

(English version)

**Question for written answer E-002101/25
to the Commission
Bart Groothuis (Renew)
(26 May 2025)**

Subject: Concerns about Chinese hacks of Deutsche Telekom and potential implications for the Commission's IT infrastructure

According to a blog post ⁽¹⁾ by the cybersecurity company Eclectic IQ, a Chinese hacker group, UNC5221, is responsible for a hack of Germany's largest telecommunications company, Deutsche Telekom, as well as its subsidiaries that provide IT services. The blog also reveals that this hacker group has targeted other strategic sectors in Europe.

According to other sources, a subsidiary of Deutsche Telekom, T-Systems, also provides services to the Commission. T-Systems has even been designated as a 'preferred supplier' of the Commission for the provision of IT infrastructure. This raises serious questions about the security of the EU's IT infrastructure.

1. Is the Commission aware of this hack, has the Commission itself been affected, and what measures does the Commission take to manage such risks?
2. Why are strategically sensitive hacks such as these not publicly disclosed, and does the Commission agree that silence about such breaches actually facilitates their continuation within Europe?
3. What steps is the Commission taking towards the Chinese authorities in response to these attacks, and what additional measures is the Commission considering to prevent such attacks in the future?

Submitted: 26.5.2025

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

The Commission is aware of media reports on Ivanti vulnerabilities being exploited by threat actors, against organisations from critical sectors including telecommunications.

The Commission cannot comment on cybersecurity matters of other entities, including private companies. The Commission works on proactive measures and has invested in state-of-the-art tools for monitoring, detection, and incident response.

The Commission relies on high levels of in-house expertise and close collaboration with peers and CERT-EU ⁽¹⁾, which is monitoring the situation and stands ready to provide further support to EU entities as needed.

The Network and Information Security Directive (NIS2 Directive) ⁽²⁾ requires entities to report significant cybersecurity incidents. Where public awareness is necessary to prevent a significant incident or to mitigate its effects, under certain conditions, the NIS2 Directive provides that the public could be informed.

As of 11 September 2026, the Cyber Resilience Act ⁽³⁾ will require manufacturers of products with digital elements to report actively exploited vulnerabilities and severe security-related incidents.

The EU has publicly condemned such behaviour as unacceptable and contrary to established norms of responsible state conduct in cyberspace.

The EU has reiterated its call for China to take appropriate action against cyberattacks emanating from its territory and to adhere to its international obligations.

The EU has emphasised that it remains ready to impose costs, including restrictive measures, against individuals or entities responsible for such activities under its cyber diplomacy toolbox and cyber sanctions regime.

The EU also continues to strengthen its cybersecurity resilience through coordinated exercises, policy frameworks, and international cyber dialogues.

¹ Büyükkaya, A., 'China-Nexus Threat Actor Actively Exploiting Ivanti Endpoint Manager Mobile (CVE-2025-4428) Vulnerability', EclecticIQ, 21 May 2025, <https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability>.

⁽¹⁾ <https://cert.europa.eu/>.

⁽²⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>.

⁽³⁾ <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>.