Il Generale Camporini difende Cavo Dragone: «Colpire con un virus la fonte di un attacco cyber è un atto difensivo.»

Pubblicato il 04/12/2025

Il Generale **Vincenzo Camporini**, già Capo di Stato Maggiore della Difesa, oggi in pensione, interviene sul tema della sicurezza informatica aprendo a una lettura non convenzionale delle contromisure digitali. In un'intervista al *Corriere della Sera*, interpellato sulle recenti affermazioni dell'Ammiraglio Cavo Dragone, l'alto ufficiale afferma che **l'impiego di un virus contro la fonte identificata di un attacco informatico può rientrare nella legittima difesa**, purché sia accertata l'origine dell'offensiva.

Minacce crescenti e attribuzione degli attacchi

Secondo Camporini, il volume e la natura degli attacchi cibernetici rivolti verso istituzioni, infrastrutture critiche e aziende continuano a crescere. L'ufficiale evidenzia che **una parte**

rilevante di queste aggressioni proverrebbe da attori riconducibili all'area russa, pur ricordando come l'attribuzione certa di un cyberattacco resti complessa per natura tecnica e per dinamiche di copertura.

La difesa cibernetica finora si è concentrata su strumenti passivi, firewall, sistemi di filtraggio, protezioni avanzate, ma, osserva Camporini, **l'evoluzione dello scenario internazionale impone di valutare risposte più incisive**.

Dalla difesa passiva alla difesa attiva

Il generale richiama l'attenzione sul fatto che la distinzione tra attacco e difesa, nel dominio digitale, è sempre più sottile. Una reazione che impiega un malware, sostiene, **può essere interpretata come una misura difensiva volta a neutralizzare la fonte dell'aggressione**, non come un atto ostile fine a sé stesso.

Il tema si inserisce nel più ampio contesto della **guerra ibrida**, in cui strumenti informatici, propaganda e operazioni clandestine si intrecciano. Anche in ambito NATO, osserva Camporini, si sta discutendo la possibilità di adottare **strumenti di difesa attiva** capaci di limitare o interrompere a monte un'aggressione digitale.

Implicazioni operative, giuridiche e strategiche

La posizione solleva questioni rilevanti. Il ricorso a un virus come risposta solleva interrogativi sul **quadro normativo internazionale**, sulla proporzionalità dell'azione e sul rischio di colpire sistemi terzi o infrastrutture civili. Resta centrale il problema dell'attribuzione: **solo un'identificazione inequivocabile dell'origine dell'attacco** può giustificare un intervento attivo.

Sono inoltre evidenziati i rischi di un'eventuale **escalation digitale**, in cui attori statuali e non statuali potrebbero rispondere con ulteriori offensive, ampliando il conflitto.

Un dibattito destinato a crescere

Le dichiarazioni di Camporini si inseriscono in un contesto in cui governi e alleanze militari sono chiamati a definire **nuove dottrine di cyber-difesa**, in grado di adattarsi a minacce in continua evoluzione. La possibilità di considerare un'azione informatica "attiva" come parte

della difesa rappresenta una svolta concettuale destinata a pesare sulle future strategie di sicurezza.

Secondo Camporini, la protezione degli Stati e delle loro infrastrutture non potrà più limitarsi alla mera resistenza passiva agli attacchi, ma dovrà includere **strumenti capaci di prevenire, interrompere e neutralizzare la minaccia alla fonte**.

Link notizia: 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