L'intervista

Urso, capo del Copasir: «È la nuova guerra, va combattuta insieme con l'aiuto della Nato»

«Codice penale non più adeguato, bisogna cambiare»

Lo stato del Paese
L'Italia si sta attrezzando, è necessario più che mai evitare il sistema 5G dei cinesi

Lotta ai criminali
Vanno combattuti con armi nuove, come l'Autorità contro il riciclaggio dell'Ue

ROMA Il presidente del Copasir Adolfo Urso è preoccupato: «L'attacco degli hacker alla Regione Lazio? Perché vi sorprendete? Sapete che la Nato, nell'ultimo vertice, ha equiparato gli attacchi cibernetici a quelli via mare, via terra, via cielo? E ha concluso che per fronteggiarli servirà ancora una volta il mutuo soccorso tra i vari Paesi. Insomma, se questa è una guerra nuova per il dominio dello spazio cibernetico, va combattuta insieme com'è sempre stato».

E l'Italia è pronta?

«L'Italia si sta attrezzando. Vi ricordo che il comitato che oggi presiedo affrontò la questione sin dall'inizio della legislatura, tre anni fa, quando con la presidenza Guerini — io ero il vice — elaborò una relazione al Parlamento, approvata all'unanimità, in cui si evidenziava come già nel 2018, prima del Covid-19, le azioni ostili cibernetiche — cito testualmente — erano aumentate del 561 per cento rispetto all'anno precedente e avevano colpito soprattutto, nel 72 per cento dei casi, i sistemi informatici di pubbliche amministrazioni centrali e locali. Quella relazione, inoltre, indicava la necessità di evitare l'utilizzo della tecnologia cinese nelle infrastrutture 5G per meglio garantire la sicurezza nazionale, cosa che sembra finalmente caratterizzare l'azione del governo Draghi».

Teme la Cina?

«Non si tratta di questo, il guaio degli attacchi cibernetici è che non è mai chiara la fonte. Mi spiego: tu in base alla tecnologia usata dagli hacker puoi ipotizzare una provenienza, ma il camuffamento in un campo come questo è molto più facile. Perciò bisogna intervenire su altri fronti: realizzare un perimetro di sicurezza cibernetico proteggendo al massimo reti, imprese, banche dati e realizzare il cosiddetto *cloud* nazionale. E poi, lo indicavamo già in quella relazione al Parlamento, si profila come sempre più necessario l'intervento del legislatore per individuare fattispecie nuove di reato, nuove aggravanti. È giusto mettere mano al codice per aggiornarlo. Gli atti di criminalità cibernetica finanziaria sono allo stato perseguibili facendo ricorso a fattispecie generiche. Questi criminali che chiedono il pagamento di riscatti con criptovalute, in Italia e all'estero, non sono una novità. Ma vanno combattuti con strumenti nuovi. Penso all'Autorità europea contro il riciclaggio appena istituita. Ecco, se posso permettermi, sono d'accordo col presidente dell'Abi, Patuelli: la sede giusta sarebbe proprio l'Italia, che nel contrasto al riciclaggio è all'avanguardia».

Finalmente sta per partire l'Agenzia per la cybersicurezza nazionale. Crede che servirà?

«Ma certo, il decreto licenziato ieri sera anche dal Senato permetterà di partire subito, colmando una grave lacuna. L'Agenzia sarà a regime con 800 dipendenti del più alto livello, presi dalla Pubblica amministrazione e poi anche attraverso gare e chiamate dirette. La resilienza cibernetica diventerà realtà con in campo le imprese, le università, la P.A. e la formazione.

L'accelerazione del passaggio al digitale, dalla profilassi vaccinale allo smart working determinato dal lockdown dovuto alla pandemia, ha aumentato a dismisura il raggio d'azione del sistema cibernetico e di conseguenza la sua vulnerabilità. Ciascuno di


Hacker, dati e stipendi a rischio
Ora i pm indagano per terrorismo
Urso, capo del Copasir: «È la nuova guerra, va combattuta insieme con l'aiuto della Nato»


Attaccato anche il sito del Consiglio dei notai
I possibili futuri target: reti energetiche, sanità e società quotate

noi, perciò, deve diventare un bravo operatore digitale che sa di backup e di chiavi d'accesso così da poter scegliere il proprio antifurto migliore e contribuire alla difesa del Paese. Altrimenti sarà meglio tornare ai lucchetti e alle inferriate».

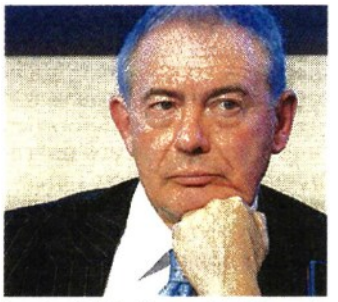
Oggi vedrà il capo del Dis Elisabetta Belloni. È un grande gioco di squadra.

«Proprio così, come l'Italia alle Olimpiadi: l'Agenzia, la nostra intelligence, la Polizia postale, la Difesa, ma anche i partiti di maggioranza e opposizione, perché quando c'è in ballo la sicurezza nazionale si gioca uniti. Le risorse del Recovery fund serviranno anche a mettere al riparo la nuova società digitale. Con un attacco cibernetico si può paralizzare il traffico delle auto con guida da remoto di una città intera, si può fermare un oleodotto com'è già successo in America e poi chiedere il riscatto. Altro che missili! Nessun allarmismo ma occhi aperti. Dietro ci possono essere estorsori comuni oppure Stati...».

A proposito, non l'allarma di più la vicenda dell'ufficiale di Marina italiano Walter Biot, arrestato con l'accusa di aver venduto documenti riservati ai russi?

«La nostra intelligence è intervenuta nel migliore dei modi. Mi preoccupano molto di più le cose che conosciamo di meno».

Fabrizio Caccia



Leader Adolfo Urso guida il Copasir