General Camporini defends Cavo Dragone: «Striking the source of a cyber attack with a virus is a defensive act.»

Published on 04/12/2025

General **Vincenzo Camporini**, former Chief of Defense Staff, now retired, speaks on the topic of cybersecurity, opening up to a non-conventional interpretation of digital countermeasures. In an interview with *Corriere della Sera*, when asked about recent statements by Admiral Cavo Dragone, the high-ranking officer states that **the use of a virus against the identified source of a cyber attack can fall under legitimate defense**, provided the origin of the offensive is confirmed.

Increasing threats and attack attribution

According to Camporini, the volume and nature of cyber attacks targeting institutions, critical infrastructures, and companies continue to grow. The officer highlights that **a significant**

portion of these aggressions would come from actors linked to the Russian area, while also noting that the certain attribution of a cyber attack remains complex due to technical nature and cover dynamics.

Cyber defense has so far focused on passive tools, firewalls, filtering systems, advanced protections, but, Camporini observes, **the evolution of the international scenario requires considering more incisive responses**.

From passive defense to active defense

The general draws attention to the fact that the distinction between attack and defense in the digital domain is increasingly thin. A reaction employing malware, he argues, **can be interpreted as a defensive measure aimed at neutralizing the source of the aggression**, not as a hostile act in itself.

The issue fits into the broader context of **hybrid warfare**, where digital tools, propaganda, and clandestine operations intertwine. Even within NATO, Camporini notes, there is discussion about the possibility of adopting **active defense tools** capable of limiting or stopping a digital aggression at its source.

Operational, legal, and strategic implications

The position raises significant questions. The use of a virus as a response raises questions about the **international legal framework**, the proportionality of the action, and the risk of hitting third-party systems or civilian infrastructures. The problem of attribution remains central: **only an unequivocal identification of the attack's origin** can justify an active intervention.

There are also highlighted risks of a potential **digital escalation**, where state and non-state actors could respond with further offensives, expanding the conflict.

A debate destined to grow

Camporini's statements are part of a context where governments and military alliances are called to define **new cyber-defense doctrines**, capable of adapting to ever-evolving threats. The possibility of considering an “active” cyber action as part of defense represents a conceptual shift destined to weigh on future security strategies.

According to Camporini, the protection of states and their infrastructures can no longer be limited to mere passive resistance to attacks, but must include **tools capable of preventing, interrupting, and neutralizing the threat at its source**.

News link: https://roma.corriere.it/notizie/cronaca/25_dicembre_03/il-generale-camporini-colpire-con-un-virus-la-fonte-identificata-di-un-aggressione-cyber-e-un-atto-difensivo-cf10679d-885f-408f-aadb-16c9bd33cxlk.shtml