

(English version)

**Question for written answer E-002269/24
to the Commission
Giuseppe Antoci (The Left)
(28 October 2024)**

Subject: Cybersecurity in Italy and the effectiveness of NRRP investments in cybersecurity

Recent IT security incidents in Italy have highlighted serious vulnerabilities in the country's critical infrastructure. In one of those incidents, a former employee of Intesa Sanpaolo was accused of having accessed, more than 7 000 times and without authorisation, the current accounts of public figures ⁽¹⁾, and the hacker Carmelo Miano was arrested for having compromised the IT systems of the Guardia di Finanza and the Ministry of Justice, including by accessing the judges' email accounts ⁽²⁾.

These incidents raise serious questions about the Italian system's ability to protect sensitive data and apply cybersecurity policies in an effective manner. It is worrying that, although funds were allocated as part of the NRRP ⁽³⁾ to improving security infrastructure, most of the steps taken seem to be limited to the drafting of analytical reports and not to making real improvements to operational capacities ⁽⁴⁾.

In the light of the above:

1. Is the Commission aware of the details of these major IT security incidents in Italy and what specific measures can it propose to prevent future cracks in the IT security of Italian institutions?
2. Will it take action to ensure that the NRRP's cybersecurity objectives are actually achieved?
3. What is its assessment of the measures Italy has taken so far to bolster the security of its critical infrastructure and what additional recommendations can the Commission provide to ensure that EU funding is used to make tangible improvements, rather than exclusively for analysis and planning purposes?

Submitted: 28.10.2024

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(28 January 2025)**

Strengthening Member States' cyber resilience capabilities, coordinating national cyber efforts and securing critical infrastructures are top priorities for the Commission, which monitors closely cyber threats and incidents affecting the EU's critical infrastructure.

The directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) ⁽¹⁾ requires from entities in 18 critical sectors, including public administration, to take risk-based cybersecurity risk-management measures and report significant cyber incidents.

The NIS 2 Directive transposition deadline for the Member States was 17 October 2024. The Commission is now assessing the Italian transposition legislation that was notified on time.

In addition, Regulation on digital operational resilience for the financial sector (DORA) ⁽²⁾ requires financial entities to develop capabilities to detect, prevent, limit the impact of information and communication technologies-related incidents, to respond and recover from them, and report major incidents. To assess the effectiveness of the entities' capabilities, DORA introduces testing requirements.

Investment 1.5 'Cybersecurity' ⁽³⁾, worth EUR 623 million, from Italy's National Recovery and Resilience Plan (NRRP) spans from creating a Cybersecurity Agency to the implementation of actions boosting Italy's cyber resilience capabilities.

In the context of Italy's fifth payment request, five milestones and targets were assessed as satisfactorily fulfilled: (i) creating the National Cybersecurity Agency (ACN), (ii) defining the national cybersecurity architecture, (iii) the start-up of a network of cybersecurity laboratories, (iv) activating a central audit unit within the ACN (v) completing five strengthening interventions.

¹ <https://www.rainews.it/articoli/2024/10/conti-spiati-i-pm-al-lavoro-si-cercano-accessi-su-pc-tablet-e-cellulari-36fd4f40-5aa2-4c62-84bd-418b78fe8809.html>

² <https://www.rainews.it/video/2024/10/carmelo-miano-lhacker-arrestato-aveva-le-password-di-46-pm-326a4c59-c772-40ba-a959-c7af24ed2705.html>

³ Target M1C1-9 — 'Support for the upgrading of T1 security structures'.

⁴ ECA Annual reports for the financial year 2023, Box 11.1 p. 405, https://www.eca.europa.eu/ECAPublications/AR-2023/AR-2023_EN.pdf

⁽¹⁾ <http://data.europa.eu/eli/dir/2022/2555/oj>

⁽²⁾ <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>

⁽³⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024PC0509>