LA STAMPA

Quotidiano

Data 02-04-2021
Pagina 1+21
Foglio 1

L'ANALISI

CYBERSECURITY PIENA DI FALLE

GIAN ENRICO RUSCONI

«I segreti Nato venduti a Mosca. Arrestato un ufficiale-spia a Roma". E' una notizia che sembra riportarci alla "guerra fredda" degli anni Cinquanta. Che ne è allora dei nuovi sistemi di sicurezza informatici, digitalizzati, di cui tanto si parla? Che ne è della "cybersicurezza" militare che sviluppata nella dimensione digitale (cyber, appunto) avrebbe dovuto rendere obsolete le modalità con cui le spie tradizionali rubano i segreti militari e statali? L'episodio di cui si parla oggi è un fatto anomalo, marginale, buono per i più svariati commenti giornalistici, oppure getta una luce imbarazzante sulla effettiva efficacia della cybersicurezza di cui dovrebbero godere innanzitutto "i segreti Nato"? Naturalmente la questione dell'efficacia non vale solo per la sicurezza cibernetica passiva, per così dire, ma anche per la cibernetica attiva.

CONTINUA A PAGINA 21

CYBERSECURITY PIENA DI FALLE

GIAN ENRICO RUSCONI

SEGUE DALLA PRIMA PAGINA

Cioè la capacità di colpire l'avversario nel suo apparato comunicativo (computer, server, reti) rendendo appunto obsoleto lo spionaggio tradizionale da esso promosso.

Si parla di "guerra fredda cibernetica". Ma è un'espressione ambigua. La "guerra fredda" storica infatti era la messa in mora, la sospensione dell'aggressività del nemico che avrebbe potuto e dovuto concretizzarsi in azioni militari distruttive - sino all'ipotesi estrema dell'uso del nucleare. Anzi era proprio questa ipotesi estrema che dava piena efficacia alla "deterrenza" storica, rendendo "fredda" la guerra, appunto. Ma la guerra cibernetica di oggi non è "fredda" in questo senso, perché agisce attivamente. Penetra nel sistema informatico del nemico arrivando in profondità sino ad alterarne gli strumenti di informazione militare. Così è accaduto, ad esempio, con il virus informatico Stuxnet creato dagli americani (in collaborazione con il governo israeliano) per sabotare la centrale nucleare iraniana di Natanz. Il virus doveva disabilitare le centrifughe della centrale, impedendo la rilevazione dei suoi malfunzionamenti e della presenza del virus stesso.

Azioni aggressive di tipo analogo sono state messe in atto dalla Russia, ad esempio, in Georgia, con il danneggiamento di impianti pubblici, l'alterazione delle informazioni governative, con azioni di propaganda con gravi ripercussioni in materia di sicurezza e difesa. Naturalmente tutte queste operazioni sono realizzate in modo da impedire l'identificazione dei diretti responsabili.

Il quadro ora descritto è complesso e non sappiamo quanto completo, ma dobbiamo abituarci a tenerlo presente. La sicurezza cibernetica è parte integrante della sicurezza nazionale e internazionale. La comunità internazionale sta investendo una grande quantità di risorse per affrontare al meglio questo campo, incentivando la cooperazione tra Stati nello scambiarsi informazioni sensibili.

L'Italia deve fare la sua parte. —


LA STAMPA
Virus, il governo accelera si studia il pass vaccinale