense Staff General of the Army Corps Luciano Portolano**.

During the presentation, Defense Minister Guido Crosetto outlined a scenario where attacks do not exclusively concern infrastructures and systems but also significantly affect the informational domain and public perception. The document emphasizes how the cognitive

dimension is now an essential element of national security, as targeted activities can impact institutional stability and collective trust.

The “Non-paper” brings together analyses from open sources, intelligence contributions, and information gathered internationally, and is intended for the Presidents of the Chamber of Deputies and the Senate of the Republic.

Hostile actors and Italian vulnerabilities: from the cognitive to the cyber domain

The document identifies four main actors capable of conducting hybrid activities against Italy and other Western countries: **the Russian Federation**, **the People's Republic of China**, **the Islamic Republic of Iran**, and **the Democratic People's Republic of Korea**.

The **Russian Federation** employs a complex set of tools, including information operations, economic pressure, activities in cyberspace, and support for affiliated groups capable of conducting actions not directly attributable. The conflict in Ukraine has consolidated the use of techniques aimed at influencing the European framework without generating military escalation.

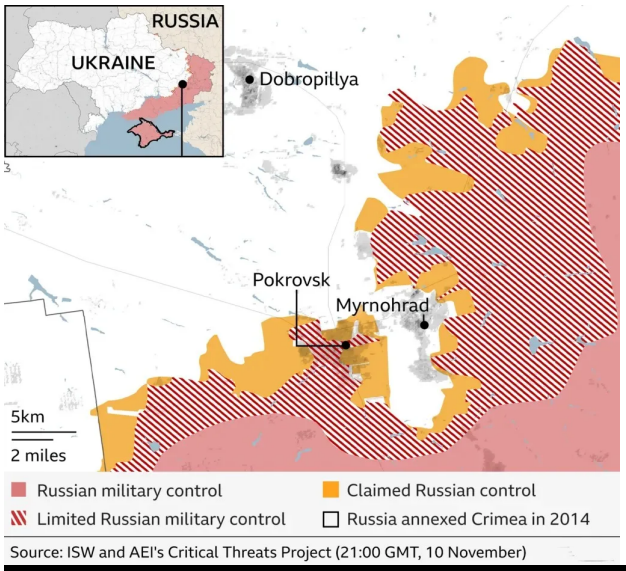
The **People's Republic of China** adopts a “multi-vector” strategy, based on the combination of economic, technological, and informational levers. European dependencies on strategic raw materials — such as rare earths, gallium, and germanium — are indicated as particularly sensitive elements. Italy shows a degree of dependency on the import of these materials above the EU average.

The **Islamic Republic of Iran** operates through a network of regional actors and initiatives affecting areas of high strategic relevance, including major maritime choke points. Italy's geographical position, strongly linked to Mediterranean and Suez Canal trade routes, necessitates continuous monitoring of regional security dynamics.

The **Democratic People's Republic of Korea** maintains a very active cyber apparatus, employed for ransomware activities, digital espionage, and resource theft in cyberspace.

The document also highlights some national vulnerabilities: energy dependence on foreign countries, the concentration of critical infrastructures on Italian territory, and the growing exposure to disinformation phenomena. According to data from the National Cybersecurity

Agency, **1,979 cyber events** and **573 incidents with confirmed impact** were recorded in 2024, with an increase compared to 2023. In the first half of 2025, a further increase was detected. The healthcare and manufacturing sectors are among the most affected.



NATO Summit Brussels (October 2024), discussion on hybrid threats. Source: Ministry of Defense.

A specific section of the document also analyzes potential interferences in democratic processes, made possible by the evolution of information manipulation techniques, including deepfake and micro-targeting. This dynamic requires strengthening cooperation between national and European institutions, especially during electoral consultations.

Building a proactive posture: national tools and international cooperation

The “Non-paper” proposes to strengthen national resilience as a central element in responding to hybrid threats. Resilience is defined in a broad sense, including technological, institutional, economic, and informational aspects.

On the international level, the document recalls ongoing initiatives within **NATO**, the **European Union**, and the **G7**. NATO has updated its strategy for countering hybrid threats, enhancing cyber support tools and strengthening its presence on the southern flank. The European Union has expanded its regulatory framework on digital security thanks to NIS2, the Cyber Resilience Act, and the Digital Services Act, while bodies like ENISA and ECCC contribute to the consolidation of common operational capabilities. The G7, by extending the mandate of the Rapid Response Mechanism to economic coercion, has also shown increasing attention to the

multidimensional nature of the threat.

Group photo of the G7 Defense Ministers Summit (Naples, October 2024). Source: Ministry of Defense

On the national level, the document presented by **Defense Minister Guido Crosetto** outlines a series of structural interventions. Among these are:

- the creation of a **Civil-Military Cyber Force**, continuously active and staffed with highly qualified personnel;
- the establishment of a **National Center for Countering Hybrid Warfare**, tasked with coordinating analysis, responses, and cooperation between administrations, businesses, and academia;
- the promotion of a **national security culture**, aimed at consolidating collective awareness and improving the ability to recognize and mitigate hybrid activities.

The document concludes by emphasizing that these initiatives do not represent just a technical response to new forms of threat but constitute a decisive step towards a more modern, integrated, and prepared national system posture. The proposals advanced by Defense Minister Guido Crosetto define a clear path: consolidating the protection of critical infrastructures, strengthening prevention and response capabilities in the cyber domain, improving institutional coordination, and expanding specialized skills.

In the vision outlined by the Minister, Italy can equip itself with an organic and highly qualified tool, capable not only of confronting hybrid activities but also of anticipating them. The project of a Cyber Force and the creation of a dedicated national center constitute, in this sense, a long-

term strategic investment, aimed at ensuring operational continuity, deterrence, and an adequate level of protection for the complexity of the current scenario.

Overall, the proposed framework represents a significant evolution of the national posture: a model that integrates prevention, analysis, response, and international cooperation, offering the country a more solid protection capability consistent with emerging challenges.

non-paper_il_contrasto_alla_guerra_ibridaDownload

News link: https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf