Università
di Genova

DIPARTIMENTO DI SCIENZE POLITICHE
E INTERNAZIONALI

Corso di Laurea Magistrale in: Security and International Relations

CYBER ARMI: rivoluzione o semplice innovazione?

SECURITY STUDIES: FROM TERRORISM TO PEACEKEEPING

Relatore

Prof. Fabrizio Coticchia

firma del Relatore:

Candidato

Manuel Arbasetti

firma del Candidato:

Arbasetti Manuel

ANNO ACCADEMICO 2021/2022

INDICE

INTRODUZIONE

Lungo tutto il corso della sua storia, l'umanità ha visto i conflitti evolversi, sia in termini di portata e capacità distruttiva che in termini della tecnologia affiancata agli eserciti tradizionali.

La storia bellica mondiale è stata caratterizzata, fino alla fine della Seconda Guerra mondiale, da una tipologia di guerra diventata nel corso del tempo una sorta di paradigma: un'attività estremamente visibile, grandi masse di persone, mezzi e infrastrutture mobilitate con l'annichilimento dell'avversario come unico obiettivo.

Così come avviene spesso in ambiti "civili", ad esempio con la creazione di Internet, anche in ambito militare alcune innovazioni tecnologiche non solo aggiungono o modificano il potenziale distruttivo di un paese piuttosto che un altro, ma alterano la stessa idea di conduzione di un conflitto per come era stata formulata fino a quel momento.

Nel periodo recente, l'innovazione tecnologica che più si avvicina a questa caratterizzazione in chiave "evolutiva" della guerra non si riferisce tanto ad una specifica arma, quanto alla possibilità di sfruttare le opportunità di azione fornite dal dominio cyber.

Vero e proprio "ambiente artificiale" essendo interamente stato creato dalla mano dell'uomo, il cosiddetto "dominio cyber" rappresenta l'ultima frontiera della conduzione bellica, ereditando il ruolo dominante in questo ambito precedentemente rivestito da terra, mare, aria e spazio extra-atmosferico[1].

In un mondo caratterizzato da una società globale sempre più interconnessa e dipendente dalle risorse informatiche in molteplici aspetti della vita di tutti i giorni (che sia economico-sociale, politico o militare) ciò che costituisce un'ottima opportunità per una maggiore comprensione reciproca, oltre ad una maggiore efficienza nelle comunicazioni, può rappresentare simultaneamente una fonte quasi inesauribile di nuove minacce in costante evoluzione.

Questa prospettiva introduce, tra gli attori governativi aventi responsabilità di decision-making, un quesito fondamentale e complicato, ovvero se privilegiare la maggiore rendita concessa dall'innovazione tecnologica o la sicurezza dei propri dati ed infrastrutture strategiche ponendo un freno allo sviluppo.

Dopo aver analizzato le conseguenze di questo "trade-off" la prima domanda che viene spontaneo porsi è sicuramente se ciò renda i Paesi più sviluppati e tecnologicamente avanzati, fino ad ora avvantaggiati dalla loro condizione di superiorità tecnologica, automaticamente più vulnerabili e suscettibili al giorno d'oggi agli effetti nocivi degli attacchi realizzati da attori extra-statali facenti uso del dominio cyber.

La sola esistenza dell'eventualità di utilizzare l'arma cyber in un'operazione militare rende necessaria una riformulazione della quantità e letalità di forza da utilizzare: è possibile pensare di condurre una

[1] https://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf

guerra utilizzando solamente questo nuovo medium o risulterà limitato nella sua efficacia operativa ad un ruolo di supporto, rendendo necessaria una congiunzione con strategie belliche più tradizionali?

La necessità di fornire una risposa chiara e condivisa a questa domanda ha diviso e divide ancora oggi sia il mondo accademico che gli esperti del settore e gli addetti ai lavori, tra chi sostiene la portata rivoluzionaria del dominio cyber in ottica bellica e chi invece lo considera semplicemente la più recente innovazione nell'infinito processo di rinnovamento della guerra.

La carenza di una definizione universale adottata all'unanimità all'interno del mondo accademico di settore non costituisce l'unico problema concettuale relativo a quest'area di indagine: un esempio emblematico di questa situazione è la dichiarazione di Michael Hayden, ex direttore della CIA e dell'NSA, in cui sostiene che "raramente un argomento di tale importanza è stato tanto dibattuto con così poca chiarezza e con altrettanta minore comprensione apparente del fenomeno stesso"[2].

Tra le righe di questa affermazione è possibile individuare il principale problema presente all'interno della narrativa relativa alla cosiddetta "guerra cibernetica": l'assenza di una chiara e dettagliata literature sul tema che possa fornire un'ossatura concettuale di base, indispensabile per individuarne la collocazione in termini semantici.

Questa tesi si pone l'obiettivo di fornire un contributo a questo complicato dibattito, sia da un punto di vista più teorico che da uno relativo all'utilizzo pratico di questo medium innovativo.

A tal proposito questa introduzione viene dedicata alla comparazione delle definizioni di "arma cyber" più condivise all'interno del mondo accademico e di settore, avvalendosi sia di paper autorevoli pubblicati sul tema che di dichiarazioni degli addetti ai lavori per tentare di tracciare un quadro che renda possibile l'individuazione di caratteristiche comuni.

Il primo capitolo ha invece come obiettivo principale l'analisi dei casi concreti più celebri di utilizzo dell'arma cyber, o quantomeno di quegli eventi dei quali possediamo informazioni adeguate ed esaustive: a tale scopo, viene preso ad esempio il caso Stuxnet, considerato universalmente come prima eventualità di utilizzo di un'arma cyber che abbia causato effetti concreti nel mondo reale.

Per rendere l'analisi il più possibile contemporanea e aggiornata, viene inoltre portato ad esempio l'elevato numero di cyber attacchi attuati dalla Federazione Russa ai danni degli Stati confinanti, tra i quali sono annoverate l'Ucraina e le Repubbliche Baltiche.

Il secondo capitolo è dedicato alle modalità con le quali gli Stati reagiscono e reagiranno nel prossimo futuro alla crescente importanza del dominio cyber e di tutte le opportunità e le minacce che ne derivano, con un focus particolare sul caso dell'Italia e sulla sua policy sul tema.

L'Italia si è infatti attivata per restare al passo con i propri alleati sia all'interno dell'UE che nell'ambito più ampio e strettamente attinente alla sfera della sicurezza dovuto alla sua presenza all'interno dell'Alleanza Atlantica.

La conclusione fornisce una possibilità per tentare di individuare gli scenari futuri più probabili e il ruolo che il dominio cyber potrà rivestire nelle relazioni tra gli Stati oltre a cercare di individuare, tramite l'analisi sopracitata, l'entità della portata evolutiva delle armi cyber.

[2] https://www.sicurezzanazionale.gov.it/sisr.nsf/letture/la-guerra-cyber-non-avra-luogo.html

Una delle caratteristiche principali che rendono problematica l'elaborazione di una definizione unica di cyberspazio, oltre che di adeguate policy per regolamentarne l'uso, è senza dubbio la natura ibrida e difficilmente inquadrabile di questo "mondo".

Su questo punto risulta illuminante il quadro delineato da Martin C. Libicki[3], il quale individua la principale peculiarità del cyberspazio rispetto ai domini più "tradizionali" (ovvero terra, aria, acqua e spazio extra-atmosferico) nella sua componente "intangibile".

Con ciò egli intende sottolineare come il dominio cyber sia estremamente complicato e prosegue nella sua analisi elencando i tre "livelli" costitutivi che lo caratterizzano: il livello fisico, sintattico e semantico[4].

Il livello fisico è riferito alle componenti tangibili e "materiali" del dominio cyber, vitali in ogni caso per il suo funzionamento, quali cavi a fibra ottica, satelliti, router e antenne: questo è il tratto distintivo che mantiene connesso il dominio cyber con il mondo reale ed è l'unica parte di esso che può essere bersaglio da parte di attacchi cinetici tradizionali.

Il livello sintattico segna il passaggio alla componente cyber propriamente detta, separata dal mondo fisico e composta dal collegamento tra gli sviluppatori e gli utenti e il mondo informatico, nello specifico le informazioni fornite dalle categorie di persone sopracitate agli strumenti informatici e in base alle quali questi stessi strumenti dipendono per svolgere le loro mansioni.

Libicki pone questo livello in una posizione gerarchicamente superiore rispetto al livello fisico, considerandolo come l'inizio vero e proprio del dominio cyber in quanto tale, soprattutto se ci si riferisce alla sua natura peculiare rispetto ai domini tradizionali: ciò però significa che quello sintattico è il primo livello vulnerabile, se non ad attacchi cinetici, all'intrusione di attori esterni al sistema desiderosi di trarre vantaggio da azioni malevole condotte attraverso strumenti informatici.

Il terzo livello, definito "livello semantico", si riferisce all'aggregazione dei dati e delle informazioni raccolte dagli strumenti informatici e alla loro analisi e/o sfruttamento.

Analizzando la concezione di "dominio cyber" che deriva dalla congiunzione di questi tre livelli si può evincere come il dominio cyber possa apparire come ristretto nelle sue modalità d'uso e nella sua portata innovativa al solo ambito "civile" ma, come tutte le invenzioni in generale, esso può essere piegato e sfruttato per operazioni maggiormente attinenti alla sfera militare-bellica.

Questa possibilità era stata paventata nel 2001 tra le righe del Quadrennial Defense Review Report (QDR), pubblicato dal Dipartimento della Difesa degli Stati Uniti: all'interno di questo documento veniva già evidenziato come la rapida ed esponenziale evoluzione tecnologica, unita alla necessità sempre più pressante di unificare a livello organizzativo le varie branche delle Forze Armate avvalendosi del dominio cyber, ponesse in essere per questo strumento la possibilità di costituire un potenziale pericolo per la sicurezza nazionale.

---

[3] Tra i maggiori esperti accademici americani in termini di cybersicurezza, Libicki è ad oggi Professore alla Frederick S. Pardee RAND Graduate School, oltre ad aver già lavorato per 12 anni alla National Defense University.

Egli ricopre inoltre la cattedra di "Maryellen and Richard L. Keiser Distinguished Visiting Professor in Cyber Security Studies" alla U.S. Naval Academy.

[4] "Cyberdeterrence and Cyberwar", Martin C. Libicki, RAND Corporation, 2009.

Il carattere pervasivo del dominio cyber, capace di abbracciare potenzialmente ogni settore della vita di tutti i giorni, in congiunzione con le nuove modalità di esercizio del potere rese disponibili da esso, contribuiscono alla formazione di un nuovo "centro di gravità clausewitziano"[5], data la possibilità di raggiungere qualsiasi bersaglio senza per forza limitarsi al settore militare.

Come sostenuto dal Generale Pietro Serino[6], l'arma cyber apre tutta una serie di scenari in cui la forza letale non sia più necessaria per ottenere il risultato desiderato da una particolare situazione.

Nello specifico, il Generale porta l'esempio di una recente esercitazione condotta dalle Forze Armate italiane durante la quale i loro specialisti "hanno paralizzato un'autoblindo Centauro senza sparare un colpo: con un virus informatico hanno bloccato il computer che controlla il motore"[7].

Nonostante queste variazioni nelle possibilità di azione, è di fondamentale importanza stabilire chiaramente una definizione di cosa sia un attacco cyber: necessita di caratteristiche specifiche per essere definito tale o qualsiasi azione malevola commessa tramite ausilio informatico rientra nella categoria?

A tal proposito risulta importante il saggio "Cyber War Will Not Take Place" dell'autore Thomas Rid (2012): al suo interno, egli ribadisce già dalle prime righe la decisione di utilizzare la definizione di atto di guerra "classica", formulata da von Clausewitz, come atto di forza per verificare l'appartenenza o meno dell'attacco cyber al suo interno.

L'autore diffida dell'uso massiccio di termini altisonanti quali "cyber war" e "cyber space", nonostante vengano largamente utilizzati specialmente nel mondo dell'informazione e persino in alcuni think tank di settore.

Egli è particolarmente scettico verso la concezione che vede la cyber war come una evoluzione inevitabile della conduzione della guerra, non a livello dei singoli Stati ma generalizzata, la quale avrebbe come culmine quella che viene definita una "cyber Hiroshima".

Secondo la sua interpretazione una vera e propria cyber war non è un'eventualità da temere in futuro, dato che tutti gli esempi di attacco informatico di cui si ha notizia e/o documentazione si presentano come evoluzione di attività belliche "arcaiche" quali sovversione, spionaggio e sabotaggio[8].

Ciò non significa che per l'autore il cyberspazio sia un luogo privo di pericoli, tutto il contrario: tuttavia queste minacce non qualificano l'insorgere di un nuovo tipo di guerra né un possibile "nuovo" 11 settembre (spesso portato come simbolo di una sorta di situazione di vantaggio degli attori non-statali o meno "interconnessi" alla rete globale).

L'autore in seguito specifica perché, secondo la sua analisi, gli attacchi cyber non rientrano nella concezione classica di atto di guerra: secondo von Clausewitz "il prerequisito per la guerra è

[5] https://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf

[6] https://www.repubblica.it/cronaca/2021/11/10/news/le_armi_cyber_cambieranno_la_guerra_l_esercito_ha_bisogno_di_nuovi_tecnici-325703400/

[7] https://www.repubblica.it/cronaca/2021/11/10/news/le_armi_cyber_cambieranno_la_guerra_l_esercito_ha_bisogno_di_nuovi_tecnici-325703400/

[8] https://www.sicurezzanazionale.gov.it/sisr.nsf/letture/la-guerra-cyber-non-avra-luogo.html

rappresentato da un atto di forza".

Questa definizione lega in maniera inscindibile guerra e violenza: in tal senso, Thomas Rid pone l'accento sulla totale assenza di violenza su esseri umani nella storia, per quanto recente, degli attacchi cyber.

Persino Stuxnet[9], il worm usato per attaccare l'impianto di arricchimento dell'uranio di Natanz, nonostante venga giustamente tenuto in considerazione tra gli attacchi cyber più "imponenti", non ha provocato alcuna vittima.

Come prima e fondamentale tappa della sua disamina, Thomas Rid fornisce una personale definizione di cyber arma, indispensabile per comprenderne la natura peculiare: "un comando/codice informatico che viene utilizzato, o concepito per essere utilizzato, allo scopo di minacciare o provocare danno fisico, funzionale o mentale a strutture, sistemi o esseri viventi".

Questa definizione può essere considerata come cardine fondamentale per comprendere la concezione dell'autore sulla classificazione di un attacco cyber come attacco armato, attuando una eventuale manifestazione di diritto di autodifesa da parte della nazione colpita.

Seguendo quanto ribadito precedentemente infatti, l'autore divide distintamente, sia a livello concettuale che relativamente alle conseguenze più pratiche, due tipologie di utilizzo dell'arma cyber: spionaggio e sabotaggio.

Con il termine "spionaggio" viene indicata l'intrusione e il pianificato furto di informazioni dall'infrastruttura cyber del bersaglio: secondo Rid, contrariamente al sabotaggio che causa una sorta di danno "fisico", avendo come obiettivo l'interruzione dell'attività di un sistema, lo spionaggio non qualificherebbe come "violenza e strumento a intento politico"[10].

Trattando uno specifico tipo di cyber arma, ovvero il malware, egli sostiene che, consistendo in un esempio di spionaggio da remoto, non può essere considerato un'arma in sé e per sé.

Il culmine di questa riflessione e classificazione consiste nel cosiddetto "danger paradox", ovvero nella doppia natura dello spionaggio cyber.

Esso viene infatti considerato a livello internazionale come una grave minaccia perfino per gli stati più solidi militarmente ed economicamente ma, allo stesso tempo, non risulta ascrivibile come arma, atto di guerra e/o attacco armato.

Rimanendo nel tema dello spionaggio cyber, anche Thomas Rid pone l'accento sul fatto che, nell'ambito in questione, la stragrande maggioranza degli episodi di utilizzo di questo strumento con fini politici sia avvenuta ad opera di attivisti e/o individui non appartenenti all'apparato di uno Stato che, dietro mandato di realtà governative o di altre "cause", hanno reso disponibile la loro expertise tecnica.

[9] Stuxnet è il nome assegnato al worm utilizzato per sabotare l'impianto per l'arricchimento dell'uranio iraniano di Natanz, la cui azione venne scoperta nel 2010 dopo aver già portato a compimento gran parte della propria azione nociva.

[10] https://www.sicurezzanazionale.gov.it/sisr.nsf/letture/la-guerra-cyber-non-avra-luogo.html

Conclusa la discussione sull'inquadratura dello spionaggio cyber nella teoria militare, l'autore analizza come questa tipologia di utilizzo presenti alcune importanti criticità, come la difficoltà nel quantificare la reale entità dei danni inflitti al bersaglio.

Il problema principale risiede nelle risorse umane e nelle skill tecniche indispensabili, una volta che le informazioni designate sono state ottenute, per decifrare/processare e far fruttare il vantaggio ottenuto.

A questa capacità Rid dà il nome di conoscenza tacita e identifica il suo obiettivo nel trasferimento delle informazioni al di fuori del dominio virtuale passando nel mondo reale, specificando inoltre: "data can be downloaded, but not experience and skills and hunches, all of which are crucial in order to understand complex processes as well as complex decisions".

Dopo aver definito e collocato concettualmente le due categorie di utilizzo dell'ausilio cyber come sabotaggio e spionaggio, l'autore continua la sua analisi con la terza tipologia di operazione, l'attacco informatico a scopo sovversivo.

Nello specifico, Rid pone una critica alla visione di questo medium come un totale rifacimento nella diffusione/organizzazione di rivolte, individuandone i pregi ma soprattutto i limiti: risulta infatti evidente come, sotto un certo punto di vista, il dominio cyber abbia incentivato e facilitato l'azione di movimenti sovversivi, giocando un ruolo importante, ad esempio, durante le primavere arabe.

Ciononostante, la relativa facilità di utilizzo di questo strumento e il graduale aumento del suo impiego nell'azione sovversiva hanno causato una consistente diminuzione nell'efficacia operativa, più dettagliatamente una dispersione dei soggetti coinvolti e di conseguenza una erosione nell'unità/disciplina della catena di comando, cardine di una qualsiasi operazione complessa e pervasiva come può essere l'organizzazione di una rivoluzione.

Un problema frequentemente portato alla luce nella maggioranza delle analisi relative al dominio cyber è l'attribuzione, ovvero la comprensione comprovata della provenienza dell'attacco, da un punto di vista geografico ma anche e soprattutto relativo al mandante dell'attacco.

Quest'ultimo punto in particolare risulta essere di fondamentale importanza per i decision-maker governativi: senza una chiara idea sulla responsabilità di un attacco cyber, la probabilità di riuscire ad individuare e portare avanti una policy di cybersicurezza efficace si complica esponenzialmente.

Nonostante il sopracitato problema dell'attribuzione complichi non poco gli sforzi di difesa e contrattacco da parte degli attori statali, la portata rivoluzionaria dell'uso del dominio cyber in un contesto bellico deve venire a patti con alcune complicazioni.

Sin dai primi momenti della sua creazione, Internet e il mondo cyber in generale hanno avuto come core concept una maggiore interconnessione tra persone ma soprattutto tra dispositivi: in un contesto del genere, l'uso malevolo del dominio cyber viene complicato dal fatto che il cyber spazio non è composto da compartimenti stagni, essendo al contrario caratterizzato da una diffusa pervasività e dall'assenza di concreti confini fisici.

Dovendo operare in un contesto simile, l'impiego delle cyber armi risulta esposto ad un importante problema relativo alla gestione di questi stessi attacchi, che potrebbero essere soggetti a "spillover" della loro azione all'interno di reti e/o dispositivi non intesi come bersaglio, ad esempio appartenenti ad altri Stati, con la probabilità di una ulteriore e non desiderata escalation del conflitto.

Risulta altresì poco probabile una capillare diffusione e impiego delle cyber armi da parte di attori non statali quali organizzazioni terroristiche, per molteplici motivi: programmare un attacco tramite l'uso di un'arma di questo tipo, facendo in modo che colpisca solamente un obiettivo specifico e che segua tutta la sua programmazione senza intoppi dovuti a bug o circostanze sfavorevoli, richiede capacità e risorse che questi attori non statali spesso non possiedono.

Come ampiamento dimostrato dallo stesso caso Stuxnet, la creazione di un arma cyber richiede ingenti risorse, un servizio di intelligence altamente efficiente che fornisca informazioni specifiche e dettagliate sul bersaglio dell'attacco e un know-how consolidato, di cui le organizzazioni non statali sono dotate molto raramente.

In un articolo sul tema scritto per l'Istituto Italiano di Studi Strategici "Nicolò Machiavelli", il dottor Stefano Mele prova a fornire una lista il più possibile esaustiva delle caratteristiche cardine che devono essere presenti in una cyber arma per essere propriamente definita come tale:

- un obiettivo specifico, implicando che "l'apparecchiatura, il dispositivo ovvero qualsiasi insieme di istruzioni informatiche" non abbia come target la diffusione generica ovunque

- la qualifica, per l'obiettivo dell'attacco, di "infrastruttura critica"

- un chiaro intento malevolo e di penetrazione attiva dei sistemi bersaglio, escludendo un semplice "disservizio"

- oltre ad essere identificato come "infrastruttura critica", il bersaglio deve anche essere dotato di adeguate misure protettive

- l'azione nociva deve causare danni concreti, tangibili o "significativamente rilevabili".

Un altro fattore che mina la possibilità per gli attori non statali di utilizzare il dominio cyber per incrementare la loro capacità offensiva riguarda paradossalmente l'incremento generale a livello internazionale dell'utilizzo delle cyber armi stesse: durante il solo 2021 si è verificato un aumento del 68% nel numero degli attacchi tramite cyber armi[11].

La conseguenza più immediata e facilmente intuibile di un tale aumento è la crescita repentina ed esponenziale degli investimenti destinati, da parte di governi ed attori privati in egual misura, nella dotazione di propri servizi di cyber security, oltre che per il loro ammodernamento, per poter essere il più possibile in grado di contrastare ulteriori attacchi.

Questo sviluppo contribuisce ad aumentare drasticamente la difficoltà nella progettazione di cyber armi in grado di penetrare e infettare server e dispositivi sempre più sorvegliati e dotati di protezioni/firewall sempre più ostici da superare.

Nonostante sia avvenuto prima, il caso Stuxnet fornisce già un chiaro esempio di questa complicatezza operativa: il worm in sé era molto sofisticato ma la riuscita dell'operazione è dipesa da fattori estranei alle specifiche tecniche, ovvero la riuscita nell'introduzione del worm nella rete dell'impianto di Natanz tramite dispositivo USB infetto.

Queste variabili esulano dal lato tecnico, che sarebbe già sufficiente per estromettere in larga parte le organizzazioni terroristiche da un ruolo di primo piano, essendo inoltre difficilmente controllabili da

[11] https://aspeniaonline.it/lelemento-cyber-nella-guerra-russo-ucraina/

parte di mandanti di un attacco cyber: la mancanza di controllo aumenta nel caso di attori non statali, che non dispongono né dell'intelligence né degli agenti infiltrati necessari per una azione simile al caso Stuxnet per introdurre uno strumento cyber nel dispositivo bersaglio.

Secondo Alessandro Curioni, autore insieme ad Aldo Giannuli del volume "Cyber War. La guerra prossima ventura", per poter essere definito tale un atto di guerra cyber deve produrre effetti concreti e danni diretti nel mondo reale.

L'autore fornisce anche un esempio concreto: "se un malware altera il funzionamento del sistema di controllo dei voli e un aereo precipita si potrebbe parlare di un atto di guerra cyber, se un malware blocca un server di posta elettronica direi di no"[12].

Un concetto su cui l'autore vuole mantenere l'attenzione è il fatto che, ad oggi, non si possa ancora parlare di conflitti condotti esclusivamente tramite strumenti cyber, ma ciò non ne sminuisce la portata innovativa.

Questi strumenti sono infatti stati protagonisti di molte operazioni, condotte parallelamente all'impiego di strategie "convenzionali" e nell'ambito di azioni di sabotaggio.

L'autore fornisce un esempio per ciascuna di queste due situazioni: nell'ambito di supporto ad operazioni cinetiche tradizionali viene citato il caso di attacchi hacker ai danni di infrastrutture energetiche ucraine attribuiti alla Russia.

Per quanto concerne invece l'uso di cyber armi per operazioni di sabotaggio, l'esempio citato dall'autore costituisce l'unico caso di operazione cyber di cui si abbia una documentazione sufficiente: il sabotaggio dell'impianto per arricchimento dell'uranio di Natanz, in Iran, probabilmente da parte dei servizi segreti statunitensi e israeliani attraverso il worm Stuxnet.

Ma, al momento attuale, non esiste una definizione strettamente univoca e universalmente accettata di "attacco cyber": ne fornisce una particolarmente dettagliata Saverio Setti, capitano RN dell'Esercito e competente nel contesto di electronic warfare.

Secondo il Capitano Setti, un attacco cyber "consiste in una azione attuata per mezzo di una rete di computer al fine di disarticolare, distruggere, degradare o impedire l'accesso a computer e reti, ovvero alle informazioni ivi contenute"[13].

In un'ottica concettuale, questa definizione pone l'attacco cyber in antitesi più che in similitudine con l'idea precedente di guerra elettronica (condotta, ad esempio, con l'ausilio di armamenti EMP) volta all'eliminazione fisica del bersaglio designato.

Infatti, lo scopo dell'attacco cyber non è univoco, dipende in larga parte dal bersaglio scelto e dall'obiettivo dell'operazione, avvalendosi di un algoritmo codificato da un computer a cui è deputata l'attivazione dell'effetto desiderato.

[12] https://luz.it/spns_article/curioni-giannuli-intervista-cyberwar/

[13] https://www.repubblica.it/cronaca/2021/11/10/news/le_armi_cyber_cambieranno_la_guerra_l_esercito_ha_bisogno_di_nuovi_tecnici-325703400/

L’attacco cyber può essere condotto in una varietà di scelta abbastanza ampia: gli esempi più utilizzati sono tramite malware e/o DDoS.

Una differenza sostanziale tra le due tipologie risiede nello scopo e negli effetti sul bersaglio designato: l’impiego di un malware corrisponde solitamente ad operazioni più “ambiziose”, dato che nella maggioranza dei casi la natura dell’operazione stessa è la diffusione di danni molteplici e ad ampio spettro quali possono essere l’ingresso occultato in reti chiuse, la sottrazione di informazioni e/o alterare il funzionamento delle reti nemiche.

L’attacco DDoS, pur essendo meno articolato e sofisticato del malware, mantiene una ragguardevole efficacia operativa, puntando non tanto a far ottenere qualcosa da una rete (come dati e informazioni) quanto piuttosto ad inficiare/intaccare la relazione server-client.

Nella macroarea dei conflitti e dell’uso della forza, la portata, a livello di importanza strategica, del dominio cyber risulta un argomento particolarmente delicato e spinoso, oltre ad essere controverso e spesso citato da attori differenti in forme spesso contrastanti, contribuendo ad una diffusa confusione concettuale.

A conferma di ciò, nonostante spesso vi siano punti in comune tra diverse definizioni, al giorno d’oggi siamo ancora ben lontani dalla stesura di una concezione comune sull’argomento tra gli addetti del settore.

Questa indecisione implica una difficoltà sensibilmente maggiorata nella stesura di policy comuni tra gli Stati per fronteggiare un’ipotetica minaccia cyber (in particolare da parte di attori non-statali), favorendo indirettamente la scuola di pensiero che propugna la pericolosità estrema di questa nuova tipologia di strumento bellico.

Nel corso dell’analisi svolta nelle righe precedenti sono stati analizzati diversi esempi di utilizzo delle cyber armi, ciascuno avente obiettivi e modalità specifiche.

Nonostante la già citata mancanza di una classificazione univoca, generalmente queste diverse categorie vengono riconosciute come autonome l’una dall’altra: in caso contrario, se venissero tutte accorpate in un unico insieme si vedrebbe comprovata la scuola di pensiero che sostiene la necessità di uno stretto controllo sul cyberspazio nella sua interezza, per evitarne qualsiasi possibile uso illecito.

Questa situazione è strettamente collegata anche alla cosiddetta “cultura cyber” posseduta dalla popolazione di ogni Paese: l’assenza, o più che altro lo scarso approfondimento e aggiornamento della consapevolezza da parte del cittadino medio del dominio cyber, oltre che della comprensione dei suoi meccanismi/strumenti di base, costituisce un importante aiuto indiretto ai perpetuatori di attacchi di questa tipologia.

Per questo motivo è più che mai richiesto l’inserimento di meccanismi, atti alla diffusione capillare di conoscenza su questo nuovo ma importante medium a livello globale, all’interno delle policy dedicate da parte dei principali decision-maker governativi.

CAPITOLO I

Stuxnet e il conflitto Russo-ucraino, due casi a confronto

I.1 Stuxnet e la sua portata innovativa

Al fine di fornire alcuni casi studio concreti relativi agli usi e modalità di impiego delle cyber armi verranno ora analizzati i casi contemporanei più celebri e di cui possediamo informazioni sufficienti: il worm Stuxnet e i ripetuti e costanti attacchi hacker subiti dall'Ucraina nel periodo successivo all'invasione russa della Crimea.

Il cosiddetto "caso Stuxnet" è tutt'ora considerato come archetipo dell'impiego malevolo delle opportunità fornite dal dominio cyber, sia da parte dell'opinione pubblica che da parte degli addetti del settore.

In particolare, l'utilizzo di questo specifico strumento cyber, nell'ambito dell'operazione Olympic Games, costituì un vero e proprio spartiacque: la sua esistenza mostrò al mondo la prova della possibilità concreta di danneggiare quella che viene definita una "infrastruttura critica" di uno Stato attraverso il medium informatico[14].

Tecnicamente parlando, Stuxnet appartiene all'insieme dei "worm", ovvero "una tipologia di malware in grado di autoreplicarsi, e fa parte della categoria degli Advanced Persistent Threat (APT)"[15].

L'obiettivo del worm in questione era l'impianto nucleare di Natanz, in Iran: nell'ambito del programma nucleare iraniano (da sempre dipinto come pacifico, ma senza prove certe di questa sua natura) questo impianto rivestiva e riveste tutt'ora un ruolo di primo piano, essendo deputato al trattamento dell'esafluoro allo stato gassoso, necessario per l'arricchimento dell'uranio (ovvero la separazione dell'isotopo U-235 dall'U-23)[16].

Questo impianto riveste particolare importanza anche nella concezione dello stesso programma iraniano da parte della comunità internazionale, dato che l'arricchimento dell'uranio costituisce una fase importante nell'utilizzo dell'energia nucleare sia per fini pacifici che per la costruzione di ordigni, ragion per cui è sempre stato osteggiato da altri attori quali gli Stati Uniti.

Tornando al worm, la prima variante fece la sua apparizione nel 2009, ma il vero e proprio "Stuxnet" venne scoperto solamente durante il giugno dell'anno dopo, quando fu individuato da VirusBlokAda[17], una società di sicurezza informatica con sede in Bielorussia.

L'opinione unanime elaborata in seguito a disamina da parte degli esperti di settore, sia all'interno di aziende che di agenzie governative, conferma questa caratteristica, quantificando la durata del processo

[14] https://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf

[15] https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/dal-caso-stuxnet-allanalisi-del-panorama-cibernetico-italiano/

[16] https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/dal-caso-stuxnet-allanalisi-del-panorama-cibernetico-italiano/

[17] L'avviso diffuso da questa ditta fu seguito da un comunicato diramato dal colosso tedesco Siemens, nel quale avvertiva i propri clienti che i loro sistemi SCADA (controllo di supervisione e acquisizione dati) erano suscettibili all'azione malevola del worm.

di creazione del worm tra i sei e i dodici mesi, ponendo inoltre l'accento sulla necessità, per la sua riuscita, di personale multidisciplinare altamente specializzato[18].

Stuxnet era stato accuratamente progettato per agire in maniera completamente autonoma verso il completamento della missione assegnatagli, senza la necessità dell'azione correttiva di un operatore, nell'ottica di rendere il più possibile complicato risalire allo sviluppatore del worm.

La portata innovativa di questo caso studio non si ferma solo alla capacità di aver causato danni tangibili e sotto gli occhi di tutti ma anche nel fatto di costituire, a tutti gli effetti, la prima volta in cui un attacco condotto attraverso il dominio cyber acquisiva portata internazionale ed usciva dai confini dello Stato di origine: ciò ha portato i media a definirlo, negli articoli usciti in quel periodo, "the cyber equivalent of the dropping of the atom bomb" e/o "a new era of warfare"[19], nonostante l'assenza di perdite in termini di vite umane.

Oltre ad essere indicato come una sorta di "araldo" di un totale rinnovamento nelle modalità di conduzione bellica, o più nello specifico di una "Revolution in Military Affairs"[20], Stuxnet è servito come apripista per la stesura dei concetti portati a difesa di questa teoria della portata rivoluzionaria del dominio cyber.

Per analizzare questi tre concetti risulta molto utile il paper scritto sul tema da Jon Lindsay, accademico ed esperto del settore, oltre ad aver servito come ufficiale nella Marina Militare statunitense, nel quale egli li elenca ed analizza nel dettaglio:

-il primo di questi concetti è la convinzione che il dominio cyber sia più vantaggioso per gli attori più deboli, donando loro quello che viene definito un "asymmetric advantage" rispetto agli attori più forti

-il secondo di questi concetti è la credenza secondo la quale la natura del dominio cyber renda più semplice ed attuabile l'offesa piuttosto che la difesa

-il terzo concetto è il cosiddetto "problema dell'attribuzione", ovvero come l'anonimità di cui generalmente gode l'attore responsabile dell'azione offensiva renda estremamente difficile la deterrenza.

Lo scopo principale del paper sopracitato è verificare la veridicità di questi tre concetti, analizzandone le proposte e confrontandole con la realtà dei fatti e la documentazione disponibile sull'accaduto.

Lindsay spiega come questa teoria, che identifica il dominio cyber come strumento rivoluzionario, abbia preso piede estensivamente, soprattutto tra gli addetti ai lavori statunitensi: egli cita in particolare le parole dell'allora Segretario alla Difesa Leon Panetta che, l'11 ottobre 2011, sostenne che "a cyber

[18] https://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf

[19] "Stuxnet and the Limits of Cyber Warfare", Jon R. Lindsay, University of California Institute on Global conflict and Cooperation, 15/01/2013.

[20] Per approfondire la teoria della "Revolution in Military Affairs" si veda "The Military Technical Revolution: A Preliminary Assessment", Andrew F. Krepinevich, Center for Strategic and Budgetary Assessments, 2 October 2002.

Inoltre si veda "The Revolution in Military Affairs, Transformation and the Defence Industry", Peter Dombrowski and Andrew L. Ross, Institute for Regional Security, Summer 2008

attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation"[21].

L'autore cita altre dichiarazioni da parte di personaggi autorevoli, sempre appartenenti al contesto statunitense, quali l'ex Presidente Barack Obama e il Direttore dell'FBI Robert S. Mueller III: tutte queste prese di posizione sul tema sono accomunate dalla medesima visione di un dominio cyber come un esempio di "game-changer" di portata globale.

Lindsay evidenzia inoltre come questo clima generale di allarmismo e sensazione di grave pericolo imminente abbia incentivato l'istituzione di nuove agenzie e meccanismi per cautelarsi contro le nuove minacce provenienti dal dominio cyber, citando in particolare l'esempio di Cina, Russia, Israele, Germania e Regno Unito[22].

In un tentativo di trovare una spiegazione per la velocità e l'estensione con le quali si è diffusa la teoria della Rivoluzione Cyber, Lindsay riflette anche sulla provenienza della literature sul tema, evidenziando come la grande maggioranza dei paper trattanti l'argomento della cybersicurezza venga dall'area della policy analysis, storicamente vicina oltre che sostenitrice della teoria nominata precedentemente.

Egli pone inoltre l'accento su come, al contrario, gli accademici più vicini al settore della cybersicurezza si siano mostrati molto spesso scettici, se non concretamente contrari, a questa visione del dominio cyber, ponendo come causa la mancanza di dati verificati ed affidabili che la sostengano.

A tal proposito viene evidenziato come, in molte delle istanze nelle quali è stato analizzato Stuxnet, si sia verificata una eccessiva concentrazione sull'effetto novità dato dalla complessità tecnologica del worm, piuttosto che sulla sua effettiva portata nociva.

La teoria della Rivoluzione Cyber, come precedentemente enunciato, sostiene l'esistenza di un vantaggio asimmetrico a beneficio degli attori più deboli, e al contempo una crescente vulnerabilità degli attori più tecnologicamente avanzati, quindi più suscettibili all'azione nociva degli attacchi cyber.

Tra gli esempi più gravi di questa ulteriore "debolezza" si cita la possibilità di disattivare la rete elettrica o di interrompere il servizio di controllo del traffico aereo: attraverso le parole di un ex-esperto dell'NSA[23], Lindsay riporta come sulla carta ciò potrebbe costituire un enorme vantaggio per la Corea del Nord, scarsamente dipendente dalla rete Internet, rispetto ad un Paese dall'alto coefficiente di connettività alla rete globale come gli Stati Uniti.

Il caso di Stuxnet, portato ad esempio da Lindsay, sembra fornire prove di una concezione opposta: sebbene la stampa e più in generale i media ne abbiano certamente ingigantito la complessità e la portata innovativa, Stuxnet resta comunque un'arma molto sofisticata se si prende come riferimento il periodo preciso della sua scoperta.

[21] Stuxnet and the Limits of Cyber Warfare", Jon R. Lindsay, University of California Institute on Global conflict and Cooperation, 15/01/2013.

[22] "Stuxnet and the Limits of Cyber Warfare", Jon R. Lindsay, University of California Institute on Global conflict and Cooperation, 15/01/2013.

[23] La National Security Agency è un'organizzazione inquadrata all'interno del Dipartimento della Difesa statunitense avente mansioni attinenti alla cybersicurezza, alla raccolta informazioni concentrandosi sia sulle possibili minacce alla sicurezza nazionale interne che esterne e lavora di concerto con CIA ed FBI.

Infatti, sia tra gli esperti di settore che tra le compagnie che si occupano di sicurezza informatica, è generalmente accettata l'idea che il worm sia il frutto dell'operato di uno Stato, data la necessità di ingenti fondi e di una sviluppata tecnologia militare.

Dopo accurate ed approfondite analisi, apparve chiaro che il worm era stato progettato e confezionato da qualcuno provvisto di grandi capacità tecniche specializzate, ingenti fondi e una profonda e capillare conoscenza del funzionamento dei vari componenti dell'impianto scelto come bersaglio.

Prendendo in considerazione queste premesse, risulta piuttosto evidente come Stuxnet rappresenti in realtà una prova contro la tesi della Rivoluzione Cyber, invece di una a favore: ideare, progettare e concretizzare un attacco cyber è infatti estremamente complesso e richiede risorse che gli attori non-statali non possiedono, siano esse di natura economica, di know-how, tecnologica e/o il possesso di sufficienti informazioni sulle infrastrutture informatiche da colpire.

Il secondo concetto, relativo alla convinzione che nel dominio cyber l'offesa sia molto più facile e praticabile della difesa, trova anch'esso scarso supporto in questo specifico caso: la conseguenza pratica dell'utilizzo del worm ebbe efficacia limitata se lo si analizza come strumento atto alla cancellazione del programma nucleare iraniano, dato che il danno che riuscì a causare contribuì "solamente" a ritardare gli sforzi iraniani, che furono comunque in grado di ripararlo in tempistiche relativamente brevi.

Nello specifico, gli sforzi iraniani relativi all'arricchimento dell'uranio vennero resi nuovamente operativi all'incirca entro un anno dalla data dell'attacco ma l'episodio di Stuxnet aveva comunque mostrato al mondo intero che la possibilità di utilizzare il dominio cyber per operazioni di natura offensiva non costituiva mera immaginazione o speculazione, ma una eventualità concreta.

L'offesa risulta più semplice della difesa all'interno del dominio cyber solamente quando si tratta di attacchi contro infrastrutture e/o programmi diventati così diffusi e comuni da costituire uno "standard" per gli utenti che ne fanno uso: l'esistenza di molti milioni di dispositivi che utilizzano tutti la stessa applicazione/sistema, come nel caso delle carte di credito o delle e-mail, consente di creare attacchi cyber non eccessivamente costosi o sofisticati che, sebbene spesso falliscano, finiscono comunque alla lunga per penetrare qualche sistema.

Ciò non corrisponde però alle casistiche contemplate all'interno della Rivoluzione Cyber: Stuxnet dimostra, infatti, come sia complicato penetrare le infrastrutture strategiche di un attore statale e riuscire a causare un quantitativo di danno sufficiente per gli obiettivi da conseguire.

In questi casi la pianificazione dell'attacco richiede mesi se non anni, sia per quanto riguarda l'elaborazione di una strategia per introdurre il file malevolo nel bersaglio che per la sua programmazione: il caso studio scelto risulta molto utile anche in questo senso.

Lindsay spiega infatti come Stuxnet sia stato sensibilmente più efficace nella sua fase di infiltrazione piuttosto che in quella di messa in pratica della sua azione malevola nel mondo fisico[24]: mentre la prima fase si basava sullo sfruttamento di componenti software e hardware relative a Windows (quindi più "standard") per moltiplicarsi ed espandersi, la seconda aveva a che fare con componenti locali

[24] "Stuxnet and the Limits of Cyber Warfare", Jon R. Lindsay, University of California Institute on Global conflict and Cooperation, 15/01/2013.

specifiche, l'incognita rappresentata dalla componente umana e i protocolli di sicurezza esclusivi dell'impianto di Natanz.

Specificatamente, il worm si attivava solamente in presenza di un certo componente presente nei software del colosso tecnologico Siemens in uso nell'impianto, ovvero WinCC (sfruttando come vettore di infezione il sistema Windows, sul quale gira questo componente).

Data la loro natura strategica, i sistemi e le infrastrutture che sfruttano questo tipo di software sono "chiusi", ovvero operano attraverso reti informatiche proprie e scollegate dalla rete Internet mondiale.

Stuxnet è stato comunque in grado di aggirare questo problema strutturale, dato che la sua principale modalità di infezione non utilizza la rete globale ma si basa su un tipo di intrusione più "analogico", ovvero attraverso l'inserimento di una chiavetta USB infetta.

Se, dopo l'inserimento e la scansione del sistema, Stuxnet individua WinCC allora esegue l'accesso tramite backdoor e contatta un server esterno per istruzioni sulla fase successiva dell'operazione: se invece il software in questione non è presente il worm cerca di replicarsi sugli altri dispositivi USB accessibili, per massimizzare la propria capacità di infezione e la probabilità di individuare WinCC.

Come ulteriore prova dalla sua natura sofisticata e attentamente progettata, Stuxnet si attiva realmente solo ed esclusivamente in presenza di condizioni precise, eseguendo una azione chirurgica di sabotaggio e arresto di processi molto specifici, minimizzando in questo modo la probabilità di essere scoperto.

Il dettaglio più sorprendente della portata innovativa del worm in questione risiede nella sua capacità di rimanere permanentemente all'interno del sistema bersaglio tramite rootkit, celandosi ai firewall e ai programmi di difesa ivi presenti ed agendo in modo da causare l'auto-danneggiamento del bersaglio.

Una volta conseguita l'individuazione del software WinCC, la fase successiva consiste nel raggiungimento e nella contaminazione dei PLC (Programmable Logic Controller) presenti nell'impianto, infettando l'applicazione "Step-7" che si occupa della loro programmazione[25].

Il controllo da parte di Stuxnet di questi strumenti ha consentito al worm di portare avanti la sua funzione nociva gradualmente e agendo completamente indisturbato, danneggiando leggermente, ma continuamente ed esponenzialmente, oltre 1000 delle 5000 turbine presenti nell'impianto di Natanz, portandole al sovraccarico.

Questo procedimento fu possibile grazie all'infezione e compromissione da parte di Stuxnet anche dei software addetti al rilevamento di malfunzionamenti delle turbine, agendo in modo da mostrare agli operatori "falsi" rapporti nei quali non vi erano dati corrispondenti ad un malfunzionamento.

Il terzo ed ultimo concetto analizzato da Lindsay sostiene la difficoltà e la scarsa credibilità di una efficace strategia di deterrenza, da parte degli attori più avanzati tecnologicamente verso gli attori deboli, dato l'anonimato concesso dal fatto di muoversi tramite il dominio cyber.

I sostenitori della teoria della Rivoluzione Cyber si concentrano sul solo fatto che Stuxnet sia stato in grado di avere un qualsivoglia effetto, senza tuttavia tenere in conto fattori considerati cruciali da

[25] https://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf

Lindsay, quali la diffusione e la gravità dei danni causati, oltre al contesto geopolitico nel quale ci si trovava ad operare nel periodo preso in esame.

Se si analizzano i danni concreti causati dal worm appare infatti evidente come, nonostante l'innegabile complessità tecnica di questo strumento, essi siano stati limitati ad un periodo abbastanza breve e ad un numero ristretto di turbine.

Relativamente al contesto geopolitico in atto, l'uso dell'arma cyber non è una scelta così facile e automatica come viene sostenuto dalla tesi della Rivoluzione Cyber: lo stesso Barack Obama successivamente ha espresso la preoccupazione che l'uso di armi cyber da parte degli Stati Uniti, se fosse stato scoperto, avrebbe potuto costituire una sorta di "giustificazione" per gli altri Stati, gruppi terroristici o anche singoli individui per eventuali attacchi di "rappresaglia"[26].

Il caso di Stuxnet ha dimostrato come, in realtà, la prospettiva di poter utilizzare il dominio cyber sia uno strumento utile per disincentivare gli Stati all'utilizzo di modalità belliche più convenzionali e dannose, esercitando una sorta di "deterrenza" da approcci troppo aggressivi: data la natura complicata e conflittuale delle relazioni interstatali nell'area mediorientale, gli Stati Uniti desideravano trovare un modo per riuscire a fermare, o quantomeno rallentare, il programma nucleare iraniano ma senza dover ricorrere all'attacco cinetico preventivato nell'approccio di Israele.

Inoltre, come descritto da Michele Perri in un articolo sul tema, la caratura "internazionale" di Stuxnet non si ferma alla sinergia tra l'intelligence statunitense ed americane, ma coinvolge in maniera radicata anche l'apporto di altri Stati terzi.

In particolare, risulta essere di importanza fondamentale, anche se subordinata rispetto al coinvolgimento degli altri due Paesi sopracitati, l'azione dei servizi segreti olandesi, specificatamente attraverso l'attività dell'agenzia Aivd, attiva specialmente nel campo dell'intelligence.

Precedentemente, il vuoto che costituiva la risposta al quesito su come avesse fatto Stuxnet a penetrare le difese dell'impianto di Natanz ed a infettarne il sistema senza essere individuato aveva costituito un grave problema per la stesura di un'efficacia strategia di difesa: il 2019 ha segnato una svolta in tal senso.

Infatti, è durante quest'anno che sono divenute di pubblico dominio le informazioni riguardo al fatto che "un ingegnere iraniano reclutato da Aivd avrebbe fornito dati critici che hanno aiutato gli sviluppatori statunitensi a indirizzare i loro codici ai sistemi di Natanz"[27].

Questa vera e propria "talpa", dopo il già citato contributo più tecnico relativo alle specifiche necessarie per la progettazione del worm, sarebbe stato essenziale anche per quanto concerne l'introduzione dello stesso all'interno della rete dell'impianto tramite dispositivo USB.

Ma l'agenzia di intelligence olandese non rappresenta l'unico intervento da parte di attori estranei al duo israeliano-statunitense: parrebbe infatti che vi sia stato l'aiuto, a vario titolo nello sviluppo di Stuxnet, da parte di servizi appartenenti a Francia, Germania e Regno Unito.

[26] "Stuxnet and the Limits of Cyber Warfare", Jon R. Lindsay, University of California Institute on Global conflict and Cooperation, 15/01/2013.

[27] Così spie olandesi (e non solo) aiutarono Usa e Israele a colpire l'Iran - Formiche.net

Dalla composizione di questo quintetto deriverebbe inoltre la scelta del nome dell'operazione, ovvero Olympic Games, un nome in codice che "richiama i 5 anelli simbolo dell'evento sportivo più famoso del mondo"[28].

Un'ulteriore eventualità possibile ma meno condivisa e diffusa nel mondo accademico e di settore è il coinvolgimento diretto della Federazione Russa: infatti, come riportato da Marie Baezner e Patrice Robin[29], data la presenza di una collaborazione tra i due Paesi nell'ambito dell'impianto nucleare di Bushehr, i ricercatori russi avevano accesso a tutti i siti nucleari su territorio iraniano.

Inoltre, la Federazione Russa avrebbe avuto sia le risorse che le capacità necessarie alla progettazione del worm Stuxnet, oltre ad un possibile movente: impedire all'Iran di sviluppare un'industria autonoma relativa all'arricchimento dell'uranio, puntando invece a mantenere la dipendenza iraniana dalle risorse russe.

La necessità di rimanere "occultati" e la difficoltà nello sviluppare correttamente il worm contribuirono, insieme alla necessità statunitense di riuscita dell'attacco cyber per evitare una risposta armata di Israele e un'opinione pubblica ostile al supporto ad operazioni cinetiche nell'area, a ritardare per molti mesi la data dell'attacco vero e proprio.

Una azione nociva eccessivamente rapida e aggressiva avrebbe infatti potuto mettere in allerta troppo velocemente la leadership iraniana o causare ulteriori danni non voluti: inoltre un qualsiasi Stato (non solo gli Stati Uniti) vedrebbe l'uso del dominio cyber come una alternativa allettante rispetto ad un attacco cinetico solo se certo della possibilità di non essere scoperto, la cosiddetta "plausible deniability"[30].

Nonostante non abbia causato danni se non ai suoi programmi bersaglio, il fatto che Stuxnet si sia diffuso in maniera incontrollata anche al di fuori dell'impianto di Natanz ha contribuito ad aumentare i sospetti sul coinvolgimento degli Stati Uniti nella sua creazione, fornendo agli investigatori molto materiale su cui lavorare: da ciò è possibile vedere come l'utilizzo delle armi cyber sia, al momento attuale, più efficace meno è sofisticato il tipo di attacco che si vuole perpetrare, dato che più un attacco è grave più sforzi saranno attuati per indagarvi.

Come si è già avuto modo di analizzare, uno dei problemi relativi all'elaborazione di politiche di contrasto agli attacchi cyber è esemplificato dal concetto di attribuzione: è infatti estremamente complicato identificare con certezza l'autore di un attacco, reso ulteriormente complesso dalla caratteristica anonimità insita nel mondo informatico.

Il caso di Stuxnet non è estraneo a questa problematica: anche se non vi è una certezza assoluta in termini di attribuzione, l'opinione più condivisa è che la paternità del worm sia da ricercarsi in uno sforzo congiunto di Israele e degli Stati Uniti, coadiuvato probabilmente dal non meglio specificato ausilio del sottobosco criminale, in particolare di provenienza russa[31].

[28] Così spie olandesi (e non solo) aiutarono Usa e Israele a colpire l'Iran - Formiche.net

[29] "Stuxnet", Marie Baezner and Patrice Robin, Center for Security Studies ETH Zurich, October 2017.

[30] "Stuxnet and the Limits of Cyber Warfare", Jon R. Lindsay, University of California Institute on Global conflict and Cooperation, 15/01/2013.

[31] https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/dal-caso-stuxnet-allanalisi-del-panorama-cibernetico-italiano/

Questa possibile collaborazione tra attori statali e mercato nero costituisce l'assioma cardine di una specifica scuola di pensiero, che individua in essa uno scambio a somma positiva (ossia vantaggioso per entrambi), all'interno del quale gli Stati sfruttano le risorse/investimenti e il know-how di attori privati, siano essi semplici ricercatori indipendenti o gruppi criminali informatici[32].

Anche da un punto di vista più "concreto", l'analisi dei casi di utilizzo delle cyber armi mostra come la maggioranza di essi sia basata su un'importante collaborazione del mondo criminale nella stesura e programmazione di tecniche/codici alla base di queste armi.

La complicatezza di progettazione, l'elevata specificità operativa e la technical expertise richiesta per lo sviluppo di una cyber arma, unita alla necessità di massimizzazione della sua azione nociva, contribuiscono a dare forza e solide fondamenta empiriche alla visione di questi strumenti come richiedenti ingenti risorse economiche, una fase di pianificazione e sviluppo lenta e dispendiosa e un team altamente specializzato.

Ciò porta inoltre a visionare questo processo di utilizzo del dominio cyber in chiave offensiva come un importante "meeting ground", che agisce da centro nevralgico di collaborazione tra gli Stati e i gruppi di cyber-criminali in un rapporto di tipo simbiotico: il primo gruppo fornisce le risorse e l'intelligence necessarie per il finanziamento e la buona resa del progetto in questione, oltre a provvedere all'infezione diretta e "analogica" del sistema bersaglio in caso di reti chiuse (come spesso si verifica in caso di infrastrutture critiche).

Il secondo gruppo invece si occupa principalmente di mettere a disposizione il know-how e la manodopera altamente specializzata necessaria per lo sviluppo e il corretto funzionamento di questo tipo di arma.

L'apporto della criminalità nel mondo del dominio cyber porta ai giorni nostri ad un progressivo rafforzamento dell'ipotesi secondo la quale questi gruppi illegali sarebbero gli interlocutori di riferimento per gli Stati che necessitano di condurre operazioni al di fuori del diritto internazionale.

Ancora più peculiare è risultato essere specificatamente il worm di Stuxnet: le informazioni disponibili sul suo sviluppo restano nebulose e portano a identificare tale processo come diviso in "compartimenti stagni".

Ogni fase sarebbe stata cioè affidata a più attori non statali completamente separati tra loro e all'oscuro dell'intento e prodotto finale, in una sorta di catena di montaggio.

Attualmente si sta assistendo alla crescita esponenziale di un mercato nero connesso alle cyber-armi sempre più florido, dato che quasi tutti questi strumenti basano la propria capacità di azione "malevola" su particolari mancanze e debolezze/falle dei sistemi operativi più diffusi, dette "zero-day", ovvero vulnerabilità che non sono ancora state scoperte e invalidate da parte delle aziende produttrici di software[33].

L'apporto innovativo derivato dalla programmazione e dall'azione del worm Stuxnet risulta fondamentale, soprattutto grazie alla sua capacità di causare danni concreti e fisici nel mondo reale

[32] https://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf

[33] https://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf

tramite il danneggiamento delle turbine dell'impianto, un avvenimento senza precedenti per il periodo di riferimento.

Questo caso costituì un precedente ma, anche se fu il primo esempio di utilizzo dell'arma cyber di cui si hanno informazioni più o meno esaustive, non fu certamente l'unico.

Negli ultimi anni l'utilizzo di attacchi condotti tramite il dominio cyber è aumentato sensibilmente e non solo attraverso i worm come Stuxnet, molto complessi e costosi da realizzare e usati come singoli attacchi, ma anche come ausilio ad operazioni di guerra "cinetica" più convenzionale.

Se si analizza il worm Stuxnet da un punto di vista di definizione, tale strumento può correttamente essere indicato come una vera e propria "cyber arma" date le specificità insite nella sua progettazione e perfezionamento: danneggia esclusivamente il sistema specifico indicato nel suo codice sorgente, attraverso specifiche zero-day vulnerabilities ed introducendosi in specifici programmi[34].

I.2 La Federazione Russa, l'Ucraina e la cyber guerriglia

Uno degli attori presenti sulla scena internazionale che più si è adoperato nel perfezionamento di questa tipologia è la Federazione Russa, nell'ottica di recupero della sua influenza del periodo sovietico.

L'esempio più attuale e di dominio pubblico attualmente riguarda i rapporti con l'Ucraina, trasformatisi progressivamente in un contesto di attrito più o meno celato segnato da attacchi cyber ricorrenti da parte della Federazione Russa contro infrastrutture di varia natura ed importanza: questo processo è culminato nella recente invasione di parte del territorio ucraino da parte dell'Esercito russo.

La natura peculiare di questo conflitto è risultata piuttosto evidente sin dalle primissime fasi dell'invasione: nello specifico è stato evidenziato il suo carattere ibrido e asimmetrico, esemplificato da una stretta collaborazione tra armamenti convenzionali, il massiccio impiego di risorse provenienti dal dominio cyber e un esteso utilizzo dell'Information Technology (particolarmente tramite disinformazione e fake-news).

Rispetto all'Ucraina, la Federazione Russa può vantare alcuni vantaggi di importanza primaria, sia dal punto di vista della capacità operativa che relativamente al proprio know-how in materia.

Più nello specifico, la Federazione Russia può schierare un "esercito" di hacker di dimensioni e capacità considerevoli, composto da individui rientranti nella fila delle forze armate russe ma anche da free-lancer e attori avulsi da ruoli statali.

Inoltre, la Federazione Russa ha avuto modo ed occasione più volte di approfondire e affinare la propria capacità in ambito cyber attraverso operazioni più o meno grandi in altre aree di interesse per il disegno geopolitico attualmente in atto.

Alcuni esempi di questa consolidata esperienza nel campo delle cyber armi si ravvisano nelle azioni intraprese, anche se con modalità e obiettivi differenti, dalla Federazione Russa contro le infrastrutture

[34] https://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf

di Estonia e Georgia tra il 2007 e il 2008[35].

L'Estonia fu il bersaglio di un attacco DDos (Distributed Denial of Service) volto a sabotare la distribuzione di servizi attinenti all'IT e al sistema bancario, causando danni consistenti e diffusi sia relativamente a strutture governative che ad aziende private.

Se l'azione contro l'Estonia può essere considerata come un attacco a sé stante, di diversa natura è stato l'attacco contro la Georgia: nello specifico, il suo utilizzo in congiunzione con una operazione bellica "tradizionale" identifica una dinamica diametralmente opposta[36].

Infatti, l'attacco cyber diretto contro la Repubblica di Georgia, svoltosi parallelamente e in concomitanza con una azione cinetica classica, permise all'esercito della Federazione Russa di azzoppare sul nascere qualsiasi possibilità di resistenza e rese molto più spedita l'occupazione e il successivo controllo del Paese.

Negli ultimi mesi questa situazione ha subito un tracollo vertiginoso, culminato nell'invasione di regioni separatiste del territorio ucraino come parte di un'operazione di guerra cinetica convenzionale: ciononostante, la degenerazione dei rapporti tra questi due paesi, in ottica di un conflitto più o meno manifesto, è iniziata nel 2015 con l'utilizzo fraudolento da parte della Federazione Russa del dominio cyber.

Ciaran Martin[37], già capo del National Cyber Security Center inglese, fornisce un quadro della condizione in Ucraina molto chiaro e calzante, ponendo l'accento su come "negli ultimi sette o otto anni, l'Ucraina ha registrato una serie di attacchi informatici mai visti in nessun altro Paese sulla Terra"[38].

Egli sottolinea una divisone netta tra la componente "scenografica" dell'azione offensiva russa contro l'ucraina, composta da esercitazioni militari massicce che simulano una vera e propria invasione via terra con annesso dislocamento di mezzi pesanti in posizione provocatoria, e una parte più nascosta e celata alla comunità internazionale.

Questa seconda componente elusiva non è per questo meno importante nel contesto conflittuale dell'area in questione: nonostante sia infatti estremamente meno visibile, ha già contribuito a causare ingenti danni, attraverso l'impiego di attacchi cyber di varia natura.

Già prima dello scoppio dell'operazione militare vera e propria, l'Ucraina era stata bersaglio di vari attacchi cyber contro le sue infrastrutture più importanti e strategiche, identificando in questi attacchi una ponderata strategia di lungo periodo volta ad indebolire la resilienza e capacità di resistenza del Paese.

---

[35] https://www.unionedirittiumani.it/newsletter/limportanza-dellarma-cyber-nel-conflitto-tra-russia-e-ucraina/

[36] https://www.unionedirittiumani.it/newsletter/limportanza-dellarma-cyber-nel-conflitto-tra-russia-e-ucraina/

[37] Oltre ad esserne stato nominato il primo Chief Executive nel febbraio 2016, Ciaran Martin fu il maggior sostenitore sin dal 2013 della necessità di creare un "National Cyber Security Centre" in seno alle agenzie addette a mansioni di intelligence e sicurezza, ponendosi tra coloro che propugnavano la tesi dell'impellente necessità di dotarsi di adeguati strumenti di difesa contro queste nuove minacce informatiche.

[38] https://www.open.online/2022/02/17/ucraina-vs-russia-guerra-informatica/

Nello specifico, dal 2015 al 2022, infrastrutture ucraine appartenenti a numerosi settori sono state colpite più volte e ad intervalli irregolari da ripetuti attacchi tramite DDoS i quali, nonostante fossero in molti casi sofisticati e ben pianificati, spesso non hanno causato danni duraturi e consistenti.

Su questa tipologia di attacchi si è espresso Justin Fier[39], analista e direttore della sezione addetta all'analisi sui flussi di attacchi cyber della società inglese di cybersicurezza Darktrace: egli, basandosi sulle informazioni raccolte dai media e provenienti dai servizi di intelligence, conferma la qualifica di DDoS di queste azioni offensive, aventi come scopo l'oscuramento di siti web/reti sovraccaricandone i server tramite elevati volumi di traffico.

Fier classifica i DDoS come una sorta di cyber attacchi di livello inferiore, sia da un punto di vista di complessità del proprio codice sorgente che di difficoltà nella loro individuazione e cancellazione, ciononostante ne riconosce la validità a livello di stupore e diffusione nell'opinione pubblica, il tutto senza essere così impattanti nella loro portata nociva da causare una reazione da parte del Paese bersaglio.

Egli, inoltre, individua un possibile secondo fine, oltre ai singoli obiettivi, dietro questi attacchi: nello specifico un ruolo di "diversivo" atto a porre l'attenzione della comunità internazionale su di questi, distogliendola da altri luoghi considerati più importanti per l'operazione russa.

In particolare, egli spiega come gli attacchi DDoS siano molto utili per dividere e indebolire le capacità dei software di sicurezza, permettendo al contempo ai responsabili degli attacchi di rimanere non visti nel sistema e di agire indisturbati nell'ottica di azioni offensive molto più dannose, quali "rubare o alterare dati sensibili, spegnere i sistemi critici, o semplicemente rimanere dormienti fino al momento più opportuno"[40].

Fier sottolinea come possano essere possibili bersagli, nel contesto di una guerriglia cyber, non soltanto infrastrutture critiche e/o strategiche, ma anche obiettivi meno ambiziosi e "importanti" quali piccole imprese e persino singoli individui.

Tra il 2015 e il 2016 alcuni attacchi cyber di provenienza russa hanno causato numerosi blackout che hanno lasciato senza energia elettrica migliaia di persone, mentre nel 2014 nell'ambito dell'annessione della Crimea alla Federazione Russa si rese necessario contare a mano le schede elettorali per le elezioni presidenziali, dopo che un attacco cyber aveva reso inagibili i sistemi informatici nazionali.

Più recentemente si è assistito ad un progressivo e costante aumento nel numero e nella portata nociva degli attacchi condotti attraverso il dominio cyber, mettendo ulteriormente a dura prova le risorse e la resistenza ucraina.

Nell'ultimo periodo, più specificatamente tra il 2021 e il 2022, le azioni della Federazione Russa condotte tramite il dominio cyber hanno subito uno sviluppo esponenziale, sia in termini di complessità che di ambizione operativa.

In particolare, nelle prime settimane del 2022 venne scoperto uno strumento molto più evoluto di quelli precedentemente utilizzati dalla Federazione Russa nell'ambito della propria politica estera, un

[39] Considerato tra gli esperti americani di punta nel settore della cybersicurezza, Fier ricopre la posizione di Director for Cyber Intelligence and Analytics per la società Darktrace, sita in Washington DC.

[40] https://www.open.online/2022/02/17/ucraina-vs-russia-guerra-informatica/

malware al quale venne assegnato il nome "WhisperGate"[41].

La scoperta di questo attacco segnò una evoluzione verso un frangente più sofisticato nell'utilizzo da parte della Federazione Russa della sua capacità relativa al dominio cyber: in particolare, la maggiore ambizione insita nella nuova strategia cyber russa risulta evidente già analizzando gli obiettivi del worm in questione, che colpì infrastrutture di qualunque tipo, governative e/o private.

Un altro punto che permette di individuare la crescente ambizione russa in questo particolare caso è la svolta, partendo proprio da WhisperGate, da una semplice volontà di inficiare o interrompere l'erogazione di servizi ad un preciso intento distruttivo rivolto a dati e strutture strategiche sul territorio ucraino.

Ulteriori analisi sulle modalità di azione di questo worm hanno rivelato una natura completamente diversa, nella programmazione e negli obiettivi, rispetto agli attacchi attuati in precedenza: lo scopo di WhisperGate è infatti strettamente paragonabile alla pratica del ransomware, che consiste nella manipolazione di dati e/o informazioni presenti in uno specifico dispositivo o nella corruzione del suo sistema operativo[42].

Dopo aver infettato strutture di varia natura e proprietà, sia governative che appartenenti ad organizzazioni no-profit, il worm ha crittografato le informazioni in esse contenute impendendone la fruizione e l'accesso completamente.

Questa azione di blocco delle informazioni ha costituito solamente la prima parte della macro-operazione di cui faceva parte WhisperGate: ad essa sono seguiti altri attacchi plurimi contro strutture governative, di proprietà delle Forze Armate e attinenti al servizio bancario.

Parallelamente è stata condotta una campagna rivolta contro la popolazione civile ucraina, condotta tramite una massiccia e capillare opera di disinformazione con SMS fasulli relativi a supposti malfunzionamenti della rete bancomat.

Tra il caso WhisperGate e il successivo utilizzo di worm nell'ambito della sua guerra ibrida, la Federazione Russa ha intervallato numerosi attacchi di portata e ambizione operativa minore tramite DDoS, nell'ottica di mantenimento di una situazione di tensione duratura in preparazione alla fase successiva della macro-operazione in Ucraina[43].

Nelle fasi immediatamente successive, l'operazione ha ripreso la sua componente più distruttiva e impattante tramite il malware "Hermetic Wiper"[44], coadiuvato da tutta una serie di micro-attacchi di supporto nuovamente tramite DDoS: in questo particolare frangente si è verificato un nuovo

[41] Identificato per la prima volta il 15 gennaio 2022 dall'azienda Microsoft, WhisperGate presenta ad una prima analisi le classiche caratteristiche del ransomware, ovvero un malware che cripta dati sensibili rendendoli nuovamente disponibili solamente dopo il pagamento di un riscatto.

[42] WhisperGate possiede però una peculiarità che contribuisce alla sua portata innovativa: come espresso da Microsoft nello stesso comunicato in cui se ne accennava la scoperta, anche se successivamente all'attacco appare un messaggio con richiesta di riscatto i dati bersaglio vengono in realtà distrutti e risultano in ogni caso irrecuperabili.

[43] https://www.unionedirittiumani.it/newsletter/limportanza-dellarma-cyber-nel-conflitto-tra-russia-e-ucraina/

[44] HermeticWiper, scoperto il 23 febbraio 2022 da esperti di cybersicurezza provenienti da più aziende SentinelLabs e Broadcom Software, causa in ultima istanza un fallimento completo del sistema infettato e identifica una sorta di continuità di progettazione con WhisperGate, essendo anch'esso un "falso ransomware".

cambiamento strategico, dato che lo scopo degli attacchi è stato modificato nel furto di dati relativi al personale militare e umanitario operante sul territorio ucraino.

Nel periodo immediatamente successivo alle azioni precedentemente citate venne scoperto dai ricercatori di ESET, un'azienda slovacca leader mondiale nel settore della digital security, un secondo malware avente come obiettivo l'eliminazione di dati importanti e sensibili presenti in dispositivi in uso in diversi settori quali sanità, energia e finanza: a questo strumento venne dato il nome di "IsaacWiper"[45].

"Hermetic Wiper" e "Isaac Wiper" sono stati in grado di causare danni ingenti e diffusi nei settori più disparati: dalla difesa alla finanza e all'informatica, che si trattasse di attori privati, enti governativi e ONG attive in queste aree.

Oltre a questi due attacchi specifici, la Federazione Russa ha enormemente diversificato la propria azione offensiva in ambito cyber, coadiuvando i due malware sopracitati ad attacchi multipli aventi come bersaglio i piani di evacuazione e i database delle varie ONG operanti sul territorio ucraino, per invalidare il più possibile l'efficacia degli aiuti umanitari.

Il 24 febbraio ha segnato la data di utilizzo della cyber arma dall'effetto più impattante e dannoso nel contesto del conflitto tra Federazione Russa e Ucraina: se infatti fino a quel momento gli attacchi russi alle infrastrutture cyber ucraine erano stati in misura variabile a sé stanti, questo ultimo esempio costituisce una congiunzione tra la guerra cinetica convenzionale e l'arma cyber, nell'ottica di una medesima grande operazione.

La paternità dell'attacco non è, ad oggi, pienamente accertata ma le indagini congiunte dei servizi americani, francesi e ucraini individuano nella Federazione Russa il principale indiziato.

L'analisi svolta da questi tre servizi ha raggiunto questo risultato basandosi sulla tempistica dell'attacco, giudicata troppo sospetta per essere una mera coincidenza, e sull'obiettivo stesso del malware, ovvero il blocco dei servizi satellitari forniti all'esercito ucraino dall'azienda Viasat, attiva nel campo delle comunicazioni oltre che appaltatrice della difesa statunitense.

L'ipotesi più accreditata vede l'uso del malware "Acid Rain"[46] per interferire con le rilevazioni satellitari dell'esercito ucraino, in un'ottica di indebolimento della sua capacità di comprendere i

[45] Identificato poche ore dopo l'inizio degli scontri sul territorio ucraino il 23 febbraio 2022, IsaacWiper portò i primi sforzi degli esperti di settore a cercare prove e/o tracce che potessero offrire delucidazioni per comprendere se si fosse di fronte ad un cosiddetto "gemello" di HermeticWiper o ad un malware a sé stante.

L'analisi effettuata da ESET ha reso evidente come vi sia una somiglianza pressocché nulla tra i due malware dato che IsaacWiper, oltre ad avere un codice completamente diverso, risulta essere molto meno sofisticato del suo predecessore, impiegando anche molto tempo a compiere la sua azione di data wiper in presenza di grandi unità di memoria.

[46] Inserito dai ricercatori Guerrero-Saade e van Amerongen all'interno di una macro-operazione volta a minare la capacità di approvvigionamento e information gathering dell'Ucraina, AcidRain aveva come scopo rendere "ciechi" i servizi di informazione ucraini tramite l'interruzione del collegamento satellitare fornito dalla società Viasat.

Svoltosi attraverso un attacco alla rete KA-SAT e rendendo inutilizzabili migliaia di modem in maggioranza su territorio ma anche in altre aree d'Europa, questo malware ha causato gravi danni alla rete satellitare ucraina ma anche a bersagli "involontari" che si avvalevano del medesimo servizio.

Un esempio che riveste particolare importanza, oltre alla sopracitata invalidazione di moltissimi modem in vari Stati, come Francia e Italia, è sicuramente il blocco di alcune turbine eoliche in Germania.

movimenti e le posizioni delle truppe russe, facilitandone il più possibile l'avanzata.

Effettivamente, questo malware è riuscito a rendere molto più caotici e complicati gli sforzi dell'esercito ucraino relativi alle comunicazioni, disturbandole tramite la distruzione e/o il danneggiamento di router e modem ma le conseguenze di questo attacco non si sono limitate al territorio ucraino.

Lo spillover dell'azione nociva del malware in questione ha coinvolto modem in tutta Europa, permanentemente compromessi per circa trentamila utenti: la situazione risulta più complicata del previsto da risolvere, dato che si potrebbe ovviare al problema solo con un ricambio di dispositivo.

Nonostante le numerose ed estese capacità cyber della Federazione Russa, la cadenza più o meno regolare degli attacchi e la costante evoluzione degli strumenti utilizzati, il dominio cyber non ha garantito quel vantaggio tattico fondamentale che ci si sarebbe aspettato nell'ambito del deterioramento delle capacità di resistenza dell'esercito ucraino.

Va però altresì detto che, come ampiamente dimostrato dal caso Stuxnet, nella grande maggioranza dei casi le reali conseguenze degli attacchi condotti tramite il dominio cyber si palesano dopo molto tempo, complici la mancanza di informazioni attendibili/verificate e la difficoltà nell'individuazione dei loro effetti.

Tralasciando questi motivi, legati più che altro alle informazioni in possesso degli analisti, vi sono altre ragioni plausibili relative alla limitata efficacia del dominio cyber precedente l'invasione dell'Ucraina ad opera della Federazione Russa: in primo luogo, è lecito pensare che l'obiettivo russo fosse una guerra "lampo", rapida e con un dispendio di risorse contenuto, basandosi su un uso moderato della forza militare convenzionale per poter poi negoziare da una posizione di vantaggio.

Una ulteriore ragione che ha contribuito a ridimensionare l'efficacia degli attacchi cyber da parte della Federazione Russa ha profonde radici storico/culturali oltre che strettamente tecnologiche: l'atavico attrito e astio tra i due Stati in questione, unito ai continui attacchi cyber subiti dall'Ucraina, ha esponenzialmente incrementato la resilienza delle infrastrutture critiche e le competenze in materia di cybersecurity dell'esercito ucraino, che è stato così in grado di contenere i danni dell'operazione russa.

Nell'ottica di una migliore difesa dalle capacità inerenti al dominio cyber della Federazione Russa, questa continua pressione ha incentivato l'ammodernamento degli strumenti atti alla difesa di infrastrutture e dati strategici, tra i quali l'allineamento alle direttive in tema di protezione dati attualmente più all'avanguardia[47].

Il contesto del conflitto russo-ucraino ha fornito un importante esempio di come il dominio cyber permetta e incentivi un ruolo crescente da parte di attori non statali, ma non come nuovo strumento nelle mani delle organizzazioni terroristiche, come paventato invece dalla tesi della Rivoluzione Cyber.

Vi è certamente stato un incremento consistente nel numero di attacchi cyber perpetrati da parte di attori non statali, ma questa categoria ha annoverato nella quasi totalità casi di singoli hacker o collettivi in appoggio ad una delle due parti del conflitto.

[47] https://aspeniaonline.it/lelemento-cyber-nella-guerra-russo-ucraina/

Nello specifico, la Federazione Russa si è avvalsa dell'ausilio fornito da parte di singoli hacker privati per ridurre al minimo la possibilità di essere scoperta e identificata, richiamando l'importanza del cosiddetto problema dell'attribuzione analizzato precedentemente: più stratificata ed identificabile è invece la congiunzione tra esercito e attori non statali da parte dell'Ucraina.

Infatti, sebbene la quasi totalità dello sforzo bellico ucraino sia gestita dalle Forze Armete, l'Ucraina ha ricevuto un supporto molto più chiaro e individuabile, mentre i legami tra Stato e privati nel caso della Federazione Russa erano caratterizzati da un approccio molto più nebuloso e celato agli occhi della comunità internazionale.

Nonostante l'Ucraina non avesse, e non abbia tutt'ora, le capacità, i mezzi, il know-how e le risorse attinenti al dominio cyber che invece possiede la Federazione Russa, la costante condizione di attrito e l'assenza di un reale intento da ambo le parti di migliorare i rapporti ha portato ad una rapida evoluzione delle capacità di cybersicurezza relativamente alle infrastrutture critiche.

L'esempio di supporto privato alla causa ucraina più recente e che ha avuto una maggiore risonanza mediatica è certamente il caso del supporto dell'organizzazione di hacker nota come "Anonymous", portato avanti tramite continui attacchi alle infrastrutture informatiche del governo russo con obiettivi quali furto e leak di dati secretati, sabotaggio e propaganda.

L'attività di questo collettivo e del gruppo "Cyber Partisans" si è concentrata su due obiettivi operativi principali, nello specifico nella contro-propaganda, diffondendo informazioni non ritoccate o nascoste dal Cremlino e rallentare/sabotare la capacità offensiva da parte delle agenzie di cyber guerriglia russe, costringendole a concentrarsi sull'autodifesa e rimuovendo risorse per ulteriori attacchi contro l'Ucraina[48].

Un altro caso, seguito da un massiccio riscontro mediatico, è stato il supporto alla causa ucraina da parte del magnate Elon Musk, che ha fornito all'esercito l'accesso al sistema satellitare Starlink sviluppato dalla sua società, data la necessità di sopperire al sabotaggio della connessione con la rete Viasat in seguito ad un attacco cyber russo[49].

Oltre alle decisioni di supporto unilaterali da parte di singoli individui, il governo ucraino ha promosso e pubblicamente incentivato la formazione di un "esercito IT informale", avente come unico requisito per entrare a farne parte il possesso delle competenze informatiche necessarie[50].

Per ovviare alle necessità logistico-organizzative questo agglomerato si avvale dell'ausilio di un gruppo sul social network Telegram, tramite il quale condividere i siti e le infrastrutture bersaglio oltre agli effetti degli attacchi andati a segno.

Alcuni attori privati, che hanno comunque espresso il loro supporto per la causa ucraina, operano in una zona più "grigia" all'interno della quale è difficile comprendere se tali attori facciano parte o meno dell'esercito informale sopracitato: un esempio su tutti è costituito dal gruppo noto come Network Battalion 65 (NB65).

[48] https://www.unionedirittiumani.it/newsletter/limportanza-dellarma-cyber-nel-conflitto-tra-russia-e-ucraina/

[49] https://aspeniaonline.it/lelemento-cyber-nella-guerra-russo-ucraina/

[50] https://www.unionedirittiumani.it/newsletter/limportanza-dellarma-cyber-nel-conflitto-tra-russia-e-ucraina/

Questo specifico gruppo si è reso protagonista di una azione che ha reso evidente una importante caratteristica dell'incremento nella diffusione degli attacchi cyber: è riuscito a condurre con successo operazioni contro infrastrutture russe rivolgendogli contro un malware "artigianale", creato a partire da un codice sorgente basato sul ransomware Conti, già utilizzato dalla stessa Federazione Russa per attacchi cyber precedenti.

Ciò contribuisce a porre l'accento su una problematica di importanza fondamentale ovvero il fatto che, già dopo la primissima situazione in cui uno strumento cyber viene usato nell'ambito di un attacco, tale strumento perda qualsiasi caratteristica o parvenza di "novità" e possa essere replicato, modificato e riutilizzato da terzi, come in questo caso.

Lo stesso caso Stuxnet è un esempio di questa eventualità, dato che al giorno d'oggi il codice sorgente del worm utilizzato nell'attacco all'impianto di Natanz può essere rintracciato nel deep web e modificato per la creazione di nuove cyber armi, dato che la vulnerabilità da esso utilizzata per agire sulle turbine non è più sconosciuta agli addetti ai lavori.

Nonostante il recente conflitto tra federazione Russa e Ucraina abbia mostrato al mondo intero come il dominio cyber, oltre ad essere un eccellente ausilio alla guerra cinetica convenzionale, possa costituire un importante mezzo di congiunzione tra pubblico e privato, ha reso altrettanto evidenti le limitazioni insite nel suo utilizzo al momento corrente.

Inoltre, lo scontro tramite attacchi cyber tra la Federazione Russa e l'Ucraina non si è limitato ai casi specifici citati in precedenza, ma prosegue parallelamente allo svolgimento del conflitto cinetico: questo sviluppo ha preso in seguito una direzione peculiare, esulando dalla semplice ripetizione di un approccio già consolidato.

Il dominio cyber ha infatti superato il confine degli Stati protagonisti diretti del conflitto, e diversi Stati estranei alle operazioni sul terreno sono divenuti bersaglio di attacchi cyber perpetrati da sostenitori di entrambi gli schieramenti: in larga parte individuabile nell'azione di attori privati vicini alla causa russa, un fattore specifico ha contribuito all'evoluzione dell'utilizzo dell'arma cyber in questo contesto: l'inclusione nel novero dei papabili bersagli di Stati "rei" di aver aiutato la causa ucraina, che sia con l'invio di armi e finanziamenti o con le sanzioni contro la Federazione Russa.

Tra questi attori statali non direttamente coinvolti nel conflitto ma rientranti nei possibili obiettivi loro malgrado per una presenza e interferenza indiretta, a vario titolo, nell'avvenimento in questione c'è anche l'Italia: essa è infatti stata oggetto di alcuni attacchi hacker nel periodo recente che, anche se non apertamente rivendicati dalla Federazione Russa, lasciano poco spazio all'indecisione sull'identità del mandante.

Recentemente è stato di conseguenza diffuso dall'Agenzia italiana per la cybersicurezza un comunicato in cui si chiede urgentemente un ammodernamento ed incremento dei programmi deputati alla difesa delle infrastrutture digitali nazionali, specificando come "sono aumentati i rischi cibernetici ai quali sono esposte le imprese italiane che intrattengono rapporti con operatori situati in territorio ucraino, derivanti da possibili danni ad obiettivi digitali di quel Paese"[51].

Infatti, uno dei tratti distintivi dell'uso del dominio cyber come arma e che richiede maggiormente attenzione, oltre ad una continua analisi, è la possibilità di oltrepassare i confini dei singoli Stati o delle

[51] https://www.open.online/2022/02/17/ucraina-vs-russia-guerra-informatica/

reti che infetta, diffondendosi così in altre infrastrutture magari nemmeno annoverate tra i bersagli dell'attacco in questione.

Le relazioni rapidamente e progressivamente deterioratesi tra l'Ucraina e la Federazione Russa hanno segnato uno spartiacque importante nella concezione e nella diffusione delle armi cyber, fotografando un incremento esponenziale nell'uso, nel numero e nella portata offensiva di questo tipo di strumenti.

Si rende necessario inoltre evidenziare come, alla luce del conflitto sopracitato, l'uso delle cyber armi contribuisca a identificare alcune problematiche e criticità: in primis, la possibilità di agire come porta d'accesso, anche se involontaria, per altri attori non direttamente coinvolti nell'azione vera e propria.

L'analista Justin Fier di Darktrace ne traccia un quadro preciso, spiegando come durante queste situazioni conflittuali altamente instabili "si crea una certa confusione e cominciano a intervenire anche gruppi criminali che non hanno niente a che fare con il conflitto"[52].

Sebbene sia molto complicato e per certi versi quasi impossibili riuscire a comprendere quali siano le reali mire di tali attori, secondo Fier "spesso l'obiettivo di questi gruppi non è politico: vogliono solo infilarsi nella polvere per mettere a segno le loro azioni. E allora anche noi possiamo diventare dei target"[53].

[52] https://www.open.online/2022/02/17/ucraina-vs-russia-guerra-informatica/

[53] https://www.open.online/2022/02/17/ucraina-vs-russia-guerra-informatica/

CAPITOLO II

Il Sistema Paese italiano

II.1 Lo stato dell'arte nel contesto italiano

Indipendentemente dal fatto che ci si trovi al giorno d'oggi in presenza di una vera e propria rivoluzione della modalità di "fare guerra" o di una delle innumerevoli innovazioni tecnologiche in ambito bellico che si sono susseguite parallelamente all'evoluzione dell'umanità, la crescente intromissione delle armi attinenti al dominio cyber nelle relazioni tra gli Stati e la loro pericolosità ha costretto questi stessi Stati a dotarsi nell'immediato di specifiche agenzie e politiche per fronteggiarne la diffusione e incrementare le proprie capacità di difesa.

Lo scopo di questo capitolo è effettuare un'analisi, il più possibile dettagliata, di tutti gli strumenti di cui si è dotata l'Italia per non farsi trovare impreparata di fronte alle sfide e alle opportunità che sono state rese disponibili dal dominio cyber, sia a livello di nuclei specializzati inquadrati all'interno delle Forze Armate che nell'ambito di specifiche agenzie governative attinenti all'IT e alla sicurezza delle infrastrutture critiche.

Nonostante non vi sia ancora a livello internazionale una chiara e dettagliata regolamentazione giuridica relativamente al dominio cyber e alle problematiche che da esso possono derivare, l'Italia può vantare un piano normativo all'avanguardia: è stata infatti tra i primi paesi orbitanti nell'UE ad intravedere la necessità impellente di dotarsi di adeguate "regole del gioco" dal punto di vista tecnico, legale e politico in quest'area.

La normativa precedente al caso Stuxnet trovava il suo fulcro nel "Codice dell'amministrazione digitale", datato 2005 e punto di riferimento per la direzione presa dalla Pubblica Amministrazione in materia di implementazione degli strumenti IT[54].

Tale normativa riveste un'importanza fondamentale come base per il quadro normativo italiano in generale in materia cyber: nello specifico il Codice si presenta come una serie di regole di condotta per lo Stato dallo Stato su come, quanto e in che misura avvalersi delle possibilità offerte dal dominio cyber per modernizzare il modus operandi della Pubblica Amministrazione.

Per poter assistere a sviluppi concreti relativi alle opportunità offensive fornite da questo strumento bisognerà aspettare il contesto internazionale successivo all'attacco cyber contro l'impianto iraniano di Natanz.

Infatti, è nel 23 gennaio del 2013 che è stato emanato il DPCM al cui interno vengono definiti gli "Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", rivestendo un ruolo cardine come apripista nella definizione e gestione degli strumenti di sicurezza informatica necessari[55].

Nel lasso di tempo compreso tra il 2013 e il 2018 è stato attuato uno sforzo massiccio e diffuso di ammodernamento e rafforzamento dei sistemi informatici facenti parte degli asset militari italiani contro la minaccia degli attacchi cyber, ma la natura fluida e in costante evoluzione di questi strumenti

[54] https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/dal-caso-stuxnet-allanalisi-del-panorama-cibernetico-italiano/

[55] https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/dal-caso-stuxnet-allanalisi-del-panorama-cibernetico-italiano/

offensivi costringe ancora oggi i policy makers a mettere in conto un processo di "inseguimento" del progresso tecnologico, il quale pare non avere fine.

Il successivo importante passo in avanti si è verificato nel 2016, quando l'Italia ha portato i suoi standard di sicurezza informatica al medesimo livello di sviluppo indicato dall'UE all'interno della direttiva EUNIS (European Union Network and Information Security) 2016/1148, avente come scopo la creazione di un continente europeo digitalmente sicuro.

Il contenuto della direttiva in questione pone in capo agli Stati Membri dell'Unione l'obbligo di dotarsi di sistemi di difesa informatica, sia riguardo le infrastrutture critiche che per quelle meno strategiche e provvedendo inoltre all'istituzione di un servizio rapido ed efficiente di risposta agli attacchi, attraverso l'obbligo di notifica alle agenzie competenti di ogni caso di azione offensiva subita[56].

Uno strumento molto utile per formare un'idea preliminare sulla crescente rilevanza ed importanza nel contesto italiano del dominio cyber sono i rapporti annuali pubblicati dalle Forze Armate: in particolare quelli stilati nel 2017 e 2018 fotografano una presenza capillare degli attacchi informatici nel novero delle azioni offensive condotte verso l'Italia, occupando una percentuale oscillante tra il 77 e il 78 % degli attacchi totali subiti durante questi due anni.

Il 2018 ha segnato una situazione caratterizzata da un'importante ambiguità: nonostante, infatti, si sia verificato un numero di attacchi verso i sistemi della Difesa più o meno coincidente con quello individuato nell'anno precedente, diverso è il discorso riguardo il numero dei bollettini contenenti la lista dei malware considerati pericolosi, pressoché raddoppiato e arrivato attualmente ad un numero molto vicino alle trecento unità.

Relativamente agli sforzi in ambito militare, i risultati più concreti sono arrivati negli ultimi anni, in particolare il 10 settembre 2018, quando il nuovo Reparto di Sicurezza Cibernetica ha dato inizio alle sue attività dopo aver raggiunto la piena capacità operativa.

Le sue competenze sono molteplici e ad ampio spettro: tra di esse figurano la scansione ad intervalli regolari delle reti strategiche dell'esercito, il mantenimento della sicurezza degli strumenti e dispositivi delle forze armate collegati ad Internet e un ruolo di vigilanza in generale verso le tecnologie presenti sui veicoli attualmente in uso.

A tal proposito, risulta chiarificatrice la definizione che ne dà il maggiore Luca Iuliano, già vicecomandante di questo nuovo reparto e divenutone comandante il 28 agosto 2020: "il nostro compito è quello di rendere sicuri, dal punto di vista cyber, le reti militari, sistemi ed equipaggiamenti, partendo dal presupposto che un'attività informatica ha impatti anche sul terreno"[57].

Egli inoltre sostiene una visione secondo la quale, tralasciando discorsi circa la disponibilità di iniziare e portare avanti una operazione bellica esclusivamente attraverso il dominio cyber, le possibili ricadute di un attacco andato a segno contro la strumentazione dell'esercito potrebbero avere conseguenze catastrofiche, quali la manipolazione degli ordini e/o l'attivazione di un'arma.

Già ad una prima analisi risulta chiaro come il nuovo Reparto di Sicurezza Cibernetica abbia sia una connotazione di difesa, essendo deputata alla protezione delle infrastrutture critiche, che di ausilio alle

[56]https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

[57] https://www.wired.it/internet/tlc/2020/07/30/cybersecurity-reparto-esercito/

truppe sul campo, assistendo nelle operazioni e coordinando l'addestramento dei soldati.

Come ha avuto modo di constatare il sottosegretario al ministero della Difesa Angelo Tofalo durante la sua visita dopo l'avvenuto raggiungimento della piena capacità operativa precedentemente enunciata[58], le aree di possibile intervento al Reparto sono varie e ad ampio spettro: nell'ambito dell'Information Technology principalmente la protezione di Reti nazionali, Infrastrutture critiche e Sistemi d'arma.

Per quanto concerne l'area della cosiddetta "Disruptive Technology" il Reparto svolge attività di controllo sulle prossime innovazioni in grado di apportare importanti cambiamenti nella gestione operativa delle attività cyber: tra di esse possiamo annoverare il 5G, l'Intelligenza Artificiale e i Big Data.

Le altre due macroaree rientranti nelle competenze del Reparto, ovvero l'Information Collection e "Cyber Command Staff and Forensic Operations", identificano un ruolo di collegamento in concerto con altre agenzie attinenti al dominio cyber facenti capo a varie branche delle Forze Armate sia per la raccolta informazioni che per la stesura e pianificazione di azioni facenti uso del mondo informatico.

Nel novero delle responsabilità assegnate a questo Reparto ve ne è anche una dal taglio più avanguardistico, ovvero "l'applicazione di componenti tecnologiche capaci di svolgere funzioni innovative e sofisticate con effetti particolarmente gravosi sulle nostre Forze, come ad esempio l'esfiltrazione di informazioni tra sistemi isolati/reti informatiche chiuse (ovvero in condizioni di Air Gapping) o l'impiego di dispositivi informatici che agiscono direttamente su piattaforme o sistemi d'arma (Cyber IED)"[59].

Il maggiore Iuliano ha posto inoltre l'accento su una questione che esula dall'ambito strettamente militare e operativo ma che ne risulta comunque strettamente legata, data l'influenza che è in grado di esercitare su di esso: lo stato embrionale degli strumenti di diritto internazionale atti a legiferare in materia cyber.

Più nello specifico, Iuliano pone l'accento su come questa situazione di incertezza influisca sulla capacità operativa dello stesso Reparto, dato che "le attività sono ridotte al minimo, perché la giurisprudenza internazionale è ancora lacunosa ed è ancora difficile portare a termine il processo di attribuzione per individuare lo stato fautore di un'offensiva"[60].

Da questa dichiarazione si può comprendere come il cosiddetto "problema dell'attribuzione" resti una spina nel fianco di elevata importanza per gli addetti ai lavori e gli esperti di sicurezza informatica a tutti i livelli, sia civile che militare, e indipendentemente dall'appartenenza o meno ad organismi governativi.

A livello organizzativo, la ricerca degli effettivi che sarebbero andati a costituire l'ossatura di questo nuovo Reparto è stata portata avanti attraverso una selezione tramite doppio bando e una formazione di carattere misto e multidisciplinare, coadiuvata dall'apporto del mondo accademico attinente allo specifico settore cyber.

[58] Tofalo visita il Reparto Sicurezza Cibernetica (difesa.it)

[59] Tofalo visita il Reparto Sicurezza Cibernetica (difesa.it)

[60] https://www.wired.it/internet/tlc/2020/07/30/cybersecurity-reparto-esercito/

Inoltre, nelle intenzioni dei suoi ideatori, il nuovo Reparto avrebbe dovuto rivestire funzioni di supervisione e coordinamento, di concerto con gli altri settori delle Forze Armate, dotate a loro volta di propri gruppi preposti alla sicurezza informatica, per raggiungere la massima efficacia operativa possibile.

A febbraio 2020 il comando e la direzione del Reparto per la Sicurezza Cibernetica sono passati al COR[61](Comando Interforze delle operazioni di rete), nell'ottica di un conclusivo assestamento organizzativo per questo nuovo strumento di difesa informatica.

Parallelamente a questo "passaggio di consegne", il sottosegretario al ministero della Difesa Angelo Tofalo ha fornito un'ulteriore delucidazione sul funzionamento a livello organizzativo, logistico ed operativo del nuovo Reparto, spiegando come "ogni singola forza armata, in armonia con lo Stato maggiore della Difesa, sta continuando a portare avanti senza sosta un lavoro specifico e articolato riguardante la trattazione del dominio cibernetico"[62].

Questo posto di primo piano recentemente assunto dalle minacce provenienti dal dominio cyber, nel dibattito relativo alla sicurezza all'interno del sistema paese italiano, ha visto la luce nel periodo immediatamente successivo alla scoperta del worm Stuxnet nel 2010, evento che mostrò alla comunità internazionale e agli addetti ai lavori di tutto il globo la possibilità più che concreta e plausibile per le armi attinenti al dominio cyber di causare danni concreti e quantificabili nel mondo fisico.

Ancor più recentemente vi è stata una ulteriore crescita nel livello di attenzione riservata, dai policy-makers italiani ma non solo, alla sicurezza informatica, dato il sensibile aumento nel numero degli attacchi di questo tipo contro le infrastrutture più disparate: per esempio, il Centro di sicurezza informatica del Regno Unito ha diffuso un comunicato in cui rivelava l'esistenza di intrusioni informatiche volte a rubare gli studi condotti per lo sviluppo di un vaccino contro il coronavirus, mentre ancora oggi persiste il sospetto di intervento informatico fraudolento nelle elezioni presidenziali americane.

Un esempio più strettamente collegato alla realtà del nostro Paese si concretizza nel proclama rilasciato nel 2019 dal CLUSIT[63], nel quale veniva ribadito come l'utilizzo delle armi cyber costituisse per gli Stati una allettante "seconda via", alternativa alle modalità di scontro più tradizionali e consolidate, regolando quasi a proprio piacimento la gravità degli attriti in base alla loro agenda senza dover mobilitare tattiche e strumenti "cinetici" e per questo più difficilmente gestibili e/o occultabili.

Inoltre, secondo gli esperti del CLUSIT, la conseguenza principale e dall'impatto più pervasivo sarebbe" una fase storica di cyber-guerriglia permanente, sempre più feroce, ovviamente non dichiarata e anzi sistematicamente negata".

Sempre nel corso del 2019 si è potuto assistere ad un rinnovamento capillare e multilivello degli strumenti di sicurezza informatica nazionali, per mantenere il livello di protezione delle infrastrutture critiche il più possibile al passo con l'estrema rapidità dell'evoluzione tecnologica del dominio cyber.

[61] Comando per le Operazioni in Rete (COR) - Difesa.it

[62] https://www.wired.it/internet/tlc/2020/07/30/cybersecurity-reparto-esercito/

[63] Sigla della Associazione Italiana per la Sicurezza Informatica: tra gli scopi di questa organizzazione, creata sul modello delle esperienze simili di altri Paesi europei, vi è la diffusione di una adeguata cultura cyber tra la popolazione e la formazione professionale di chi lavora nel settore.

Questa carica innovativa ha trovato compimento nella creazione e attivazione del Computer Security Incident Response Team (CSIRT), inquadrato all'interno del Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri e incaricato della stesura a livello tecnico-operativo della metodologia d'azione italiana ad un livello multidisciplinare, andando a riguardare prevenzione e gestione incidenti e favorendo la cooperazione in ambito di sicurezza informatica con gli altri Paesi Membri dell'Unione Europea tramite la rete CSIRT, quando questi sono coinvolti, tramite information e skill-sharing[64].

Il 2021 è stato un anno molto prolifico per il processo, in costante evoluzione e rimaneggiamento, di ammodernamento e stesura in maniera chiara di una policy italiana ad ampio respiro, in grado di garantire consoni livelli di protezione e difesa delle infrastrutture critiche contro i possibili usi offensivi degli strumenti cyber.

Il contesto più strettamente istituzionale ha visto la concretizzazione dei progressi fatti con la creazione dell'Agenzia per la Cybersicurezza Nazionale, seguendo anche l'esempio di Francia e Germania che si erano già dotate in precedenza di uno strumento simile, e portando avanti gli importanti step già intrapresi con l'attuazione del Perimetro di Sicurezza Nazionale Cibernetica.

La pandemia causata dal virus SARS-CoV-2 ha implicato, in Italia come nel resto del mondo, una ulteriore ascesa nella visibilità ed importanza riservata alla sicurezza informatica e al mondo cyber in generale: il massiccio ricorso da parte di aziende, appartenenti a tutti i settori, al lavoro in modalità "smart- working" ha reso più che mai necessaria e fondamentale la dotazione di sistemi informatici e reti efficienti e sicure, sia per i privati che per i servizi alla cittadinanza.

Su questo specifico punto è intervenuta Nunzia Ciardi, direttore del Servizio Centrale della Polizia Postale e delle Comunicazioni, descrivendo in particolare come "la pandemia ha aumentato la superficie d'attacco, visto che quello che non potevamo fare fisicamente lo facevamo online, dal lavoro agli acquisti alla sanità e i reati informatici, di conseguenza, sono aumentati esponenzialmente"[65].

Per contribuire alla stesura di un quadro chiaro su quanto abbia influito il Covid19 sul livello di minaccia proveniente dal dominio cyber, Ciardi ha provveduto a fornire alcuni numeri sul tema:

-50 casi di minacce gravi segnalate dal Centro nazionale per le Infrastrutture Critiche, 45 delle quali rivolte al solo settore sanitario, comprensibilmente divenuto il bersaglio principale in periodo pandemico

-un aumento del 600% nel numero degli attacchi cyber a scopo di "phishing", ovvero malware nascosti dietro a mail invitanti a scaricare file tematici apparentemente innocui

-segnalazioni, di parte di ben 28 aziende, di frodi informatiche subite e ammontanti ad un valore totale di 25 milioni di euro.

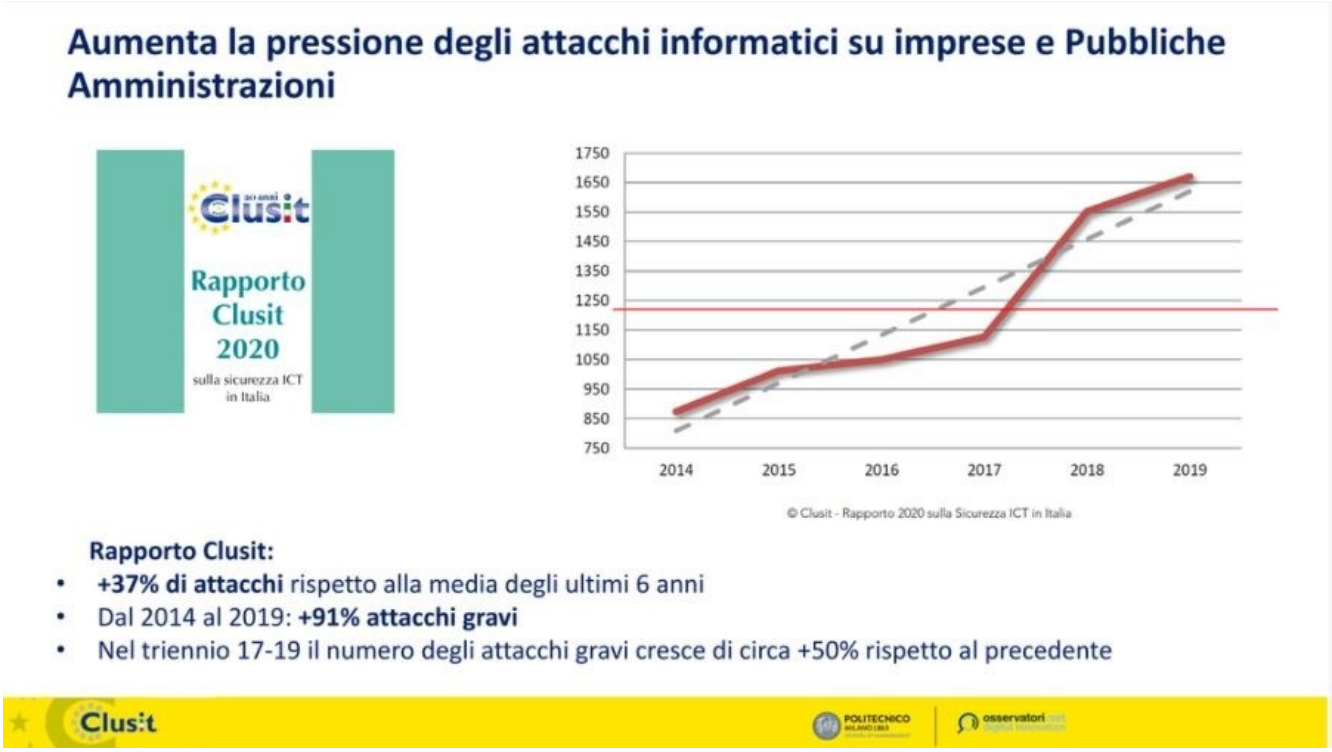
Vi sono numerose prove documentate sullo sfruttamento fraudolento, da parte di attori ostili di varia natura, della situazione emergenziale creatasi con la comparsa del Covid-19 per incrementare la propria azione offensiva tramite il dominio cyber: nello specifico, il consueto rapporto annuale pubblicato dal CLUSIT ha evidenziato un situazione molto negativa, etichettando il 2021 come "l'anno peggiore di

[64] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

[65] Cybercrime in aumento durante il lockdown | Ministero dell'Interno

sempre"[66] relativamente al grado di sofisticatezza delle minacce provenienti dal dominio cyber e alla loro capacità offensiva.

Nonostante ciò, i rapporti forniti sempre dal CLUSIT relativi agli anni precedenti mostrano come, in realtà, la situazione manifestatasi nel 2021 non sia un'evoluzione improvvisa ma, piuttosto, la continuazione di una tendenza preesistente: il rapporto relativo al 2020 in particolare permette di comprendere la prima fase, cronologicamente parlando, di questo rende negativo[67].



Come si può evincere dal grafico sovrastante, dal 2014 il numero degli attacchi cyber ha continuato ad aumentare di anno in anno, particolarmente tra il 2017 e il 2019, sia in termini strettamente numerici che di gravità dell'azione offensiva.

Il già menzionato rapporto relativo invece al 2021 conferma questa tendenza, evidenziando come "nel solo 2020 gli attacchi gravi sono cresciuti del 29% rispetto al 2019"[68]: nonostante all'interno del rapporto vengano analizzati solamente gli attacchi denunciati pubblicamente, i numeri indicano un forte incremento di questa tipologia di attacchi.

[66] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

[67] Rapporto Clusit 2020 : SecurityOpenLab.it

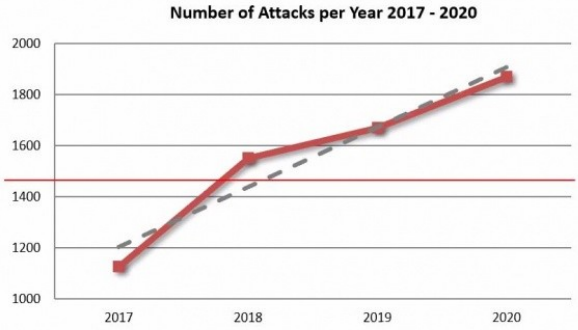
[68] Rapporto Clusit 2021: come e quanto ha colpito il cybercrime nel 2020 : SecurityOpenLab.it

Quali sono i numeri del campione ?

Negli ultimi 10 anni abbiamo analizzato e classificato in media 100 attacchi gravi di dominio pubblico al mese, 94 nel 2017, 129 nel 2018, 137 nel 2019 e 156 nel 2020.

- **11.959** attacchi gravi analizzati dal gennaio 2011 al dicembre 2020 (di cui oltre metà, **6.220,** dal 2017).

- 873 nel 2014
- 1.012 nel 2015
- 1.050 nel 2016
- **1.127 nel 2017**
- **1.552 nel 2018**
- **1.670 nel 2019**
- **1.871 nel 2020**



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Nel quadriennio 2017-2020 il numero di attacchi gravi che abbiamo analizzato è cresciuto del +66% (da 1.127 a 1.871).
Il numero di attacchi rilevati nel 2020 segna una differenza del +29% rispetto alla media degli attacchi per anno del triennio precedente (1.450).

Lo stesso Covid-19 è stato usato per definire una nuova area tematica all'interno della quale è stato possibile pianificare e attuare tutta una serie di attacchi informatici: nelle prime fasi della pandemia, infatti, il virus è sato il fulcro tematico del 10% degli attacchi cyber perpetrati dalla fine di gennaio 2020.

All'interno dello stesso Rapporto è possibile notare come "i cybercriminali hanno sfruttato la situazione di disagio collettivo, nonché di estrema difficoltà vissuta da alcuni settori - come quello della produzione dei presidi di sicurezza (ad esempio delle mascherine) e della ricerca sanitaria – per colpire le proprie vittime"[69].

Concentrandosi appunto sulla ricerca sanitaria, è evidenziato nel Rapporto come oltre la metà degli attacchi cyber portati a termine avesse scopo di crimine cyber vero e proprio, mentre nella restante metà dei casi l'obiettivo era lo spionaggio e/o il furto di informazioni, su tutti riguardo gli studi relativi allo sviluppo dei vaccini.

Volendo invece quantificare l'efficacia di questi attacchi cyber e la loro capacità offensiva, le analisi svolte dal CLUSIT hanno permesso di verificare che, all'interno del numero di attacchi individuati e dei quali è stato comprovato l'avvenuto successo, il 56% dei casi ha avuto un impatto giudicato "alto" e "critico" mentre il restante 44% ne ha avuto uno "medio".

Tutte queste percentuali contribuiscono a delineare un quadro nel quale è possibile notare non solo un aumento generale nel numero di attacchi cyber verificatisi durante l'anno, ma anche una rapida evoluzione in negativo per ciò che concerne la gravità ed ambizione nella scelta dei sistemi individuati come obiettivo.

Concentrandosi sulla situazione fotografata all'interno del sistema paese italiano, risultano di fondamentale importanza i dati raccolti all'interno del Documento di Sicurezza Nazionale, sezione della relazione presentata annualmente al Parlamento da parte del DIS (Dipartimento delle

[69] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

Informazioni per la Sicurezza) nella quale vengono elencate ed analizzate le politiche intraprese al fine di garantire la protezione delle infrastrutture critiche.

Tra le informazioni reperibili al suo interno, si può comprendere come il numero degli attacchi cyber condotti contro l'Italia abbia subito un aumento del 20%: gli obiettivi prevalenti sono stati i sistemi attinenti all'Information Technology utilizzati da soggetti pubblici, in particolare nell'ottica delle Amministrazioni locali, che hanno registrato un aumento del 30 % nella quantità di attacchi informatici subiti rispetto all'anno precedente.

Passando invece ai dati riguardanti il settore privato, gli attacchi informatici si sono rivolti principalmente contro le infrastrutture appartenenti al sistema bancario (11%), il settore sanitario (7%), che ha visto l'aumento più significativo data la natura dell'emergenza globale in atto, e l'Information Technology (11%).

Passando da dati raccolti su coloro che hanno subito gli attacchi a quelli sui soggetti che li hanno pianificati e messi in pratica si può notare come il "cybercrime" sia il contesto dominante all'interno del quale i fautori di questi attacchi trovano motivazione e collocamento: la restante parte degli attacchi cyber può essere ricondotta ad attività di Espionage e Information Warfare[70].

Il rapporto più recente, relativo all'anno tutt'ora in corso, si pone in continuità con la tendenza negativa fotografata negli anni precedenti ma con un ulteriore aumento rispetto all'anno prima, precisamente del 10% in termini numerici senza però tralasciarne anche la gravità.

La crescente pericolosità di questi strumenti annovera tra le sue cause un'organizzazione a livello logistico migliorata da parte degli attori che ne fanno uso: all'interno del rapporto viene specificato come "la nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata"[71].

Anche la metodologia d'azione e la scelta dei bersagli non restano esenti da cambiamenti radicali ed evoluzioni nella loro conduzione: il rapporto permette di individuare una strategia molto più mirata per quanto riguarda i sistemi colpiti: in ordine di importanza, l'obiettivo prediletto è risultato essere l'abito governativo/militare, seguito dal settore informatico, dagli attacchi ad obiettivo multiplo, la sanità e l'istruzione[72].

Mentre quasi tutti questi ambiti hanno registrato in linea generale un incremento nel numero degli attacchi rispetto agli anni precedenti, gli attacchi ad obiettivi multipli hanno subito un calo dell'8% rispetto al 2020 e l'istruzione ha visto un numero pressocché stabile e costante del 9%.

La risposta governativa italiana a questa situazione di sensibile aumento della presenza e pericolosità, nell'arena nazionale ed internazionale, degli attacchi cyber ha trovato il suo centro nella promulgazione del Perimetro di Sicurezza Nazionale Cibernetica, documento che "prevede sia obblighi legali volti al rispetto di stringenti misure di sicurezza e alla notifica degli incidenti, sia specifiche disposizioni in materia di forniture di determinati beni, sistemi e servizi ICT destinati a essere impiegati su reti, sistemi

[70] Rapporto Clusit – Clusit

[71] Rapporto Clusit – Clusit

[72] Rapporto Clusit – Clusit

informativi e per l'espletamento dei servizi informatici utilizzati dai soggetti inclusi nel Perimetro stesso per l'esercizio della funzione/servizio essenziale per la sicurezza nazionale"[73].

Nonostante i rapidi e sostanziali progressi già compiuti negli anni precedenti, il processo di mantenimento "up to date" della policy italiana relativa al dominio cyber è continuato anche nel 2020 attraverso la prevista approvazione di ben cinque decreti sul tema[74].

Dei cinque decreti attuativi presenti nella roadmap del Perimetro (quattro DPCM e un DPR), quattro sono già stati approvati: lo scopo di questi documenti può essere riassunto nella stesura di una lista elencante tutti quegli strumenti ed infrastrutture sui quali concentrare le proprie capacità di sicurezza informatica, perché considerati come aventi valore strategico e cruciali per la sicurezza nazionale.

Più nello specifico, il DPCM 131 del 30 luglio 2020 contiene al suo interno una lista completa e precisa degli attori rientranti nel Perimetro di Sicurezza Nazionale Cibernetica, insieme ai settori in cui essi operano, oltre alle "modalità di elaborazione, aggiornamento e trasmissione degli elenchi dei beni ICT"[75].

Nonostante il carattere profondamente "burocratico" e non collegato al lato tecnico del settore della sicurezza informatica possano portare a identificare questo DPCM come un documento di importanza minore, la sua rilevanza risulta al contrario fondamentale: la presenza di una conoscenza chiara e adeguatamente aggiornata dei sistemi attinenti alla sfera delle infrastrutture critiche è oltremodo cruciale per la stesura di un'efficacie strategia di salvaguardia.

Il secondo decreto, ovvero il DPR (Decreto del Presidente della Repubblica) n.54 del 5 febbraio 2021, concerne invece la sicurezza riguardante programmi e/o prodotti acquistati da parte dei soggetti presenti all'interno della lista del Perimetro Nazionale di Sicurezza Cibernetica, analizzata e supervisionata dal CVCN (Centro di Valutazione e Certificazione Nazionale) e dai Centri di Valutazione dei Ministeri degli Affari Interni e Difesa.

Il terzo decreto (nuovamente un DPCM, più precisamente il n.81 del 14 aprile 2021) riguarda più concretamente gli obblighi assegnati ai singoli attori del Perimetro Nazionale per quanto concerne le corrette procedure da seguire per notificare l'insorgere di azioni offensive rivolte contro le infrastrutture informatiche nazionali, attraverso una nuova classifica in ordine di gravità del danno subito.

Oltre a questa lista, all'interno del decreto è stato elaborato un elenco delle principali misure di sicurezza, tratte dal Framework Nazionale per la Cybersecurity e Data Protection, appositamente pensate per la protezione dei sistemi precedentemente citati, ciascuno dei quali dovrà necessariamente beneficiare di apposito processo di implementazione di tali misure.

Il DPCM del 15 giugno 2021 tratta e disciplina le corrette procedure da adottare per garantire un adeguato livello di sicurezza informatica in casi di "affidamento di forniture di beni, sistemi e servizi ICT, destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi

[73] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

[74] https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/dal-caso-stuxnet-allanalisi-del-panorama-cibernetico-italiano/

[75] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

informatici"[76], dovendo inoltre notificare e produrre una documentazione esaustiva sui dettagli di queste azioni al CVCN o ai Centri di Valutazione in seno ai Ministeri competenti.

Il contenuto del decreto è centrato sulla divisone principale tra componenti hardware e software il cui uso sia collegato alle telecomunicazioni come settore, sia per fornitura di servizi che per protezione di infrastrutture attinenti all'area in questione, oltre alla possibilità di ulteriori usi "per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali"[77].

Scopo ultimo di questi decreti attuativi, e del Perimetro di Sicurezza Nazionale Cibernetica nella sua interezza, è fornire un corpus di procedure e strategie coerente, efficiente e in grado di stare al passo con l'evoluzione delle minacce che lo Stato si trova, e si troverà, ad affrontare relativamente al dominio cyber.

II.2 L'Agenzia per la Cybersicurezza Nazionale

Dal punto di vista relativo alla creazione di veri e propri organi competenti nella gestione del dominio cyber, il passo in avanti più recente e di ampio respiro è l'istituzione dell'Agenzia per la Cybersicurezza Nazionale: istituita con il D.L.n.82 del 14 giugno 2021, questa agenzia, avente sede a Roma e dotata di personalità giuridica, ha rappresentato innanzitutto un esempio concreto della volontà, da parte dell'Italia, di colmare il divario operativo che ancora la separava dalle nazioni europee più all'avanguardia nella gestione degli elementi nocivi provenienti dal dominio cyber.

Roberto Baldoni, che già aveva ricoperto il ruolo di Vicedirettore generale del DIS con delega alla cybersecurity, in corrispondenza della sua nomina a Direttore di questa nuova Agenzia ha contribuito a fornire un quadro d'insieme sul ruolo operativo rivestito da essa: egli infatti spiega come l'Agenzia "sarà l'Autorità nazionale per la cybersicurezza per la coordinazione tra soggetti pubblici coinvolti in materia di cybersecurity a livello nazionale e promuoverà la realizzazione di azioni comuni orientate alla sicurezza e alla resilienza cyber per la digitalizzazione di tutto il sistema paese"[78].

Nonostante la nomina di Baldoni simboleggi la volontà di mantenere un certo grado di continuità con le precedenti modalità d'azione, provenendo egli dal DIS, la nuova Agenzia segna allo stesso tempo un importante evento di cesura, dato che ingloba in sé altre agenzie e competenze precedentemente assegnate ad istituzioni differenti.

L'Agenzia ha un esteso grado di autonomia, essendo completamente esterna alle agenzie di intelligence, seguendo l'esempio fornito dalle esperienze precedenti di Francia e Germania: infatti l'Agenzia attualmente ingloba lo CSIRT (Computer Security Incident Response Team) italiano e il Nucleo di Sicurezza Cibernetica, prima entrambi sotto la diretta supervisione del DIS.

[76] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

[77] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

[78] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

Come evidenziato da Francesco Bechis[79], la questione dell'estensione delle competenze poste in seno alla nuova Agenzia, oltre che del suo livello di autonomia operativa, ha causato ampi ed accesi dibattiti all'interno dei responsabili governativi orbitanti attorno ai vari partiti politici: più nello specifico, il grosso del dibattito menzionato si è verificato all'interno del Copasir, il comitato parlamentare che svolge il ruolo di controllore sulle attività nazionali d'Intelligence.

La questione ha rivestito una grande importanza anche e soprattutto per la composizione partitica dei deputati facenti parte del gruppo che ha proposto alcuni emendamenti, tutt'altro che ininfluenti, alle attività dell'Agenzia: tra essi figurano infatti tre deputati del PD (ovvero Alberto Pagani, Enza Bruno Bossio e Stefano Ceccanti) e uno della Lega (ovvero Massimiliano Capitanio).

Questo gruppo eterogeneo, aiutato anche dall'iniziativa parallela dei deputati di Italia Viva Luciano Nobili e Marco Di Maio, ha condensato le criticità poste nei riguardi degli articoli 4 e 6 del decreto-legge istitutivo dell'Agenzia (il dl 82/2021), concernente il livello e le modalità di controllo parlamentare sull'operato e l'organizzazione della stessa.

Gli emendamenti avanzati dai deputati sopracitati hanno come filo conduttore la richiesta di un ridimensionamento del controllo esercitato dal Copasir sulla struttura e organizzazione dell'Agenzia: essi chiedono che l'assetto organizzativo della nuova istituzione sia dettagliatamente comunicato prima alle commissioni parlamentari competenti, piuttosto che al Copasir.

Inoltre, viene richiesto che siano queste stesse "commissioni parlamentari competenti" le autorità di controllo alle quali dovrà rendere conto il Cic[80].

Valutazioni di natura prettamente politica hanno toccato anche la posizione il ruolo dello stesso Presidente del Copasir, svolto dal senatore del partito di Fratelli d'Italia Adolfo Urso: tra gli emendamenti proposti vi è infatti la richiesta che la precedenza nell'essere informati sulle nomine della dirigenza dell'Agenzia sia assegnata ai due Presidenti delle Camere, invece che ad esso.

Vi è una chiara matrice politica alla base di questa sorta di accanimento contro la figura del Presidente del Copasir: questo era stato infatti oggetto di una contesa molto attiva tra Lega e Fratelli d'Italia, dato che la prima desiderava la continuità con l'amministrazione precedente attraverso la riconferma di Raffaele Volpi, mentre il secondo partito invocava l'assegnazione del ruolo in quanto unico partito d'opposizione (secondo la legge 124/2007).

Nonostante la componente del calcolo politico sia innegabilmente di primaria importanza, le perplessità gravitanti attorno alla classificazione della nuova Agenzia hanno una loro ragion d'essere anche all'interno della questione su chi sia realmente legittimato a dettare le linee guida sul suo operato.

Il dibattito si divide principalmente in due diverse "scuole di pensiero", entrambe aventi in comune la necessità di verificare se il Copasir sia o meno la scelta corretta come autorità di controllo in questo specifico caso: la prima sostiene che, dato che il Copasir svolge un ruolo pervasivo nel controllo dei Servizi Segreti, "spetta ad altri organismi, alla Camera come al Senato, il controllo parlamentare dell'agenzia, che con i Servizi collabora, ma ne è al di fuori"[81].

[79] Agenzia Cyber, il controllo al Copasir? Ecco cosa si dice in Parlamento - Formiche.net

[80] Il Comitato Interministeriale per la Cybersicurezza, organo che raggruppa i ministri competenti in materia e che vigila sull'azione dell'Agenzia di concerto con il premier.

La seconda sostiene invece che, in quanto organismo preposto alla vigilanza sulla Sicurezza della Repubblica, il Copasir sia più che indicato, oltre che competente, per il controllo sulla sfera cyber dell'Intelligence nazionale.

Inoltre, l'Agenza ha visto assegnatole tutte le mansioni relativa alla sicurezza informatica, riservate inizialmente al Ministero dello Sviluppo Economico, al Presidente del Consiglio e all'Agenzia per l'Italia Digitale, oltre alla supervisione del Perimetro di Sicurezza Nazionale Cibernetica.

Per essere più precisi, tra le responsabilità in capo all'Agenzia vi sono "l'elaborazione della Strategia nazionale di cybersicurezza e il supporto alle attività del Nucleo per la cybersicurezza, rappresentando inoltre l'Autorità nazionale competente e il punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi".

Come enunciato precedentemente, tra le questioni normative approfondite all'interno dei decreti attuativi del Perimetro di Sicurezza vi è senz'altro la "certificazione" per verificare l'idoneità, a livello di standard di sicurezza, di un prodotto da interfacciare con le infrastrutture critiche del Paese: tale funzione era stata esercitata fino a quel momento da organi competenti (come il CVCN) sotto la supervisione del Ministero dello Sviluppo Economico.

Nello specifico, il sottosegretario Angelo Tofalo spiega come, all'interno dell'Agenzia, "il CVCN è la struttura tecnica che, insieme ad una rete di Laboratori accreditati, si occuperà di verificare la sicurezza e l'assenza di vulnerabilità note in beni, sistemi e servizi ICT, con l'obiettivo di innalzare il livello di cybersicurezza e di resilienza delle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese"[82].

Oltre al compito di analisi degli strumenti in dotazione del sistema paese italiano, il CVCN si è visto assegnare anche un compito dalla natura più "coercitiva", nello specifico è dotato della facoltà di imporre ulteriori analisi eccezionali in presenza di componenti hardware e software particolarmente critici o sensibili alle minacce provenienti dal dominio cyber.

Da ciò deriva inoltre la responsabilità, in capo a questo organo, di mantenere aggiornati e al passo coi tempi le varie metodologie di analisi, certificazione e i requisiti minimi di sicurezza.

Ulteriore novità collegata all'istituzione della nuova Agenzia è la collaborazione stretta e quanto più necessaria con il mondo accademico, sia a livello universitario che di ricerca, coinvolgendo inoltre tutta la filiera produttiva del settore: l'Agenzia ha infatti tra le sue priorità "la formazione, la crescita tecnico professionale e la qualificazione delle risorse umane nel campo della sicurezza informatica, anche attraverso l'assegnazione di borse di studio, di dottorato e di assegni di ricerca"[83] nell'ottica di eliminare, o almeno limitare, il problema della mancata diffusione di una "cultura cyber" tra la popolazione.

Oggetto di numerosi dibattiti negli ultimi mesi, data la sua importanza fondamentale sia a livello di credibilità internazionale dell'Italia che per le sue possibili ricadute positive sull'economia nazionale del periodo post-Covid 19, il PNRR (Piano Nazionale di Ripresa e Resilienza) rappresenta la risposta

[81] Agenzia Cyber, il controllo al Copasir? Ecco cosa si dice in Parlamento - Formiche.net

[82] Cybersicurezza : Operativo in Italia il Centro di Valutazione e Certificazione (angelotofalo.com)

[83] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

italiana sulle modalità di attuazione del "Next Generation EU", iniziativa europea avente lo scopo di coordinare la ripresa comunitaria su molti livelli, in particolare quello economico-sociale, dopo la crisi innescata dalla pandemia.

Ammontando a circa 210 miliardi di euro, il programma del Piano è diviso in vari obiettivi, tra i quali figurano la transizione ecologica, l'inclusione sociale, la digitalizzazione e, importante ai fini di questa analisi, l'innovazione del sistema paese.

Questi ultimi due punti nello specifico sono strettamente collegati e interdipendenti con una efficace e competitiva capacità di cyber security: un aumento diffuso e capillare della digitalizzazione, nella Pubblica Amministrazione come nel privato, creerà numerosi vantaggi ma anche molte opportunità di uso fraudolento del dominio cyber e di conseguenza è fondamentale mantenere al passo le capacità nazionali di prevenzione e difesa delle infrastrutture critiche.

Tra le principali modalità d'azione inquadrate negli otto miliardi di euro destinati alla digitalizzazione della Pubblica Amministrazione vi è certamente l'upgrade, sia a livello di sicurezza nella protezione dei dati che nell'efficienza dei servizi forniti alla cittadinanza, delle infrastrutture di cui si avvale la stessa Pubblica Amministrazione relativamente all'erogazione di servizi cloud.

La principale criticità che costituirebbe il "bersaglio" di questa strategia è l'eccessiva frammentazione e scarsa interoperabilità delle infrastrutture attuali: il superamento di questa lacuna operativa rivestirebbe un ruolo di grande importanza nel percorso intrapreso recentemente dall'Italia verso un adeguato e congruo standard di sicurezza informatica[84].

I finanziamenti relativi alla cybersicurezza previsti all'interno del PNRR non si riferiscono solamente a strategie completamente nuove come quella sopracitata, ma prevedono anche potenziamenti di misure pregresse e già operative: un esempio emblematico di questa casistica è il rafforzamento delle modalità d'azione già previste dal Perimetro di Sicurezza Nazionale Cibernetica.

Oltre all'incremento nell'efficienza operativa della Pubblica Amministrazione, il PNRR prevede tutta una serie di miglioramenti a livello tecnico degli strumenti attinenti all'Information Technology in uso presso le varie infrastrutture di cui si avvale il sistema paese italiano: tra questi upgrade previsti è possibile individuare la copertura del territorio nazionale con reti ultraveloci in fibra ottica, il tanto discusso 5G e un aumento nel campo degli investimenti per il monitoraggio satellitare per incentivare gli attori privati a spingere nell'innovazione in questo campo.

Come già accennato precedentemente in questa analisi, tutti questi sforzi da parte dell'Italia si configurano come la "via nazionale" per adempiere agli obiettivi comunitari descritti nelle iniziative a livello europeo sui medesimi temi, sintetizzabili in due principali documenti, la Direttiva NIS2 e la Direttiva CER.

Il primo documento costituisce la versione rielaborata e migliorata della Direttiva UE 2016/1148[85] relativa alla "Network and Information Security" (NIS) che la Commissione Europea aveva pubblicato precedentemente il 16 dicembre 2020: sufficientemente innovativa e al passo con le tecnologie del periodo e le minacce ad esse correlate, oltre a fornire un importante contributo alla sicurezza

[84] Tra i problemi principali del Sistema Paese italiano quello che risulta più evidente ed impattante è sicuramente la mancanza, o comunque lo sato molto embrionale, della "cultura cyber" posseduta dalla popolazione oltre ad una arretrata digitalizzazione della P.A.

[85] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/

informatica comunitaria, la prima Direttiva NIS era però caratterizzata da una scarsa possibilità di attuazione concreta nella sua interezza.

Proprio per ovviare a questa problematica invalidante, la Commissione Europea ha deciso di proporre un upgrade del documento in questione, spinta anche dalla rapida corsa, attuata da attori con intenti malevoli, verso crescenti livelli di minaccia e pericolosità: tra le migliorie presenti si annoverano una definizione più stringente di quali siano i requisiti minimi di sicurezza e un controllo più severo sulla supply chain, oltre a velocizzare ed ottimizzare la procedura di segnalazione degli incidenti insieme a misure punitive più severe ma allo stesso tempo più concrete nella loro applicabilità[86].

La proposta di revisione della direttiva NIS, fornita dalla Commissione Europea, può essere sintetizzata in tre macro-obiettivi cardine:

-migliorare il livello di sicurezza informatica generale per quanto riguarda il mercato interno dell'UE, rivolgendosi in parte alle società ed aziende di grandi e medie dimensioni del settore che operano nell'area in questione, ed elaborando inoltre un quadro normativo chiaro e concreto che disciplini la messa in pratica dei nuovi standard di sicurezza richiesti, i quali dovranno essere applicati automaticamente.

Da un punto di vista di definizione, il nuovo documento propone la sostituzione della distinzione tra "Operatore dei Servizi Essenziali" (o OSE) e "Fornitori di Servizi Digitali" (o FSD) con quella tra "Entità Essenziali" e "Entità Importanti"[87].

-fondamentale per il raggiungimento di un livello di sicurezza comunitario elevato e competitivo, la riduzione del gap tecnologico e normativo sarebbe attuata tramite una miglioria della procedura di segnalazione incidenti da parte dei privati, come le aziende, in caso di attacco: questa procedura sarebbe costituita da un approccio in due fasi, la prima delle quali consistente nella presentazione entro 24 ore di un primo rapporto preliminare alle autorità competenti, al quale sarebbe seguito un rapporto conclusivo da presentare entro un mese e facente parte della seconda fase.

-agevolare l'interscambio tra i Paesi Membri dell'Unione sia a livello di informazioni e capacità tecniche che di consapevolezza della portata del fenomeno in questione, portando al contempo ad un miglioramento nella rapidità ed efficienza della capacità dell'UE di gestire a livello comunitario le crisi di impatto e gravità maggiore.

Ultima ma non per importanza, nella proposta è prevista l'istituzione di una rete organizzativa di collegamento UE-Cyber Crises chiamata EU-CyCLONe, in un'ottica di crescente capacità di coordinamento a livello comunitario per ciò che concerne la difesa delle infrastrutture critiche, sia da un punto di vista di know-how tecnologico che di scambio di informazioni.

Per mantenere un certo livello di continuità con la struttura del quadro normativo precedente e al contempo renderlo più efficiente e al passo coi tempi, la Commissione Europea ha presentato una proposta di revisione parallela riguardante la Direttiva sulla Resilienza delle Entità Critiche (o CER), il

[86] https://www.cybersecurity360.it/cybersecurity-nazionale/verso-la-nis-2-ce-laccordo-in-europa-ecco-le-novita-su-soggetti-coinvolti-e-obiettivi/

[87] https://www.agendadigitale.eu/sicurezza/cyber-security-il-punto-sulla-strategia-italiana-cosa-abbiamo-fatto-e-cosa-resta-da-fare/

cui obiettivo era ed è tutt'ora il mantenimento del livello più alto possibile di sicurezza e protezione delle infrastrutture per quanto concerne l'approvvigionamento del mercato comunitario europeo.

Andando oltre il punto di vista normativo e governativo, un altro asset importante nonché motivo di orgoglio per il sistema paese italiano è l'esistenza di attori privati di spicco e all'avanguardia nel settore: un esempio calzante di questo ulteriore vantaggio strategico è rappresentato dal gruppo Leonardo, costituito da nove imprese e sovvenzionato al 79% dallo Stato italiano.

I settori nei quali opera questa azienda sono molteplici e spaziano dalla sicurezza informatica alle telecomunicazioni e radar, dal comparto missilistico all'aerospaziale.

Pur avendo ovviamente un rapporto stretto e privilegiato con lo Stato italiano, Leonardo è presente in una ventina di Paesi per un totale del 58% dei suoi siti di produzione e fornisce i propri servizi e prodotti a circa 150 Paesi in tutto il mondo.

Principalmente diffusa, oltre che in Italia, in Polonia, Regno Unito e Stati Uniti, Leonardo si è ormai diffusa e sviluppata in modo capillare anche in Francia e Germania: tra i clienti di maggior rilievo dell'azienda non vi sono soltanto i singoli Stati, ma anche alcune tra le principali organizzazioni internazionali, come la NATO e l'UE.

Anche se Leonardo costituisce certamente l'esempio più immediato ed universalmente riconosciuto, non è sicuramente l'unico caso di joint action tra lo Stato italiano e attori privati nell'ottica di ottimizzazione delle proprie capacità di difesa contro attacchi informatici: è infatti doveroso menzionare il caso di Yarix, azienda attiva nel campo della cyber security e del "disaster recovery".

Fondata nel 2001, Yarix svolge un ruolo di prim'ordine nel contesto nazionale in quanto società a capo della divisione Digital Security all'interno di Var Group, a sua volta orbitante intorno a Gruppo SeSa S.p.A., leader in Italia per quanto concerne il settore dell'Information Technology.

Questa azienda riveste particolare importanza anche a livello internazionale, essendo dotata di un laboratorio hi-tech a Tel Aviv nel quale un gruppo di esperti altamente qualificati elabora, progetta e testa continuamente i più recenti progressi nel campo della sicurezza informatica.

Yarix controlla inoltre un Cognitive SOC (Security Operation Centre) dedito alla sorveglianza e monitoraggio delle reti informatiche aziendali tra i più moderni e all'avanguardia del mondo: attivo tutti i giorni per ventiquattro ore al giorno e dotato di innovative misure di sicurezza fisica e biometrica, questo centro possiede la capacità di individuare e intercettare tempestivamente un possibile attacco cyber non appena viene ricevuto il segnale di un tentativo di intrusione in atto[88].

L'azienda, sin da primissimi tempi successivi alla sua fondazione, ha mantenuto stretti rapporti di collaborazione con lo Stato italiano e le sue agenzie, fornendo alle Forze dell'Ordine nazionali il proprio know-how e collaborando in particolar modo per quanto riguarda la formazione di agenti e funzionari oltre alla consulenza, specialmente in casi in cui si rendevano necessarie particolari competenze in digital forensics a supporto delle azioni protettive da parte delle agenzie governative addette alla pubblica sicurezza.

Questo rapporto di collaborazione ha assunto un carattere molto più strutturato e duraturo nel 2016, quando è stato messo nero su bianco tramite la firma di un Protocollo di Intesa tra Yarix e la Polizia di

[88] https://www.yarix.com

Stato per la prevenzione e il contrasto dei crimini informatici sui sistemi deputati alla protezione delle infrastrutture critiche.

Il Protocollo in questione si è reso necessario per assicurare un adeguato livello di supervisione, controllo e protezione del Sistema Paese, soprattutto dal punto di vista economico e sociale, essendo questo ormai fortemente integrato e dipendente dall'ausilio degli strumenti provenienti dal dominio cyber.

Lo strumento primario per il raggiungimento di questi obiettivi è lo sviluppo di un processo di "cooperazione mirata" tra attori Statali e privati: oggetto di questa intesa è principalmente la condivisione ed analisi di informazioni che possano essere utilizzate in un'ottica di prevenzione e/o contrasto di azioni offensive condotte tramite strumenti informatici contro la sicurezza dei sistemi protetti da Yarix, per segnalare in maniera rapida ed efficace situazioni di criticità e/o vulnerabilità di questi stessi sistemi e per tentare di individuarne l'origine, sia geografica che a livello di mandante.

All'interno del documento viene prevista anche la possibilità, in caso di situazioni di emergenza grave ed immediata, di comunicazione diretta e joint action tra i due attori firmatari per assicurare una risposta rapida e tempestiva alle minacce più urgenti.

La stesura di una corretta ed efficacie strategia di difesa dalle minacce cyber oltre che di un adeguato sfruttamento delle potenzialità offerte dal dominio da cui esse provengono riveste un ruolo di primo piano anche nel dibattito politico interno al nostro Paese, ogni partito avente la sua specifica visone sul tema.

Intervistato relativamente alla posizione del suo partito, Alessio Butti, deputato di Fratelli d'Italia e vicepresidente della commissione "Ambiente, territorio e lavori pubblici", pone sì l'accento sulla necessità per l'Italia di dotarsi di adeguate misure e politiche di sicurezza informatica ma sottolinea allo stesso tempo l'esigenza di mantenerle il più possibile sotto il controllo nazionale, avvalendosi in maniera minima di strumenti di altri Paesi o forniti da aziende estere.

Per ribadire la posizione sulla questione sovranità, Butti ha evidenziato la principale ragione di disaccordo tra il governo Draghi e il suo partito, ovvero il divario tecnico esistente tra l'Italia e altri Paesi giudicati più avanzati in materia cyber[89].

Butti sostiene infatti che, allo stato attuale, in Italia siano presenti piccole e medie realtà operanti nel settore dei servizi cloud in grado di fornire servizi all'avanguardia in questo ambito: aziende alle quali, secondo l'opinione sua e del suo partito, avrebbe dovuto essere destinato il grosso degli investimenti presenti nel PNRR ed evidenziando come Francia e Germania abbiano intrapreso una politica simile.

Sempre relativamente al problema nell'affidarsi ad attori esterni al contesto nazionale, Butti pone l'accento su di un'ulteriore questione attinente però alla sfera del diritto, specificando che "nel caso delle società americane di cloud, i dati personali degli italiani che saranno da loro ospitati sono sottoposti alla giurisdizione del Cloud Act americano, con violazione della nostra sovranità, con il nostro ordinamento che non può opporsi in alcun modo alle richieste degli apparati di sicurezza stranieri"[90].

[89] Cloud, 5G, rete unica? La parola chiave è sovranità. Parla Butti (FdI) - Formiche.net

[90] Cloud, 5G, rete unica? La parola chiave è sovranità. Parla Butti (FdI) - Formiche.net

Relativamente alla decisione se avvalersi o meno di strumenti e servizi informatici di origine cinese, citando l'esempio dell'uso di TikTok da parte di alcuni politici italiani e del 5G, egli ribadisce la necessità di analizzare ogni caso attraverso la lente della reciproca convenienza, con particolare attenzione naturalmente agli interessi italiani.

In quest'ottica, egli evidenzia come sia indispensabile scindere la componente ideologica dalla protezione degli interessi nazionali, specificando che, mentre in Italia sono state sospese le operazioni attinenti all'uso del 5G, sia tra i membri dell'UE che tra le aziende d'oltreoceano vi è chi continua ad intrattenere rapporti commerciali con la Cina.

Nell'ottica della protezione degli interessi nazionali, Butti pone il suo partito a favore degli sforzi comunitari a livello europeo relativi all'indipendenza dell'UE a livello tecnologico e alla regolamentazione delle attività di aziende Big Tech: egli sostiene inoltre che sia indispensabile al giorno d'oggi attuare la medesima strategie di protezione di propri interessi a livello globale, indipendentemente dal soggetto in questione.

Riguardo al polo opposto dello schieramento politico, sullo stesso tema è intervenuta Anna Ascani, vicepresidente del Partito Democratico e sottosegretaria al ministero dello Sviluppo Economico: intervistata su temi analoghi a quelli portati all'attenzione del deputato Butti, il suo intervento è sicuramente utile per tracciare le principali direttrici del programma cyber del suo partito.

Anche per il Partito Democratico i servizi cloud rivestono un'importanza fondamentale nel panorama tecnologico odierno ma, al contrario di quanto sostenuto da Fratelli d'Italia, non considerano come prerequisito indispensabile la totale appartenenza al contesto italiano delle infrastrutture necessarie a tali servizi: ciononostante Ascani riconosce come "lo sviluppo dei data center rappresenti per l'Italia e per l'Italia e per l'Europa una grande opportunità di crescita industriale e di posizionamento sul mercato globale delle tecnologie"[91].

Relativamente al ruolo comunitario nella regolamentazione delle attività dei colossi tecnologici e dell'antitrust, Ascani sostiene la stesura di approcci comuni a livello dell'UE, sottolineando però che la forza delle istituzioni europee non risiede strettamente nella centralizzazione delle decisioni ma nella "sintesi dei contributi apportati dalle diverse authority nazionali"[92].

All'interno dell'intervento viene inoltre posta l'attenzione sul ruolo specifico dell'Italia nell'inizio e nell'evoluzione di questo processo, portato ad esempio sia l'allineamento normativo del contesto nazionale alla regolamentazione europea e il ruolo del Paese nella stesura della stessa.

Interrogata sulle controversie relative all'uso del già citato TikTok, Ascani considera questa applicazione in maniera similare agli altri social media, specificando l'importanza di strategie comunitarie riguardanti la protezione della privacy, dei dati personali e la regolamentazione nella fruizione di servizi di questo tipo da parte dei minori.

Per quanto riguarda la possibilità di utilizzare il 5G e la gestione dei rapporti con fornitori cinesi considerati come attori "ad alto rischio", Ascani ritiene che la scelta migliore risieda nella garanzia di un ambiente caratterizzato sì dalla libera concorrenza ma mantenendo al primo posto la protezione dei

[91] Cloud, 5G e Big Tech. Ascani spiega il piano tech del Pd - Formiche.net

[92] Cloud, 5G e Big Tech. Ascani spiega il piano tech del Pd - Formiche.net

dati dei cittadini italiani ed europei da possibili usi fraudolenti dei loro dati personali, facendo riferimento per esempio ai legami poco chiari tra TikTok e il Partito Comunista cinese.

Ascani infine difende quanto è già stato attuato attraverso i finanziamenti del PNRR, in particolare l'istituzione del Polo Strategico Nazionale, strumento comprendente le società Tim, Leonardo, Cdp Equity e Sogei ed inquadrato come cardine della "Strategia Cloud Italia" messa a punto dal governo italiano con l'intento di trasferire su cloud il 75% dei servizi attinenti alla Pubblica Amministrazione entro il 2026.

CONCLUSIONE

Nell'analisi effettuata nei capitoli precedenti è stato possibile, attraverso gli esempi forniti dal worm Stuxnet e dalla cyber-guerriglia effettuata ormai da anni da parte della Federazione Russa contro l'Ucraina, giungere alla conclusione che, allo stato attuale, la carenza di dati attendibili e verificabili sui casi in cui si fa uso del dominio cyber in chiave offensiva (data anche dal fatto che restano secretati per anni prima di essere fruibili) risulta molto complesso fornire una valutazione universale e definitiva dell'impatto del dominio cyber sulla conduzione bellica e le sue modalità.

Stuxnet in particolare costituisce una casistica all'interno della quale convivono caratteristiche a favore sia della tesi della Rivoluzione Cyber che della visione dell'arma cyber semplicemente come l'ultimo ritrovato tecnologico: la complessità della sua struttura e del codice sorgente, unita all'eccezionalità e al primato nella possibilità di causare danno concreto nel mondo fisico, contribuiscono ad accentuarne il carattere innovativo e la portata rivoluzionaria.

Allo stesso modo però sono presenti elementi che contraddicono quanto appena enunciato: nonostante Stuxnet sia stato effettivamente in grado di causare il danno concreto per cui è giustamente considerato un evento spartiacque, le conseguenze reali di questo attacco sono state piuttosto contenute, sia a livello di potenza offensiva (avendo danneggiato "solo" 1000 turbine su 5000) che in termini di durata nel tempo, dato che l'Iran è riuscita a riattivare completamente il programma di arricchimento dell'uranio relativamente in fretta.

Si potrebbe obbiettare sostenendo come l'obiettivo dell'attacco fosse, in realtà, una sorta di "test operativo" mirato più a verificare l'utilità sul campo di un'arma cyber come sostituzione ad un attacco cinetico diretto e a rallentare gli sforzi iraniani più che a fermarlo permanentemente.

Anche se si sostenesse questa interpretazione, la conclusione che ne verrebbe fuori metterebbe comunque in risalto una situazione complessivamente molto più sfaccettata e complicata di quanto inizialmente previsto dalla teoria della Rivoluzione Cyber.

Ad avvalorare la teoria della Rivoluzione Cyber però contribuiscono le conseguenze, in vari ambiti, dovute a Stuxnet ma più al fatto che sia stato usato che al danno strettamente detto che è stato in grado di causare[93]: dal punto di vista sociopolitico, l'apparente successo del worm ha contribuito grandemente a screditare agli occhi della popolazione la credibilità e l'efficacia del governo iraniano nella difesa delle infrastrutture critiche del Paese.

Sul lato più economico, l'attacco all'impianto di Natanz ha avuto in primis conseguenze relative ad un aumento importante delle spese del governo iraniano in termini di sostituzione delle turbine danneggiate, dato che l'embargo internazionale impedisce all'Iran l'approvvigionamento sul mercato globale, oltre ad aver costretto il Paese ad acquistare l'uranio arricchito da altri stati.

L'esigenza di un rapido miglioramento delle capacità di cybersicurezza nazionali, dopo una violazione di questa portata, ha certamente costituito una nuova voce particolarmente pesante nel bilancio annuale

[93] "Stuxnet", Marie Baezner and Patrice Robin, Center for Security Studies ETH Zurich, October 2017.

iraniano: in particolare, la creazione di una unità cyber all'interno della Guardia Rivoluzionaria ha contribuito sia all'aumento delle spese che al sospetto internazionale intorno alle azioni dell'Iran.

Condurre con successo un attacco verso un'infrastruttura critica appartenente ad un altro Paese è molto più difficile rispetto ai normali malware e ransomware nascosti in link inviati via mail o tramite messaggi a singoli individui: queste strutture si avvalgono molto spesso di reti modificate e chiuse, rendendo indispensabile l'utilizzo di modalità di introduzione dell'arma più "analogiche".

Inoltre, l'utilizzo del dominio cyber in chiave offensiva viene considerato come una alternativa utile rispetto alle modalità di attacco cinetico solamente se resta possibile la "plausible deniability", ovvero se il perpetratore dell'attacco può, in maniera convincente e credibile, restare nell'anonimato e allontanare qualsiasi accusa di responsabilità.

Questa possibilità è però inversamente proporzionale all'ambizione nella scelta del bersaglio e al danno causato: infatti, più esso è strategico per il Paese in questione e più è grande e visibile il danno causato, maggiore saranno allora le risorse e gli sforzi assegnati alle investigazioni per scoprirne il responsabile: alla fine, un uso massiccio del dominio cyber come arma porterebbe ad invalidare la sua principale componente vantaggiosa, togliendo buona parte della sua attrattiva.

Ciò che per i sostenitori della Rivoluzione Cyber rappresentava la principale minaccia dovuta all'utilizzo massiccio delle armi cyber, ovvero il "vantaggio asimmetrico" fornito da questi strumenti agli attori non statali e più deboli come le organizzazioni terroristiche, trova scarso riscontro nell'analisi effettuata: le armi cyber che potrebbero potenzialmente essere fonte di interesse per queste realtà sono assolutamente al di fuori della loro portata, sia in termini di risorse economiche che di expertise necessaria per progettarle.

La situazione di costante attrito, su vari livelli, tra la Federazione Russa e l'Ucraina ha inoltre dimostrato come anche Paesi tecnologicamente avanzati e dotati delle risorse necessarie per la creazione e uso delle armi cyber debbano affrontare elevate difficoltà per impiegare efficacemente questi strumenti, soprattutto se il bersaglio è anch'esso adeguatamente difeso: nel contesto del conflitto attuale, ci si sarebbero aspettati attacchi ambiziosi da parte russa sia negli obiettivi che nei danni causati, ma ciò non è avvenuto.

Non vi sono stati blocchi totali della fornitura di energia elettrica, né sono stati sabotati gli sforzi logistici e organizzativi nell'evacuazione dei civili o nella stesura delle manovre militari: non è chiaro se la Federazione Russa abbia deliberatamente scelto di non impiegare i suoi mezzi cyber più sofisticati nella convinzione che il conflitto in Ucraina sarebbe stato di breve durata e poco dispendioso in termini di risorse e perdite di vite umane tra i ranghi dell'esercito oppure se la motivazione sia da ricercare nella stessa natura interconnessa del dominio cyber a livello globale.

Esso, infatti, non concede una precisione chirurgica per quanto riguarda gli attacchi, i quali possono subire un effetto noto come "spillover", ovvero la fuoriuscita dell'azione nociva dell'arma cyber dai confini del bersaglio prestabilito in altri sistemi.

Nel caso della Federazione Russa, una casistica simile avrebbe potuto portare ad un coinvolgimento come parte attiva del conflitto da parte dei Paesi facenti parte della NATO, un'eventualità che Putin ha sempre cercato di evitare: la probabilità di un intervento congiunto a livello NATO in un caso del

genere è stata paventata dal 2016, quando i membri dell'Alleanza Atlantica hanno deciso di estendere l'ombrello protettivo dell'articolo 5 della Carta Atlantica anche agli attacchi cyber[94].

La crescente attenzione rivolta dalle istituzioni italiane analizzate nel caso studio del secondo capitolo ha mostrato come, indipendentemente che si consideri il dominio cyber uno strumento rivoluzionario o meno, la crescente dipendenza dai sistemi informatici in tutti gli aspetti della vita nel periodo attuale sia sufficiente per occupare un posto importante nella protezione del sistema paese di molti Stati.

La diffusione sempre più capillare di know-how relativo al dominio cyber e di strategie/modalità di difesa e/o contrattacco in caso di attacchi attinenti a questo strumento renderà in futuro sempre più complicata, lunga e dispendiosa la progettazione di armi cyber efficaci, soprattutto in presenza di obiettivi ambiziosi come è stato per il caso di Stuxnet.

Attualmente la possibilità di fornire una analisi accurata e complessiva della portata rivoluzionaria delle armi cyber è fortemente limitata dallo scarso numero di attacchi di cui si ha notizia, dalla poca varietà nella loro composizione e modalità d'uso da esso derivata e dal fatto che l'accesso alla documentazione attinente alla maggior parte di questi avvenimenti non è liberamente fruibile da parte del mondo accademico del settore.

Un esempio pratico di come l'evoluzione del contesto geopolitico internazionale vada assolutamente tenuto in considerazione, soprattutto per quanto concerne le grandi potenze, si riferisce agli attriti esistenti negli ultimi anni tra Stati Uniti e Cina, come spiegato da Stefano Mele in un suo articolo sul tema: citando in particolare l'attacco del 2015, attribuito alla Cina, rivolto allo U.S. Office of Personnel Management e culminato nel furto delle schede personali di più di 4 milioni di dipendenti[95].

Anche in questo caso l'uso dell'arma cyber ha avuto risultati ambivalenti: sebbene infatti la Cina abbia potuto trarre dei vantaggi dagli attacchi effettuati nel corso degli anni sia contro agenzie governative che contro attori privati (come esempi si possono le citare le operazioni Titan Rain[96] e GhostNet[97]) è facile constatare come la Repubblica Popolare sia stata in seguito costretta a ridimensionare l'utilizzo di questi strumenti interrompendone bruscamente l'impiego per favorire un clima distensivo con gli Stati Uniti.

Questo brusco cambio di rotta ha contribuito ad aumentare sensibilmente i sospetti statunitensi che il mandante degli attacchi da loro precedentemente subiti nel corso degli anni fosse proprio la Repubblica Popolare, dato l'improvviso cessare di questi eventi: nonostante gli Stati Uniti non siano comunque riusciti a provarne direttamente il coinvolgimento, la Cina si trova in una situazione mediana molto complessa.

---

[94] https://aspeniaonline.it/lelemento-cyber-nella-guerra-russo-ucraina/

[95] https://www.ispionline.it/it/pubblicazione/cyber-security-un-fronte-sempre-piu-caldo-13894

[96] Con questo nome viene indicata da parte del governo statunitense una serie di attacchi cyber multipli, attribuiti ad agenzie interne alle Forze Armate cinesi secondo una analisi da parte dell'istituto di sicurezza "SANS Institute", mirati a carpire informazioni sui sistemi informatici di varie agenzie operanti su suolo americano come Lockheed Martin, Sandia National Laboratories, Redstone Arsenal e persino la NASA.

[97] GhostNet, operazione di cyber sorveglianza scoperta nel marzo 2009 dopo oltre 10 mesi di investigazioni da parte del gruppo di ricerca canadese Info War Monitor, aveva l'obiettivo di infiltrare sistemi informatici strategici di varia natura, tra i quali figurano ambasciate, ministeri degli Esteri in più di 103 Paesi e soprattutto i sistemi posseduti dagli esiliati Tibetani.

Ciononostante, anche gli Stati Uniti attraversano una situazione similare, anche se in termini difensivi e di contrattacco: diversamente dalla Cina, che viene considerata da molti come "potenza emergente", gli Stati Uniti provengono da uno status di grande potenza preesistente che deve essere difeso e mantenuto, ponendo anch'essi in una situazione di indecisione, costantemente in bilico tra il desiderio di rispondere all'offesa subita e l'esigenza di mantenere un approccio più cauto per evitare di incentivare l'aggravarsi del processo.

Quanto è stato analizzato in queste righe porta, in conclusione, a considerare il dominio cyber e le armi da esso derivate come strumenti caratterizzati da una forte componente innovativa ma, complice lo stadio embrionale dell'uso di questi strumenti oltre che della disponibilità di informazioni attendibili su di essi, non definibili attualmente come portatori di una rivoluzione totale delle modalità di conduzione di un conflitto.

Allo stato attuale le armi cyber risultano infatti molto più efficaci come misura preparatoria e di ausilio per operazioni cinetiche (come nel caso dell'invasione russa dell'Ucraina) e/o utilizzate con prudenza e parsimonia, diluite nel tempo e tenendo a freno una eccessiva ambizione nella scelta dei bersagli, per mantenere un anonimato credibile.

Secondo Stefano Mele, "pensare-e poi implementare-accordi che contengano misure di confidence-building, tese soprattutto ad evitare una corsa agli armamenti e a identificarne i limiti in termini di target e strumenti utilizzabili, è certamente un passo a cui guardare in maniera favorevole"[98].

La stesura di un piano di tale ambizione e portata risulta però molto complessa, data la necessità di bilanciare i vantaggi ottenuti con l'uso nocivo del dominio cyber e l'esigenza di agevolare un clima distensivo tra i due Paesi.

Al governo di Pechino potrebbero infatti continuare a far gola le possibilità fornita dalle armi cyber per quanto concerne la sottrazione fraudolenta di know-how tecnologico e/o lo spionaggio industriale: ciò però potrebbe valere anche per gli attori privati operanti sul suolo cinese, attratti dai possibili guadagni derivanti dal furto di dati ad industrie e istituzioni.

Ulteriori ricerche e analisi sul tema dovranno essere condotte nei prossimi anni, approfittando della costante de-secretazione di documenti chiave relativi all'impiego di armi cyber, di un numero probabilmente maggiorato di casi analizzabili e dell'evoluzione nel contesto geopolitico internazionale.

[98] https://www.ispionline.it/it/pubblicazione/cyber-security-un-fronte-sempre-piu-caldo-13894

BIBLIOGRAFIA E SITOGRAFIA

https://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf

"Cyberdeterrence and Cyberwar", Martin C. Libicki, RAND Corporation, 2009.

https://www.repubblica.it/cronaca/2021/11/10/news/le_armi_cyber_cambieranno_la_guerra_l_esercito_ha_bisogno_di_nuovi_tecnici-325703400/

https://www.sicurezzanazionale.gov.it/sisr.nsf/letture/la-guerra-cyber-non-avra-luogo.html

https://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf

https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/dal-caso-stuxnet-allanalisi-del-panorama-cibernetico-italiano/

"Stuxnet and the Limits of Cyber Warfare", Jon R. Lindsay, University of California Institute on Global conflict and Cooperation, 15/01/2013.

"The Military Technical Revolution: A Preliminary Assessment", Andrew F. Krepinevich, Center for Strategic and Budgetary Assessments, 2 October 2002.

"The Revolution in Military Affairs, Transformation and the Defence Industry", Peter Dombrowski and Andrew L. Ross, Institute for Regional Security, Summer 2008.

Così spie olandesi (e non solo) aiutarono Usa e Israele a colpire l'Iran - Formiche.net

"Stuxnet", Marie Baezner and Patrice Robin, Center for Security Studies ETH Zurich, October 2017.

https://www.unionedirittiumani.it/newsletter/limportanza-dellarma-cyber-nel-conflitto-tra-russia-e-ucraina/

https://www.open.online/2022/02/17/ucraina-vs-russia-guerra-informatica/

https://aspeniaonline.it/lelemento-cyber-nella-guerra-russo-ucraina/

https://www.wired.it/internet/tlc/2020/07/30/cybersecurity-reparto-esercito/

Tofalo visita il Reparto Sicurezza Cibernetica (difesa.it)

Comando per le Operazioni in Rete (COR) - Difesa.it

Cybercrime in aumento durante il lockdown | Ministero dell'Interno

Rapporto Clusit 2020 : SecurityOpenLab.it

Rapporto Clusit 2021: come e quanto ha colpito il cybercrime nel 2020 : SecurityOpenLab.it

Rapporto Clusit – Clusit

Agenzia Cyber, il controllo al Copasir? Ecco cosa si dice in Parlamento - Formiche.net

Cybersicurezza : Operativo in Italia il Centro di Valutazione e Certificazione (angelotofalo.com)

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/

https://www.cybersecurity360.it/cybersecurity-nazionale/verso-la-nis-2-ce-laccordo-in-europa-ecco-le-novita-su-soggetti-coinvolti-e-obiettivi/

https://www.yarix.com

Cloud, 5G, rete unica? La parola chiave è sovranità. Parla Butti (FdI) - Formiche.net

Cloud, 5G e Big Tech. Ascani spiega il piano tech del Pd - Formiche.net

https://www.ispionline.it/it/pubblicazione/cyber-security-un-fronte-sempre-piu-caldo-13894