UNIVERSITÀ DEGLI STUDI DI PERUGIA
Dipartimento di Filosofia, Scienze Sociali, Umane e della Formazione

Corso di Laurea
in
Scienze per l'Investigazione e la Sicurezza

CYBER SECURITY E ATTIVITA' D'INTELLIGENCE

LAUREANDO
Cristiano Pieri
MATR.

RELATORE
Prof.ssa Maria Caterina Federici

Anno Accademico 2018-2019

INDICE

Premessa

Nella società in cui viviamo, grazie alle capacità algoritmiche sempre più evolute, la trasformazione digitale è in costante accelerazione in relazione alla quantità enorme di dati disponibili, alla potenza computazionale e alla larghezza di banda in continua crescita. Tale evoluzione ha dato e darà vita a repentini cambiamenti con notevoli riflessi sull'economia di quei paesi che sapranno meglio interpretare questa trasformazione dal punto di vista sociale, normativo e tecnologico.

Sono sfide importanti per il prossimo futuro anche per i responsabili della sicurezza nazionale, che dovranno costantemente tenere conto dell'accresciuto livello di complessità e sofisticatezza degli attacchi cyber, con particolare riguardo all'uso combinato di strumenti offensivi sviluppati ad hoc con quelli presenti nei sistemi target impiegati in modo ostile, nonché al "riuso" di oggetti malevoli (malware) finalizzati a ricondurne la matrice ad altri attori (cd. operazioni false flag).

Tali sfide, di competenza degli apparati d'intelligence sono condotte, com'è noto, da AISE ed AISI sotto il coordinamento rafforzato della componente "core" del DIS, che ha il compito di adottare gli accorgimenti necessari a salvaguardare lo sviluppo delle cyber operation, di evitare eventuali ed ulteriori danni ai target dell'architettura nazionale cyber e di consentire la disseminazione di misure di prevenzione per la difesa di reti e sistemi strategici adeguate all'effettivo livello di rischio.

Scopo di questa breve ricerca è quello di illustrare in che modo l'evoluzione digitale ha cambiato il modo in cui viviamo generando un nuovo spazio di interazione, il c.d. cyberspace, come parte integrante della vita personale e sociale.

Cambiamenti radicali che hanno assunto anche per l'intelligence una funzione decisiva, al punto che numerosi Stati hanno creato degli apparati specifici dedicati alla cyber intelligence. In Italia, ad esempio, con il DPCM del 17.02.2017 è stato istituito il Nucleo per la Sicurezza Cibernetica (NSC), inserito all'interno del Dipartimento per le Informazioni e Sicurezza (DIS), con il compito di assicurare una risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei Ministeri competenti in materia.

Tale risposta inizia, ad esempio, con l'individuazione delle principali minacce per la sicurezza nazionale, ovvero:

- **disinformazione**: il ruolo delle fake news non è stato mai tanto evidente come negli ultimi due anni, ove elezioni democratiche in tutto il mondo sono state influenzate forse in maniera decisiva da falsi account social aventi il compito di diffondere informazioni false costruite ad hoc per orientare il voto di ampie fasce di popolazione verso il candidato più gradito all'attaccante di turno (o di chi l'ha assoldato);
- **radicalizzazione online**: la rete, ed in particolare il *dark web*, è il fulcro della nuova propaganda jihadista in quanto permette alle cellule terroristiche di comunicare, coordinarsi e condurre le proprie attività anche in assenza di un comando centrale;
- **interruzione di servizi essenziali**: motivo per il quale la protezione cibernetica delle infrastrutture critiche è divenuta oggetto della c.d. Direttiva NIS, la quale impone obblighi di sicurezza più stringenti in capo agli operatori di servizi essenziali, obblighi di segnalazione degli incidenti cyber e rafforza la cooperazione a livello nazionale e comunitario;
- **spionaggio industriale**: è noto come alcuni Stati abbiano assunto a vero e proprio obiettivo strategico il furto di know how aziendale di Paesi più avanzati.

Pertanto, è interessante conoscere durante questo percorso, quali sono i principali rischi che si evidenziano a livello sistemico con particolare riguardo all'attività di intelligence, con il paradosso che mentre vent'anni fa si era alle prese con il problema della carenza di informazioni, ci si trova ora in una condizione di sovrabbondanza di informazioni.

CAPITOLO I

Informatizzazione e cyber crime

1.1 – L'informatizzazione nelle attività umane.

Dall'invenzione della ruota (3.500 a.C.), che ha permesso all'uomo di coprire distanze in tempi sempre più rapidi, fino allo sviluppo in tempi più recenti dell'intelligenza artificiale applicata ad automi con caratteristiche considerate tipicamente umane, la società ha subito in meno di 200 anni di storia tanti e tali cambiamenti che hanno inciso fondamentalmente su tutti gli aspetti della vita umana.

In particolare, lo sviluppo tecnologico ha determinato la trasformazione progressiva di tutta una serie di attività umane che vengono svolte con l'ausilio di congegni sempre più sofisticati. Si pensi a tutto quel complesso di attività domestiche, agricole, produttive etc. che oggi sono svolte in larga parte con tecnologie sempre più adeguate alle esigenze personali, professionali, di lavoro, di svago etc.

Ad esempio, oggi si parla di *smart house* o casa intelligente, che indica una struttura dotata di un impianto di domotica integrato, in grado di comunicare con *smartphone*, *tablet* e altri dispositivi per migliorare sicurezza e funzionalità della propria abitazione e degli elettrodomestici utilizzati. Una casa completamente automatizzata che l'utente può gestire con un semplice click per regolare ad esempio l'illuminazione migliorando resa e consumi, o per avviare processi quali l'accensione di allarmi, la videosorveglianza e l'utilizzo di elettrodomestici.[1]

Risulta evidente quindi, che nel momento storico in cui viviamo, le scoperte scientifiche e le invenzioni hanno scatenato un effetto sorprendente e trainante dell'evoluzione umana: dalla prima rivoluzione industriale (1750) segnata dall'adozione di macchine a vapore, alla seconda (1870) innescata dall'utilizzo del motore a scoppio e dell'elettricità, alla terza rivoluzione industriale (1950) legata all'introduzione dell'elettronica e dell'informatica nei processi produttivi. Quest'ultima, conosciuta anche come "rivoluzione digitale", coincide con il passaggio dalla meccanica, dalle tecnologie elettriche e da quelle analogiche alla tecnologia digitale, che si è sviluppata nei Paesi più avanzati con l'adozione e la proliferazione dei computer digitali e dei sistemi di conservazione dei documenti.

[1] https://www.ilmessaggero.it/casa/news/casa-news/smart_home/3874450.html

Con l'espressione terza rivoluzione industriale si indica anche tutta quella serie di processi di trasformazione della struttura produttiva e più in generale del tessuto socioeconomico, avvenuti a partire dalla metà del Novecento nei paesi sviluppati e caratterizzati da una forte spinta all'innovazione tecnologica e al conseguente sviluppo economico della società. Una rivoluzione legata, quindi, alla nascita dei computer, dei robot, dei satelliti, dell'esplorazione planetaria etc.

Con l'attuale quarta rivoluzione industriale, più comunemente conosciuta come "Industria 4.0", si è potuto assistere dal 2011 in poi alla nascita di modelli, strategie e paradigmi nuovi di gestione delle attività economiche e scambi commerciali: dallo sviluppo di nuovi prodotti e servizi, alla ricerca e innovazione, fino alla validazione e alla produzione con un alto grado di automazione e interconnessione.

Le componenti più importanti che hanno determinato questo cambiamento sono:

1) **I big data,** che riguardano una raccolta di dati molto estesa in relazione al volume, alla velocità e alla varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o di conoscenza. Questi dati possono arrivare da ogni genere di fonte e possono essere di ogni tipo: dalle carte di credito ai telefoni, dalla navigazione internet ai videogames, dalla sanità al modo di guidare. In realtà i dati di questo tipo anche in passato venivano raccolti per ricerche di ogni tipo ma quello che cambia al giorno d'oggi è la quantità, l'utilizzo e la velocità di acquisizione.

   Infatti, ora vi è la capacità di utilizzare in tempo reale tutta questa enorme massa di informazioni per analizzare, elaborare e successivamente creare modelli di comportamento da utilizzare poi in mille modi diversi.

2) **Gli analytics**, ossia il complesso delle tecniche e degli algoritmi necessari per estrarre dai dati delle informazioni utili e ricavarne un valore, come sta avvenendo nello sviluppo di tecniche di intelligenza artificiale, che può giocare un ruolo fondamentale nel prossimo futuro. Un esempio applicativo è il *machine learning*, ossia l'apprendimento automatico delle macchine, attualmente ben poco diffuso a livello industriale, ma che dovrebbe subire una vera e propria esplosione nei

prossimi mesi e anni.[2]

3) **L'interazione tra esseri umani e macchine** come il *touch screen* e i comandi vocali, fino allo sviluppo di sistemi di realtà aumentata per l'ottimizzazione degli spazi di lavoro e dei processi produttivi.[3]
4) **L'additive manufacturing**, che riguarda avanzate tecnologie in grado di sviluppare oggetti tridimensionali sovrapponendo sottili strati di materiale uno sull'altro attraverso l'ausilio della programmazione digitale; si tratta in pratica di un processo totalmente meccanizzato che permette di concretizzare nello spazio disegni tridimensionali elaborati al computer. Oltre all'uso industriale di questa componente, ulteriori sviluppi si segnalano in campo medico e scientifico.[4]

A seguito di questa rivoluzione ancora in atto si è anche coniato il concetto *di smart factory* che si compone di 3 parti:

1) *Smart production*: nuove tecnologie produttive che creano collaborazione tra tutti gli elementi presenti nella produzione ovvero collaborazione tra operatore, macchine e strumenti.
2) *Smart service*: tutte le "infrastrutture informatiche" e tecniche che permettono di integrare in modo collaborativo i sistemi e le aziende tra loro (fornitore-cliente) con le strutture esterne (strade, contesti urbani, gestione dei rifiuti, ecc.).
3) *Smart energy*: sistemi più performanti dei consumi energetici creando e riducendo gli sprechi secondo i paradigmi tipici dell'energia sostenibile.

Oggi, grazie a questo nuovo approccio, le imprese hanno la possibilità di incrementare la propria competitività ed efficienza tramite l'interconnessione di impianti e persone,

---

[2] L'apprendimento automatico è strettamente legato al riconoscimento di pattern (modelli) e alla teoria computazionale dell'apprendimento ed esplora lo studio e la costruzione di algoritmi che possano apprendere da un insieme di dati e fare delle predizioni su questi, costruendo in modo induttivo un modello basato su dei campioni. L'apprendimento automatico viene impiegato in quei campi dell'informatica nei quali progettare e programmare algoritmi espliciti è impraticabile; tra le possibili applicazioni citiamo il filtraggio delle e-mail per evitare spam, l'individuazione di intrusioni in una rete o di intrusi che cercano di violare dati, il riconoscimento ottico dei caratteri, i motori di ricerca e la visione artificiale.

[3] Il *touch screen* o *touch screen* a volte chiamato anche "schermo sensibile al tocco" o "schermo tattile", è un particolare dispositivo elettronico, frutto dell'unione di uno schermo ed un digitalizzatore, che permette all'utente di interagire con un'interfaccia grafica mediante le dita o particolari oggetti. Il touch screen è allo stesso tempo un dispositivo di input e output.

[4] https://www.archiproducts.com/it/notizie/l-additive-manufacturing-sbarca-in-campo-medico_46721

sfruttando la cooperazione delle risorse interne ed esterne ed aggregando e analizzando anche consistenti quantità di dati.

E queste possibilità vanno di giorno in giorno moltiplicandosi grazie ai continui investimenti in campo di: *internet of things, big data, cloud computing, robotica collaborativa, realtà aumentata e virtuale, stampa 3D, veicoli autonomi, nanotecnologia e biotecnologia, intelligenza artificiale* etc. [5] Come si è fatto cenno, quest'ultima invenzione è finalizzata a risolvere problemi e svolgere compiti e attività tipici della mente e dell'abilità umane. Guardando al settore informatico, potremmo identificare l'intelligenza artificiale come la disciplina che si occupa di realizzare sistemi hardware e software in grado di "agire" autonomamente e risolvere problemi, compiere azioni etc.[6]

L'interesse che oggi si concentra intorno a questa disciplina si dispiega sia nel calcolo computazionale (basti pensare a sistemi hardware molto potenti, di ridotte dimensioni e con bassi consumi energetici), sia nella capacità di analisi in *real-time* ed in tempi brevi di enormi quantità di dati e di qualsiasi forma.[7]

Nonostante non sia possibile prevedere quale sarà lo sviluppo dell'intelligenza artificiale in termini di diffusione e consolidamento, esistono prove evidenti del fatto che la definizione di un piano di trasformazione tecnologica e una corretta implementazione della stessa, indipendentemente dai sistemi utilizzati, sta avendo un forte impatto sui cittadini, sulle imprese e sulla Pubblica Amministrazione soprattutto in termini di sicurezza.

Infatti, con l'aumentare dell'interconnessione nel mondo digitale e soprattutto con l'uso di internet, il tema della cyber security diventa sempre più importante al fine di prevenire e limitare dei rischi che possono causare anche ingenti danni. Tema che è diventato anche il pilastro fondamentale per la tutela dello sviluppo tecnologico, che non riguarda solo la sicurezza delle reti ma anche tutti gli altri aspetti e settori delle

---

[5] "L'intelligenza artificiale è una disciplina appartenente all'informatica che studia i fondamenti teorici, le metodologie e le tecniche che consentono la progettazione di sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana." (da Wikipedia)

[6] Vedasi anche *http://www.intelligenzaartificiale.it/*

[7] *Real-time* è riferito alla tecnica dell'elaborazione elettronica dei dati in tempo reale.

attività umane.

Pertanto, lo sviluppo di tecnologie informatiche e telematiche (ICT), sempre più sofisticate ed efficienti, ha favorito l'insorgere di nuove forme di attività illecite, meglio definite come reati informatici o *cyber crime* di cui parleremo in seguito.

1.2- Il cyberspazio e le nuove forme di criminalità.

Il termine "cyberspazio" ha origine dalla parola greca *kyber* che vuole dire "navigare" e sta ad indicare uno spazio effettivamente navigabile. L'inventore di questa espressione è lo scrittore William Gibson che nel suo romanzo "Neuromante" del 1984 lo descrisse come uno spazio digitale e navigabile, un mondo elettronico visuale e colorato nel quale individui e società interagiscono attraverso le informazioni.

Per Gibson il cyberspazio è *"Un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici...Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano..."*. [8]

In altri termini, questo universo di reti digitali e di computer è un nuovo fronte culturale ed economico, un mondo nel quale multinazionali, corporazioni e pirati informatici si scontrano per la conquista dei dati e delle informazioni.

Esso è rappresentato da un ambiente virtuale che consente di accedere a tutte le informazioni raccolte in banche dati rendendo possibile l'interscambio fra molteplici utenti.

Così come lo immaginava Gibson, oggi il cyberspace viene definito come un ambiente composto da infrastrutture computerizzate tra cui software, hardware, utenti, big data e tutte le interrelazioni che esistono tra loro. Fanno parte di questo ambiente soprattutto *internet of things*, le reti di comunicazione e tutti quei dispositivi dotati di connessioni i cui caratteri principali sono l'illimitatezza e l'immaterialità.

Tale spazio immateriale e incalcolabile, realizzatosi con lo sviluppo del *cloud computing*,

[8] *Vds*. di W. Gibson, "Neuromante", pag. 54, ed. Ace Book, 1984.

comporta anche diversi rischi circa la "volatilità" delle informazioni memorizzate, la crittografia eventualmente utilizzata e il tipo di approccio alla sicurezza dei dati. [9]

Tuttora questi processi si realizzano e si moltiplicano in modo smisurato attraverso l'uso di internet che, da mezzo di interazione e condivisione, è diventato il centro operativo di gran parte delle operazioni politiche, sociali, economiche e commerciali.

L'incremento di questa interazione tra individui, aziende e istituzioni per scopi finanziari, economici e sociali, ha creato nuove opportunità anche per le attività criminali tra cui: la pornografia, la pedofilia, i virus informatici, l'uso di droghe, l'incitamento alla violenza e al razzismo, la pirateria online, la clonazione di carte di credito, la modifica di smart-card televisive o telefoniche, le molestie a sfondo sessuale, il cyberterrorismo, gli attacchi informatici a banche di dati etc.

Tali attività presenti nel cyberspace vengono definite "cyber crime" e si distinguono dalle classiche attività criminali per il fatto che la vittima non può percepire l'attacco fisicamente perché la maggior parte di esse vengono realizzate nel "dark web", la parte oscura di internet. [10]

Per capire meglio questo concetto bisogna distinguere il "deep web" dal "surface web" ovvero la parte di internet dove sono presenti tutte quelle pagine web e quei contenuti che sono accessibili al grande pubblico e dove le informazioni vengono indicizzate dai motori di ricerca. Questo "strato" di internet è composto essenzialmente da pagine web statiche che risiedono in un server web e sono disponibili ad essere visualizzate dai vari navigatori.[11]

Solo il 4% dei contenuti realmente presenti in internet sono accessibili in questo strato superficiale al di sotto del quale troviamo il deep web, che erroneamente viene accostato a comportamenti criminosi o illegali. In realtà, questo strato di internet è costituito da tutta una serie di contenuti, non direttamente indicizzati dai normali motori di ricerca per vari motivi che sono di solito assolutamente legali e legittimi.

---

[9] In informatica con il termine inglese *cloud computing* si indica un paradigma di erogazione di servizi offerti *on demand* da un fornitore ad un cliente finale attraverso la rete Internet, a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita.

[10] *Cfr.* https://www.kaspersky.it/resource-center/threats/deep-web

[11] http://digicult.it/news/esplorare-il-deep-web-un-dilemma-tra-conoscenza-e-sicurezza/

Lo strato più profondo e segreto del deep web viene chiamato “dark web”, formato dalle famose “dark net” (reti oscure), [12] dove sono presenti contenuti nascosti intenzionalmente ai comuni navigatori accessibili soltanto attraverso appositi strumenti.

I siti presenti in queste reti utilizzano strumenti di anonimato (Tor o I2P) per nascondere la loro effettiva collocazione. Gli strumenti utilizzabili per entrare in queste reti sono dei veri e propri protocolli di connessioni, predisposti per garantire la navigazione attraverso una rete parallela quasi impossibile da tracciare. Per poter capire bene questa suddivisione a strati, è necessario immaginare internet come un grande iceberg: nella punta che fuoriesce dall’acqua possiamo collocare il “surface web”, all'interno del quale navighiamo tutti i giorni, mentre nella parte sommersa, dove comincia a mancare il sole, possiamo collocare il “deep web”, per poi scendere fino in fondo e trovare il “dark web”, ossia la parte oscura.

Il metodo più sicuro e più diffuso per navigare in anonimato attraverso la parte oscura di internet è senza ombra di dubbio il sistema di comunicazione Tor (The Onion Router)[13].

Il suo utilizzo è finalizzato a proteggere la privacy con la possibilità di condurre delle comunicazioni confidenziali senza che vengano tracciate e monitorate le attività degli utenti.

Tor è basato sulla seconda generazione del protocollo The Onion Router e il suo funzionamento è concettualmente molto semplice: i dati che appartengono a una comunicazione non transitano direttamente dal client al server, ma passano attraverso i server di Tor, che agiscono da “Proxy Server”, costruendo un percorso crittografato a strati.

Il traffico viene indirizzato ad almeno tre server diversi prima di inviarlo alla destinazione e per ciascuno dei tre server c'è un livello di crittografia diverso.

I principali obiettivi degli attacchi cyber sono i furti di dati, di denaro e di identità che comportano per le imprese gravi danni non solo economici, ma anche di immagine causati dalla perdita di affidabilità[14].

[12] https://www.itseducation.asia/deep-web.htm

[13] https://www.whoishostingthis.com/blog/2017/03/07/tor-deep-web/ ult. cons. 21/06/2019

Detti attacchi sono favoriti spesso da un livello basso di protezione dei sistemi che, non essendo protetti, subiscono l'uso dei "malware", ossia programmi informatici predisposti per rubare informazioni o recare danni al sistema informatico[15]. Esistono vari tipi di malware e più diffusi e utilizzati sono:

- *ransomware*, un programma che blocca l'accesso ai file dei computer e cui segue la richiesta di un riscatto. È molto diffuso nelle e-mail, link o banned pubblicitari;
- *spyware*, sono programmi che carpiscono informazioni legale alle attività online di un utente (password, ecc.).

I malware sono solo una piccola parte degli strumenti utilizzati dai praticanti del cyber crime e la loro massima diffusione è incentrata nel dark web, dove si è creato un vero e proprio mondo criminale.

In ultimo giova ricordare una recente tipologia di attacco sistemico, il c.d. "Advanced Persistent Threat o APT**"**, che si trova sempre più al centro dell'attenzione per due primati "negativi": [16]

- Il primo è l'elevato danno che sono in grado di arrecare, ulteriormente aggravato dall'alto livello di efficacia che solitamente riescono a conseguire.
- Il secondo è la difficoltà incontrata dalle soluzioni di protezione di tipo più tradizionale nel contrastarle efficacemente.

Questo perché le APT rappresentano una minaccia che non si limita a una semplice intrusione rivolta a inserire un malware ma che punta, invece, a predisporre un attacco continuativo nel tempo che prosegue fino a quando l'attaccante non è riuscito nel suo intento di penetrare all'interno della rete del suo target.

Le motivazioni che spingono i cyber criminali verso questo accanimento possono essere di tipo politico, sociale o finanziario. Un attacco APT non si affida solo alla tecnologia ma anche e soprattutto allo studio dei soggetti che utilizzano le tecnologie, per riuscire a individuare il punto di maggiore vulnerabilità all'interno dell'organizzazione attaccata.

APT è un processo di attacco che segue regole precise e determinate e che è stato

---

[14]Cfr. Cyber Criminalite https://www.international.gc.ca/crime/cyber_crime-criminalite.aspx?
[15]Cfr. What is a Malware https://www.lifewire.com/what-is-malware-2625933 21/06/2019
[16] https://en.wikipedia.org/wiki/Advanced_persistent_threat

studiato e definito tanto da poter essere ricondotto a cinque fasi specifiche:

- **Il livello zero** è quello di preparazione dell'attacco, in cui viene effettuata l'investigazione e sono utilizzati semplici tool per raccogliere le informazioni sull'organizzazione target e sui soggetti indirettamente collegati a essa. Tra questi ultimi possono esserci aziende partner, collaboratori o clienti dell'organizzazione sotto attacco, spesso aggirati con l'uso di tecniche di social engineering al fine di ottenere informazioni che, separatamente, possono sembrare poco rilevanti ma che, se correlate tra loro, possono fornire chiavi per la compromissione della sicurezza.
- **La fase 1** di un attacco mirato è quella di penetrazione iniziale in cui si cerca di installare un malware per ottenere la compromissione del primo sistema (solitamente uno poco importante e quindi più vulnerabile) che sarà deputato a costituire il tassello di partenza per la costruzione di una vera e propria piattaforma di attacco.
- **La seconda fase** prevede la messa a punto della piattaforma di attacco, in cui l'hacker partendo dal primo pc compromesso, riesce a espandere la propria presenza e controllo a una pluralità di sistemi collegati all'interno della rete.
- **La terza fase** prevede un'investigazione sui sistemi interni, resa possibile dal fatto di essere già saldamente presenti all'interno della rete: prevede l'analisi delle vulnerabilità sui server, degli hot-fix installati o della tipologia di comunicazione utilizzata. A questo livello gli hacker sfruttano una backdoor per scaricare informazioni.
- **L'ultima fase** è quella dell'attacco vero e proprio verso il target prefissato, durante la quale vengono sottratte informazioni chiave attraverso la backdoor e in cui l'attacco viene costantemente ripetuto.

La predisposizione di una protezione efficace dovrà quindi confrontarsi con le vulnerabilità associate a ognuna di queste fasi, predisponendo contromisure in grado di operare non solo in modo efficace ma anche sinergico tra loro.[17]

Le citate attività illecite hanno indotto il legislatore alla individuazione di nuove

[17] https://www.tomshw.it/business/trend-micro-promossa-a-prima-azienda-per-la-sicurezza-delle-pmi/

fattispecie di reato con la previsione di sanzioni sempre più efficaci al fine di scongiurare la vasta gamma di pericoli cui gli utenti vanno incontro usando gli strumenti informatici.

In Italia, la prima vera normativa contro il cyber crime è stata la legge 547 del 1993, che ha modificato e integrato le norme del codice penale e del codice di procedura penale relative alla criminalità informatica.

In particolare, circa le norme del codice penale, le fattispecie di reato contemplate dalla citata legge sono:

art. 392: esercizio arbitrario delle proprie ragioni con violenza sulle cose allorché un programma informatico venga alterato, modificato o cancellato in tutto o in parte ovvero sia impedito o turbato il funzionamento di un sistema informatico o telematico;

art. 420: attentato ad impianti di pubblica utilità che si concreti in un danneggiamento o distruzione di sistemi informatici o telematici di pubblica utilità, ovvero di dati, informazioni o programmi in essi contenuti o ad essi pertinenti;

art. 491-bis: falsità in documenti informatici;

art. 615-ter: accesso abusivo ad un sistema informatico o telematico;

art. 615-quater: detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

art. 615-quinquies: diffusione di programmi diretti a danneggiare o interrompere un sistema informatico;

artt. 616, 617-quater, 617-quinquies e 617-sexies: violazione della corrispondenza e delle comunicazioni informatiche e telematiche;

art. 621: rivelazione del contenuto di documenti segreti;

art. 623-bis: trasmissione a distanza di dati;

art. 635-bis: danneggiamento di sistemi informatici o telematici;

art. 640-ter: frode informatica.

Circa il codice di procedura penale, invece, è stato introdotto l'art. 266 bis, che consente l'intercettazione del flusso di comunicazioni relativo a sistemi informatici (nei procedimenti relativi ai reati indicati nell'art. 266) ed è stato modificato l'art. 268 con l'inserimento del comma 3 bis, che detta regole per il pubblico ministero e per i difensori delle parti circa la procedura di acquisizione dei flussi di comunicazioni

informatiche o telematiche.

Successivamente la citata legge 547/93 è stata riformulata dal legislatore italiano con l'adeguamento alla Convenzione di Budapest del 23 novembre 2001, che è il primo accordo internazionale riguardante i crimini commessi attraverso internet o altre reti informatiche, con l'obiettivo di realizzare una politica comune fra gli Stati membri, attraverso l'adozione di una legislazione appropriata, finalizzata a combattere il crimine informatico in maniera coordinata.

Con la ratifica della Convenzione disposta con legge n. 48/2008, sono stati riscritti i reati cibernetici con un'ottica diversa soprattutto in relazione ad un modello di riferimento, che consente di riformulare ed adeguare il quadro dei reati cibernetici alle autorevoli indicazioni provenienti dall'orientamento internazionale in materia.

Circa le modifiche al codice penale il legislatore, muovendo dalle fattispecie già introdotte dalla legge 547/1993 contro la criminalità informatica, ha operato alcuni interventi rispondenti a mere esigenze di riforma del diritto interno di cui:

- la soppressione della definizione di "documento informatico" ai fini penali (art. 491-bis c.p.);[18]
- l'introduzione di due nuovi delitti in materia di firme elettroniche (artt. 495-bis e 640-quinquies c.p.);
- la riformulazione soltanto dei reati di danneggiamento informatico: dal delitto-ostacolo concernente i "dispositivi" maligni (art. 615-quinquies c.p.), alle ben quattro ipotesi incriminatrici distinte a seconda che riguardino dati "privati" (art. 635-bis c.p.) o di "pubblica utilità" (art. 635-ter c.p.), sistemi informatici "privati" (art. 635-quater c.p.) o di "pubblica utilità" (art. 635-quinquies c.p.);
- l'estensione a tutti i reati informatici della responsabilità "amministrativa" delle persone giuridiche (ex d.lgs. 231/2001).

[18] L*'art. 3, comma 1, lett. b), della legge 18 marzo 2008, n. 48 ha abrogato la seconda parte della disposizione che recitava: "A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli". Ora dunque si rinvia alla normativa amministrativa, nello specifico all'art. 1, lettera p), del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) che definisce il documento informatico come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*

Circa il codice di procedura penale, invece, il legislatore ha introdotto ulteriori norme processuali, in merito alla raccolta di prove e indagini informatiche, tenendo conto delle esigenze di immodificabilità degli elementi di prova, che per loro natura rischiano continuamente di essere alterati o resi inutili. In particolare, con le modifiche aggiuntive all'art. 244 c.p.p. è stato previsto, in tema di ispezioni informatiche, che l'autorità giudiziaria possa disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Pertanto, considerato che prima della legge n. 48/2008 non venivano specificati in alcun modo i criteri per l'esecuzione delle perquisizioni ai fini dell'acquisizione della prova, è stato aggiunto all'art. 247 c.p.p. il comma 1 bis con il quale si stabilisce che "*Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*"

Anche in materia di sequestro di corrispondenza è stata prevista, con l'introduzione dell'art. 254-bis c.p.p., la possibilità di sequestrare dati informatici presso i fornitori di servizi informatici, telematici e di telecomunicazioni. Così dicasi per la custodia e la responsabilità del custode delle cose sequestrate (art. 259 comma 2 c.p.p.) e per alcune garanzie circa il sequestro e la custodia di cose deperibili come i dati informatici, che possono essere conservati anche in luoghi diversi dalla cancelleria o segreteria dell'ufficio giudiziario competente (modifica dell'art. 260 comma 2 c.p.p.).

Sempre in tema di perquisizione è stato introdotto all'art. 352 c.p.p. il comma 1 bis con il quale è stato previsto che "*Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni,*

programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi." Inoltre, con la citata legge n. 48 del 2008, è stato integrato il comma 2 dell'art. 354 c.p.p., con il quale si prevede che la polizia giudiziaria nel compiere gli accertamenti urgenti, finalizzati alla conservazione delle tracce e cose pertinenti al reato o ad evitare l'alterazione di luoghi e cose, non vengano alterati, dispersi o comunque modificati anche i dati, le informazioni, i programmi informatici e i sistemi informatici o telematici. In particolare, gli ufficiali di polizia devono adottare le misure tecniche per fare in modo che i dati si mantengano integri all'interno del sistema, effettuandone un duplicato attraverso una procedura che assicuri l'aderenza perfetta all'originale.

Infine, onde evitare che la perquisizione possa risultare eccessivamente lesiva della privacy o invasiva nella sfera personale degli individui, è stato modificato anche l'art. 248 c.p.p. relativo alla richiesta di consegna di dati, informazioni e programmi informatici. In questo caso l'Autorità Giudiziaria, anziché procedere direttamente alla perquisizione, può richiedere al possessore del dispositivo informatico di consegnare i dati o i file da analizzare.

Questo è per sommi capi il quadro dell'attuale disciplina dei reati informatici considerando che, se da un lato il cyberspazio offre l'opportunità di gestire un'infinità di attività (anche di natura professionale o comunque lavorativa), di ottenere in tempo reale notizie di cronaca, informazioni culturali, occasioni di acquisto in negozi virtuali, proposte di lavoro, viaggi organizzati etc., dall'altro, lo stesso spazio è utilizzato da persone senza scrupolo per compiere attività illecite. Infatti, parallelamente al rapido aumento dei rischi dovuti all'uso illecito dei sistemi informatici, sono accresciute in modo esponenziale anche le esigenze di cyber security, ovvero di protezione degli stessi da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti con conseguenti costi sociali non di poco conto. [19]

Tutto ciò perché tali sistemi, collegati in rete, sono diventati per la criminalità nazionale

[19] Il D.P.C.M. 24 gennaio 2013, art. 2, c. 1, lett. i) definisce la cyber security come quella "*condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi*".

e transnazionale un proficuo strumento per i traffici illegali e per il riciclaggio di denaro sporco grazie anche all'online banking, che consente di aprire conti più facilmente e di far seguire al denaro rotte indefinite.

Un'attività illecita sviluppatasi, come abbiamo visto, soprattutto nel "*dark web*", detto anche "lato oscuro del web", che è inaccessibile ai motori di ricerca perché appoggiato su reti sovrapposte a internet (*darknet*) ed è una base di supporto soprattutto per la criminalità organizzata, capace di gestire le tipiche attività illegali in maniera molto più veloce e sicura.[20]

Una criminalità sempre più specializzata ed esperta che fa uso anche di speciali software e della steganografia per occultare gli indirizzi IP e per nascondere i messaggi attraverso i pixel delle immagini digitali. [21]

Tutte le Forze di Polizia sono impegnate costantemente a livello nazionale ed internazionale per prevenire e reprimere reati come la pedopornografia, la violazione dei dati personali, le molestie, gli attacchi alle infrastrutture critiche e altre fattispecie previste dalla normativa vigente,[22] ma soprattutto ora per contrastare il *cyber terrorismo*, che riguarda le operazioni condotte in rete dai terroristi (propaganda, arruolamento di potenziali proseliti, raccolta denaro, organizzazione attentati.

Anche i responsabili dell'intelligence nazionale ed internazionale pongono costantemente l'accento sulla necessità di utilizzare software sempre più sofisticati ed efficaci per individuare all'interno del web tutte le informazioni ed i collegamenti tra gruppi terroristici al fine di prevenire attacchi contro persone che, per le modalità di esecuzione, non hanno nessuna opportunità di difendersi. Di qui il problema di tracciare ed individuare le attività terroristiche attraverso la rete e di trovare, anche

---

[20] Vedasi di Enrico Marro "*Ecco il lato oscuro del web e che cosa nasconde*", il Sole 24 Ore del 4 dicembre 2016.

[21] Vedasi voce Wikipedia: "*La steganografia può trovare uso in ogni forma di comunicazione, è sufficiente che mittente e destinatario abbiano concordato un codice non vincolato ai normali simboli alfabetici. Ad esempio, un mittente potrebbe inviare un file di immagine innocuo e regolare il colore di ogni centesimo di pixel per corrispondere a una lettera nell'alfabeto. La modifica è così sottile che qualcuno che non lo sta cercando in modo specifico è improbabile che noti la modifica*."

[22] Vedasi Rapporto della Polizia Postale e delle Comunicazioni sull'attività svolta nel 2018 dove si legge che: "L'ultima modalità della violenza sulle donne è il fenomeno del c.d. stupri virtuali: all'interno di gruppi chiusi i partecipanti di sesso maschile condividono foto, ricercate sui social o copiate da contatti WhatSapp, di donne ignare, ritratte nella loro vita quotidiana, dando poi sfogo a fantasie violente e comportamenti offensivi."

dal punto di vista legislativo, le soluzioni adeguate al fine di contrastare più efficacemente l'estremismo islamico e prevenire il fenomeno della radicalizzazione online. [23]

1.3 La guerra cibernetica

Il termine guerra cibernetica (noto nell'ambito operativo militare del mondo anglofono come *cyberwarfare*) è l'insieme delle attività di preparazione e conduzione di operazioni di contrasto nello spazio cibernetico. Si può tradurre nell'intercettazione, nell'alterazione e nella distruzione dell'informazione e dei sistemi di comunicazione nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione. [24]

A differenza dei "normali" attacchi informatici, si tratta di azioni compiute con specifici scopi politico-militari da speciali apparati militari o da organizzazioni cyber criminali finanziate, comunque, da entità governative.

Si presentano come vere e proprie operazioni militari combattute all'interno del cyberspazio che, per come è concepito, può essere suddiviso in tre differenti livelli:

1) nel livello fisico troviamo computer, server, dispositivi informatici in genere, cavi, satelliti e altre infrastrutture necessarie a mantenere attive le linee di comunicazione;
2) al livello sintattico appartengono gli applicativi e le altre soluzioni software che forniscono le istruzioni per il corretto funzionamento dei sistemi presenti a livello fisico;
3) nel livello semantico sono incluse le interazioni umane con i sistemi del livello fisico e sintattico e con le informazioni che generano.

---

[23] Secondo la definizione dell'FBI, il cyberterrorismo è un "*premeditato attacco a sfondo politico, da parte di gruppi subnazionali o agenti clandestini, contro i mezzi d'informazione, sistemi, dati e programmi informatizzati, che si traduce in violenza contro obiettivi non combattenti*". Vedasi anche sul tema di Fabio Ghioni e Roberto Preatoni "*Ombre Asimmetriche – la guerra cibernetica e i suoi protagonisti*", Robin Edizioni, Roma 2005.

[24] Cfr. in Riccardo Busetto, *Il dizionario militare: dizionario enciclopedico del lessico militare*, Bologna, 2004, Zanichelli,

Anche se in modo diverso, tutti e tre i livelli sono vulnerabili e, dunque, possibili obiettivi della cyberguerra[25].

Gli attacchi al livello fisico possono essere condotti attraverso "normali" operazioni di guerra, utilizzando armi e strategie convenzionali. Ciò porta alla distruzione fisica delle varie infrastrutture hardware o di telecomunicazione cosi da renderle inutilizzabili e paralizzarle. Attacchi di questo tipo sono avvenuti nella guerra dell'ex Jugoslavia nel 1999 o della seconda Guerra del Golfo, quando le infrastrutture governative in Serbia e in Iraq vennero distrutte e rese inutilizzabili.

Gli attacchi a livello sintattico, pur perseguendo lo stesso obbiettivo degli attacchi del livello precedente, prevedono l'utilizzo di sole armi informatiche. In questo caso i sistemi computerizzati sono attaccati utilizzando malware di vario tipo, a seconda del danno che si vuole procurare: virus o criptoloker che possono essere utilizzati per distruggere tutti i dati presenti negli hard disk;[26] trojan e spyware per infiltrarsi nei sistemi informatici del nemico e trafugare dati e informazioni oppure spiarne mosse e comportamenti. Allo stesso modo anche gli attacchi DDoS possono essere utilizzati per rendere inservibili le infrastrutture comunicative dell'avversario.[27]

Gli attacchi a livello semantico possono essere considerati come una "categoria" di attacchi di social engineering. In questo caso, gli attaccanti provano a manipolare gli avversari con campagne phishing attraverso i social network al fine di impossessarsi di dati di grande rilievo.

Negli ultimi anni la guerra cibernetica è diventata una delle forme di guerra più efficaci ed è utilizzata con l'intento di infliggere danni a chi presiede i governi e le economie ritenute dannose; il punto di forza è che questo tipo di guerre non comportano costi elevatissimi come quelle dove si adottano le armi convenzionali. La natura segreta della guerra cibernetica ci riporta all'era dello spionaggio durante la guerra fredda. Le

---

[25] In lingua inglese guerra si traduce con due termini: war, che indica più generalmente il concetto, lo stato, la condizione; warfare si riferisce invece oltre a ciò anche alla condotta della guerra e alle operazioni militari.

[26] "*CryptoLocker" è un trojan comparso nel tardo 2013, perfezionato poi nel maggio 2017. Questo malware è una forma di ransomware infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione. Symantec stima che circa il 3% di chi è colpito dal malware decide di pagare. Alcune vittime dicono di aver pagato il riscatto ma di non aver visto i propri file decriptati*." Vds. *https://it.wikipedia.org/wiki/CryptoLocker*

[27] Vds. https://it.wikipedia.org/wiki/Denial_of_service

stime indicano che ben 120 paesi hanno sviluppato dei sistemi per utilizzare internet come arma d'attacco.

La Cina, ad esempio, ha uno degli eserciti più avanzati che opera nel cyber spionaggio con stima ad oggi di 100.000 unità ed è considerata il nemico pubblico numero uno quando si parla di guerra cibernetica.[28]

Già 10 anni fa gli hacker cinesi avevano sabotato i sistemi informatici di Google e altre 35 grandi compagnie americane. L'obiettivo dell'attacco, passato alle cronache come Operazione Aurora, era sottrarre informazioni sensibili sull'*intelligence* e sui cinesi che vivevano negli Usa. Gli attacchi continuarono nel 2010 contro grandi colossi industriali, come Westinghouse nel settore nucleare, e U.S. Steel, secondo gruppo americano dell'acciaio. Si scoprì che dietro gli attacchi informatici c'era una sezione segreta dell'esercito cinese, con sede a Shanghai, che agiva sotto lo pseudonimo di Ugly Gorilla (oggi ufficialmente conosciuta come Unità 61398). Gli attacchi cibernetici cinesi contro l'economia americana sono stati talmente frequenti e diffusi che nel 2014, James Comey, allora direttore dell'FBI dichiarò: "*Possiamo distinguere le grandi aziende americane in due categorie: quelle che sanno di esser state attaccate dagli hacker cinesi e quelle che ancora non lo sanno.*" Secondo l'FBI, tutti o quasi i big dell'economia Usa erano stati hackerati dalla Cina.

La prima *cyber-escalation* si concluse nel 2015, quando Obama e Xi Jinping raggiunsero un accordo sulla *cybersecurity* per ridurre lo spionaggio economico e il furto di informazioni sensibili. Tra i risultati dell'intesa: una "linea rossa" Washington-Pechino per le comunicazioni d'emergenza e due incontri annuali per la cooperazione sul cyberspazio.

La competizione tra Usa e Cina sul futuro del web è tornata alla ribalta lo scorso dicembre, con l'arresto di Meng Wanzhou, figlia del fondatore di Huawei. Secondo le agenzie di *intelligence* Usa, Huawei non è un gruppo indipendente dal regime cinese e le sue reti potrebbero esser già state usate per cyber-spionaggio e attacchi cibernetici. I dubbi derivano dal fatto che Ren Zhengfei, fondatore di Huawei, era un ingegnere dell'Esercito Popolare di Liberazione e oggi è un potente membro del partito

[28] *Cfr.* C. S. Gray, Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling, Strategic Studies Institute, Carlisle PA, April 2013

comunista cinese. Inoltre, dando attuazione al principio della *national cyber sovereignty* annunciato da Xi Jinping nella Dichiarazione di Wuzhen, dal 2017 la legge cinese impone alle compagnie delle telecomunicazioni di partecipare a operazioni di *intelligence* se richiesto dal Governo. Condizioni che hanno spinto Washington ad allertare gli alleati a non servirsi di Huawei per i propri network 5G, mentre dalle dichiarazioni di Ken Hu, *chairman* di Huawei, si scopre che la società cinese avrebbe già accordi con 66 Paesi. Si comprende anche perché il Pentagono ha voluto bloccare le collaborazioni sul 5G tra Huawei e i giganti digitali Usa come AT&T e Verizon.

La reazione di Washington non riguarda solo il caso Huawei. A preoccupare la Casa Bianca è il rischio di vedere l'Occidente nella morsa digitale cinese. Pechino ha infatti lanciato politiche e cantieri internazionali per unire il mondo con progetti non solo economico-finanziari e commerciali (come la Banca asiatica d'investimento per le infrastrutture o la Belt and Road Initiative), ma anche tecnologici e informatici. Sia nel 13° Piano quinquennale sia nel documento Made in China 2025, il Governo cinese ha dichiarato "strategici" gli interessi legati alle tecnologie per il cyberspazio. Se la Cina dovesse raggiungere questi traguardi, un numero enorme di informazioni sensibili saranno gestite da tecnologie cinesi come quelle dei social, delle dinamiche elettorali, delle transazioni finanziarie, delle innovazioni industriali, fino a quelle dei settori della difesa.

Giova ricordare, che nel "Rapporto sulle minacce globali" pubblicato a gennaio 2019 dalle agenzie federali Usa dell'Intelligence Community (Worldwide Threat Assessment), oggi il terrorismo è solo la quarta minaccia alla sicurezza nazionale perché ai primi posti ci sono gli attacchi cibernetici**,** le interferenze nella politica nazionale e il rischio nucleare. Nel citato rapporto si legge che i maggiori pericoli in termini di *cybersecurity* provengono da Russia e Cina e quest'ultima avrebbe già i mezzi tecnologici per bloccare o distruggere infrastrutture fisiche nel territorio Usa, come la rete di trasporto del gas.

La nuova *cyber-escalation* potrebbe attenuarsi o degenerare in vista del possibile accordo commerciale fra Pechino e Washington, ma restano aperti tanti altri fronti dello scontro tecnologico. Tra i motivi che hanno spinto gli americani ad alzare i livelli

di guardia è la rivoluzione del *quantum computing* e le applicazioni dell'intelligenza artificiale (Aper scopi militari.

L'esempio più importante è il *multidomain command and control*, tecnologia che combina in tempo reale i dati di tutti gli ambiti delle operazioni di attacco e difesa in una visione olistica (senza tralasciare il cyberspazio).

La questione più delicata è quella della gestione trasparente e neutrale delle tecnologie cinesi che stanno rinnovando le infrastrutture del web dalle quali passeranno infiniti flussi di informazione. Saranno usate per cooperare con o contro gli Usa? Cosa succederà in caso di attacchi alla democrazia americana? Il tema è molto delicato, nonostante l'inchiesta guidata da Robert Mueller abbia acclarato l'assenza di ingerenze nella campagna elettorale del 2016. Pensiamo al caso del *deepfake*, cioè la manipolazione iperrealistica di video mediante nuove funzioni dell'Artificial Intelligence che creerà le prossime ondate di disinformazione sul web. Gli esperti del *deepfake* spiegano le capacità di inganno di questa tecnologia: "non basterà vedere per credere". La Defense Advanced Research Projects Agency sta sviluppando algoritmi capaci di smascherare il *deepfake*. Tuttavia, sono sforzi vani se la rete, e i suoi supporti tecnologici, si riveleranno contrari alle manovre difensive Usa o non collaborativi. Gli Usa e l'Occidente possono fidarsi delle tecnologie *made in China*?

Trump ha dato grande attenzione alla *cybersecurity*, firmando pochi mesi dopo il suo insediamento un ordine esecutivo per rafforzare la difesa informatica delle infrastrutture critiche. Nonostante le nuove misure di sicurezza, secondo Rob **J**oyce della National Security Agency, l'accordo del 2015 sarebbe stato violato dalla Cina. Ecco perché, lo scorso settembre, con la pubblicazione della National Cyber Strategy, la Casa Bianca è tornata ad accusare Pechino. Nello stesso mese, l'attuale Consigliere per la sicurezza nazionale dell'amministrazione Trump, John R. Bolton ha dichiarato che il Presidente aveva siglato un ordine esecutivo "classificato" per dare più potere alla National Security Agency e al Cyber Command. Bolton si è limitato a dire che Trump ha concesso maggiore libertà d'azione all'*intelligence* per estendere e velocizzare le *cyber operation* necessarie per la difesa della sicurezza nazionale, forse anche confidando in un effetto deterrenza.

Gli Usa stanno dando un segnale chiaro al mondo: mentre la Cina costruisce il suo impero per il controllo del cyberspazio Washington non starà a guardare e i sistemi di difesa americani sono pronti alla prima vera grande guerra dell'era digitale. A riguardo, uno spunto utile lo offre Graham T. Allison, della Harvard Kennedy School e autore del libro *Destinati alla guerra. Possono l'America e la Cina sfuggire alla trappola di Tucidide?* Ricordando Tucidide, il dilemma delle relazioni fra Cina e Usa appare evidente: l'ascesa della potenza dell'una e la paura dell'altra rese la guerra inevitabile. Lo scontro tra *raising power* cinese e *ruling power* americano è iniziato da tempo e ora che l'accordo del 2015 è di fatto superato, non sappiamo fin dove si spingeranno Pechino e Washington.[29]

Come abbiamo già precedentemente accennato, un altro paese pesantemente coinvolto e considerato una potenza di guerra cibernetica è la Russia, alla quale è stata attribuita la vittoria a sorpresa di Trump alle elezioni presidenziali degli Stati Uniti. Per tale operazione l'esercito informatico di Putin aveva preso di mira ben 39 stati degli Stati Uniti che non sono risultati le uniche vittime.

Ad esempio, già nel 2018 l'Ucraina ha accusato la Russia di attacchi mirati ai propri sistemi di sicurezza, un allarme che si è diffuso a livello globale arrivando a colpire società situate in Australia.

Anche la Corea del Nord oltre a sfoggiare il suo arsenale militare, ha a disposizione anche un arsenale informatico: un cyber esercito comunemente noto come "Unità180", operativo all'interno della principale agenzia di spionaggio della Corea del Nord.

Gli obbiettivi dell'Unità180 comprendono Stati Uniti e Corea del Sud ma anche altri Paesi. Infatti, da alcune indagini sono scaturite prove secondo le quali la Corea del Nord sia implicata in un attacco informatico su scala globale di tipo "ransomware", noto come "WannaCry", che ha infettato oltre 300.000 computer in 150 Paesi.

L'attacco è riuscito addirittura a infettare i sistemi informatici degli ospedali del Regno Unito, causando l'annullamento di operazioni e la perdita di dati.[30]

[29] Di Matteo Laruffa vds. *https://eastwest.eu/it/retroscena/cyberspazio-guerra-usa-cina*

[30] Cfr. *The National Defense Strategy of the United States of America*, Washington D.C., September 2002, cit.p. 1. URL: http://www.state.gov/documents/organization/63562.pdf [consultato il 22-06-2019]

La Corea del Nord è stata collegata ad un attacco informatico alla Banca Centrale del Bangladesh dove sono stati rubati 81 milioni di dollari. Questo attacco era finalizzato a reperire i fondi necessari per sviluppare gli armamenti nucleari.

Oggi, relativamente alle capacità di difesa e di attacco cyber war, gli Stati Uniti sono al primo posto sia per la professionalità del proprio esercito cibernetico sia per le strutture informatiche in dotazione. La seconda potenza a livello informatico è inaspettatamente Israele che recentemente ha formato un'alleanza con gli Stati Uniti per monitorare bene l'Iran e i suoi progressi in campo nucleare e informatico. Da questa alleanza è scaturito il primo e il più famoso caso di guerra cibernetica, che risale all'anno 2010 e prende il nome di "Stuxnet", uno dei virus più distruttivi mai realizzati nella storia.

In particolare, siccome il programma nucleare dell'Iran già dal 2006 stava preoccupando gli Stati Uniti, Bush diede l'ordine segreto di realizzare questo cyber attacco nella centrale nucleare di Natanz. Di conseguenza, le centrifughe (più di 1000) dedicate all'arricchimento dell'Uranio235 impazzirono andando fuori controllo (da 1064 giri/minuto passarono a 1410 giri/minuto) ed esplosero.

Il compito di sferrare l'attacco venne assegnato all'N.S.A (National Security Agency) in collaborazione con l'Unity8200 dell'Israel Defence Force. In poco meno di 4 anni venne realizzato appunto Stuxnet, che era in grado di agire sui PLC Siemens Simatic S7-300, adibiti al controllo delle centrifughe. Dato che le centrali Iraniane non erano presenti in rete, gli attaccanti si inserirono nella rete locale per diffondere il virus ed è stato assodato che l'attacco partì dalla centrale stessa attraverso una chiavetta USB infetta. Sempre nel 2010 versioni potenziate di Stuxnet attaccarono l'Iran infettando oltre il 60% di tutti i computer. Successivamente il virus, essendo stato potenziato da Israele per facilitarne la diffusione, andò fuori controllo causando danni importanti sulle reti diffuse in internet.

Dalle analisi fatte venne fuori che Stuxnet era una vera e propria macchina da guerra (cibernetica) poiché aveva delle caratteristiche mai viste prima: sfruttava 4 esploit chiamati "zero-day" che ancora non erano noti alle società di sicurezza, utilizzava un falso certificato Microsoft per sembrare autentico, non destava sospetti e non entrava in azione se non aveva individuato l'obiettivo per il quale era stato realizzato. Infine,

restituiva un falso feedback di controllo senza segnalare allarmi per far credere ai controllori della centrale che tutto stava procedendo senza problemi [31].

Come abbiamo visto, l'attuale quadro della guerra cibernetica è alquanto complesso e sarà ancora più complicato per l'uso dei diversi sistemi di attacco e di difesa intelligenti che potrebbero, qualora fuori controllo, causare danni inimmaginabili.

In ultima analisi possiamo definire la "guerra cibernetica" come "*un'azione da parte di uno Stato atta a penetrare i sistemi informatici o le reti di un altro Stato con la finalità di causare danni o distruzione*" [32].

In tal senso, dietro alla messa in atto di un'offensiva cibernetica vi è la ben precisa intenzione di colpire il nemico arrecandogli dei danni concreti, nel perseguimento di obiettivi politico-strategici più ampi; [33] lo strumento cibernetico è utilizzato per costringere chi subisce l'attacco a piegarsi alla volontà di chi lo attua ed un tale potenziale coercitivo, a partire dal punto di vista economico/organizzativo, può possederlo soltanto uno Stato (che poi questo effettui l'attacco cibernetico "direttamente" o, come spesso accade, preferisca delegare, in particolare nel tentativo di sottrarsi ad eventuali responsabilità davanti alla comunità internazionale, è un altro discorso).[34]

---

[31] Cfr. *Zero Day Vulnerability* URL: https://www.sciencedirect.com/topics/computer-science/zero-day-vulnerability [consultato il 22-07-2019]

[32] Clarke, Richard A., Knake, Robert K., Cyber War. The Next Threat to National Security and What to do About It, New York, Harper Collins Publishers, 2010.

[33] Gori, Umberto, "Cyberspazio e relazioni internazionali: implicazioni geopolitiche e geostrategiche", in Gori Umberto e Lisi Serena (a cura di), Information Warfare 2012. Armi cibernetiche e processo decisionale, Milano, Franco Angeli editore, 2013.

[34] Martino Luigi "*La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica*" Centro Studi Strategici, Internazionali e Imprenditoriali (CSSII), febbraio 2014.

CAPITOLO II

La minaccia cibernetica in Italia

2.1 – L'impatto degli attacchi cyber in Italia

In Italia, la pubblica amministrazione e le aziende sono seriamente a rischio di cyber attacchi. Lo confermano non solo gli esperti di cyber security dell'intelligence ma anche l'analisi di Yoroi-Cibaze, che ha analizzato le ricadute nel nostro Paese nel caso "Collection 1" e di quelle successive nonché il rapporto Clusit 2019.

Circa l'analisi dell'intelligence, nel documento di sicurezza nazionale del 2018, dedicato alla minaccia cibernetica in Italia, emerge un numero complessivo di azioni ostili più che quintuplicato rispetto al 2017, prevalentemente in danno dei sistemi informatici di pubbliche amministrazioni centrali e locali (72%).

Un'analisi più approfondita degli eventi, che hanno interessato i soggetti pubblici, attesta un incremento pari a oltre sei volte (+561%) rispetto all'anno precedente.

È stato rilevato, in particolare, un sensibile aumento di attacchi contro reti ministeriali (24% delle azioni ostili, in aumento di 306 punti percentuali) e contro infrastrutture IT riconducibili ad enti locali (39% del totale del periodo in esame, con una crescita in termini assoluti pari a circa 15 volte).

Le citate attività sono da ascrivere in larga parte ad azioni di stampo hacktivista, tra cui la richiamata campagna "#OpBlackWeek", volta a screditare le Istituzioni nazionali, ad opera delle principali crew attive nel panorama italiano: Anonymous Italia, LulzSec ITA ed AntiSec ITA.

A tali formazioni vanno attribuiti anche gli attacchi contro risorse web e social media delle principali forze politiche nazionali (assimilate, ai fini della presente rilevazione, ai "soggetti pubblici" ed inserite nella categoria "Altro", di cui rappresentano circa un quarto del totale), impiegati per veicolare messaggi di dissenso e protesta, specie in prossimità della tornata elettorale del 4 marzo.

Ai medesimi collettivi è da ricondurre pure un cospicuo numero di attacchi – più che triplicati rispetto al 2017 – in danno di soggetti privati, afferenti per lo più i settori delle telecomunicazioni (6%) e dei trasporti (6%, triplicati rispetto al 2017), con particolare focus verso operatori del settore energetico (11%) e relativi fornitori (questi ultimi computati nell'ambito della categoria "Altro"), in linea con il rilancio internazionale delle campagne "#OpNuke" ed "#OpGreenRights": la prima, nata come forma di

protesta per lo sviluppo dell'energia nucleare, la seconda, attuata in favore dell'impiego di fonti di energia sostenibili.

Per ciò che concerne gli attori ostili, il trend del 2018, in linea di continuità con quello degli ultimi anni e in coerenza con quanto appena descritto, ha identificato l'hacktivismo come la minaccia più consistente (66%), almeno in termini numerici. Tale dato va ascritto alla fase di particolare fermento che ha interessato i già citati Anonymous Italia, LulzSec ITA ed AntiSec ITA, caratterizzata da rinnovata capacità di pianificazione delle campagne ostili e dalla ricerca di una maggiore indipendenza da risorse tecnologiche di terze parti.[35]

L'analisi di Yoroi-Cibaze, invece, è riferita a raccolte di dati trafugati, provenienti da innumerevoli fonti tra cui molte anche in Italia. Questo archivio comprende centinaia di milioni di e-mail e password trafugate, disponibili all'interno di piazze di scambio e mercati del cybercrime. Sono sette "collezioni" per oltre 87 gigabyte, nel cui interno ci sono riferimenti a ben 219 portali web italiani con il dominio ".it". La loro presenza all'interno dei "dump" si colloca al sesto posto della classifica relativa ai top level domain nazionali. [36]

Questo posizionamento fornisce prove sulla permeabilità del panorama cyber del nostro Paese, che nel corso degli anni ha subito attacchi e intrusioni da parte di attori di minaccia in ambito criminale, con ordini di grandezza comparabili rispetto a nazioni storicamente più digitalizzate.

In ultimo, anche il rapporto Clusit ha rivelato un drastico aumento degli attacchi informatici. Dal 2011 al 2017 si sono registrati in media 88 attacchi mensili, nel 2018 il numero è salito a 129. Questa impennata segna un aumento del 38% rispetto agli attacchi del 2017 che, complessivamente, sono minori di quelli avvenuti in un solo mese del 2018. Per il 2019 sono previsti una media di circa 150 cyber attacchi mensili.

---

[35] Vds.Relazione sulla politica dell'informazione per la sicurezza 2018

[36] "*Il dump, in informatica, è un elemento di un database contenente un riepilogo della struttura delle tabelle del database medesimo e/o i relativi dati, ed è normalmente nella forma di una lista di dichiarazioni SQL. Tale dump è usato per lo più per fare il backup del database, poiché i suoi contenuti possono essere ripristinati nel caso di perdita di dati. I database "corrotti" (ossia, i cui dati non sono più utilizzabili in seguito ad una modifica "distruttiva" di qualche parametro di formato) possono spesso essere rigenerati mediante l'analisi del dump. I dumps di database sono spesso pubblicati dai progetti di software libero o di contenuto libero, in modo tale da consentire il riutilizzo o il forking dei database cui si riferiscono.*" Vds. *https://it.wikipedia.org/wiki/Dump*

Da tener presente che nel 2018 in Europa le aziende non erano ancora obbligate per legge a rilevare i dati degli attacchi e, a seguito dell'obbligo poi previsto dal Cybersecurity Act [37], nello stesso anno è stato registrato rispetto agli anni passati un aumento degli attacchi gravi con finalità di cybercrime (+43,8%) e di quelli riferibili ad attività di cyber espionage (+57%)[38]. Questi dati mostrano come le tecnologie in continua evoluzione vengano sfruttate da malintenzionati per compiere furti di informazioni. Restano i dati il principale bersaglio di hacker, prediligendo, così, l'uso di malware all'impiego di cryptominers[39] per l'acquisizione illegale di cryptovalute[40]. Gli attacchi stealth tramite Atp (+55,6%) e 0-Day (+66%) hanno fatto registrare un forte aumento d'impiego. Questo aumento ha fatto allarmare gli esperi perché queste tecniche sono molto costose e impegnative e gli hacker tendono a utilizzarle il meno possibile. Un cambio di abitudini negli attacchi potrebbe significare un repentino e necessario adattamento degli attuali standard di difesa. Gli esperti del Clusit hanno più volte sottolineano la necessità di suddividere gli attacchi in base alla loro gravità e soprattutto in base ai loro bersagli. Tramite queste suddivisioni gli esperti di cybersecurity possono pianificare una miglior difesa a seconda del tipo di attacco e alla tipologia di possibili vittime. Sono stati riscontrati degli aggravamenti degli effetti negli attacchi, poiché quelli critici sono aumentato del 7%. Gli attacchi con impatto definito medio diminuiscono del 10% e quelli di categoria alta rimango quasi invariati con un aumento del 2%; vi è quindi una tendenza da parte dei cyber criminali a compiere attacchi più elaborati. Da gennaio a giugno del 2019 il 37% degli smart building è stato vittima di un attacco informatico, rischiando di vedere compromessi i sistemi di automazione negli edifici intelligenti. Nella maggior parte dei casi non si è trattato di minacce sofisticate, pur essendo offensive in grado di intervenire sui sensori che governano il funzionamento automatizzato di ascensori, impianti di vario genere come quello di ventilazione, di climatizzazione, di elettricità, di fornitura idrica, di video

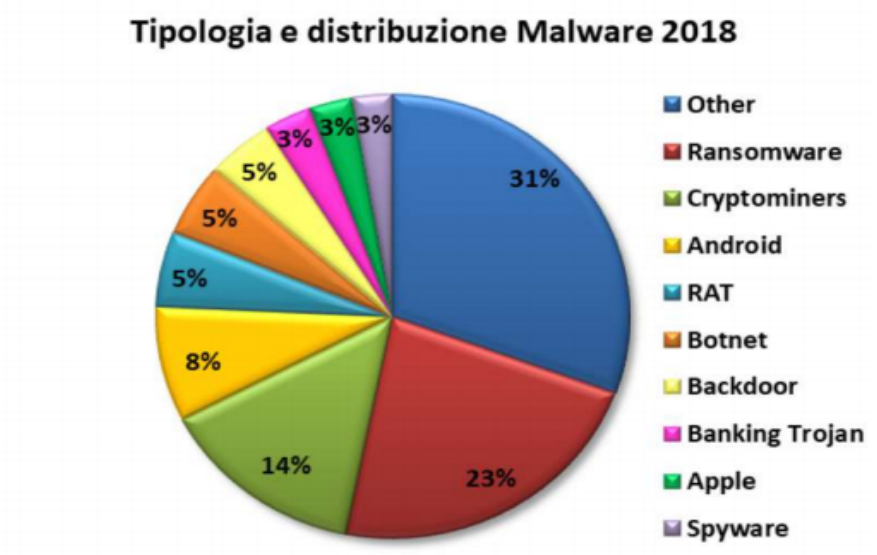
[37] È stato pubblicato sulla Gazzetta ufficiale dell'Unione europea il testo definitivo del Cybersecurity Act, il Regolamento (UE) 2019/881 del Parlamento Europeo.

[38] L'Atto o la pratica di ottenere segreti e informazioni senza il permesso e la conoscenza del detentore delle informazioni attraverso internet mediante l'uso di server proxy.

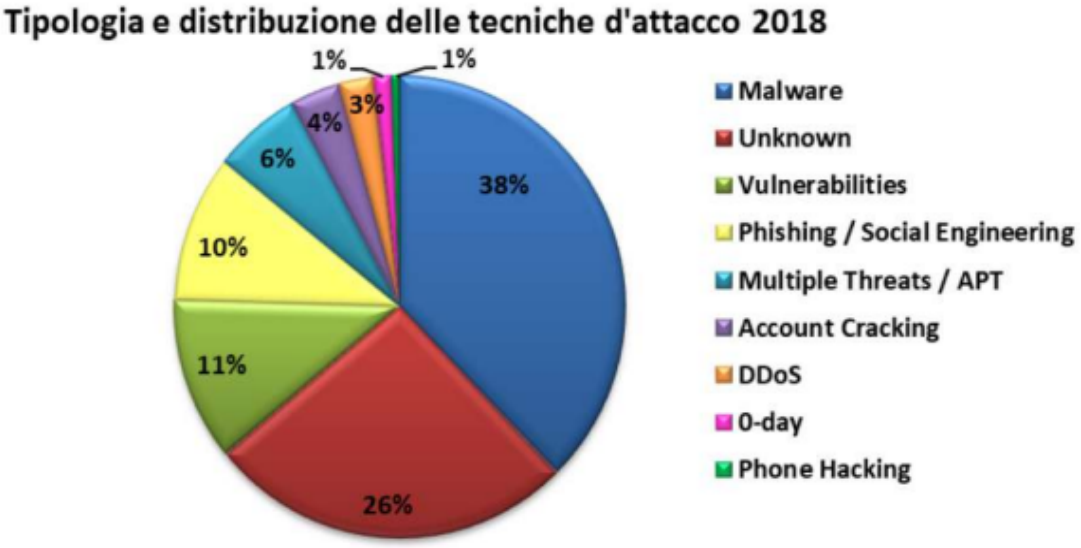
[39] Processo di mining bitcoin che utilizza un datacenter remoto con potenza di elaborazione condivisa.

[40] Rappresentazione digitale di valore basata sulla crittografia.

sorveglianza, o allarmi antincendio e sistemi di controllo degli accessi e molte altre informazioni critiche e sistemi di sicurezza.



Fonte:© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia



Fonte:© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

L'11% dei computer la gestione dei smart build è stato attaccato da spyware, il 10% sono stati attaccati da worm mentre il 7.8% è stato oggetti di tentativi di phishing e solo il 4.2% è stato vittima di ransomware. Il 26% delle minacce proveniva da Internet mentre il 10% dei casi responsabili sono stati i supporti rimovibili. L'Italia è al primo posto con la percentuale più alta di attacchi subiti ai computer per i smart building con il 48,5%.

2.2 - Sicurezza Nazionale e minaccia cibernetica.

Il panorama della minaccia continua a caratterizzarsi per l'elevata rimunerativitá dello strumento cyber per gli attori ostili, in ragione dell'ampia disponibilità di tool offensivi e dei bassi livelli di rischio operativo. Dal monitoraggio delle Tecniche, Tattiche e Procedure (TTP) utilizzate è emerso un elevato livello di complessità e sofisticatezza delle azioni, l'uso combinato di strumenti offensivi sviluppati ad hoc con quelli presenti nei sistemi target impiegati in modo ostile, nonché il "riuso" di oggetti malevoli (malware) allo scopo di ricondurne la matrice ad altri attori (cd. operazioni false).[41]

In tale contesto, lo sforzo più significativo posto in essere dai responsabili dell'intelligence ha riguardato il contrasto di campagne di spionaggio digitale, gran parte delle quali verosimilmente riconducibili a gruppi ostili strutturati, contigui ad apparati governativi o che da questi ultimi hanno ricevuto linee di indirizzo strategico e supporto finanziario. Quanto alle finalità perseguite, gli attacchi hanno mirato, da un lato, a sottrarre informazioni relative ai principali dossier di sicurezza internazionale e, dall'altro, a danneggiare i sistemi informatici di operatori, anche nazionali, attivi nello Oil&Gas, nonché quelli di esponenti del mondo accademico italiano, nell'ambito di una campagna globale mirante a profilare settori d'eccellenza di università e centri di ricerca. Sul fronte delle infrastrutture di attacco, i gruppi responsabili di azioni di cyber-espionage hanno proseguito nell'impiego di servizi IT commerciali (domini web, servizi di hosting, etc.), forniti da provider localizzati in diverse regioni geografiche che, anche per rendere difficoltoso il processo di individuazione/attribuzione, mentre, sul versante dei vettori, è rimasto elevato il ricorso alle tecniche di spear-phishing, che hanno ancora una volta garantito alti tassi di successo alle azioni intrusive, attesa pure la persistente, scarsa consapevolezza delle vittime.[42] Tra queste ultime si sono annoverate, non di rado, figure apicali di Istituzioni e di primarie realtà del settore privato, nei confronti delle quali l'attaccante ha svolto attività di profilazione funzionali rispetto ad azioni di social engineering e, in alcuni casi, al reclutamento di natura convenzionale. Si sono confermati, inoltre, target privilegiati i soggetti coinvolti nella

[41]Cfr. *Relazione sulla politica dell'informazione e per la sicurezza* URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf

[42]Ibidem

supply chain ICT – tra cui Managed Service Provider (MSP)[43], società di consulenza, produttori/rivenditori di tecnologie e altri operatori che forniscono supporto tecnologico a terzi destinatari di un volume di attacchi accresciuto rispetto al passato.

Qui, l'attaccante ha colpito le infrastrutture tecnologiche degli obiettivi finali tramite la violazione preventiva di quelle dei fornitori, abusando sovente anche delle relazioni di fiducia connesse al rapporto contrattuale. Attenzione è stata rivolta anche alla cd. minaccia ibrida[44], considerata quale impiego combinato di strumenti convenzionali e non, le cui traduzioni operative sono risultate amplificate grazie alla digitalizzazione che ha interessato ogni aspetto della vita sociale, arrivando ad esplicitarsi anche in operazioni di influenza/ingerenza poste in essere per condizionare il corretto svolgimento di fondamentali dinamiche dei processi democratici. Anche qui, senza il rischio di esposizioni per l'attaccante, attesa la sua capacità di mantenersi al di sotto di una soglia rilevabile di responsabilità, e con l'impiego di un quantitativo di risorse notevolmente inferiore rispetto a quelle necessarie per condurre azioni convenzionali.

La cyber intelligence nazionale, al pari di quanto fatto dalle comunità intelligence dei principali partner internazionali, ha istituito agli inizi del 2018 un esercizio ad hoc teso a cogliere, all'interno del perimetro definito dal quadro normativo vigente, eventuali indizi di influenza, interferenza o condizionamento del processo elettorale del 4 marzo. Tale esercizio è stato riattivato nel mese di novembre in vista dell'appuntamento per il rinnovo del Parlamento europeo.

Quanto all'hacktivism, nel cui ambito hanno continuato ad operare sigle minori sotto l'egida del più noto collettivo digitale "Anonymous Italia", le sortite più significative hanno riguardato l'avvio, ovvero il proseguimento di una serie di operazioni, tra cui "#OpBlackWeek"[45], con la pubblicazione online di dati estrapolati da sistemi di istituzioni operanti nei settori dell'Istruzione, del Lavoro, della Sanità, dei Sindacati, delle Forze dell'ordine, dei Comuni e delle Regioni.

---

[43] Servizio che viene preso in carico, erogato e controllato da un fornitore esterno.

[44] Cfr. *Minacce ibride, che sta facendo l'Europa per la sicurezza e il ruolo dell'Italia* URL: https://www.agendadigitale.eu/sicurezza/minacce-ibride-che-sta-facendo-leuropa-per-la-sicurezza-e-il-ruolo-dellitalia/

[45] Cfr. *Hacker, riaperto il blog di Anonymous Italia* URL: https://www.cybersecitalia.it/hacker-riaperto-blog-anonymous-italia/5418/

Si è confermato di segno limitato l'attivismo di individui e gruppi riconducibili al cyberterrorismo[46], che hanno fatto registrare anche nel 2018 l'utilizzo di piattaforme social e di applicazioni di messaggistica per lo più con finalità di propaganda e proselitismo. A distanza di cinque anni dalla sua istituzione, il Tavolo Tecnico Imprese (TTI): una delle più riuscite esperienze nazionali di partenariato pubblico-privato nel settore ha attestato come la collaborazione tra Istituzioni ed operatori strategici sia nodale per un Paese che aspira a mettere in sicurezza il suo perimetro cibernetico.

Sullo sfondo di un accresciuto interscambio di dati tecnici, il TTI ha continuato ad essere la sede di iniziative finalizzate alla condivisione di analisi sui profili di rischio connessi all'impiego di determinate soluzioni tecnologiche, favorendo, al tempo stesso, lo scambio informativo su malware e campagne ostili in danno di specifici settori economico-industriali.

2.3 - Il quadro strategico nazionale per la sicurezza dello spazio cibernetico.

Nel 2013, con il cd. "Decreto Monti", l'Italia ha delineato per la prima volta la sua architettura di sicurezza cibernetica, provvedendo a sistematizzare, sia pure con la legislazione vigente, le molteplici competenze di settore distribuite tra diversi attori istituzionali.[47] Ciò ha consentito l'avvio dell'accrescimento delle capacità cyber nazionali, opportunamente guidato dagli atti di indirizzo strategico e operativo. Pur a fronte dei positivi risultati raggiunti, le evoluzioni che hanno interessato la materia sono: in primis, quelle connesse con la Direttiva NIS (Network and Information System) sulla sicurezza della UE che ha imposto, da un lato, una verifica dell'efficacia dell'architettura nazionale a fronte della crescente sofisticazione della minaccia e della rilevanza strategica dei target cui la stessa si rivolge e, dall'altro, degli impegni assunti

[46]il Ct consiste in operazioni condotte sul Web e motivate politicamente con lo scopo di provocare gravi conseguenze come la perdita di vite umane o consistenti danni economici, o comunque terrore. Per altri, il Ct consiste in attacchi o minacce di attacchi contro computers, reti, ed informazioni ivi archiviate, al fine di intimidire o costringere un governo o la sua popolazione a determinati comportamenti al fine di conseguire effetti politici o sociali. Altri ancora definiscono il Ct come atti che bloccano o distruggono nodi computerizzati delle infrastrutture critiche come internet, le telecomunicazioni, le reti elettriche, il sistema bancario

[47]Cfr. *Testo Decreto Monti*: https://www.gazzettaufficiale.it/eli/id/2012/03/24/12A03524/sg

dall'Italia in ambito internazionale, dove i principali alleati hanno conseguito avanzati assetti difensivi e, non di rado, offensivi. Gli esiti di tale verifica si sono tradotti nel "DPCM GENTILONI" che, sempre ad invarianza del quadro normativo primario vigente, è intervenuto razionalizzando ulteriormente l'architettura delineata nel 2013[48]. Tale provvedimento ha ridefinito le attribuzioni del Presidente del Consiglio dei Ministri e del CISR nel campo della sicurezza cibernetica, in linea con le funzioni di deliberazione, consulenza e proposta, a supporto del Presidente del Consiglio attribuite al CISR dall'articolo 7bis del decreto-legge n. 174/2015 in caso di crisi, assegnando al Direttore Generale del DIS un ruolo attivo e centrale nella gestione ordinaria e straordinaria della cyber security in Italia. Questi, infatti, è chiamato a definire le linee di azione di interesse generale, al fine di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti nazionali e ad individuare le più avanzate soluzioni tecnologiche a sostegno delle attività di prevenzione, contrasto e risposta agli incidenti che interessino amministrazioni, enti pubblici e operatori privati.[49]

Le misure di razionalizzazione dell'architettura e di riposizionamento del Nucleo per la Sicurezza Cibernetica (NSC, chiamato ad operare in chiave sia di prevenzione e preparazione che di risposta e ripristino (response & recovery), sono state accompagnate dalla nomina del Vice Direttore Generale Cyber del DIS, cui spettano:

- le funzioni di raccordo degli attori che compongono il framework nazionale;
- l'attuazione delle misure di potenziamento previste dal Piano d'Azione-PA, annesso al Piano Nazionale, tra cui spicca l'unione tra CERT-N e CERT-PA anche in vista della costituzione del CSIRT chiamato ad interfacciarsi, ai sensi della Direttiva NIS, con il CSIRT europeo;
- l'avvio di iniziative volte a realizzare un "Centro nazionale di Ricerca e Sviluppo in Cybersecurity", nonché un "Centro nazionale di crittografia".[50]

Iniziative, queste ultime, che potranno essere proficuamente sviluppate, in linea con quanto fatto da altri Paesi tecnologicamente avanzati, nell'ambito di una entità

[48]Cfr. *DPCM 17 febbraio 2017* URL:https://www.gazzettaufficiale.it/eli/id/2012/03/24/12A03524/sg
[49]Cfr. *DIS* URL: http://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html
[50]Cfr. *L'Italia avrà presto il suo Computer Security Incident Response Team* URL:https://www.difesaesicurezza.com/cyber/italia-avra-presto-il-suo-computer-security-incident-response-team-csirt/

istituzionale in grado di fungere da stimolatore, collettore e incubatore. Si tratta, in sostanza, di prevedere la costituzione di una Fondazione per la sicurezza cibernetica, attraverso cui dare vita ad un'effettiva alleanza tra istituzioni, aziende e mondo accademico, così da favorire lo sviluppo di linee di ricerca mirate nell'ottica di delineare appropriate architetture digitali nazionali intorno al concetto di sicurezza.

Tali architetture devono rispondere, in un contesto di profonda trasformazione digitale, alla complessità delle minacce presenti e future, assicurando una "continuità di servizio", che possa abilitare un organico sviluppo economico e sociale del Paese.

A tal fine, gli operatori convenzionati hanno partecipato a seminari dedicati al tema delle minacce di tipo avanzato e persistente e alla crittografia. Questi ultimi, organizzati dagli afferenti al Comitato Nazionale per la Ricerca in cyber security, al Consiglio Nazionale delle Ricerche (CNR), alle Università facenti parte del Consorzio Nazionale Interuniversitario per l'Informatica (CINI) e al Consorzio Nazionale Interuniversitario per le Telecomunicazioni, sono stati tenuti presso la Scuola di formazione del Sistema di informazione per la Sicurezza della Repubblica.

Inoltre, nell'ottica di promuovere una integrazione progettuale ed operativa tra Intelligence, Industria ed Università e allo scopo di garantire l'efficace impiego delle capacità hightech nazionali a protezione del nostro Paese, si è tenuta il 28 e 29 novembre del 2017, la quarta edizione dell'ICT4INTEL 2020[51], dedicata ai social media.

L'obiettivo è stato quello di cogliere a fronte degli impatti prodotti dall'uso massivo dei social network sulle tradizionali attività di ricerca, raccolta ed analisi delle informazioni, le potenzialità offerte dalla tecnologia per mitigare i rischi derivanti da tale fenomeno.

Nell'occasione, particolare rilievo è stato attribuito alla necessità di un presidio che, proprio attraverso la partnership pubblico-privato, garantisca la tutela delle libertà e dei diritti fondamentali dei cittadini nella dimensione digitale. A supporto di tali libertà, è stata varata la prima campagna nazionale di formazione per la promozione di un utilizzo consapevole delle tecnologie ICT, denominata "Be Aware. Be Digital". Lanciata dal DIS in occasione della celebrazione del decennale della legge di riforma del Comparto, l'iniziativa, coordinata con il Ministero dell'Istruzione, dell'Università e della

[51]Cfr. *Cyber , Nasce il polo tecnologico* URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cyber-lintelligence-incontra-il-privato-nasce-il-polo-tecnologico.html

Ricerca, mira ad aumentare la consapevolezza dei rischi cyber, allo scopo di consentire un più sicuro esercizio della libertà nel web. Una campagna, quindi, tesa ad accrescere in un'ottica incrementale, la capacità di discernere le situazioni di reale vantaggio da quelle che privano delle libertà fondamentali. Due le categorie target: i giovani, per definizione "nativi digitali", e le piccole e medie imprese (PMI), in quanto tessuto produttivo su cui si fonda la parte più significativa della ricchezza nazionale. Vale evidenziare, inoltre, come tale ultima iniziativa sia destinata ad incontrare terreno fertile, considerato che la galassia di medie e piccole imprese nazionali è destinataria dal 2016 del Framework Nazionale per la Cybersecurity, strumento mediante il quale si è voluta agevolare, nell'ambito di quelle realtà imprenditoriali già consapevoli, l'introduzione del principio di gestione strutturata del rischio cyber. Il rafforzamento delle PMI nazionali consentirà di incrementare la resilienza delle filiere produttive nazionali. Tuttavia, l'aumento della resilienza di un Paese rispetto ad attacchi di tipo cibernetico può soltanto essere efficacemente affrontato se il Paese si doterà di una workforce adeguata.

In ultima analisi, abbiamo di fronte un problema di formazione molto vasto che include sia i lavoratori attivi che le future generazioni. Formazione che va dalla cultura di base fino alla ricerca dei talenti. Molte iniziative sono in atto a livello locale e nazionale e su di esse anche il Sistema di informazione per la Sicurezza della Repubblica conta per poter incrementare sia il livello generale della sicurezza, sia le capacità operative direttamente gestite.

2.4 - Il piano nazionale per la protezione cibernetica e la sicurezza informatica.

Con decreto del Presidente del Consiglio dei Ministri in data 27 gennaio 2014 sono stati adottati per la prima volta il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" ed il "Piano nazionale per la protezione cibernetica e la sicurezza

informatica", in attuazione dell'articolo 3, comma 1, del decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013. [52]

Successivamente, con decreto del Presidente del Consiglio dei Ministri del 17 febbraio 2017 rubricato "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", è stato adottato il nuovo "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica."

Tale Piano Nazionale costituisce la roadmap per l'adozione, da parte dei soggetti pubblici e privati, delle misure prioritarie per l'implementazione del Quadro Strategico Nazionale, sulla base di un dialogo attivo e interattivo che vede nella protezione cibernetica e nella sicurezza informatica nazionali non solo un obiettivo ma, soprattutto, un processo che coinvolge tutti gli attori interessati, a vario titolo, alla tematica cyber. [53]

Sicuramente apprezzabile è lo sforzo da parte dell'Amministrazione di definire in brevissimo tempo dall'adozione del nuovo DPCM anche la nuova versione del Piano Nazionale. Le indicazioni previste nel Piano appaiono abbastanza complicate per almeno due ordini di fattori:

- il documento possiede una struttura istituzionale "complessa", che si articola nella presenza di una pluralità di soggetti, atti e documenti la cui semplificazione è uno degli obiettivi individuati dal Piano stesso;
- le modalità con cui sono riportati gli indirizzi operativi presenti.

Infatti, gli 11 obiettivi operativi sono decomposti in 34 sotto-obiettivi a loro volta espansi in 93 classi di attività: risulta così un elenco di 127 punti.[54] Peraltro, l'assenza nel piano di qualunque riferimento temporale per l'adozione delle iniziative per il conseguimento dei diversi obiettivi operativi nonché la mancanza di indicatori atti a qualificare il conseguimento degli stessi, unitamente alla sostanziale assenza di indicazioni sulle risorse finanziarie da utilizzare, rappresentano gli elementi di maggior debolezza del Piano. In questo senso si evidenzia che, sebbene il Piano rappresenti un

[52] I documenti sono resi disponibili sul sito istituzionale del Governo (www.governo.it) e su quello del Sistema di informazione per la sicurezza della Repubblica (http://www.sicurezzanazionale.gov.it/).

[53] Presidenza del Consiglio dei Ministri (2013), Quadro Strategico Nazionale per la Sicurezza nello Spazio Cibernetico

[54] *Idem come sopra.*

aggiornamento di quello adottato nel 2013, non si sofferma in alcun modo ad analizzare lo stato di attuazione dei diversi obiettivi strategici al fine di evidenziare la "strada già percorsa" ma si limita a sottolineare che le principali direttrici dell'intervento di revisione hanno riguardato:

- l'indirizzo operativo 1 (Potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare), che è stato allineato rispetto all'esperienza operativa maturata nell'ultimo biennio al fine di potenziare le capacità complessive di risposta integrata ad eventi cibernetici.
- l'indirizzo operativo 5 (Operatività delle strutture nazionali di incident prevention, response e remediation), in cui sono state considerate le esigenze di potenziamento degli attuali CERT, la necessità di costituire le strutture previste dalla Direttiva NIS (CSIRT, punto unico di contatto nazionale, Autorità nazionale) e le modalità di coordinamento tra i vari attori – attuali e futuri – dell'architettura (CERT e CSIRT, Comparto, CNAIPIC, Difesa, AgID, ecc.), in una prospettiva di progressiva unificazione dei CERT pubblici.

A rendere più complessa l'analisi del documento è l'introduzione di un "Piano di Azione" che "raccoglie le iniziative individuate per garantire il necessario ed effettivo cambio di passo in termini di innalzamento dei livelli di sicurezza dei sistemi e delle reti del nostro Paese, cui il citato DPCM 17 febbraio 2017 intende fornire un deciso impulso." [55] Tale piano di azione individua otto obiettivi:

1) revisione del Nucleo per la Sicurezza Cibernetica,
2) contrazione della catena di comando per la gestione delle crisi cibernetiche,
3) riduzione della complessità dell'architettura nazionale, mediante soppressione e accorpamento di organi,
4) progressiva unificazione dei CERT,
5) istituzione di un centro di valutazione e certificazione nazionale ICT,
6) fondazione o fondo di venture capital,
7) istituzione di un Centro nazionale di ricerca e sviluppo in cybersecurity,
8) costituzione di un Centro nazionale di crittografia.

[55] Piano di Azione

Oltre ai citati obiettivi verranno analizzati in seguito nel dettaglio i seguenti punti.[56]

- *Potenziamento della capacità di intelligence, di polizia e di difesa civile e militare*: l'obiettivo mira a creare un'approfondita conoscenza delle vulnerabilità non solo del fattore tecnologico ma anche di quello umano e delle minacce cibernetiche che le sfruttano mediante una valutazione in continuo delle stesse che includa sia i soggetti istituzionale, che i soggetti privati. Pertanto, è quindi necessario sviluppare capacità di raccolta, elaborazione e disseminazione delle informazioni e della gestione della conoscenza che ne deriva. La fase di analisi deve completata con lo sviluppo delle capacità di contrasto alla minaccia cibernetica sia in termini di miglioramento delle capacità di attribuzione di un attacco cyber che le capacità di risposta integrata, secondo regole d'ingaggio e protocolli prestabiliti, adeguando il quadro normativo per creare pool d'intervento tecnici in supporto, in caso di gravi eventi cibernetici, alle amministrazioni centrali e ai gestori di servizi essenziali e di infrastrutture critiche.[57]
- *Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati*:

  tale indirizzo ha l'obiettivo di potenziare il coordinamento e la cooperazione non solo tra i diversi soggetti pubblici, ma anche tra questi e i soggetti privati, considerato che questi ultimi si occupano delle infrastrutture critiche nazionali. Da qui l'esigenza di favorire l'operatività dei già esistenti sistemi di collaborazione e di relazioni fiduciarie tra settore pubblico e privato nonché favorire l'attività di tavoli istituzionali, tavoli tecnici ed organismi competenti che prevedono la partecipazione di gestori di servizi essenziali, di operatori di infrastrutture critiche informatizzate nazionali.

  Sul piano operativo va potenziato il sistema di info-sharing, anche attraverso l'adozione di linguaggi strutturati e comuni mediante definizione di specifici standard di valutazione e format di comunicazione[58].

  Vanno, inoltre, consolidati i canali di dialogo e consultazione tra le istituzioni ed il settore privato, nell'ottica dell'approccio "Sistema Paese", nonché favorita la

[56]Belviolandi S. (2017), Rapporto Clusit 2017 sulla sicurezza IT e Cybercrime: l'Italia vittima dei Ransomware,

[57]Tosato F. , Taufer M. (2016), Evoluzione del Quadro di sicurezza cibernetica nazionale in prospettiva futura, Relazione C.e.s.i.

[58]Ibidem

partecipazione del settore privato ad esercitazioni internazionali sulle tematiche della protezione delle infrastrutture critiche informatizzate.[59]

Il fattore umano rappresenta un elemento essenziale per qualunque strategia efficace di sicurezza. In quest'ottica è fondamentale poter disporre sia di figure professionali qualificate che di una cultura della sicurezza a tutti i livelli. Dunque, è fondamentale formare e addestrare il personale con un focus specifico sulla tematica della cyber security collaborando con enti universitari e di ricerca.

In questo contesto sarebbe stato auspicabile una riflessione sui requisiti professionali da richiedere a coloro che operano su sistemi critici e sulla necessità di una loro formazione continua.

Il carattere transnazionale del cyberspace e la sua pervasività richiedono un approccio internazionale alla tematica, per questo tutti i singoli Stati devono necessariamente agire sinergicamente per far fronte alla minaccia cyber. Ciò impone il rafforzamento della cooperazione bilaterale e multilaterale instaurando rapporti strutturati di cooperazione con i Paesi membri della NATO, della UE e con le nazioni partner anche mediante la promozione della partecipazione dei soggetti nazionali, pubblici e privati, ai Progetti ed ai finanziamenti dell'Unione Europea.

Organizzare, su base periodica, esercitazioni nazionali di sicurezza informatica, stimolando la partecipazione dei principali operatori di servizi essenziali e dei gestori di infrastrutture critiche o i settori strategici nazionali; è necessario anche coordinare la partecipazione nazionale, nella componente pubblica e privata, alle esercitazioni pan-europee.

- *Operatività delle strutture nazionali di incident prevention, response e remediation:* La rapida evoluzione tecnologico-informatica comporta un altrettanto veloce obsolescenza delle norme che disciplinano materie correlate alle tecnologie dell'informazione e della comunicazione. Pertanto, esse necessitano di periodiche revisioni e aggiornamenti anche alla luce della necessità di finalizzare il quadro normativo relativo alle infrastrutture critiche nazionali informatizzate nonché di

[59] GU Serie Generale n.87 del 13-4-2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali". (17A02655) Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017

identificare gli strumenti tecnici, inclusi quelli relativi all'indirizzamento, necessari all'attribuzione di responsabilità in caso di violazioni di sicurezza (e delle relative sanzioni) da parte di amministratori ed utenti delle reti di interesse.

- *Compliance a standard e protocolli di sicurezza*:

la compliance a standard e protocolli di sicurezza, elaborati sia a livello nazionale che a livello mondiale consente di garantire un comune livello qualitativo della protezione informatica dei sistemi e delle reti. Occorre però provvedere all'identificazione, adozione, aggiornamento e verifica degli standard di riferimento, delle best practices e delle misure e requisiti minimi per la sicurezza delle reti**.**

Un altro aspetto è quello della certificazione degli apparati, strumenti e processi adottati sia per la gestione delle informazioni classificate che dagli operatori di servizi essenziali.

La garanzia dell'affidabilità e della sicurezza di componenti hardware e software impiegate da infrastrutture critiche e da soggetti che svolgono attività di rilevanza strategica per il Paese richiede la realizzazione di una catena di approvvigionamento di componenti sicure e resilienti dal punto di vista della sicurezza cibernetica, supportata da un processo flessibile e veloce di validazione, verifica e certificazione. Questo si potrà perseguire anche grazie alla costituzione di un laboratorio governativo di verifica che sottoponga ad analisi comparativa i sistemi ICT di interesse delle Amministrazioni e delle infrastrutture critiche di interesse nazionale.

Per gestire correttamente un evento cyber con un impatto significativo sulla popolazione è necessario predisporre un coordinamento sulla Situation Awareness dei contenuti e delle informazioni, allo scopo di rendere efficaci i flussi comunicativi al fine di essere in grado di fornire, ove necessario o opportuno, un'informazione completa, corretta, veritiera e trasparente, senza con ciò creare inutili allarmismi che verrebbero ad amplificare l'impatto economico e sociale dell'evento stesso.

- *Risorse*:

punto di partenza per un'oculata pianificazione finanziaria e per la ripartizione delle risorse è l'analisi dei costi di eventi cibernetici occorsi o potenziali per poter definire coerentemente le priorità e le risorse/costi associati alle diverse misure di cyber-security e di cyber-defence per la protezione delle infrastrutture critiche e per lo

sviluppo delle capacità operative fondamentali, sia per le componenti materiali e strumentali che per quelle relative al personale. Prerequisito per tale attività è lo sviluppo di una capacità di misurazione dell'impatto di eventi cyber ma non risultano previsioni su specifici finanziamenti destinati al miglioramento della protezione cyber.[60]

Pertanto, comprendere il rischio del sistema Paese connesso con la minaccia cyber è un elemento fondamentale per una corretta identificazione delle azioni da adottare. Questo si declina mediante l'individuazione di una metodologia di cyber risk management univoca e condivisa a livello strategico e l'adozione di il piano di valutazione dei rischi (come previsto anche dalla Direttiva NIS).

2.5 - La Direttiva N.I.S

Il 6 luglio 2018 il Parlamento Europeo ha adottato la direttiva sulla sicurezza dei sistemi delle reti e dell'informazione, NIS. Essa rappresenta il primo insieme di regole sulla sicurezza informatica univoco a livello dell'Unione Europea.

L'obiettivo della direttiva è raggiungere un livello elevato di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti i Paesi membri dell'UE.[61]

I tre punti chiave della direttiva NIS sono:

- migliorare le capacità di cybersecurity dei singoli Stati dell'Unione;
- aumentare il livello di cooperazione tra gli Stati dell'Unione;
- obbligo di gestione dei rischi e di riportare gli incidenti di una certa entità da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali.

Relativamente al miglioramento delle capacità dei singoli Stati dell'Unione, la direttiva NIS sottolinea alcuni aspetti necessari per rispettare i criteri adottati. Ogni Stato infatti dovrà dotarsi, qualora già non l'avesse, di una strategia nazionale di cyber security che definisca gli obiettivi strategici, le politiche adeguate e le misure di regolamentazione.[62]

---

[60] Cfr. *Il Piano nazionale per la protezione cibernetica e la sicurezza informatica* URL: https://www.sicurezzaegiustizia.com/il-piano-nazionale-per-la-protezione-cibernetica-e-la-sicurezza-informatica/

[61] Cfr. *Banca D'Italia (2016), G7 Fundamental elements of Cybersecurity for the financial sector, Report*

[62] Cfr. Belviolandi S. (2017), *Rapporto Clusit 2017 sulla sicurezza IT e Cybercrime: l'Italia vittima dei Ransomware,*

Tra gli aspetti che una strategia nazionale dovrebbe includere vengono citati gli obiettivi strategici, le priorità nazionali, la governance, l'individuazione di misure proattive, di risposta e di recovery; sensibilizzazione, formazione ed istruzione; incentivazione della cooperazione tra settore pubblico e settore privato; lista degli attori coinvolti nella attuazione della strategia.

Sempre in questo punto, la direttiva NIS richiede agli Stati di designare una o più autorità competenti per il controllo dell'applicazione della direttiva stessa a livello nazionale. Un singolo punto di contatto dovrà essere designato da ognuno degli Stati membri, con il compito di assicurare la cooperazione internazionale e di collegarsi con gli altri Stati attraverso meccanismi di cooperazione identificati della direttiva stessa.[63]

Ogni Stato dovrà infine designare uno o più CSIRT (Computer Security Incident Response Team) responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti. Dovranno inoltre fornire analisi sui rischi e incidenti e aumentare il grado di consapevolezza. Fondamentale anche per i CSIRT è la cooperazione internazionale e l'information sharing.

La cooperazione tra i vari enti dei singoli Stati membri è un punto veramente fondamentale della direttiva NIS. Proprio per questo è stato stabilito un gruppo di cooperazione che faciliti i rapporti tra gli Stati membri e che aumenti la fiducia. Questo gruppo di cooperazione sarà composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA (European Union for Network and Information Security Agency). Le quattro aree di lavoro del gruppo saranno: pianificazione, guida, segnalazione e condivisione.

L'ultimo dei punti principali della direttiva riguarda gli operatori dei servizi essenziali per la Nazione e i fornitori di servizi digitali.

Gli operatori di servizi essenziali sono aziende pubbliche o private che hanno un ruolo importante per la società e l'economia, quelli che comunemente vengono chiamate "infrastrutture critiche". La direttiva NIS obbligherà queste entità a dotarsi di misure di sicurezza appropriate e di notificare all'autorità nazionale competente gravi incidenti di

[63]Cfr. Laboratorio Nazionale di Cyber Security (2015), *Il Futuro della Cyber Security in Italia, Consorzio Interuniversitario Nazionale per l'Informatica*

sicurezza secondo parametri di numero di utenti coinvolti, durata dell'incidente e diffusione geografica. Le misure di sicurezza richieste comprendono:

- prevenzione dei rischi;
- garantire la sicurezza dei sistemi, delle reti e delle informazioni;
- capacità di gestire gli incidenti.

Queste entità verranno identificate direttamente da ogni Stato membro, all'interno dei seguenti ambiti: energia, trasporti, banche e società finanziarie, salute, acqua ed infrastrutture digitali. I criteri che determineranno quali enti saranno inclusi in questa lista sono:

- l'essenzialità del servizio offerto per il mantenimento di attività critiche in ambito economico e sociale;
- il servizio dipende da sistemi informatici;
- se l'incidente di sicurezza rischia di avere effetti gravi e significativi sulla fornitura di un servizio essenziale.

Anche i fornitori di servizi digitali saranno tenuti, secondo la direttiva NIS, ad attuare misure di sicurezza appropriate e a notificare incidenti rilevanti. Oltre alle misure già previste per gli operatori di servizi essenziali, le misure di sicurezza relative ai fornitori di servizi digitali prevedono alcuni fattori specifici, come ad esempio la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i test e la conformità a norme internazionali. Per quanto riguarda i parametri per la valutazione di un incidente rilevante che va segnalato, vi sono oltre a quelli già elencati prima, anche l'entità dell'interruzione del servizio e l'impatto sulle attività economiche e sociali. Tra i fornitori di servizi digitali la direttiva NIS cita i mercati on-line, i servizi di cloud e i motori di ricerca. Non rientrano in questa categoria invece le piccole e medie imprese.[64]

l'Italia ha dato attuazione alla Direttiva NIS (UE) 2016/1148, recependola nell'ordinamento nazionale, con Decreto Legislativo 18 maggio 2018, n.65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018.

[64]Cfr.Lorusso S., *L'insicurezza dell'era digitale, tra cybercrimes e nuove frontiere dell'investigazione,*2011

Tale direttiva, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

Gli OSE sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e ‘'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.

Gli FSD sono le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Gli obblighi previsti per gli FSD non si applicano alle imprese che la normativa europea definisce "piccole" e "micro", quelle cioè che hanno meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro.

Tanto gli OSE che gli FSD:

- sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l’impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
- hanno l’obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al Computer Security Incident Response Team (CSIRT) italiano, informandone anche l’Autorità competente NIS di riferimento.

  Gli FSD sono stati chiamati ad applicare le prescrizioni dettate dal decreto di recepimento a partire dal 24 giugno 2018, data di entrata in vigore del provvedimento, valutando la rilevanza degli incidenti sulla base dei criteri e delle soglie indicati nel Regolamento (UE) 2018/151 del 30 gennaio 2018

  I soggetti giuridici non identificati come OSE e che non sono FSD possono inoltrare al CSIRT notifiche volontarie degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati. Ciò poiché l’intento della Direttiva NIS e del relativo decreto di recepimento è quello di favorire la più ampia diffusione di una consapevole cultura nel campo della cybersecurity e di un conseguente

accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni.

Il Computer Security Incident Response Team (CSIRT) italiano:

- definisce le procedure per la prevenzione e la gestione degli incidenti informatici; § riceve le notifiche di incidente, informandone il DIS, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al Nucleo per la Sicurezza Cibernetica;
- fornisce al soggetto che ha effettuato la notifica le informazioni che possono facilitare la gestione efficace dell'evento; § informa gli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'OSE o del FSD nonché la riservatezza delle informazioni fornite;
- garantisce la collaborazione nella rete di CSIRT, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di best practices. Il CSIRT italiano sarà istituito presso la Presidenza del Consiglio dei ministri mediante unificazione del Computer Emergency Response Team (CERT) Nazionale e del CERT-PA, assumendone i compiti. Nelle more della definizione di funzionamento e organizzazione della nuova struttura (demandata ad un DPCM da adottare entro il 9 novembre 2018):
- le funzioni del CSIRT italiano sono svolte dal CERT-N unitamente al CERT-PA, con una ripartizione di ruoli e responsabilità secondo le attuali constituency (Pubblica Amministrazione per il CERT-PA, settore privato per il CERT-N) e con l'introduzione di uno scambio informativo rafforzato e di specifiche procedure di gestione delle notifiche;
- il CERT-N garantisce la cooperazione a livello europeo, anche nell'ambito della rete di CSIRT, in stretto raccordo con il CERT-PA

Le Autorità competenti NIS, quali responsabili dell'attuazione del decreto:

- vigilano sulla sua applicazione ed esercitano le relative potestà ispettive e sanzionatorie, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica. Salvo che il fatto costituisca reato, la violazione da parte di OSE e FSD degli obblighi previsti dal decreto legislativo

comporta l'irrogazione di sanzioni amministrative pecuniarie fino ad un massimo di 150.000 euro; la reiterazione determina l'aumento fino al triplo della sanzione prevista;

- procedono ad identificare gli OSE entro il 9 novembre 2018 (consultando, laddove necessario, le Autorità competenti NIS degli altri Stati Membri), individuando anche le soglie in ragione delle quali un incidente è da considerarsi pregiudizievole per la sicurezza delle reti e dei sistemi informativi. Se un evento implica anche violazione di dati personali, le Autorità competenti NIS operano in stretta cooperazione con il Garante per la protezione dei dati personali. Al riguardo, sono in corso approfondimenti per propiziare un raccordo tra gli obblighi introdotti dal Decreto legislativo di recepimento della Direttiva NIS e quelli previsti dal nuovo Regolamento europeo per la protezione dei dati personali (GDPR);
- possono predisporre linee guida per la notifica degli incidenti e dettare specifiche misure di sicurezza, sentiti gli OSE. L'elenco nazionale degli OSE è istituito presso il Ministero dello sviluppo economico e viene aggiornato, almeno ogni due anni, a cura delle Autorità competenti NIS.

Il punto di contatto unico NIS assicura, a livello nazionale, il coordinamento delle questioni relative alla sicurezza delle reti e dei sistemi informativi e, a livello europeo, il raccordo necessario a garantire la cooperazione transfrontaliera delle Autorità competenti NIS italiane con quelle degli altri Stati membri, con il Gruppo di cooperazione istituito presso la Commissione europea anche attraverso l'elaborazione di linee guida e lo scambio di informazioni e best practices e la rete dei CSIRT UE. Rientra tra i compiti del punto di contatto unico NIS trasmettere:

- al Gruppo di cooperazione, entro il 9 agosto 2018 (e in seguito annualmente), una relazione sulle notifiche ricevute, contenente numero e natura degli incidenti e le azioni intraprese da OSE e FSD;
- alla Commissione UE, entro il 9 novembre 2018 (e in seguito ogni due anni), le informazioni per verificare l'attuazione della Direttiva NIS in Italia. Quale punto di contatto unico NIS è stato designato il Dipartimento Informazioni per la Sicurezza (DIS), in ragione del ruolo svolto nell'architettura cyber nazionale.

Allo scopo di agevolare le Autorità competenti NIS nell'adempimento dei compiti loro affidati, verrà istituito, attraverso un apposito DPCM, un Comitato tecnico di raccordo.
Il Comitato opererà presso la Presidenza del Consiglio dei ministri, riunendo i delegati dei Ministeri-Autorità competenti NIS e i rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.
A valle del recepimento della Direttiva NIS, sarà integrata di un apposito addendum la Strategia nazionale di sicurezza cibernetica, adottata dal Presidente del Consiglio dei ministri, sentito il Comitato Interministeriale per la Sicurezza della Repubblica (CISR).
La direttiva NIS rappresenta, quindi, un fondamentale passo verso un mercato unico digitale, una opportunità di crescita economica oltre che una difesa da minacce sempre più presenti nella vita quotidiana dei cittadini e delle imprese europee. Ovviamente però la reale efficacia della direttiva dipenderà da come sarà implementata dagli Stati membri, e da quanto questa implementazione sarà in linea con gli obiettivi originali della direttiva stessa.

CAPITOLO III

Cyber security e attività di intelligence

3.1 – L'analisi del Rischio.

Siamo in un momento storico dove i cyberattacchi non sono mai stati cosi elevati, non solo grazie alla maggiore attività dei cyber criminali, ma anche per la continua espansione del cyberspace e della diffusione dei cloud, mobile e internet of things.

Gli investimenti sulla cyber security dei privati, delle aziende e delle microimprese sono sempre maggiori.

È impossibile garantire totalmente la sicurezza e occorre considerare che ha un costo crescente quindi in un contesto di scarsità di risorse è necessario utilizzare una logica di analisi del rischio. In tutte le organizzazioni dove il sistema di gestione della sicurezza ha raggiunto un discreto livello di maturità, è presente un documento di analisi del rischio che viene applicato a processi, applicazioni e altri asset. Questi documenti descrivono le minacce da cui l'organizzazione intende difendersi e come lo fa.

Per analizzare il rischio è necessario per primo definire il risk appetite, che stabilisce quanto l'organizzazione è disposta a esporsi all'impatto del realizzarsi di una minaccia, successivamente viene attribuito a ogni minaccia il suo grado di probabilità potenziale di realizzarsi e l'impatto che questo rischio avrebbe sull'organizzazione per quanto riguarda la riservatezza, l'integrità e la disponibilità.[65]

Verificate quali misure sono state adottate per proteggere l'asset oggetto di valutazione, il rischio viene riclassificato, per verificare se l'impatto residuo è accettabile, secondo quanto stabilito dal risk appetite. Nel caso in cui l'impatto non sia accettabile, occorre elaborare una strategia tesa a diminuire il rischio fino a renderlo accettabile.[66] Non bisogna considerare l'analisi del rischio un'attività di esclusiva competenza dei sistemi informativi, in quanto l'analisi del rischio deve tener conto di tutti i processi e gli asset tutelati, anche quelli non informatici: è necessario proteggere non solo i database, ma anche gli edifici in cui essi sono conservati. L'analisi dei rischi, come gli altri documenti, va aggiornata ogni qual volta che sono introdotti nuovi

[65] Cfr. *Analisi del rischio, investire di più per proteggere l'azienda dal cyber crime* URL: https://www.cybersecurity360.it/legal/privacy-dati-personali/investimenti-di-sicurezza-in-azienda-fondamentali-per-una-corretta-analisi-del-rischio/

[66] Cfr. G.J. Rattray, *An Environmental Approach to Understanding Cyberpower, in Cyberpower and National Security*

trattamenti o avvengono variazioni sostanziali in modo da garantire un livello di sicurezza adeguato.

I modelli di analisi dei rischi comunemente utilizzati sono basati su questionari, tratti dalle best practice[67]. Le contromisure di sicurezza sono opportunamente declinate e adattate nella realtà e contesto organizzativo in esame.

Un questionario, indirizzato a uno o più intervistati, è composto da più domande: per ciascuno si richiede una valutazione del grado di implementazione del controllo. Le risposte dell'intervistato indicano, quindi, il grado di maturità dell'organizzazione rispetto a quella determinata contromisura di sicurezza.

Non essendo sempre chiaramente definite le responsabilità su determinati asset o attività, può risultare difficile identificare i giusti referenti custodi della conoscenza e del sapere. Inoltre, a causa di vincoli temporali o di risorse, le informazioni raccolte sono spesso parziali e poco dettagliate. Ne conseguono risultati "aggregati" o al più assortimento di dati, con un alto grado di approssimazione e inefficaci al fine di una mirata analisi dei rischi.

In secondo luogo, i modelli di analisi dei rischi tradizionali si basano principalmente sull'assunto che uno scostamento dalle best practice scelte come riferimento, e quindi utilizzate per generare le checklist di valutazione dell'efficacia delle contromisure di sicurezza, equivalga a un aumento del rischio. Quest'ipotesi rappresenta uno dei limiti maggiori riguardo l'efficacia delle analisi dei rischi, essendo ancora basate sul concetto di benchmark o differenza rispetto a uno standard, spesso di industry diverse o cross-industry[68].

Un ulteriore limite dei modelli di analisi dei rischi tradizionale deriva dall'associazione contromisura-rischio. In un contesto in cui i rischi sono in continua evoluzione, non è facile eseguire una mappatura delle minacce, né tantomeno correlarne la probabilità di accadimento.

[67]Si intendono le esperienze, le procedure o le azioni più significative, o comunque quelle che hanno permesso di ottenere i migliori risultati, relativamente a svariati contesti e obiettivi preposti.

[68]Ridefinizione dei confini tradizionali tra i settori attraverso l'integrazione di prodotti/servizi, asset/tecnologie e dati, ampliando e migliorando l'ecosistema.

3.2 - Gestione del rischio a livello sistemico

Nonostante i consistenti sforzi effettuati in questi ultimi anni, non vi è oggi alcuna possibilità di disporre di sistemi non vulnerabili, specialmente considerando che l'errore umano risulta determinante nella stragrande maggioranza degli incidenti e attacchi cyber odierni.

La complessità e i metodi di attacco utilizzati da hacker e cyber criminali diventano sempre più sofisticati e i vettori di attacco diventano sempre più accessibili anche a persone che non possiedono conoscenze tecniche di altissimo livello; basti pensare alle possibilità offerte dal dark web di reperimento di un malware per poche centinaia di dollari. Il problema si amplifica ulteriormente considerando la poca consapevolezza degli utenti che, non conoscendo pienamente i rischi in cui potrebbero incorrere, sono quotidianamente esposti ad una quantità elevatissima di minacce. Il rischio cyber necessita, dunque, di azioni mirate e coordinate per essere gestito in modo adeguato. Tali azioni devono necessariamente coinvolgere tutti gli aspetti organizzativi e tecnologici di un'azienda, abilitando in questo modo un approccio integrato di prevenzione del rischio e protezione del bilancio di impresa[69]. Nel febbraio 2016, da un'iniziativa del CIS Sapienza e del Laboratorio Nazionale di Cybersecurity, è stato presentato il primo Framework Nazionale di Cyber Security (FNCS) che, costruito sulle basi proposte dal Framework del NIST, ha lo scopo di "offrire alle organizzazioni un approccio volontario e omogeneo per affrontare la cyber security al fine di ridurre il rischio legato alla minaccia cyber"70. Costituito da 98 sotto-categorie, il FNCS agisce da ponte tra strumenti di Enterprise Risk Management e IT & Security Standard, definendo un terreno condiviso per qualsiasi tipo di organizzazione, indipendentemente dalla dimensione o dal settore, allineando le pratiche di cyber security ma mantenendo la necessaria neutralità rispetto alle pratiche di Risk

[69] Cfr. *Gestire il rischio cyber con un'assicurazione e il Framework nazionale per la cyber security: come fare* URL:https://www.agendadigitale.eu/sicurezza/gestire-il-rischio-cyber-con-unassicurazione-e-il-framework-nazionale-per-la-cyber-security-come-fare/

[70] Framework Nazionale di Cyber Security (FNCS)

Management aziendali quanto rispetto alla tecnologia che ogni attore adotta[71]. Inoltre, in un ambiente dove le minacce cyber si modificano continuamente e allo stesso tempo aumentano a ritmi esponenziali, il FNCS non si presenta come un documento statico ma in continua evoluzione, attraverso la possibilità di un suo aggiornamento costante sulla base dei rapidi cambiamenti relativi alle tecnologie, alle pratiche di Risk Management o alle stesse minacce.

É necessario introdurre un ulteriore strumento utile per la gestione del rischio: il pensiero sistemico. Il principio di questo pensiero è l'elaborazione di un modello causale che enfatizzi il ruolo dell'intreccio tra processi organizzativi, politiche e ritardi temporali nell'influenzare i fenomeni dinamici aziendali. Bisogna, infatti, riconoscere nella struttura del sistema le relazioni causa-effetto non lineari, intrecciate e a volte ritardate nel tempo. Il pensiero sistemico dà un vantaggio notevole, portando l'azienda un passo avanti nel tempo, mostrando i cicli nascosti, i fenomeni che si ripetono, si rafforzano e si bilanciano nel tempo, introducendo la dinamica dei sistemi che fornisce una metodologia per la modellazione e la successiva simulazione automatizzata. Nei sistemi complessi quali quelli aziendali, esistono delle interdipendenze tra gli elementi del sistema, le quali generano dei cicli (loop), che sono combinazioni di relazioni tra singoli elementi dove ogni elemento è sia causa che effetto dell'altro. Per comprendere e definire in maniera adeguata un sistema complesso bisogna definire l'area di studio e ricercare gli elementi chiave che determinano il fenomeno. Una volta trovati questi elementi si dovrà descriverli tramite variabili univoche e collegarli fra loro grazie a "link", o archi, in modo da evidenziarne l'influenza reciproca[72].

Sono necessari per la gestione del rischio a livello sistemico 15 controlli essenziali[73] di Cyber security, la cui corretta applicazione ha, come immediata conseguenza, una riduzione importante, ma non totale, del rischio. I Controlli Essenziali hanno una

---

[71] Cfr. *Gestire il rischio cyber con un'assicurazione e il Framework nazionale per la cyber security: come fare* URL:https://www.agendadigitale.eu/sicurezza/gestire-il-rischio-cyber-con-unassicurazione-e-il-framework-nazionale-per-la-cyber-security-come-fare/

[72] Cfr. *Gestire il rischio cyber con un'assicurazione e il Framework nazionale per la cyber security: come fare.* URL: https://www.agendadigitale.eu/sicurezza/gestire-il-rischio-cyber-con-unassicurazione-e-il-framework-nazionale-per-la-cyber-security-come-fare/

[73] Per controllo essenziale intendiamo una pratica relativa alla cybersecurity che, qualora ignorata oppure implementata in modo non appropriato, causa un aumento considerevole del rischio informatico.

validità limitata nel tempo, dovuta alla dinamicità della minaccia cyber. C'è, quindi, la necessità di mantenere aggiornati tali controlli per rispondere in modo adeguato all'evoluzione tecnologica e di questo tipo di minaccia. Successivamente, verranno analizzati i 15 controlli essenziali:

- il primo stabilisce che deve essere presente e aggiornato un inventario di sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno dell'azienda;
- il secondo controllo stabilisce che i servizi web (social network, cloud computing, posta elettronica) offerti da terze parti a cui si è registrati sono quelli strettamente necessari;
- il terzo controllo stabilisce che devono essere individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti;
- il quarto controllo stabilisce che deve essere nominato un responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici;
- il quinto controllo stabilisce che devono essere individuate e rispettate le leggi e i regolamenti con rilevanza in tema di cyber security che risultino applicabili nell'azienda;
- il sesto controllo stabilisce che tutti i dispositivi che lo consentono devono essere dotati di software di protezione (antivirus, antimalware) regolarmente aggiornato;
- il settimo controllo stabilisce che le password devono essere diverse per ogni account, devono avere una complessità adeguata e deve essere utilizzato il più sicuro sistema di autenticazione disponibile, ossia l'autenticazione a due fattori;
- l'ottavo controllo stabilisce che il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri, l'accesso è opportunamente protetto, i vecchi account non più utilizzati sono disattivati;
- il nono controllo stabilisce che ogni utente può accedere solo alle informazioni di sua necessità e competenza;
- il decimo controllo stabilisce che il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (ad esempio, riconoscere allegati e-mail) e che i vertici

aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza;

- l'undicesimo controllo stabilisce che la configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi e che le credenziali di accesso di default sono sempre sostituite;
- il dodicesimo controllo stabilisce che sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda e che i backup sono conservati in modo sicuro e verificati periodicamente;
- il tredicesimo controllo stabilisce che le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (ad esempio, firewall e altri dispositivi/software anti-intrusione);
- il quattordicesimo controllo stabilisce che in caso di incidente (ad esempio, qualora venisse rilevato un attacco o un malware) debbano essere informati i responsabili della sicurezza e i sistemi debbano essere messi in sicurezza da personale esperto.
- il quindicesimo e ultimo controllo stabilisce che tutti i software in uso, inclusi i firmware, sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

In conclusione, è possibile stabilire che applicando questi controlli a livello sistemico, si avrà una notevole riduzione del rischio di attacchi cyber.[74]

3.3 - Le attuali strategie di difesa attiva.

Una delle tematiche di sicurezza informatica più trattate e approfondite degli ultimi tempi è senza dubbio l'adozione dell'intelligenza artificiale a difesa delle aziende: l'AI al servizio della cybersecurity permette di potenziare le capacità predittive dei sistemi di difesa delle aziende e delle organizzazioni pubbliche e private di qualsiasi dimensione da cyber attacchi sempre più sofisticati. Bisogna, quindi, riuscire a rispondere in tempo reale ad eventuali minacce. Per questo motivo, si ricorre sempre più spesso al machine learning per rilevare e mitigare le minacce, ma il vero potenziale dell'intelligenza

[74]Cfr. *2016 Italian Cybersecurity Report Controlli Essenziali di Cybersecurity URL:http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf*

artificiale nella cybersecurity consiste nella capacità di effettuare previsioni realistiche di attacchi quando questi non sono neanche avvenuti.[75]

Mai come in questi ultimi tempi, infatti, rimane più che valido il vecchio motto secondo cui prevenire è meglio che curare. I tradizionali sistemi di sicurezza costruiti per contrastare attacchi basati su file usati come vettori di infezione ormai non bastano più a fermare gli attacchi perpetrati nel cyberspazio. Oggi si stanno diffondendo i cosiddetti malware fileless che non infettano più i file archiviati negli hard disk delle potenziali vittime, bensì cercano di colpire obiettivi diversi. La prima tipologia di attacco fileless si è diffusa già nel 2001 con l'uso dei worm Code Red e SQL Slammer, che sfruttavano la vulnerabilità così detta "in memory" di Windows attraverso l'esecuzione di un codice maligno direttamente nella memoria RAM dei computer. Le infezioni provocate da attacchi di questo tipo non sono in genere persistenti (la disinfezione è implicita nel riavvio del PC, ma bisogna considerare che se un semplice PC viene spento ogni sera e riavviato ogni mattina raramente questo accade per un server)[76]. Un'altra tipologia è quella con metodi persistenti: l'attaccante ottiene la persistenza sui sistemi compromessi caricando un payload in memoria in modo che l'infezione possa essere resa persistente anche dopo il riavvio di Windows attraverso specifici script o task schedulati. Un terzo metodo è il "dual use tools", ossia l'utilizzo con scopi malevoli di applicazioni lecite (ad esempio, notepad.exe, utilizzabile per modificare o leggere file oppure comandi eseguiti tramite PowerShell per la modifica di permessi utenti).[77]

Nell'attività di intelligence, il concetto di sicurezza cyber coincide con quello di sicurezza delle informazioni in senso ampio, cioè, nell'idea di "difesa attiva", che deve tener conto della raccolta permanente e selettiva delle informazioni circa le capacità cyber dei propri avversari nonché di tutte quelle operazioni legate alle PSYOP (psychological operations) e più in generale alla guerra psicologica, come dimostrano le numerose

[75]Cfr. J. S. Nye, *The Future of Power, PublicAffairs,* New York, 2011.

[76]Cfr. M. C. Libicki, *Cyberdeterrence and Cyberwarfare*, RAND, Santa Monica (CA) 2009.

[77]Cfr. *L'intelligenza artificiale a difesa delle aziende: nuove strategie di cybersecurity.* URL: https://www.cybersecurity360.it/cultura-cyber/lintelligenza-artificiale-a-difesa-delle-aziende-nuove-strategie-di-cybersecurity/

azioni di ingegneria sociale condotte "colpendo" dipendenti di aziende straniere tramite l'impiego di profili fake costruiti ad arte sui social media.[78]

In ultimo, giova ricordare la recente tendenza delle strategie di difesa attiva sull'accrescimento della protezione e della resilienza ad attacchi, nonché sulla promozione dello sviluppo secondo logiche di security-by-design di comunicazioni wireless, servizi cloud e sistemi di controllo industriale; tecnologie, queste, nodali per il processo di trasformazione digitale nelle Pubbliche Amministrazioni e nel settore industriale. In particolare, il DIS ha sostenuto la creazione, all'interno del Consorzio Interuniversitario Nazionale per l'Informatica (CINI), di un Laboratorio Nazionale di Intelligenza Artificiale e Sistemi Intelligenti (IA&SI), attesa la rilevanza dell'intelligenza artificiale quale fattore per lo sviluppo economico e sociale del Paese.[79]

Nel nuovo scenario degli attacchi la sicurezza gioca d'anticipo, il mutato scenario del cybercrime impone una protezione che sia sempre più "by design", che segua l'evoluzione delle applicazioni fin dalla loro nascita, mettendole al riparo da attacchi futuri.

Stiamo infatti assistendo ad un cambiamento graduale ma inesorabile dell'ambiente in cui le aziende operano che sta comportando una mutazione delle logiche della protezione, con il cloud che è sempre più vettore di nuovi ambienti applicativi o di infrastrutture che le imprese non vogliono più tenere in casa.

Di fatto, in un mondo sempre più interconnesso, non esiste più un perimetro aziendale definito e difendibile, ma si va sempre più verso confini sfumati e difficilmente controllabili con i vecchi sistemi di sicurezza "statici". Da qui l'esigenza di adottare applicazioni software sicure fin dalla progettazione e quindi prive di vulnerabilità e punti deboli sfruttabili durante un attacco informatico.

Per questo motivo, come detto in premessa, l'intelligenza artificiale deve essere vista come la nuova frontiera delle soluzioni a difesa della sicurezza nazionale e delle aziende: l'AI al servizio della cyber security permette di potenziare le capacità predittive

[78]Cfr. *Cyber Security: la strategia cinese.* URL:https://www.babilonmagazine.it/cina-cyber security/

[79] Vds. Relazione sulla politica dell'informazione per la sicurezza ed.2018

dei sistemi di controllo e quindi potrebbe mettere le organizzazioni pubbliche e private di qualsiasi dimensione al riparo da cyber attacchi sempre più sofisticati.[80]

3.4 - Le prospettive future.

Quanto più si sviluppa la tecnologia legata a "Internet of things", big data e, nel prossimo futuro, quella collegata all'Intelligenza Artificiale del cognitive computing, tanto più emergeranno forme nuove e sempre più sofisticate di minacce cibernetiche. Basterebbero queste poche parole per capire l'importanza sempre crescente che la cyber security assumerà nel prossimo futuro.

Se si vuol entrare in maggiori particolari, l'orizzonte da prendere in considerazione non potrà superare quello di uno-due anni, data la velocità incredibile del progresso tecnologico. Qualsiasi altra pretesa sconfinerebbe nella science fiction.

Innanzitutto, bisogna aggiungere una nota di ottimismo: se è certo che i miliardi di dati potranno essere utilizzati per scopi illegali da criminali e terroristi, nonché da avversari politici ed economici, è altresì vero che le tracce digitali da essi lasciate possono essere utilizzate dagli analisti a fini previsionali e di identificazione delle fonti.

Inoltre, normative internazionali come il GDPR, esecutivo da maggio 2018, dovrebbero progressivamente limitare la frequenza e la virulenza delle minacce, imponendo obblighi e pesanti sanzioni alle imprese europee, estendibili però anche a livello mondiale. Risulta che soltanto un 20-30% delle aziende sia pronto ad adeguarsi alle imposizioni del Decreto. L'anello più debole, anche in questo caso, è quello umano.

Un'altra contromisura, sempre prevista dal decreto comunitario, riguarda la prassi di agevolare per quanto possibile la produzione di hardware e software nello spazio dell'UE e dell'occidente intero. Non si può, infatti, non tener conto che il cyberspazio è caratterizzato da strategie competitive e conflittuali.

Infine, le misure di difesa tradizionali, come le complicate e sempre mutevoli password, dovranno cedere il passo a tecniche crittografiche e biometriche, per non parlare di quelle quantistiche.[81]

[80] https://www.cybersecurity360.it/soluzioni-aziendali/intelligenza-artificiale-e-cyber-security-nuove-strategie-a-difesa-delle-aziende/

In ultimo, giova ricordare il recente decreto-legge n. 105 contenente "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" pubblicato il 21 settembre 2019 sulla Gazzetta Ufficiale.

Tale provvedimento introduce disposizioni volte ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Tale obiettivo strategico può declinarsi secondo una serie di linee di azione. Tra queste potrebbero essere considerate le seguenti:

- **L'individuazione** dei soggetti pubblici e privati che rientrano nel perimetro cyber nonché la **definizione** dei criteri per assicurare l'innalzamento e l'armonizzazione della sicurezza delle reti, dei sistemi informativi e dei servizi informatici;
- Il **consolidamento** dei ruoli e delle responsabilità nella gestione tecnica delle varie strutture che ad oggi sono incaricate della sicurezza cibernetica. A titolo di esempio, diventa fondamentale la piena operatività del Centro di Valutazione e Certificazione Nazionale (**CVCN**) che, istituito presso il MISE, ha il compito di assicurare che i prodotti ICT utilizzati da attori con rilevanza strategica per il sistema-Paese rispondano a specifici requisiti di sicurezza. L'utilità primaria della valutazione/certificazione della Sicurezza di un sistema/prodotto è fornire una stima del livello di sicurezza secondo standard condivisi da tutti i soggetti coinvolti e di garantire che tale stima venga eseguita da una terza parte indipendente rispetto ai soggetti stessi;
- La **definizione** delle modalità per assicurare il procurement di beni e servizi ICT sicuri ed affidabili destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti.

[81] Cfr. *Il futuro della cyber security, tra nuove minacce e segnali di ottimismo URL: https://www.agendadigitale.eu/sicurezza/il-futuro-della-cyber-security-tra-nuove-minacce-e-segnali-di-ottimismo/*

L’esigenza, emersa già nel mese di maggio quando sono state sottoposte a consultazione pubblica le ***Linee guida*** specifiche di AGiD, necessita di una traduzione operativa per la standardizzazione di tutto il processo di approvvigionamento e per l’estensione delle garanzie relative alla cyber security alle supply chain;

- **L’istituzione** di un sistema di vigilanza e controllo sul rispetto degli obblighi introdotti;
- La **definizione** delle modalità di gestione e di notifica degli incidenti per i soggetti inclusi nel perimetro cyber, in ottemperanza anche alle esigenze derivanti da specifici obblighi normativi nazionali ed internazionali (come il GDPR e la NIS).

CONCLUSIONI

Un contesto cibernetico sempre più sfidante richiede un adeguamento progressivo delle infrastrutture di cybersecurity e cyberdefense.

La risposta nazionale e internazionale dovrebbe essere attivata tramite un contatto diretto con il Nucleo per la Sicurezza Cibernetica (NSC). La necessità di protezione delle infrastrutture critiche istituzionali e civili da minacce sempre più sofisticate e organizzate (schemi da operazione militare) richiede un servizio del genere.

Gli strumenti tipici dell'intelligence monitorerebbero e contrasterebbero operazioni di ricognizione cibernetica, utilizzate per la preparazione di un potenziale attacco.

La stretta collaborazione con le aziende e il mondo dell'accademia sarebbe il catalizzatore, lo strumento finale per l'adozione di standard condivisi e best practices nella prevenzione del cyber spionaggio a fini economici. Tali misure migliorerebbero le capacità di resilienza nazionali. In conclusione, rendere l'Italia un paese competitivo politicamente, economicamente e militarmente nello scenario mondiale, richiede di affinare la struttura nazionale di cybersecurity, in linea con quella dei principali alleati. Il perimetro di sicurezza nazionale cibernetica di cui al decreto-legge n. 105 del 21 settembre 2019 rappresenta il punto di partenza di questo tortuoso cammino e l'inizio dell'avventura italiana nel cyberspace.

BIBLIOGRAFIA

Aldo Giannuli "*Come i servizi segreti stanno cambiando il mondo. Le strutture e le tecniche di nuovissima generazione al servizio delle guerre tradizionali, economiche, cognitive, informatiche*" Ponte alle Grazie, 2018

Antonio Teti*, Cyber Espionage e Cyber Counterintelligence, Spionaggio e controspionaggio cibernetico*, Rubbettino, 2018

C. S. Gray, "*Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling, Strategic Studies Institute*", Carlisle PA, April 2013

Barlow J. P. (1996), *A Declaration of the Independence of Cyberspace, Davos*, Switzerland

BBC News (2017), *Cyber-attack: Europol says it was unprecedented in scale*, 13 maggio

Belviolandi S *"Rapporto Clusit 2017 sulla sicurezza IT e Cybercrime: l'Italia vittima dei Ransomware"* (2017), 22 febbraio

Camodeca D. (2017*), Attacco Cibernetico su scala mondiale, riscatto in Bitcoin*, 13 maggio

Langevin J., McCaul R., Michael T., Charney S.,Raduege H. (2008), *Securing Cyberspace for the 44th Presidency,Center for Strategic and International Studies Washington DC*

Rid T.(2013), *Cyber War Will Not Take Place*, Oxford U.P.

Clarke R.A., Knake R.K. (2014), *Cyber War*, Tantor Media

W. Gibson, "*Neuromante*", 1984

SITOGRAFIA

www.cybersecurityframework.it

www.archiproducts.com

www.kaspersky.it

www.itseducation.asia

www.whoishostingthis.com

www.international.gc.ca

www.lifewire.com

www.tomshw.it

www.uscert.gov

www.sciencedirect.com

www.sicurezzanazionale.gov.it

www.cybersecitalia.it

www.gazzettaufficiale.it

www.difesaesicurezza.com

www.sicurezzaegiustizia.com

www.cybersecurity360.it

www.cybersecurityframework.it