Cyberwar, cybersecurity e privacy

Giovanni Reccia
Colonnello della Guardia di Finanza, plurilaureato e abilitato alle professioni di avvocato, di revisore legale dei conti e di giornalista pubblicista, già comandante del Nucleo Frodi Tecnologiche

Fabio Pascucci
Dottore in Giurisprudenza, Scienze politiche, Economia e Scienze della sicurezza economico finanziaria, è Ufficiale superiore della Guardia di Finanza e ha svolto numerosi incarichi pluriennali presso Uffici e C.E.D. del settore informatico

Il recente Rapporto Clusit[1] ha evidenziato che nel 2021 gli attacchi informatici nel mondo sono aumentati del 10% rispetto all'anno precedente e, al contempo, sono diventati sempre più gravi anche in termini di danno. Gli attacchi crescono in quantità, ma anche in qualità, secondo la valutazione dei livelli di impatto dei singoli incidenti che tiene conto degli aspetti di immagine, economici, sociali e le ripercussioni dal punto di vista geopolitico.

Il Rapporto ha sottolineato come il 79% degli attacchi rilevati ha avuto un impatto "elevato", contro il 50% del precedente anno: si sono verificati nel 45% dei casi nel continente americano, ma in leggero calo rispetto al 2020, mentre sono cresciuti quelli 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). Per la prima volta dopo diversi anni, i ricercatori di Clusit hanno rilevato che i cyber criminali non colpiscono più in maniera indifferenziata obiettivi molteplici (cosiddetti "Multiple targets"), ma mirano a bersagli ben precisi: al primo posto c'è quello governativo/militare, con il 15% degli attacchi totali, in crescita del 36,4% rispetto all'anno precedente.

[1] Rapporto Clusit – Edizione di marzo 2022

L'attuale conflitto russo-ucraino ha spinto l'opinione pubblica a concentrare l'attenzione proprio sulla cyberwar. La guerra cibernetica è costituita da una serie di attacchi informatici che prendono di mira diverse strutture pubbliche di un paese. Lo scopo è quello di minare, mediante il ricorso ad azioni malevole compiute nell'ambito del cyberspazio, i sistemi necessari per il corretto funzionamento di uno Stato. "*Oggi il cyberspazio è come l'Europa del 1914, prima dello scoppio della Prima Guerra Mondiale. I governi sono dei sonnambuli. Non comprendono il potere della nuova tecnologia e le conseguenze dovute all'errata interpretazione delle attività altrui*"[2]. Questa autorevole dichiarazione mostra il grave pericolo che una guerra cibernetica potrebbe provocare, generando eventi dannosi quali il fallace funzionamento di reti e sistemi informatici, l'intercettazione di dati, la compromissione delle infrastrutture destinate alla produzione e alla distribuzione di gas, luce e acqua o delle reti finanziarie e commerciali, ovvero la paralisi dei sistemi dei trasporti.

Secondo un altro recente rapporto Microsoft, gli hacker del governo russo avrebbero effettuato un totale di 237 attacchi informatici all'Ucraina, soltanto tra il 23 febbraio e l'8 aprile di quest'anno. Gli attacchi, destinati a distruggere i sistemi informatici, miravano anche a raccogliere informazioni o diffondere disinformazione[3]. Di contro, si è scatenata la rappresaglia nei confronti della Russia da parte di Anonymous, che, con la "*dichiarazione pubblica di guerra cibernetica*" ha lanciato una serie di attacchi ai siti di informazione, agenzie di stampa statali, siti di colossi energetici e piccole biblioteche locali, sollecitando apertamente la popolazione russa ad insorgere contro il proprio Presidente. In un articolo pubblicato nel 2013 su una rivista militare russa, il generale Valerij Gerasimov, Capo di Stato Maggiore pro tempore, ha scritto: "*Nel XXI secolo abbiamo osservato una tendenza a rendere le linee di demarcazione tra lo stato di guerra e lo stato di pace sempre più sfumate*"[4]. Questa affermazione tratteggia perfettamente i contorni della cyberwar, in cui sembra che non accada nulla fino a quando non ci si accorge di pagine web devastate e rese temporaneamente non fruibili, alterazione di informazioni riservate e di dati personali, attacco ad infrastrutture essenziali relative, ad esempio, ai servizi energetici, idrici, di combustibili, di comunicazioni, nonché a servizi commerciali.

La guerra ibrida pervade ogni aspetto di coloro che la subiscono ed accan-

[2] A. Klimburg, affiliato della Harvard Kennedy School del Government Belfer Center.
[3] Rainews 24 aprile 2022.
[4] R. Brooks, *How everything became war and the military became everything: tales from the pentagon,* New York, NY, Simon & Schuster, 2017.

to alle strategie militari convenzionali si affianca un massivo ricorso allo strumento informatico:

- operazioni di hackeraggio, condotte anche da gruppi non necessariamente riconducibili a governi;
- attività di intelligence e di spionaggio cyber, portate avanti in prossimità dell'invasione armata;
- azioni di sabotaggio con utilizzo di malware.

Cyber attacchi del tipo Distributed Denial of Service (DDoS) mirano a saturare le risorse esposte in rete, come ad esempio un sito web di un'agenzia governativa o di una banca, con l'intento di rendere non più disponibile il servizio. Atti di questo tipo potrebbero avere un effetto sulla popolazione, generando una catena di paura nel momento in cui non si riesca più ad accedere alla funzione di home banking, oppure di consultazione degli organi di stampa resi irraggiungibili.

Queste campagne creano anche disinformazione: falsa propaganda e diffusione di fake news tendono a manipolare ed ingannare l'opinione pubblica e ingenerare in essa confusione. Alla stessa stregua, strumenti come social network e applicazioni di instant messaging consentono di diffondere comunicazioni finalizzate a destabilizzare il contesto che si va ad aggredire. L'obiettivo è quello di suscitare malcontento e sfiducia nelle istituzioni, al fine di creare terreno fertile per una possibile azione militare e rendere la popolazione avversaria più accondiscendente e meno aggressiva, soprattutto meno pronta alla resistenza.

In questo scenario così minaccioso, cosa rischia l'Italia e quali potrebbero essere le contromisure da attuare?

Il 20 maggio scorso, gli hacker russi o filorussi di Killnet hanno "bombardato" siti istituzionali italiani, compresi quelli di alcuni ministeri, tra i quali il Ministero degli Esteri, quello dell'Istruzione e quello dei Beni culturali. La polizia postale si è messa al lavoro per mitigare gli effetti dell'azione; parimenti, la Procura di Roma ha aperto un fascicolo di indagine che confluirà in quello già aperto, per accesso abusivo a sistema informatico, dopo l'attacco informatico rivendicato dal collettivo filorusso che ha colpito altri siti istituzionali, tra cui quello del Senato e dell'Istituto Superiore di Sanità, alcuni giorni precedenti. "*Un attacco a cui è molto difficile poter reagire*" ha spiegato il direttore dell'Agenzia per la Cybersicurezza Nazionale durante l'audizione alla Commissione Affari costituzionali[5]. Lo stesso gruppo di

[5] www.camera.it. Il 17 maggio 2022, alle ore 13.30, la Commissione Affari costituzionali ha svolto, in videoconferenza, l'audizione del direttore generale dell'Agenzia per la cybersicurezza nazionale (Acn), Roberto Baldoni.

hacker, tuttavia, anche se ha dichiarato guerra a dieci paesi ritenuti «russofobi e nazisti», tra cui anche l'Italia, ha smentito il suo coinvolgimento. Ciò anche a testimonianza del fatto che o non è così agevole risalire all'origine geografica e al vero colpevole degli attacchi sferrati o siamo in piena disinformazione da guerra informatica.
Per corroborare l'azione di risposta alle incursioni esterne al nostro sistema informatico, il 17 maggio scorso, è stata approvata la Strategia Nazionale di Cybersicurezza 2022-2026 con cui il Governo mira ad affrontare una pluralità di sfide quali:

- il rafforzamento della resilienza nella transizione digitale del sistema Paese;
- il conseguimento dell'autonomia strategica nella dimensione cibernetica;
- l'anticipazione dell'evoluzione della minaccia cyber;
- la gestione di crisi cibernetiche;
- il contrasto alla disinformazione online[6].

Tuttavia, manca ancora molto per poter raggiungere gli obiettivi fissati, anche perché in questo campo l'Italia si è mossa in ritardo rispetto ad altri Paesi come Francia, Germania e la stessa Russia. Rafforzare la resilienza significa anche puntare sulla formazione di personale specializzato, la cui mancanza è una delle debolezze dell'Italia[7]. Un secondo obiettivo è il raggiungimento dell'autonomia strategica: l'Agenzia, per esempio, ha invitato le aziende italiane a dismettere l'uso di tecnologie russe nei sistemi di sicurezza informatica.
A questo punto, appare evidente come una guerra cibernetica metta in crisi prima di tutto la tutela della privacy dello Stato, delle sue istituzioni e soprattutto dei suoi cittadini. La guerra ibrida coinvolge uno stato-nazione che perpetra attacchi informatici su un altro, ma è possibile che gli attacchi siano effettuati da organizzazioni terroristiche o attori criminali che non appartengono ad apparati statali, che cercano di promuovere l'obiettivo di una nazione ostile per scopi propri di natura economica. Quando si perpetrano azioni di spionaggio, con esfiltrazione di informazioni sensibili, o atti di contro-propaganda, con tentativi di controllare i pensieri delle persone che vivono o combattono per un paese bersaglio, la manipolazione dei dati riservati diventa inevitabile.
La domanda allora è d'obbligo: stiamo andando nella direzione giusta?

[6] Comunicato ANSA del 18 maggio 2022.
[7] www.cybersecitalia.it Cybersicurezza, R.Baldoni, *Servono professionisti, va creata da zero una forza lavoro competente*, 10 febbraio 2022.

L'ordinamento italiano di settore è strutturato su piani diversi ove operano Istituzioni diverse, per quanto in parte collegate tra loro nel reciproco scambio di dati. In materia di Privacy vi è l'Autorità Garante che definisce le politiche in tema di protezione dei dati personali, avendo anche contezza degli incidenti informatici. Per gli attacchi hacker vige un sistema giuridico in cui opera la Polizia Postale che, rilevando le azioni illegittime, interessa le Autorità Giudiziarie competenti per lo svolgimento delle relative indagini di polizia giudiziaria in ragione dell'abusivo accesso informatico effettuato dagli attaccanti, mentre, contemporaneamente, sotto il profilo della Sicurezza Interna, ai fini dell'analisi e dei riscontri e della difesa dagli attacchi, opera l'Agenzia di Cybersicurezza Nazionale[8]. Tuttavia questi attori istituzionali si muovono in un ambito tendenzialmente nazionale, quando invero si dovrebbe operare con una Difesa cyber in sinergia con le altre Nazioni europee o aderenti alla NATO ai fini di una sicurezza dalla cyberwar ed adottando azioni di contrasto, anche di risposta all'aggressore. Al momento non riusciamo ad individuare facilmente chi sono gli aggressori informatici che lanciano gli attacchi DDOS, ma è evidente che se si trattasse di gruppi criminali o legati a forme di antagonismo sociale le strategie di contrasto poste in essere a livello nazionale potrebbero essere sufficienti, anche solo in tema di controllo, prevenzione ed identificazione degli autori (se nazionali); laddove invece tali azioni fossero programmate da Stati aggressori che cercano di destabilizzare funzionalmente o economicamente il Paese, allora ci troveremmo in un ambito di cyberwar e probabilmente i mezzi in campo non sarebbero sufficienti. Basti pensare che ad oggi è difficile avere certezze sulla provenienza di un attacco informatico in assenza di un accordo di natura internazionale che coinvolga il maggior numero possibile di nazioni in uno scambio continuo di informazioni[9]. È evidente che in una crisi di guerra non vi sarà mai uno scambio di dati o notizie, se non con i paesi alleati. Neanche è possibile fare affidamento sui corretti comportamenti informatici dei cittadini in quanto è la difesa dagli attacchi che deve essere loro garantita.

Il citato gruppo hacker Killnet, a inizio giugno, ha preso di mira direttamente il CSIRT – Computer Security Incident Response Team del Governo italiano – per oltre dieci ore consecutive. Le capacità degli esperti del CSIRT sono state talmente elevate da respingere completamente l'attacco, nonostante

[8] Senza voler considerare l'AGID che si interessa della digitalizzazione del Paese in corrispondenza dell'ENISA europea.

[9] Su questa necessità vedi l'editoriale dei medesimi autori del numero 1 della rivista Privacy& di gennaio 2022.

fosse stato orchestrato e condotto da 80 diversi Paesi contemporaneamente per rendere più difficoltosa la strategia di difesa. Questo a testimonianza di quanto sia necessario, ancora una volta, un coordinamento a livello internazionale per alzare le più efficaci barriere di sicurezza informatica nel perimetro nazionale.

Lo status giuridico di questo nuovo campo di battaglia virtuale, che poi così irreale non è, non appare ancora molto chiaro, poiché non esiste una normativa internazionale che regoli l'uso delle armi cibernetiche. Tuttavia, questo non significa che la guerra cibernetica non sia oggetto anche di studi giuridici. Una risposta la possiamo trovare nel Cooperative Cyber Defense Center of Excellence (CCDCoE), che ha recentemente pubblicato il Tallinn Manual[10]. Questo manuale, frutto del lavoro di una équipe di accademici internazionali, indipendenti ed esperti di diritto internazionale umanitario e dell'uso della forza, fornisce le linee guida in merito all'applicabilità delle categorie del diritto internazionale al cyber-warfare e alle cyber-operation.

Il processo di redazione ha avuto inizio nel 2007 a seguito di un potentissimo attacco informatico sferrato dalla Russia a danno di siti internet di governo, banche e organismi di informazione estoni. Si trattò del primo attacco cibernetico che, secondo le tesi dell'epoca, sarebbe stato di una portata tale da legittimare l'applicazione dell'articolo 5 del Patto Atlantico, autorizzando di fatto la difesa collettiva di uno stato aggredito. In seno alla NATO venne quindi fondato il NATO-CCDCoE, con sede proprio a Tallinn, con l'obiettivo di ampliare la cooperazione fra gli stati parte dell'Alleanza nel settore della difesa cibernetica.

Questo sforzo di creare il primo corpus legislativo in materia di cyber-warfare, pur essendo privo di valore giuridico, risulta di assoluta utilità e di strettissima attualità, essendo riconosciuto come il testo di riferimento in caso di attacchi informatici che violano il diritto internazionale e come i paesi aggrediti possono rispondere a tali violazioni. Il Manuale reinterpreta il diritto internazionale operando un'analogia tra il mondo fisico e quello cibernetico; pur essendo stato sviluppato all'interno della NATO, in alcun modo i risultati riflettono una posizione ufficiale dell'Alleanza o vincolano gli appartenenti alla stessa. Tuttavia, atteso che l'approccio dei principali attori internazionali in merito ai rapporti diplomatici sui temi della cyber-security risulta spesso quasi completamente incentrato sul dialogo diretto e bilaterale, sarebbe auspicabile che al più presto si cominciasse a ragionare

[10] https://ccdcoe.org/ sito della NATO Cooperative Cyber Defence Centre of Excellence (CCDOE).

in maniera più strutturata proprio in seno agli organismi internazionali (NATO e Nazioni Unite in primis). Dato il livello di maturità che anche questi profili hanno assunto dal primo Tallinn Manual del 2013 ad oggi e l'ormai continuo utilizzo del cyber-spazio da parte dei governi per attività di influenza, spionaggio e di minaccia alla sicurezza delle infrastrutture, sarebbe opportuno che la tematica venisse affrontata a livello multilaterale, in seno agli organismi internazionali[11].

Il motivo principale dell'approccio bilaterale è certamente legato al fatto che le relazioni a due offrono numerosi vantaggi rispetto a quelle multilaterali, anche e soprattutto nel caso in cui il tema impatti su sistemi giuridici e culturali spesso molto differenti tra di loro, come nel caso della cyber-security[12]. Si deve considerare ad ogni modo che i cyber-attacchi possiedono caratteristiche comparabili agli attacchi del tipo *boots on the ground*[13], specialmente con riguardo alle conseguenze che possono derivarne per l'integrità fisica, la vita e la distruzione di proprietà pubblica o privata. Queste operazioni presentano però una dimensione intrinsecamente transfrontaliera, rendendo la loro regolamentazione difficile da attuare, al punto di sfuggire alle norme del diritto internazionale. Punto fondamentale dell'analisi è il riconoscimento dell'uso della forza militare come legittima difesa a seguito di attacchi cibernetici che, in relazione ai loro effetti e alle loro modalità, integrino la definizione di attacco armato secondo il diritto internazionale. Di fronte a queste attività, dovrebbero essere riconosciuti gli elementi caratterizzanti le possibili condotte tenute e soprattutto il profilo e l'identità degli operatori, attraversando i molteplici e differenti impianti giuridici, compresi gli aspetti collegati alla protezione dei dati personali.

Sul piano della tutela dei dati, infatti, possiamo affermare che, sotto la pressione della guerra cibernetica, i governi di molti paesi hanno attuato politiche operative di sicurezza nazionale mediante un approccio di difesa a più livelli, che includono:

- la protezione dell'ecosistema informatico;
- l'aumento di consapevolezza nella sicurezza informatica;
- la promozione di standard aperti per combattere le minacce informatiche;
- l'implementazione di un quadro nazionale di garanzia della sicurezza informatica;

[11] S. Mele, https://www.askanews.it/, 6 febbraio 2017.

[12] S. Mele, https://www.analisidifesa.it/, 8 febbraio 2017.

[13] "Truppe sul campo". Vedi anche A. Rigoni, V. Durazzano, *Da attacchi cyber a "boots on the ground"?* Istituto per gli studi di politica internazionale https://www.ispionline.it/ articolo del 22 aprile 2022.

- il lavoro con le organizzazioni private per migliorare le loro capacità di sicurezza informatica;
- la difesa del settore privato[14].

In sintesi, con la cyberwar vengono meno la privacy e la cybersecurity, ma se il diritto alla riservatezza dei dati ha un suo naturale sviluppo in tempo di pace, labili e sfumati sono oggi i confini tra Sicurezza Informatica e Difesa Cibernetica, che possono svilupparsi contemporaneamente sul territorio nazionale ma con effetti diversi, a cui devono corrispondere azioni di contrasto dinamiche attraverso organismi non unici e con ruoli differenti.

[14] A. Rubino, *Cyberwar: cos'è, tipologie di attacchi cibernetici e soluzioni per combattere la guerra ibrida*, https://www.cybersecurity360.it, 5 maggio 2022.