# AGENZIA DELLA CYBERSICUREZZA NAZIONALE: il nuovo direttore

**- 14 marzo 2022 -**

Le dimissioni del direttore dell'Agenzia per la Cybersicurezza Nazionale Roberto Baldoni, a seguito della massiccia ondata di attacchi informatici condotti dal gruppo russo NoName057, hanno brevemente riaperto la giostra delle nomine.

Baldoni, che certamente esperto del settore lo era in quanto già coordinatore del Comitato Nazionale per la Ricerca in Cybersicurezza, direttore esecutivo del CINI, nonché laureato nel settore, è stato quindi sostituito dall'ex prefetto di Roma, Bruno Frattasi, chiaramente non esperto nell'ambito della cybersicurezza, come riportato in diversi articoli di giornale, ma grande e stimato conoscitore della pubblica amministrazione e capace servitore delle istituzioni.

Sul fatto che il nuovo titolare della posizione di direttore come sostituto del prof. Baldoni debba o meno avere competenze specifiche e in quale misura, è stato un tema centrale delle opinioni espresse dai vari commentatori ma tra le righe di ciò che è stato detto o scritto sino ad ora non si è mai trovata alcuna considerazione riguardante l'unico aspetto che meriterebbe di essere approfondito ovvero l'opportunità o meno di lasciare alla politica il controllo di tale organismo e la veste operativa che ci si prefigge di dargli.

Quando si parla di cybersicurezza bisogna rendersi conto che qualsiasi piano di intervento deve presumere la garanzia di un certo tipo di continuità, non è possibile pensare di ideare un piano per la cybersicurezza nazionale senza che nelle radici di esso vi sia la possibilità di sopravvivere all'ottovolante della politica e dei cambi di governo, che a regola vedono la nomina di nuovi sostituti che puntualmente si

trovano a smontare e riprogettare l'intero comparto e la sua filosofia di funzionamento così come ideata dal predecessore, di fatto ripartendo da zero con la certezza della perdita di gran parte delle risorse umane impiegate sino a quel momento.

Alla domanda "Baldoni ha fallito?", la risposta corretta è sì e no. Sì, ha fallito perché il paese ha subito diversi attacchi hacker la cui caratura e origine non sono chiare ma il sospetto è che siano le solite scorribande fatte di attacchi DDoS o defacciamenti, poco importa l'origine geografica. E no, Baldoni non ha fallito, perché ha fallito la politica, delineando nelle stesse premesse per la creazione dell'organismo di cybersicurezza statale la certezza della sua fallibilità o addirittura della sua inutilità.

Ciò perché da sempre in Italia la missione dei vari tentativi di organizzare un organismo di cybersicurezza statale ha sempre avuto (erroneamente) un'accezione difensiva, il che in poche parole significa sempre e solo da una parte il dover rincorrere le falle di sicurezza e dall'altra la formazione di enti e aziende ai fini della prevenzione e della correzione delle falle di sicurezza.

Si è quindi sempre trattato di fare cybersicurezza, passatemi l'allegoria, facendo l'equivalente informatico del catenaccio calcistico mentre in realtà si dovrebbe fare tutt'altro e con tutt'altri strumenti.

Quali? Come? Vediamolo insieme.

Innanzitutto andrebbe seriamente preso atto che fare cybersicurezza oggi significa dover far fronte ad attacchi di guerra asimmetrica condotti da paesi che svolgono operazioni aggressive o di guerra contro lo Stato italiano, con la consapevolezza che tali operazioni possano essere condotte sia da stati nemici che da stati alleati.

Tralasciamo la questione dei defacciamenti e degli attacchi DDoS che oramai oltre che essere alla portata perfino di impuniti adolescenti, possono essere parzialmente arginati anche da un organismo di cybersicurezza analogo a quelli che sino ad oggi si è cercato di organizzare. Diverso discorso va fatto in relazione alle operazioni di cyberguerra vera e propria ovvero:

- operazioni di spionaggio politico
- spionaggio industriale
- attacchi alle persone al fine di controllarne l'operato attraverso il ricatto
- infiltrazione in organismi governativi
- vendita di prodotti tecnologici contenenti spyware all'origine
- installazione preventiva di rootkit o backdoor nelle infrastrutture critiche nazionali.

Per inquadrare meglio la situazione, ecco alcuni esempi specifici.

Il primo è Echelon, l'impianto di spionaggio telematico messo in opera dagli USA e utilizzato anche contro stati alleati, Italia inclusa. Lo sa bene Silvio Berlusconi.

Il secondo è relativo alla guerra di spionaggio militare-industriale messo in opera dalla Francia ai danni di un'azienda italiana produttrice di velivoli militari. Sia l'hacker che operava per conto della Francia che il manager italiano di security che all'epoca si trovò ad arginare tali tentativi di spionaggio erano amici di chi scrive questo articolo; a distanza di qualche anno e a bocce ferme ci ritrovammo tutti insieme a parlare proprio di quegli episodi.

Il terzo è relativo agli attacchi informatici messi in opera dal governo cinese. Già nel lontano 2004 conoscevo hacker cinesi incaricati dal governo della RPC di penetrare all'interno dei server dell' Unione Europea così come, quando in visita all'Università Tecnologica e di Telecomunicazioni di Beijing mi fu chiaro che a interi dipartimenti universitari venissero affidati compiti quali l'analisi dei firewall e VPN straniere al fine di trovarne vulnerabilità così come l'analisi matematica degli algoritmi di cifratura RSA per poter decrittare messaggi crittografati.
Stiamo parlando di un periodo in cui Internet non aveva ancora trovato la sua massima diffusione e da allora la Cina si è via via fatta sempre più aggressiva, complice il fatto che per motivi di convenienza economica le è sempre stato perdonato tutto, quasi ad incoraggiarla indirettamente a perseverare, perché tanto non si sarebbe verificata alcun tipo di ritorsione a quelli che sono dei veri e propri atti di guerra. Oggi si parla anche di spyware affogato nel firmware o peggio ancora, nell'hardware di apparecchiature di produzione cinese, telefoni cellulari inclusi e

quelli li abbiamo sempre in tasca. Possiamo solo immaginarci, a distanza di quasi vent'anni, quali passi avanti abbia fatto la Cina nella conduzione della guerra cibernetica.

Per avere una reale possibilità di contrastare tutto ciò è necessario adottare nuovi metodi e nuovi mezzi.

In relazione ai metodi, è giunto il momento di rendersi conto che è necessario più che mai togliere dalle mani della politica la possibilità di governare l'organismo di cybersicurezza nazionale. Gli attacchi che subisce il nostro Paese sono vere e proprie operazioni militari e quindi militare deve essere la caratura e il controllo del nostro organismo di difesa. Così facendo, non solo lo si contraddistinguerebbe correttamente ma si eliminerebbe la possibilità che ad ogni cambio di governo o all'avvento di nuovi scandali strumentalizzati dalla stampa ai fini della politica, tutto ciò che è stato fatto sino a quel momento venga smantellato e si debba ripartire da zero, con grande gaudio del nemico.

Per quanto riguarda i mezzi, poco importa se il direttore di tale organismo sia del settore, quello che importa nella posizione che ricopre sono le sue capacità manageriali e la volontà di ascoltare i suoi sottoposti, quelli si con grandi competenze tecniche. E così come accade in qualsiasi ambito militare dove per difendersi è necessario prima imparare a sparare, questo nuovo organismo dovrebbe adottare un'attitudine proattiva, invece che perseverare nell'adottare soluzioni passive.
Gli attacchi vanno prevenuti e per prevenirli, il solo applicare le patch di sicurezza e gli opportuni comportamenti in rete non è sufficiente.

Baldoni ha dovuto far fronte a degli attacchi espliciti, laddove i più pericolosi sono stati quelli silenti, spesso operati attraverso l'utilizzo di vulnerabilità di tipo "oday" ovvero vulnerabilità per le quali non esiste ancora una patch di sicurezza o peggio, la vulnerabilità è del tutto sconosciuta.

E per andare a caccia di questi ultimi l'organismo di cybersicurezza dovrebbe dotarsi di un apposito dipartimento che si relazioni o si infiltri, dipendendo dal caso, con l'ambiente hacker dal quale essi vengono generati. Tale organismo

dovrebbe essere dotato di un budget di spesa, perché spesso per entrare in possesso di questi specifici oday è necessario corrispondere una somma di denaro.

In ultimo, per poter operare correttamente e nel pieno delle proprie capacità, è necessario garantire ai membri di tale organismo una speciale dispensa giuridico-legale perché per poter agire nell'ambiente degli oday o per potersi infiltrare, è spesso necessario doversi "sporcare le mani".

E con "sporcare le mani" si intende la massima latitudine possibile.

Chi ha orecchie per intendere, intenda.

Roberto Preatoni
(CISINT Research Analyst)