L'aumento della minaccia cyber nell' attuale contesto internazionale e l'istituzione dell'Agenzia per la Cybersicurezza Nazionale

Il cyberspazio[1] è diventato un dominio di importanza strategica per lo sviluppo economico, sociale e culturale di un paese, ed è quindi fondamentale tutelarne gli aspetti più rilevanti con disposizioni normative, progettualità ed attività che necessitano non solo accordi internazionali e nazionali, ma soprattutto una adeguata sinergia tra pubblico e coinvolgimento privato nella sua governance e gestione, tenendo conto allo stesso tempo delle esigenze connesse alla sicurezza nazionale, nonché la tutela delle libertà individuali ed economiche. Nell'attuale contesto internazionale, considerato il preoccupante aumento della minaccia cyber occorre, in particolare, tutelare le attività che si svolgono nel web da quattro tipi di minacce: innanzitutto quella relativa al cybercrime che contempla tutte quelle attività dolose con intento criminale svolte nel cyberspazio, come truffe o frodi su Internet, furto di identità, furto di dati o di proprietà intellettuale che colpiscono imprese ed utenti, poi quella minaccia più specifica relativa allo spionaggio informatico che si sostanzia nella acquisizione indebita di dati riservati, non necessariamente di valore economico o commerciale, ma che possono avere impatto sulla sicurezza di persone ed enti pubblici o privati, fino a quella dello Stato. La terza e quarta minaccia sono invece individuabili nel cyber terrorismo finalizzato allo sfruttamento ideologicamente motivato delle vulnerabilità dei sistemi con l'intento di influenzare uno stato e/o un'organizzazione internazionale e/o un numero indeterminato di utenti della rete e infine nel *cyber warfare*, minaccia relativa a quelle attività e operazioni svolte in ambito cyber con l'obiettivo di conseguire un vantaggio operativo di rilevanza militare. L'attuale contesto internazionale pone sempre più in evidenza come il cyber risk, in continua ed esponenziale crescita, rappresenti non solo una sfida da affrontare ma anche un'opportunità che deve essere colta, e che non può essere lasciata in secondo piano, tanto che la Cyber defense italiana costituisce soltanto un aspetto del più ampio contesto della sicurezza all'interno dello spazio cibernetico, nel quale una molteplicità di attori è chiamata ad intervenire con l'obiettivo di incrementare la resilienza italiana e la capacità di risposta in caso di crisi cibernetiche[2].

Le strategie, le azioni e le sinergie di difesa attiva necessitavano da tempo di una Agenzia più strutturata che garantisse in maniera unitaria e coordinata, un maggiore un rafforzamento della sicurezza dell'apparato nazionale, assicurando inoltre una più adeguata "resilienza degli operatori e dei fornitori di funzioni essenziali statali, mediante l'adozione di beni, prodotti e servizi che dovrebbero essere concepiti come più sicuri e resistenti rispetto alle sempre crescenti minacce cyber"[3]. Per rispondere a queste pressanti esigenze, stante l'enorme crescita degli attacchi informatici[4], il Governo Draghi, nell'ottica di unificare e potenziare

sotto il profilo tecnico operativo, le attività di protezione dalle minacce informatiche, con il decreto legge 82 del 2021[5], ha istituito l'Agenzia per la cybersicurezza nazionale con personalità giuridica di diritto pubblico e una propria autonomia patrimoniale, amministrativa, organizzativa e finanziaria. L'Agenzia, che è deputata a svolgere il rilevante ruolo di Autorità nazionale di cybersicurezza, ha compiti di protezione, resilienza e innovazione in tema di sicurezza informatica, compresa la decisiva tutela della sicurezza nazionale nello spazio cibernetico, assicurando il coordinamento tra soggetti pubblici coinvolti in materia.

L'Agenzia, che ha il rilevante compito di promuovere la realizzazione di azioni comuni volte a garantire la sicurezza e la resilienza cibernetica necessarie allo sviluppo digitale del Paese, è stata volutamente creata al di fuori dell'Intelligence ed è sotto il diretto controllo del Comitato parlamentare per la sicurezza della Repubblica, il quale verifica che l'attività del sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione e delle leggi. Roberto Baldoni che è stato chiamato a dirigere l'Agenzia, ha saputo dotarla sul piano dell'organico di personale altamente specializzato in frequente crescita, tenuto conto che tale ente deve svolgere anche il ruolo di Autorità nazionale di certificazione della cybersicurezza, oltre che Autorità nazionale competente in materia di sicurezza di sistemi informatici e alla sicurezza delle reti e Centro nazionale di coordinamento nell'ambito della industriale in materia di cybersicurezza[6].
La legge istitutiva ha conferito al Presidente del Consiglio dei ministri, in via esclusiva, la responsabilità generale e l'alta direzione, dell'Agenzia, assegnando le direttive e promulgando disposizioni per il funzionamento e l'organizzazione dell'Agenzia[7], infatti quale capo del governo ha anche la responsabilità generale delle politiche di cybersecurity, ed annualmente è tenuto a trasmettere al Parlamento una relazione sull'attività svolta dall'Agenzia. Nell'ambito dell'Agenzia per la cybersicurezza nazionale opera il *Computer Security Incident Response Team Italia*, CSIRT, organo essenziale per l'attività tecnico operativa, dato che ha l'obiettivo di migliorare l'efficacia della prevenzione in merito agli attacchi cyber nei confronti di privati o soggetti pubblici, diffondendo informazioni e intervenendo nei casi di emergenza. Mentre, il Centro di Valutazione e Certificazione Nazionale CVCN, che opera sempre all'interno dell'Agenzia svolge il delicato compito di controllare la sicurezza di beni, sistemi e servizi ICT, adottando delle metodologie che saranno impiegate durante i processi di valutazione del livello, di sicurezza tra cui quello relativo alla predisposizione dell'analisi di rischio[8].

Infine, sempre nell'ambito l'Agenzia nazionale per la cybersicurezza è istituito il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica, il quale ha come fine precipuo quello di potenziare la difesa del nostro Paese, con particolare riguardo all'azione di tutela delle infrastrutture critiche del paese che sono individuate nel sistema delle telecomunicazioni e dei trasporti, l'industria della difesa, gli istituti finanziari, mentre il Nucleo per la cybersicurezza (NCS), ha il compito di rafforzare, sotto il profilo tecnico operativo la resilienza cyber di tali *asset* strategici, svolgendo funzioni di prevenzione e preparazione ad imminenti situazioni di crisi e per l'attivazione delle procedure di allertamento. Il primo organo riunisce il direttore dell'agenzia, il presidente del consiglio, l'autorità delegata e i Ministri degli esteri, dell'interno, della giustizia, della difesa, dell'economia, dello sviluppo economico, della transizione ecologica, dell'università, della transizione digitale e delle infrastrutture. Il comitato[9], inoltre, deve proporre al Presidente del Consiglio gli indirizzi generali che devono essere perseguiti, l'alta sorveglianza riguardo l'attuazione della strategia e la promozione delle iniziative per favorire la collaborazione tra i vari soggetti istituzionali di settore[10].

Il nucleo per la Cyber sicurezza agisce, invece, a un livello prevalentemente tecnico operativo, ponendosi come organo permanente che si occupa degli aspetti connessi alla prevenzione, alla preparazione e alla gestione di eventuali situazioni di crisi. L'agenzia[11], quindi, si pone come punto di riferimento unico della sicurezza cibernetica, con il compito di redigere la strategia nazionale di sicurezza cibernetica e garantire lo svolgimento di azioni comuni per il raggiungimento di più alti livelli di resilienza nazionale, preoccupandosi anche di assumere le funzioni relative al perimetro di sicurezza nazionale cibernetica, operando, infine, come autorità di certificazione della cybersecurity. Tuttavia, non tutto il settore della Cyber sicurezza compete alla nuova Agenzia, che infatti lavorerà in stretto contatto con altri comparti, alle Forze di Polizia resta l'attività di cyber-investigation[12], mentre in via esclusiva delle Agenzie AISI e AISE le operazioni di cyber-intelligence ed in tale ambito il dialogo tra i vari attori per gli aspetti più rilevanti e di comune interesse, viene svolto dal comitato interministeriale per la Cyber sicurezza e dal nucleo per la Cyber sicurezza. Più in generale, il piano nazionale per la protezione cibernetica e per la sicurezza informatica si compone di sei specifici indirizzi strategici: il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese; il miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati; l'incentivazione della cooperazione tra istituzioni ed imprese nazionali; la promozione e la diffusione della cultura della sicurezza cibernetica[13], il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica ed infine il rafforzamento delle capacità di contrasto alle attività e contenuti illegali online. Peraltro, i principi cardine estrapolabili dalle politiche di cyber-security, tanto in ambito internazionale quanto europeo, pongono in

evidenza che è indispensabile favorire un approccio comune riguardo le principali questioni strategiche, in completa armonia logica con la globalità di tale dominio. Pertanto, focalizzare su tali indirizzi anche il quadro strategico nazionale rappresenta un elemento fondamentale per l'efficienza e la coerenza le politiche di sicurezza nazionali nel delicato settore.

Da queste rilevanti linee strategiche derivano degli specifici indirizzi operativi da attuare per i prossimi anni che possono individuarsi: nel potenziamento della capacità di intelligence, di polizia e di difesa civile e militare, nel potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati, nella promozione e diffusione della cultura della sicurezza informatica con periodiche azioni di formazione ed addestramento, nelle iniziative di cooperazione internazionale[14] e nella pianificazione nello sviluppo di esercitazioni finalizzate a testare in concreto l'operatività delle strutture nazionali di prevenzione degli incidenti informatici, procedure di risposta e recupero dei sistemi informatici attaccati. Altri indirizzi operativi da attuare sono stati individuati infine nella valutazione, predisposizione e promozione di opportuni interventi tecnici e legislativi da armonizzare con la conformità agli obblighi internazionali assunti e soprattutto con i vigenti standard e protocolli di sicurezza, nel supporto allo sviluppo industriale e tecnologico, nella comunicazione strategica e operativa, nel reperimento delle risorse necessarie ad attuare i citati interventi operativi, compresa l'adeguata implementazione di un sistema di cyber risk management nazionale. Nel 2021 gli attacchi nel mondo sono aumentati del 10% rispetto all'anno precedente, e sono sempre più gravi, dato che le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata come emerge nei due più recenti rapporti dell'associazione italiana per la sicurezza informatica CLUSIT[15].

L'impatto economico della criminalità informatica è notevole[16] soprattutto in ambito economico ed industriale, ma non disdegna colpire le istituzioni pubbliche e con maggiore facilità gli utenti più deboli. Secondo i ricercatori del CUSIT nel 2021 il 79% degli attacchi informatici rilevati ha avuto un impatto "elevato", contro il 50% dell'anno precedente, in particolare il cybercrime si conferma la motivazione principale dell'86% dei cyber attacchi, in crescita rispetto all'81% del 2020, un trend che non accenna a diminuire[17]. Per la prima volta dopo diversi anni i ricercatori del Clusit hanno rilevato che i cyber criminali non colpiscono più in maniera indifferenziata obiettivi molteplici, ma mirano a bersagli ben precisi: al primo posto c'è l'obiettivo governativo/militare, con il 15% degli attacchi totali, in crescita del 36,4% rispetto all'anno precedente; segue il settore informatico, colpito nel 14% dei casi (+3,3% rispetto al 2020), gli obiettivi multipli (13%, in discesa dell'8%) e la sanità, che rappresenta al pari il 13% del totale degli obiettivi colpiti, in crescita del 24,8% rispetto ai dodici mesi precedenti, segue l'istruzione, pari al 9% del totale[18]. Nel nostro paese i settori più colpiti si confermano quello delle aziende bancarie, finanziarie e assicurative, oltre che la Pubblica Amministrazione, obiettivi che insieme costituiscono circa il 50% dei casi. A questi settori particolarmente bersagliati dall'azione dei criminali informatici[19] si aggiunge quello dell'industria che ha presentato l'aumento più significativo, dal 7% del 2020 al 18% del 2021. Difatti, il volume sempre crescente dei dati aziendali e delle informazioni sulle risorse personali archiviate nel cyberspazio, recentemente incoraggiato dal crescente ricorso al sistema cloud, rende l'attacco informatico potenzialmente molto redditizio pur essendo relativamente privo di rischi per l'attaccante. Non sorprende quindi che l'impatto economico della criminalità informatica sia sempre più preoccupante, ciò è particolarmente rilevante e dannoso per paesi come l'Italia, per i quali il furto di know-how scientifico, tecnologico e originale dell'azienda è un danno diretto al loro vantaggio comparativo esistente, minando la loro competitività sui mercati globali.

La criminalità informatica è anche una preoccupazione crescente poiché gli enormi profitti illeciti che genera vengono spesso reinvestiti dai cyber criminali nella ricerca di nuove vulnerabilità del sistema e nello sviluppo di capacità offensive più sofisticate, efficienti e di facile utilizzo, rendendo la criminalità informatica una grave minaccia alla stabilità, prosperità e sicurezza del Paese. In tale ambito senza dubbio un ruolo decisivo per il rafforzamento della tutela da queste gravi minacce sarà assicurato all'operatività dall'Agenzia nazionale per la cybersicurezza. Se l'approccio strategico all'analisi e alla gestione delle minacce alla sicurezza italiana di tale agenzia è il pilastro imprescindibile sul quale costruire anche la tutela dai rischi derivanti dal cyber-spazio, la sicurezza informatica e delle informazioni, non sarà meno importante il ruolo assunto dagli operatori privati, sempre che il loro prezioso contributo si collochi anche sotto il profilo tecnico e procedurale nel processo istituzionale volto alla difesa in concreto della sicurezza nazionale e alla gestione delle crisi successivamente alle minacce dei cyber criminali. In particolare sarà rilevante l'efficace e tempestivo contributo di quegli operatori privati che gestiscono infrastrutture critiche di importanza nazionale ed europea, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici, i quali da una parte sono chiamati a comunicare ogni significativa violazione della propria sicurezza o dell'integrità dei propri sistemi informatici al Nucleo per la sicurezza cibernetica e, dall'altra, sono tenuti scrupolosamente ad adottare le misure di sicurezza predisposte dall'Agenzia per la cybersicurezza nazionale.

Ufficiale dell'Arma dei Carabinieri

Note

1 - Termine coniato per la prima volta dallo scrittore canadese William Gibson deriva dalla parola greca Kyber che vuol dire “navigare” e indica uno spazio navigabile, unendo i due termini ‘cyber information’ e ‘space’ creando un nuovo termine adatto a descrivere la realtà virtuale. Questo termine, con la nascita di Internet, indica quel luogo virtuale in cui la comunicazione attraverso le reti informatiche avviene. Una classica definizione di cyber space è stata fornita dal Pentagono, che nel 2008 “come il regno delle reti informatiche nel quale le informazioni vengono immagazzinate, memorizzate, condivise e diffuse, una realtà astratta che connette ad un’unica rete di devices di tutto il mondo, consentendo agli utenti che ne fanno uso di interagire tra loro.

2 - R. BALDONI, R. DE NICOLA, “Il Futuro della Cyber Security in Italia”, in *Consorzio Interuniversitario Nazionale Informatica*, 2015, Tenuto conto che in ambito militare la difesa da potenziali attacchi cibernetici può interessare varie strutture, il Comando per le operazioni in rete che è stato istituito nel 2020, ha valenza interforze, è l’organo preposto al contrasto di Cyber attacchi alle strutture della difesa e in caso di attacchi di rilevanza nazionale.

3 - Così in V. DE LUCA, F. VOCE, G. M. TERZI DI SANT’AGATA, Il ruolo dell’Italia nella sicurezza cibernetica: Minacce, sfide e opportunità, Milano, Franco Angeli, 2018.

4 - Già dal 24 gennaio 2013 l’Italia si era dotata per la prima volta di una struttura di sicurezza cibernetica di tutela delle infrastrutture critiche, con l’istituzione nell’ambito del Dipartimento delle Informazioni per la Sicurezza, di un Nucleo per la Sicurezza Cibernetica con il compito di supportare operativamente gli Enti colpiti da attacchi informatici in grado di causare crisi cibernetiche di particolare rilevanza per la sicurezza nazionale e di un tavolo interministeriale per la prevenzione di tali crisi.

5 - Il decreto legge nr. 82, successivamente convertito con modifiche nella legge nr. 109 del 4 agosto del 2021, che oltre a istituire l’agenzia per la cybersicurezza nazionale, divenuta operativa l’1 settembre 202, riconsidera l’intera architettura nazionale cibernetica.

6 - Per consentire all’Agenzia di cominciare la sua attività, considerato che ha l’obbligo di predisporre una relazione annuale trasmessa al parlamento dal presidente del Consiglio dei ministri, il decreto ha istituito una dotazione finanziaria di 2 milioni di euro per il 2021 è una locazione cumulativa di 529 milioni di euro per il periodo che va dal 2021 al 2027. I fondi che sono stati stanziati dovranno coprire inoltre le retribuzioni dei 300 funzionari che daranno operatività all’agenzia e gli stipendi saranno equiparati a quelli dei dipendenti della Banca d’Italia.

7 - In particolare l’art. 4 del D.L. 82/2021, istituisce, presso la Presidenza del Consiglio dei ministri, il Comitato interministeriale per la cybersicurezza, al quale spetta la vigilanza, la consulenza e la proposta in materia di politiche di cybersicurezza. In estrema sintesi i compiti si indentificano nel supporto alla condivisione di informazioni e alla scelta di migliorare pratiche e misure nei confronti della cybersecurity e dello sviluppo tecnologico, scientifico e industriale in tema di cybersicurezza e nel sostegno all’adozione delle necessarie iniziative a sostegno di una collaborazione, efficace tra le istituzioni e gli operatori privati interessati alla cybersecurity a livello sia internazionale sia nazionale, oltre che di proporre al Presidente del Consiglio dei ministri degli indirizzi generali da seguire in tema di politiche di cybersicurezza nazionale e di svolgere la sorveglianza sull’attuazione della strategia nazionale di cybersecurity.

8 - Il Centro di Valutazione e Certificazione Nazionale, per la valutazione di beni, sistemi e servizi ICT destinati a essere impiegati su infrastrutture che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato, è operativo da 30 giugno 2021 , mentre il 30 luglio 2022 è entrato in vigore il regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra tale centro, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell’interno e del Ministero della difesa.

9 - Viene presieduto dal direttore dell’agenzia o dal vicedirettore e ne fanno parte il consigliere militare del presidente del consiglio, un rappresentante di ciascuna delle agenzie di intelligence, della Protezione civile e di ciascuno dei ministeri presenti nel comitato già menzionato.

10 - Che costituisce il punto di contatto nazionale richiesto dalla direttiva dell’Unione Europea 2016/1148 come meglio descritto da R. BRIGHI, P. G. CHIARA, “La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE”, in Federalismi. it, 2021, 21, pp. 18-42.

11 - Caratterizzate dall’insieme di procedure ed azioni investigative finalizzate le attività di individuazione e contrasto delle molteplici forme criminali che si svolgono nel mondo digitale, o di indagine, e contemplano in particolari analisi e recupero dei dati forensi per la prova digitale di un crimine, fondamentali per individuarne gli autori e di bloccare le loro tecniche di aggressione dei sistemi telematici. Secondo Cybercrime Magazine, il costo previsto per le potenziali minacce della criminalità informatica per l’economia globale sarà di 10,5 trilioni di dollari all’anno entro il 2025, con un impatto che non si limita ai soli aspetti economico commerciali ma che si ripercuotono con effetti ben più dannosi sulla salute e sulla sicurezza di intere popolazioni.

12 - Tra cui l’individuazione della Strategia Cloud Italia con la pubblicazione, il 13 settembre 2021, del documento sintetico di indirizzo strategico per l’implementazione e il controllo del cloud nella Pubblica amministrazione.

13 - Mediante l’analisi comparata delle cyber-strategy dei Paesi europei con una strategia già formalizzata, individuando i seguenti elementi comuni a tutte le cyber-strategy comunitarie: la fissazione di trattati, leggi e regole di condotta nazionali e/o internazionali ad hoc, lo sviluppo dei rapporti diplomatici e rafforzando le partnership internazionali, garantendo la protezione dei diritti fondamentali, sulla privacy e/o sulla libertà di espressione, minacciati dal cyber-crime, la creazione di apposite strutture politiche e decisionali per far fronte alla minaccia. Completano questi obiettivi comuni l’azione tesa a incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici, con il rafforzamento della condivisione delle informazioni (anche tra pubblico e privato), l’early warning e le capacità di incident response, compresa l’esigenza aumentare la consapevolezza pubblica della minaccia e l’importanza della cyber-security per limitare gli effetti degli attacchi ed infine incrementare il numero delle figure professionali ad hoc per tutelare il cyber spazio. Come meglio precisato in AA. VV., Cyber Warfare 2018: Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche. Italia, Franco Angeli Edizioni, 2019

14 - Nata nel 2000 presso il Dipartimento di Informatica dell’Università degli Studi di Milano, è la più autorevole associazione italiana nel campo della sicurezza informatica che si relaziona con Enti pubblici privati nazionali ed internazionali che operano nel tema. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. I suoi obiettivi possono essere riassunti nei seguenti punti: diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini; partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo; contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza e promuovere l’uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

15 - Secondo il rapporto Clusit del 2022 gli attacchi crescono in quantità e in qualità si sono verificati nel 45% dei casi ancora nel continente americano Sono invece cresciuti gli attacchi verso l’Europa, che superano un quinto del totale (21%, contro il 16% dell’anno precedente), e verso l’Asia (12%, rispetto al 10% del 2020).

16 - Tra gli attacchi gravi di dominio pubblico, l’11% è riferibile ad attività di spionaggio e il 2% a campagne di guerra dell’informazione.

17 - Tra i trend cybersecurity più rilevanti del 2021 per l’Italia, si osserva la continua crescita dei malware e botnet, con un numero di server compromessi che fa segnare un netto +58%. La penetrazione delle infezioni inizia ad essere rilevante anche nel mobile, con la presenza nelle prime posizioni di FluBot, un malware per dispositivi Android che si distribuisce attraverso link di phishing condivisi grazie a SMS o app di messaggistica.

18 - Che utilizzano il Malware come prima tecnica di attacco, ma per la prima volta dal 2018 scende sotto la soglia del 40% (38%, -3% rispetto al 2021), seguono le tecniche sconosciute (22%), il Phishing e il Social Engineering (13%,) e lo sfruttamento delle Vulnerabilità (11%). Aumenta rispetto al 2021 il ricorso a tecniche multiple (8%) e DDoS (4%,). In definitiva gli attacchi sono meno mirati ma sempre in crescita e sempre più complessi, mantenendo alto il fattore di rischio di un rilevante danno ai sistemi informatici.