Il cyberspazio: definizioni, minacce e strumenti di contrasto istituzionali.

Di Giovanni dott. Salvatore

INDICE

Introduzione

Definire il ciberspazio oggi è molto complesso; digitando la parola sul motore di ricerca di *Google* si ottengono più di trentuno mila pagine di risposta. Ma dare un significato il più circostanziato possibile risulta necessario per poter avviare un approfondimento come vuol essere il presente elaborato. Non avremo la presunzione di fornire la definizione "giusta" ma daremo al lettore la nostra interpretazione per poi analizzare brevemente quanto il ciberspazio sia ormai parte essenziale delle nostre vite; e più approfonditamente quali pericoli presenta e quali strumenti sono necessari per contrastare questi pericoli.

L'autorevole sito della enciclopedia Treccani[1] nella sezione lessico del XXI secolo definisce il neologismo come l'insieme di tutti i sistemi digitali di connessione, acquisizione e condivisione delle informazioni; avvertendo al contempo che il termine si è diffuso come sinonimo di internet. Nella nostra accezione partiremo dalla prima affermazione ampliandone il concetto includendo nel "nostro" cyberspazio anche tutte quelle tecnologie che "escono" dal computer e invadono in maniera, più o meno pervasiva, la nostra vita reale. Estendiamo, cioè, la visione di colui che ha coniato il termine: lo scrittore di fantascienza William Gibson che in un racconto del 1982 dal titolo *Burning Chrome* pubblicato nella rivista Omni[2] e successivamente nel suo romanzo *Neuromancer*, usò per la prima volta *cyberspace;* nata dalla fusione di cibernetica, che indica i fenomeni biologici, artificiali o misti di autoregolazione, con spazio per definire un "luogo" da contrapporre allo spazio reale che nel suo lavoro definiva *meatspace*, ovvero "mondo della carne"[3].

Ma davvero il mondo del computer, di internet, degli 0 e 1 che sfrecciano in tutto il globo possono influenzare la nostra vita? Il primo è più immediato effetto lo si scorge dall'approccio psicologico/linguistico entrato nell'uso comune del modo con cui ci si riferisce ad esso. Infatti utilizziamo ampiamente metafore spaziali per la fruizione della rete; normalmente usiamo la parola navigazione per riferirci alla rassegna delle pagine web di interesse e per condividere file utilizziamo le parole afferenti al trasporto merci quali caricare, scaricare, spedire; i singoli elementi costitutivi del web sono denominati siti, e gli

1 Treccani, la cultura degli italiani; http://www.treccani.it/enciclopedia/cyberspazio_%28Lessico-del-XXI-Secolo%29/

2 Omni è stata una rivista di fantascienza e scienza pubblicata negli Stati Uniti e in Gran Bretagna, che conteneva articoli riguardanti fatti scientifici e piccoli racconti fantascientifici. Il primo numero fu pubblicato nell'ottobre del 1978, e l'ultimo nell'inverno del 1995, con una versione via internet che durò fino al 1998.

3William Gibson, Neuromancer, Ace Books, 1997;.

ambiti posti sotto il controllo del proprietario del sito vengono detti domini. Analogamente di tipo spaziale sono le analogie con le quali, normalmente, definiamo le azioni connesse : ”sono andato su Youtube”, “sono stato un’ora su Facebook” oppure “ho fatto un giro in Internet”.

Ma l’impatto sul mondo reale non afferisce solo alla sfera linguistica, lo spazio informatico pervade più aspetti della nostra vita di quanto ci aspettiamo. In questa introduzione ci limiteremo ad una fugace disanima di questi aspetti rimandando ai capitoli successivi l’approfondimento di quelli che interessano il comparto sicurezza in senso lato. Attraverso la rete di calcolatori circolano tutti i servizi offerti dalle pubbliche amministrazioni o associazioni ed aziende private. E anche se per alcune prestazioni dobbiamo rivolgerci ai vari sportelli aperti al pubblico il nostro interlocutore per risolvere la necessità prospettata interrogherà sicuramente un archivio informatico.

Molto più evidente è la dipendenza da internet del mondo bancario finanziario. A prescindere dalle banche operative solo su internet anche quelle più tradizionali offrono ai loro clienti servizi di *home-banking*, usufruiscono di terminali agli sportelli ed utilizzano sistemi di erogazione del contante attraverso postazioni ATM (c.d. *bancomat*). Per il loro corretto funzionamento tutte queste apparecchiature devono disporre di un collegamento in rete. E tutto questo per soddisfare le più elementari operazioni; impensabile immaginare il corretto funzionamento del sistema borsistico mondiale senza l’uso di connessioni informatiche.

Anche il sistema produttivo di qualunque paese del mondo dipende da reti di comunicazioni; forse solo il sistema puramente artigianale costituito da micro imprese potrebbe farne a meno. Per tutto il resto l’uso dei robot nelle catene di montaggio, dei calcolatori per il monitoraggio delle fasi produttive e dei sistemi di comando e controllo, per non parlare di quelli di sicurezza prevedono un altissimo tasso di informatizzazione.

Nel campo medico si sta radicando sempre più la così detta telemedicina che rappresenta la nuova frontiera per la cura delle malattie: dallo svolgimento delle visite, alla gestione dei rapporti medico paziente, all’ausilio del medico in sala operatoria. I pazienti possono stabilire un contatto diretto con il personale sanitario grazie a portali specifici che consentono di effettuare vere e proprie visite virtuali tramite video conferenza o semplicemente tramite uno scambio di domande e risposte. Ma c’è di più, la diffusione sempre più marcata di applicazioni (c.d. App.) dedicate alla salute offre la possibilità di monitorare alcune delle nostre più basilari funzioni vitali in tempo reale e trasmetterli al medico curante. Internet ha aperto ad un nuovo modo di concepire il controllo delle

condizioni cliniche; i medici hanno la possibilità di conoscere il nostro stato di salute ed intervenire prontamente in caso di bisogno, modificando, per esempio, la frequenza del peacemaker impiantato nel paziente e collegato in rete. Tramite sensori applicati ai *computer* o *smartphone* o *tablet* ogni utente ha la possibilità di farsi visitare direttamente da casa con risparmi in termini di tempo e costi considerevoli.

Altro settore fortemente dipendente dalle connessioni in rete è quello dei trasporti. Sia che si esamini il trasporto aereo, sia quello navale che quello ferroviario a lunga percorrenza o urbano il tasso di automazione è presente in ogni aspetto di tali attività. Dal controllo dei mezzi di locomozione, al monitoraggio dei movimenti, per arrivare fin alla più semplice attività di prenotazione di un viaggio l'utilizzo di elaboratori elettronici risulta indispensabile. E questa automazione sta pervenendo a livelli molto più vicini alla vita di tutti i giorni; paesi con forte vocazione alla informatizzazione sono arrivati perfino a gestire in maniera automatica la regolazione del traffico potendo intervenire sui singoli semafori presenti in città.

E cosa dire della scuola? Prepotentemente spinta dalla crisi pandemica del Covid-19 ad una informatizzazione forzata.

Un ultimo spunto di riflessione, pur nella consapevolezza che l'elenco risulta infinito, riguarda il vasto mondo dei sistemi di produzione dell'energia. Esso comprende sia i processi della generazione di energia elettrica, che già si declina in vari modi dalla centrale a carbone a quella nucleare, sia l'industria estrattiva di idrocarburi, passando per la distribuzione attraverso elettrodotti, gasdotti, oleodotti, raffinerie eccetera. Con i livelli di consumi, e di conseguenza produzione attuali sarebbe impossibile ottenere i risultati raggiunti senza l'uso di *computer*.

Tutte le situazioni appena accennate non sono però scevre da rischi. Dal più banale guasto che può inficiare momentaneamente l'erogazione di alcuni servizi, all'attacco mirato motivato dai più svariati propositi. Va da se che ad ogni eventuale blocco dei vari sistemi non corrisponderà la stessa incidenza in termini di pericolosità, però non va trascurata la possibilità che alcuni di essi potrebbero rivelarsi persino letali. Provenienti generalmente da una fonte anonima gli attacchi informatici posso essere eseguiti per diverse finalità: chi li considera attività ludiche e li realizza per dimostrare la propria bravura, chi li compie per eseguire furti, alterazione o distruzione di specifici obiettivi per attivismo o vendetta. Se poi gli attacchi provengono da terroristi o entità statali si entra nel mondo della *ciberguerra* ed è proprio contro questo tipo di minacce che lo Stato ha il

dovere di difendere se stesso ed i propri cittadini. Ed è proprio su questo ultimo punto che il presente studio intende soffermarsi.

Capitolo 1
Introduzione allo spazio/mondo Cyber

Che cos'è lo spazio cyber

Anche se nell'introduzione si fa accenno ad una prima definizione di cyberspazio, pare necessario estenderne ulteriormente il significato al fine di chiarire l'accezione che questo lavoro si propone di fornire. Per cyberspazio intenderemo quel "luogo-non luogo" dove tutte le attività per essere eseguite al meglio delle loro possibilità hanno bisogno di un *computer* o dispositivi elettronici che necessitano di una connessione fra loro e/o con il mondo di *internet*. Gli esperti ci indicano che *world wide web* non è la sola rete di connessione possibile, esistono infatti reti *intranet* private o addirittura reti locali non direttamente collegate in *internet* ma anche queste entità necessitano comunque di sistemi operativi e software in qualche maniera collegate con il resto della tecnologia. Quindi è considerato *cyberspazio* l'archivio dell'anagrafe del nostro comune di residenza, il sistema di allarme di una industria e recentemente anche quello di casa nostra, i sensori di controllo di una centrale elettrica, le telecamere che monitorano il traffico di una città eccetera.

Altre interpretazioni propongono una visione stratificata del *cyberspazio*[4] suddividendolo in quattro strati interconnessi fra loro: uno strato fisico, costituito da infrastrutture e dispositivi; uno strato logico, che comprende i servizi che assicurano la trasmissione dei dati; uno strato costituito da applicazioni e programmi, che permette agli esseri umani di interfacciarsi con le macchine; e uno strato dell'informazione e dell'interazione sociale, che è quello che più aiuta ad intendere il *cyberspazio* come spazio geografico. Ma le due definizioni non sono in contrasto fra loro, semmai la seconda è più puntuale nella distinzione dei singoli componenti ma, vista come insieme, coincide con la prima.

Il *cyberspazio* conta già milioni di elementi ed è in atto un processo di continua assimilazione di ulteriori componenti che rendono questo spazio sempre più grande. Ultimamente si sente parlare di internet delle cose[5], intendendo con questa locuzione una

4 Frederick. Douzet, La géopolitique pour comprendre le cyberespace,rivista di geopolitica Hérodote 2014/1; p. 3-21.

5[5]Davide Bennato, Il computer come macroscopio. Big data e approccio computazionale per comprendere i cambiamenti sociali e culturali, Franco Angeli, 2015

famiglia di tecnologie il cui scopo è rendere qualunque tipo di oggetto, di per se senza una vocazione digitale, un dispositivo collegato ad *internet* con proprietà di monitoraggio e controllo. Per rendere meglio l'idea già alcuni elettrodomestici possono essere controllati a distanza: dalle serrature che si aprono e chiudono con lo *smartphone*; al termostato che regola automaticamente la temperatura dell'appartamento e che si può accendere o spegnere a distanza, telecamere che consentono di monitorare l'appartamento quando non si è in casa; e il frigorifero che ti avvisa quando un alimento sta per terminare o per scadere; e ognuno di loro è in grado di avvertirti o avvertire il centro assistenza in caso di guasto o malfunzionamenti. Ma l'*internet* delle cose non è solo domotica; le nostre autovetture diventano sempre più "intelligenti" e collegate. Dal monitoraggio dei parametri di funzionamento e dal rilevamento di guasti si è passati al controllo remoto dell'apertura delle porte in caso di smarrimento delle chiavi, alla profilazione del nostro stile di guida per determinare l'ammontare del premio da pagare alle assicurazioni. Non tralasciando nemmeno l'aggiornamento delle situazioni di traffico così da poter disporre di un percorso sgombero da parte del nostro navigatore.

Per non parlare poi della realtà aumentata che ci permette di visionare dati e contenuti multimediali sovrapponendoli a ciò che circonda l'utente anziché costringerlo a guardare un supporto visivo. Ed in più il dispositivo opportunamente connesso alla rete è in grado di riconoscere gli elementi dell'ambiente circostante e reperire e visualizzare tutte le informazioni afferenti.

E non c'è limite alle possibilità di espansione, basta avere fantasia. Un buffo esempio è rappresentato da *iCPooch***,** inventato da una ragazzina di soli quattordici anni, permette di restare in contatto con il proprio animale domestico anche a distanza. Oltre ad avere un schermo dove è possibile trasmettere dei videomessaggi il *device* è anche un *dispenser* per il cibo così da permettere al proprietario di prendersi cura dell'amico a quattro zampe anche da molto lontano.

Il diffondersi di queste tecnologie farà si che arriveremo in breve alla totale interconnessione del pianeta. Tutti saranno connessi con tutti, tutto sarà connesso con tutto; e questo genererà ulteriori trasformazioni nelle relazioni di ogni genere: personali, commerciali ed economiche, politiche e sociali, statuali e perfino delle relazioni internazionali[6]. In particolare sotto quest'ultimo punto di vista il grosso dell'attenzione è stato rivolto all'esercizio del potere statale per via dalla porosità dei confini nel

6 Cristiano Giorda, Cybergeografia. Estensione, rappresentazione e percezione dello spazio nell'epoca dell'informazione, Tirrenia Stampatori, Torino, 2001

cyberspazio. Questo stato di cose porta ad un ripensamento del ruolo degli Stati e mette in discussione la rappresentazione del mondo ed i rapporti di forza fra le potenze come lo abbiamo inteso sin ora. Così oggi costituisce un vantaggio geopolitico il controllo delle infrastrutture fisiche del *cyberspazio*. Le rivalità scaturite da questa nuova necessità di primeggiare è stato paragonato alla competizione per le risorse naturali ed è stato indicato come il quinto dominio della conflittualità fra gli stati[7]; un nuovo terreno di scontro tra gli attori geopolitici tradizionali nel quale però nuovi soggetti hanno la possibilità di inserirsi data la sua natura "fluida" che consente a tutti gli attori di interferire, sia a livello fisico che a livello logico, con costi estremamente più bassi rispetto alla costituzione di eserciti e armi avanzate, pedine, quest'ultima, esclusive delle grandi potenze.

Il tipo di "armi" non militari utilizzabili per combattere in questo scenario rende le infrastrutture *cyber*, prevalentemente civili, i nuovi obiettivi da dover proteggere contro un nemico che il più delle volte "agisce nelle ombre". Il campo di scontro non è più un "territorio" che segue le leggi della fisica, ma uno spazio dove non ci sono ne leggi naturali ne codici legislativi e non valgono i trattati internazionali; di fatto nel ciberspazio regna una situazione di anarchia resa sistemica e strutturale dalla natura degli elementi che lo compongono[8].Si è creato, più o meno volutamente, un meccanismo di diffusione del potere.

E così il cyberspazio si trasforma in un dominio fonte di pericolose minacce alla sicurezza nazionale e allo stesso tempo un nuovo terreno su cui sviluppare una politica di potenza per aumentare e rivendicare la propria posizione nell'arena internazionale.

Moltissimi attori oggi accedono al *cyberspazio* quotidianamente per lavoro, per svago, per affari, ma anche per delinquere o compiere azioni di sabotaggio o vero e proprio terrorismo; per tale motivo gli operatori statuali deputati alla difesa di un paese devono giocoforza essere presenti ed intervenire per reprimere o prevenire reati o azioni che posso addirittura arrivare ad attentare l'integrità dello stato stesso[9]. In pratica il *cyberspazio* è divenuto un nuovo territorio dove lo stato deve in qualche modo operare con criteri uguali a quelli fin qui adottati per la difesa politico-militari dei confini o per il controllo del territorio.

---

7 Luigi. Martino, La Quinta Dimensione della Conflittualità. La rilevanza Strategica del Cyberspace e i Rischi di Guerra Cibernetica, CSSI - Centro Universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII) ttp://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf.

8 Iacopo Chiarugi, Nicolò De Scalzi, Luigi Martino, Marco. Mayer, La politica nell'era digitale. Dispersione o concentrazione del potere?, in Umberto Gori, Luigi Martino (a cura di), Intelligence e Interesse nazionale, Aracne, agosto 2015.

9 Per non far sembrare questa una affermazione esagerata basti pensare al c.d. *Russia Gate* che sta movimentando la vita politica americana nel quale si ipotizza una intromissione di *hacker* russi nelle elezioni presidenziali che hanno visto trionfare Donald Trump.

Il cyberspace non ha influenza solo sui computer

Definito per grandi linee che cosa è il cyberspazio appare facile immaginare quanto un guasto o un attacco mirato non abbia conseguenze solo "all'interno dello schermo" del computer. Sono innumerevoli gli esempi di attacchi informatici che hanno avuto ripercussioni nella vita di molti cittadini, o di azioni miranti al perseguimento di uno specifico obiettivo militare. In quest'ultimo caso con implicazioni geopolitiche evidenti.
La difficoltà di attribuzione delle responsabilità fa si che non sia possibile pianificare azioni di rappresaglia immediata; molto spesso sono necessari giorni, a volte settimane, prima di accorgersi di aver subito un attacco. Ed anche se ci si accorgesse in tempo reale di attività ostili difficilmente si riuscirebbe a risalire con certezza all'origine dell'attacco limitando l'azione di risposta alla sola predisposizione di misure volte a fermare l'attacco ed evitare che provochi gravi conseguenze.

Famoso l'esempio, salito all'onore delle cronache mondiali, dell caso di un attacco globale, a fini di estorsione, perpetrato attraverso l'uso di un *malware*[10] del tipo *ransomware* che blocca l'accesso ad un computer e offre al suo proprietario la restituzione dei propri dati in cambio di un riscatto. Questo programma denominato *WannaCry* è stato in grado di colpire numerose aziende ed alcune istituzioni pubbliche importanti. A quanto è dato sapere, in molti preferiscono non pubblicizzare la loro vulnerabilità, la maggiore criticità per il "mondo reale" dell'azione di *wannacry* si è avuta in Inghilterra dove l'attacco informatico ha creato problemi ad alcuni ospedali del regno causando l'impossibilità di accedere ai dati dei pazienti. Gli ospedali e le cliniche sono state costretti a respingere i malati, compresi quelli con le patologie più gravi. Il problema è stato risolto grazie alla intuizione di un giovane ricercatore che ha trovato un "*kill switch*", una sorta di sistema di sicurezza che permetteva di bloccare la pericolosità del virus. La felice risoluzione del problema ha fatto sorgere non poche considerazioni. Pare accertato che questo *malware* sia stato prodotto dalla National Security Agency statunitense per attaccare sistemi informatici basati sul sistema operativo Microsoft Windows. A sostegno di questa tesi contribuisce proprio questa sorta di sistema di sicurezza in grado di controllare l'attività del virus. Perché mai un creatore di virus che ha intenzione di estorcere più denaro possibile si debba preoccupare di inserire una via di fuga/salvezza? La N.S.A. si è comportata come fa qualunque esercito regolare quando crea un campo minato: nel depositare le mine sul

10 *Malware*, abbreviazione per *malicious software* (che significa letteralmente *software* malintenzionato, ma di solito tradotto come *software* dannoso), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un *computer*, rubare informazioni sensibili, accedere a sistemi informatici illegalmente.

terreno queste vengono minuziosamente segnalate in una carta per poi essere eliminate quando cessa la necessità della difesa. La seconda considerazione è che adesso si può ragionevolmente dubitare sulla sicurezza del sistema operativo *windows*; e non tanto per le innumerevoli falle non previste, e presenti in buona fede[11], sfruttate dagli *hacker* di tutto il mondo per violare i sistemi informatici, quanto per le "porte di accesso" occulte lasciate di proposito e condivise con le agenzie di sicurezza americane. Terza considerazione: il *malware* non aveva un obiettivo specifico e ha colpito indiscriminatamente in tutto il mondo ed in ogni campo, è stato colpito anche l'impianto di assemblaggio Renault in Slovenia che ha interrotto la produzione per alcune ore. E' stata quindi l'attività di uno o un gruppo di criminali ricattatori o una sorta di esercitazione per testare la validità della metodologia di attacco un po' come si faceva negli anni quaranta e cinquanta per testare le armi nucleari?

Sicuramente concepito come attacco intenzionale e mirato, e di relativamente facile attribuzione seguendo la logica del "*cui prodest*", è stato il noto episodio di *Stuxnet*: virus indirizzato ad interferire col programma nucleare iraniano. Si scoprì che il virus aveva una firma certificata che gli consentiva di superare i controlli del sistema operativo senza troppi problemi ed ingannare gli antivirus che non riuscivano ad identificare il file come pericoloso. Il *modus operandi* del virus era semplice ma geniale: programmato per colpire alcuni dispositivi di controllo di processi industriali, denominati genericamente SCADA, prodotti dalla tedesca Siemens si rivelava eccellente nell'attività di ingannatore sabotando le centrifughe di arricchimento dell'uranio e contemporaneamente segnalando il perfetto funzionamento dei sistemi. Sebbene la sua presenza sia stata rilevata in diverse centrali in tutto il mondo *stuxnet* è stato in grado di riconoscere in quale impianto si trovava, e attivarsi solo per il bersaglio prestabilito, in particolare la centrale nucleare iraniana di Bushehr, ritenuta da molti come una potenziale fabbrica di armi atomiche.

Sia che si tratti di attacchi di criminali o di agenzie statali è ormai chiaro che un attacco informatico può benissimo influire sul corretto funzionamento di una intera nazione e incidere pesantemente sulla vita dei cittadini. Va da se che in caso di conflitto aperto tra due nazioni le "operazioni" nel *cyberspazio* non si discosterebbero molto dalle normali azioni di guerra e quindi tali atti si possono annoverare a pieno titolo fra gli strumenti bellici a disposizione di una nazione, ancorché non contemplate e regolamentate dal diritto dei conflitti armati. Ma le "armi" del *cyberspazio* posso facilmente essere utilizzate da singoli o gruppi criminali o peggio da terroristi che con poco sforzo organizzativo e legittima speranza di assoluta impunità possono compiere attentati con enormi effetti distruttivi.

11 cosiddetti *zero-day,* cioè vulnerabilità non note alle società di creazione di *software* e antivirus.

Il mondo cyber è un Soft Target!

Dall'analisi di quello che gli esperti definiscono "*soft target*" si evince come il *cyberspazio* rientra, purtroppo, a pieno titolo nella categoria dei bersagli "morbidi", facili. Per potersi definire *soft* un obiettivo deve rispondere a determinate e ben specificate caratteristiche distintive. Aree aperte e spaziose con atmosfere invitanti e rilassanti che non suscitano sensazioni di pericolo e quindi attenzione. Questi luoghi dispongono di molteplici entrate ed uscite e spesso esistono accessi diretti da strade ad alta intensità di traffico o stazioni della metropolitana. Rientra nella norma vedere avventori con pacchi o bagagli voluminosi e ordinariamente presentano grandi parcheggi situati nel perimetro o nelle immediate vicinanze. Queste aree raramente dispongono di sistemi di difesa passiva e protocolli di sicurezza attivi per rispondere ad una eventuale minaccia. Anche quegli esercizi che dispongono di guardie di sicurezza spesso sono disarmate e mancanti della formazione e delle attrezzature necessaria per fronteggiare un attacco terroristico. In più il gran numero di persone che accedono quotidianamente ai siti non consente ne un adeguato screening su individui e mezzi che transitano ne un monitoraggio di eventuali comportamenti sospetti riconducibili alla preparazione di un attentato quali ad esempio il sopralluogo del sito, il trasporto e la dislocazione di esplosivi o armi. Tra i "bersagli morbidi", quindi, si possono annoverare i centri commerciali, le scuole, i cinema, gli ospedali, i parchi, gli stadi, gli alberghi, le stazioni ferroviarie eccetera. Sebbene la distinzione non è mai netta, e può mutare anche in riferimento a particolari eventi contingenti, la controparte è rappresentata dagli *hard target*: aree o plessi che in genere limitano l'accesso al pubblico, hanno sufficienti misure di sicurezza in grado di fornire un elevato livello di protezione contro un attacco. Rientrano in questa categoria gli edifici governativi, le installazioni militari , le ambasciate, le centrali nucleari eccetera. In posizione mediana si pongono gli aeroporti in quanto pur possedendo le caratteristiche dei soft target, essendo stati luoghi privilegiati di attentati terroristici in passato, dispongono di sistemi di sicurezza maggiorati rispetto a tutti gli altri. Per questi motivi risulta facile capire perché gli attacchi contro obiettivi morbidi sono attraenti per le organizzazioni terroristiche perché presentano caratteristiche operative che li rendono vulnerabili e facili da sfruttare, garantendo così un maggiore successo dell'azione.

Mutatis mutandis il concetto di *soft target* si può serenamente estendere al *cyberspazio*. Come in un centro commerciale ci sono innumerevoli porte di accesso, il traffico dei dati è talmente vasto e continuo che risulta difficile monitorarlo; per cui

prevenire attraverso un “controllo dei movimenti” un eventuale attacco non rientra fra le attività facilmente realizzabili. Per quanto possano essere sofisticate e attenzionate da parte delle autorità preposte, le misure di sicurezza rientrano nella sfera di pochi e iper-specializzati professionisti o aziende che comunque sono in grado di approntate misure per prevenire situazioni anomale che sono già state documentate. Per questo gli sforzi negli attacchi sono principalmente volti a scoprire punti deboli dei sistemi in quel momento sconosciuti che quindi costituiscono una via di accesso indisturbata e potenzialmente a disposizione di tutti i sapienti digitali.

Per violare un dispositivo di sicurezza informatica non è necessario disporre di attrezzature costose; gli aggressori informatici non hanno quasi mai bisogno di essere fisicamente vicini ai loro obiettivi e i loro attacchi posso facilmente attraversare i confini nazionali con un’alta probabilità di restare anonimi.

Secondo i dati raccolti da Kaspersky[12] lungo tutto l’arco del primo trimestre del 2020 le soluzioni *anti-malware* di Kaspersky Lab hanno complessivamente respinto ben 479.528.279 attacchi condotti attraverso siti Internet compromessi, dislocati in 190 paesi diversi[13]. Per tali motivi anche le infrastrutture tecnologiche degli attori più attenti alla sicurezza che dispongono di risorse economiche da investire nel settore, che nel mondo reale rientrerebbero nella categoria degli hard target, presentano pressoché le stesse vulnerabilità dei soggetti più ingenui con conseguenze enormemente maggiori rispetto all’utente medio in caso di attacco. Va da se che gli obiettivi sensibili di una nazione, presenti nel cyberspazio, siano i bersagli più ambiti delle mire degli attori “cattivi” sia che si tratti di competitori, attivisti, terroristi, gruppi criminali o semplici hackers che agiscono nel cyberspazio per fini diversi, più o meno svincolati dal controllo o dal mandato di stati o grandi organizzazioni.

Immaginiamo un attacco informatico ad una centrale nucleare in grado di provocare un incidente con fuoriuscita di radiazioni. Un attentato così sarebbe il sogno di ogni giovane jiadista.

12 è un'azienda russa con sede a Mosca fondata nel 1997 specializzata nella produzione di software progettati per la sicurezza informatica.

13 https://securelist.it/it-threat-evolution-q1-2020-statistics/62536/

Capitolo 2:
Difesa e *Cyber threat*

Perché è necessario parlare di difesa

Lo scontro nel *cyberspazio*, cosi come in qualunque altro luogo, è generato dalla contrapposizione di interessi concorrenti; dato che lo spazio cibernetico include sia elementi digitali che fisici, scambio di idee, condivisione e diffusione delle informazioni, coinvolgimento politico e sociale, scambi economici e commerciali, cavi, satelliti, *routers*, *computer* di amministrazioni pubbliche e private, appare evidente che contiene elementi che hanno rilevanza economica, politica, strategica per la sicurezza nazionale di tutti gli attori che a vario titolo interagiscono con esso; in pratica tutti i paesi del mondo. Così sviluppare nuove capacità e nuovi strumenti per migliorare la sicurezza del sistema *cyber* rappresenta una sfida della massima importanza per la crescita e per il benessere e la sicurezza degli stati e dei suoi cittadini. La correlazione tra prosperità economica di una nazione e la qualità delle sue infrastrutture *cyber* sarà sempre più stretta e un paese, per stare nel gruppo delle nazioni più sviluppate, dovrà migliorare la sicurezza *cyber* nella società, nel sistema industriale e nella pubblica amministrazione. Proprio per questa ragione, molti paesi avanzati stanno progettando e realizzando piani strategici nazionali che coinvolgono pubblico, privato e ricerca che puntano a rafforzare la difesa delle infrastrutture critiche nazionali, delle organizzazioni governative, delle aziende e dei singoli.

I rischi associati allo spazio cibernetico sono di diversa natura e sono legati tanto alle relazioni fra stati che alla presenza di attori non statuali. Anche se ad oggi le situazioni di confronto o conflitto fra stati, c.d. *cyberguerra*, censiti si contano in poche unità il vero terreno di scontro si manifesta nel campo del *cyberspionaggio* a danno di apparati governativi, civili e militari, ma anche di imprese private. Attualmente, dunque, le minacce più probabili nello spazio cibernetico provengono da attacchi di gruppi, sostenuti o tollerati da governi, e dallo spionaggio informatico di reparti di intelligence che cercano di penetrare i sistemi informatici di paesi esteri a fini politici, economici e militari. A titolo d'esempio esaminiamo l'impatto economico degli attacchi informatici sulle piccole e medie imprese che, come noto, sono l'asse portante della struttura economica della Unione

Europea ed in particolare dell'Italia. Un rapporto del *World Economic Forum*[14] ha affermato che nel 2016 il *cybercrime* ha generato un volume d'affari di almeno 12 miliardi di dollari evidenziando che si tratta di un dato sottostimato, e che il costo in Europa è stato calcolato in oltre 750 miliardi di dollari considerando le perdite dirette, le perdite di tempo, le perdite di opportunità di business e le spese per riparare i danni. A questi andrebbero sommate anche i danni di immagine che possono solo essere stimati.

Spostandoci nella sfera delle relazioni fra gli stati sorge quindi il problema di come regolare la conflittualità sul *cyberpazio* e come considerare un attacco informatico. A tal proposito, rimane una questione aperta se un attacco portato attraverso "*internet*" costituisca o meno un attacco armato e quale reazione è possibile adottare. Un gruppo di esperti indipendenti, sotto il patrocinio della NATO nell'aprile del 2013 ha pubblicato il risultato di un approfondito studio, durato tre anni, riguardante la relazione fra *cyberspazio* e diritto internazionale nella sua parte riguardante il diritto bellico e il diritto umanitario[15]. Sulla base di questo documento durante il vertice NATO del settembre 2014, i capi di stato dei paesi membri hanno avallato una nuova "*Cyber Defence Policy*" che include la difesa dello spazio cibernetico nel compito di difesa collettiva dell'alleanza atlantica facendolo rientrare fra gli eventi in grado di attivare l'articolo 5.

Nonostante le iniziative internazionali volte alla definizione di norme condivise per la regolazione del *cyberspazio*, a causa della volontà di molti stati di mantenere la massima libertà d'azione per le proprie attività di *intelligence* o per i propri attacchi cibernetici non si è ancora riusciti a pervenire ad una soluzione unanimemente accettata.

Da queste premesse appare chiara la continua corsa all'implementazione delle infrastrutture fisiche del *cyberspazio* in aree geografiche che ricadono sotto il controllo di uno stato; Il possesso/controllo di tali strutture da un vantaggio geopolitico e una superiorità strategica rispetto a tutti gli altri competitori. Un classico esempio è costituito dai c.d. data center, solitamente un edificio che ospita un numero elevato di apparecchiature e infrastrutture informatiche in grado di contenere una grande quantità di dati e di garantirne la sicurezza fisica e gestionale. La quantità e la qualità dei dati immagazzinati permette di creare una "nuova linea del potere" che a ragione è stata

14 Il Forum economico mondiale(nome originale in inglese: World Economic Forum, conosciuto anche come Forum di Davos) è una fondazione senza fini di lucro con sede a Cologny, vicino a Ginevra, in Svizzera, nata nel 1971, La fondazione organizza ogni inverno un incontro tra esponenti di primo piano della politica e dell'economia internazionale con intellettuali e giornalisti selezionati, per discutere delle questioni più urgenti che il mondo si trova ad affrontare, anche in materia di salute e di ambiente. La fondazione pubblica numerosi documenti di approfondimento, sotto forma di report e analisi di scenario.

15 Cfr Autori vari, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press 2013. Reperibile all'indirizzo web https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

definita la geopolitica dei dati[16].Questi "centri" ospitano quantità gigantesche di informazioni forniti dagli utenti ai sistemi del fornitore il c.d. *Cloud Computing*. Dove non è presente il *data center* i governi possono controllare la trasmissione e sono in grado di incrociare i dati per ricavarne informazioni o statistiche avanzate, ma non hanno una sufficiente rete di "sensori" a livello globale per poter studiare in tempo reale quello che avviene nel mondo. Non hanno la base dati e la capacità di calcolo tale da poter trasformare con efficacia tali informazioni in azione strategica con valore geopolitico e geoeconomico. Possono fare azioni di data mining[17] specifico su informazioni liberamente accessibili su Internet, azioni avanzate di *Open Source Intelligence* ma mancano di capacità computazionali di previsione equiparabili a quella dello Stato e delle società private[18]" che detengono i data center, società ed istituzioni per lo più statunitensi. Il "controllo" di cui si tratta, rappresenta il salto di qualità nella raccolta dati iniziata con *ECHELON*[19]. Se prima i dati venivano raccolti tramite un sistema passivo di ascolto indiscriminato adesso la maggior parte delle informazioni sono rese accessibili dall'utente stesso o trasmesse in automatico dalle macchine.

Capitolo a se stante è l'utilizzo del *cyberspazio* da parte di organizzazioni terroristiche e non solo a fini di propaganda, addestramento, autofinanziamento e pianificazione. A causa dell'aumento della loro competenza tecnica, la capacità di questi gruppi di rappresentare un pericolo reale alle infrastrutture critiche di un paese fa si che questa sia diventata la più grave minaccia a cui far fronte. Non è un caso che nelle relazioni al Parlamento delle agenzie di informazione e sicurezza[20] da alcuni anni i nostri 007 hanno incluso la minaccia cibernetica per l'Italia come una realtà da non sottovalutare, individuandone due aspetti principali: il *cyberspionaggio* per fini industriali e la *cyberjihad*.

Allo stato attuale lo spazio *cyber* si presenta come uno spazio a-normato, privo di gerarchie formali o autorità sovrane con poteri giuridicamente vincolanti capaci di influenzare in modo effettivo l'azione degli altri attori presenti sulla scena, o legittimata

16 Francesco Vitali, La geopolitica economica dei dati e il futuro del dominio. Dal controllo alla previsione. Il potere tra social media e manipolazione dell'azione sociale, in Nomos & Khaos. Rapporto Nomisma 2011-2012 sulle prospettive economico-strategiche, pp. 207-231, Agra 2012.

17 Il data mining è l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di un sapere o di una conoscenza a partire da grandi quantità di dati (attraverso metodi automatici o semi-automatici) e l'utilizzo scientifico, industriale o operativo di questo sapere

18 Francesco Vitali, La geopolitica economica dei dati e il futuro del dominio. Dal controllo alla previsione. Il potere tra social media e manipolazione dell'azione sociale, op. cit.

19 Il termine Echelon è un nome in codice che si riferisce ad una rete informatica, segreta fino al 1997, capace di controllare l'intero globo e di intercettare, selezionare e registrare ogni forma di comunicazione elettronica. E' composta da satelliti artificiali, super computer e un certo numero di stazioni a terra in grado di ricevere informazioni dai satelliti artificiali presenti in orbita.

20 Cfr. https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html anni 2018, 2019, 2020

all'uso della forza. L'assenza di un quadro giuridico di riferimento certo, continuerà a pesare sulla possibilità di *governance*. Come nella migliore tradizione delle relazioni internazionali.

l'unico aspetto che vede tutti d'accordo è quello relativo al contrasto del *cybercrime*, ritenuto di primaria importanza per i forti impatti economici che presenta. Le aree interessate dalla criminalità sul *cyberspazio* non sono, come potrebbe sembrare ad una prima disamina, di secondaria importanza; infatti accanto al furto e manipolazione di dati sensibili, clonazione di carte di credito e truffe informatiche si commettono nel mondo *cyber* reati gravi quali il traffico di armi e droga, la pedopornografia, la tratta di esseri umani, il turismo sessuale, il riciclaggio di denaro sporco e i pagamenti illeciti attraverso le *criptvalute*, e tanto altro ancora.

Gli attori della difesa cyber

Definito a grandi linee il *cyberspazio* e le opportunità e i pericoli che da esso derivano e chiarito quanto la sicurezza del mondo *cyber* rappresenti una delle esigenze principali di chi opera a garanzia degli interessi pubblici o privati, apparirà evidente che in questo "nuovo mondo" sono chiamate ad agire tutte le componenti che nel mondo fisico sono deputate alla sicurezza; ognuno secondo i propri profili di competenza. Così i corpi di polizia di occuperanno di perseguire e prevenire i crimini; gli "eserciti" inventeranno nuove armi di attacco e di difesa per combattere in questo nuovo scenario; le agenzie di intelligence si muoveranno alla ricerca di informazioni per prevenire attività potenzialmente pericolose o architetteranno operazioni di disinformazione o sabotaggio a danno del "nemico".

Così come nel mondo reale le attività svolte da ogn'una delle agenzie di difesa non sono a compartimenti stagni, specialmente per quelle oggetto d'interesse dell'intelligence; la trasversalità nelle azioni e lo scambio di informazioni, risultati e obiettivi risulta di fondamentale importanza anche nella realtà *cyber*. Ma le agenzie di sicurezza da sole non bastano, le loro azioni devono essere promosse e sostenute da una vera e propria politica della *cyber* sicurezza che non si confronti solo con la componente tecnica e tecnologica ma che sia in grado di cogliere aspetti sociali, legali ed economici del problema e che sia in grado di intuire i cambiamenti e immaginare possibili scenari futuri; solo in tal modo si potranno riconoscere le minacce alla capacità di funzionamento delle infrastrutture critiche

e si potranno predisporre per tempo strumenti in grado di prevenire azioni ostili e al contempo assicurare una efficace azione di contenimento delle conseguenze. In tal senso si è mossa la commissione europea, infatti nel 2013 ha presentato due documenti "La strategia sulla sicurezza informatica"[21] e "Uno spazio informatico aperto e sicuro"[22], recante la visione dell'Unione europea sul modo per prevenire e rispondere ad attacchi informatici. La strategia è articolata in cinque priorità: conseguire la resilienza informatica; ridurre drasticamente la criminalità informatica; sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune; sviluppare le risorse industriali e tecnologiche per la sicurezza informatica; istituire una coerente politica del ciberspazio in seno all'Unione europea. Nel documento si auspicava il rafforzamento della cooperazione UE NATO nei confronti delle minacce ibride[23]. Il Consiglio Giustizia e affari interni ha, tra l'altro, approvato conclusioni sul miglioramento della giustizia penale nel *ciberspazio* e il rafforzamento della rete di autorità giudiziarie ed esperti nel settore della criminalità informatica con il sostegno di Eurojust. L'obiettivo della rete è agevolare lo scambio di competenze, le migliori pratiche e altre conoscenze ed esperienze pertinenti in materia di indagini e perseguimento di reati informatici. Attraverso una direttiva[24] sono stati pervisti, in particolare, i reati di accesso illecito a sistemi di informazione; l'interferenza illecita relativamente ai sistemi; l'interferenza illecita relativamente ai dati; l'intercettazione illecita. La direttiva prevede altresì un apparato sanzionatorio nei confronti delle persone giuridiche ritenute responsabili dei reati informatici. Allo scopo di potenziare l'efficacia dello sforzo al contrasto della minaccia *cyber* è stata affiancata all'apposita agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)[25]un reparto in seno all'EUROPOL denominato centro europeo per il *cybercrime*. Europol ha istituito il Centro europeo per la lotta contro la *cybercriminalità* (EC3)[26]. L'attività dell'EC3 si articola in tre aree: competenza legale, strategica e operativa. In estrema sintesi l'EC3 funge da hub centrale per informazioni e *intelligence* criminali sostenendo le indagini degli Stati membri e fornendo supporto tecnico-digitale per le indagini e le operazioni.

21 Reperibile sul sito http://europa.eu/rapid/press-release_IP-13-94_it.htm consultato il 05/07/2017

22 http://europa.eu/rapid/press-release_IP-13-13_en.htm

23 Per "minacce ibride" si intende una serie di attività che spesso combinano metodi convenzionali e non convenzionali e che possono essere realizzate in modo coordinato da soggetti statali e non statali pur senza oltrepassare la soglia di guerra formalmente dichiarata.

24 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

25 è stata creata nel 2004 dal Regolamento 460/2004 ed è pienamente operativa dal 1º settembre 2005. ENISA ha sede a Candia, sull'isola diCreta (Grecia)

26 Il Centro Europeo contro il Cybercrimine (in inglese "European Cybercrime Centre; sigla EC3 con quartier generale a L'Aia (Paesi Bassi), è il corpo dell'Europol, la polizia dell'Unione europea, che coordina le attività transfrontaliere delle forze dell'ordine contro il crimine informatico e agisce come centro di competenza tecnica in materia.

Le forze di polizia

Analogamente al crimine tradizionale, quello informatico può assumere varie forme ed essere perpetrato praticamente sempre e ovunque. il crimine informatico è, dopotutto, semplice “crimine” con l'aggiunta di qualche sorta di componente “informatica”. Ed analogamente al crimine tradizione le forze di polizia sono chiamate a contrastarlo.

Il principale sforzo operativo si concentra nella direzione del continuo adeguamento delle risposte alle nuove frontiere tecnologiche della delinquenza. Infatti il tradizionale inseguimento fra guardie e ladri ora si manifesta nella capacità dei primi di essere al passo con i secondi per competenza e abilità nel saper utilizzare e monitorare il *cyberspazio* che è sempre in continua evoluzione.

Come per qualunque attività di polizia anche chi si muove nel *cyberspazio* compie investigazioni di polizia giudiziaria per reprimere tutti quei reati correlati al computer e per tutte le fattispecie criminali che sono poste in essere con l'ausilio dei più recenti strumenti tecnologici/informatici o che mirano a creare danno alle infrastrutture digitali. L'attività di polizia giudiziaria, tratta i reati in materia di: *hacking:* intrusioni; danneggiamenti informatici; telefonia fissa e cellulare; *voip; privacy:* diritto d’autore; video; musica; *pay-tv*; pedofilia on-line; commercio elettronico; truffe; riciclaggio; frodi con carte di credito; frodi legate all’*home banking*; eversione politica e terrorismo; stupefacenti; armi ed esplosivi; prostituzione; ovvero tutte le fattispecie di reato tradizionali che hanno come fine o strumento per la loro realizzazione il mezzo informatico. Va da se che il *modus operandi* di questi operatori non si limita al mero monitoraggio di *chat-line*, *social network* e quant’altro di simile; al fianco di queste attività vengono svolte investigazioni nel così detto *deep* e *dark web*[27] dove hanno luogo le attività criminose più importanti. Garantiti dall’anonimato e utilizzando canali noti solo a pochi adepti si effettuano attività illegali nel settore della pedopornografia, del traffico di armi e droga. Esempio eclatante di tale commercio illecito è rappresentato dal sito di commercio elettronico” *Silk Road*” che funzionava nel *dark web* e poteva essere raggiunto attraverso i servizi del *software* di anonimato TOR. I prodotti venduti su *Silk Road* erano classificati come prodotti di contrabbando o illegali dalla maggioranza delle giurisdizioni mondiali. *Silk Road* è stato definito come l’*e-bay* delle

27 Il deep web (Web sommerso), è l'insieme delle risorse informative del World Wide Web non segnalate dai normali motori di ricerca. Secondo una ricerca sulle dimensioni della rete il Web è costituito da oltre 550 miliardi di documenti mentre Google ne indicizza circa il quattro per cento. Per Dark Web s’intende la navigazione web in anonimato.

droghe[28]. Più volte chiuso dall'FBI nel 2015 il suo creatore è stato arrestato, grazie ad agenti sotto copertura infiltrati nella sua piattaforma, e condannato in primo grado all'ergastolo per i reati di associazione per delinquere, frode informatica, distribuzione di false identità, riciclaggio di denaro, traffico di droga su internet e cospirazione per trafficare droga.

L'esempio della "via della seta" ci illustra come i reparti di polizia che si occupano di investigazioni sul *web* utilizzano "strumenti classici" quali l'attività sotto copertura, l'uso di delatori e informatori, pedinamenti e intercettazioni. Ovviamente essendo le polizie strutture deputate all'applicazione della legge, gli anglofoni parlano di *law enforcement*, si muovono maggiormente nella cornice della repressione dei reati in accordo e sotto la supervisione delle rispettive autorità giudiziarie. Ovviamente, operando anche come polizia di prevenzione, non trascurano le attività di "controllo del territorio" al fine di non permettere la commissione dei reati e garantire l'integrità e la funzionalità della rete informatica, ivi compresa la protezione delle infrastrutture critiche informatizzate.

Nel nostro paese la funzione di polizia su *internet* è affidata alla specialità "polizia postale e delle telecomunicazioni" della Polizia di Stato dal Decreto del Ministro dell'Interno datato 28 aprile 2006, pubblicato in G.U. 193 del 20 agosto 2006 avente titolo "Riassetto dei comparti di specialità delle Forze di polizia". Con un altro decreto dello stesso dicastero del 9 gennaio 2008 è stata istituita una unità specializzata, interna al servizio di polizia postale dedicata alla prevenzione e repressione dei crimini informatici diretti al danneggiamento delle infrastrutture critiche nazionali denominata "Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.I.C.)". Come cita il sito "Commissariato di PS online"[29] il valore aggiunto che il centro rappresenta, nel panorama della protezione delle Infrastrutture critiche deriva dalla realizzazione di una sala operativa, disponibile 24 ore su 24 e 7 giorni su 7, in qualità di punto di contatto univoco dedicato alle I.C nonché dall'utilizzo di collegamenti telematici esclusivi e protetti, tra il C.N.A.I.P.I.C. e le I.C., per il condiviso, reciproco e costante trasferimento dei dati e delle informazioni utili all'esercizio delle funzioni di valutazione, prevenzione e repressione delle minacce e dei crimini informatici.

Nel quadro degli sforzi della polizia nel contrastare le minacce cyber degno di nota è il progetto denominato "Of2cen", volto alla creazione di un centro per l'analisi, la prevenzione e la lotta contro le minacce informatiche rivolte ai servizi bancari online e ai meccanismi di gestione del denaro. Partner del progetto sono la Guardia di Finanza,

28 https://it.wikipedia.org/wiki/Silk_Road sito consultato il 05/07/2017

29 https://www.commissariatodips.it/profilo/cnaipic.html.

l'Associazione Bancaria Italiana, vari istituti di credito nazionali, fra i più importanti, e alcune imprese che si occupano di *cybersicurezza*. "Of2cen" con la sua piattaforma di scambio informazioni, raccoglie le segnalazioni di operazioni sospette che vengono comunicate dalle banche alla polizia, facilita lo scambio di informazioni di indirizzi Ip e di dati bancari fraudolenti.

Le forze armate

Considerazioni su una possibile guerra che sfrutti interamente le potenzialità del *cyberspazio* trasformandolo in campo di battaglia sono iniziati a diffondersi qualche ventennio fa. La consapevolezza del potenziale bellico del *cyberspazio* ha indotto le nazioni con una superiorità in campo tecnologico e militare a promuovere studi ed approfondimenti sulle problematiche connesse ed a ridefinire il loro approccio classico alla guerra in funzione delle novità introdotte dalla rivoluzione informatica. In particolare è stata avvertita la necessità di discriminare Il singolo furto di informazioni, ancorché perpetrato contro *server* militari, o accessi non autorizzati a dati segreti, da un attacco volto a limitare o distruggere attività di "Stati e organizzazioni, attraverso azioni politicamente motivate"[30]. Tuttavia questa nuova forma di guerra presenta alcuni limiti che occorre tenere in considerazione, e vale a dire che non può essa, da sola, disarmare o distruggere il nemico, e soprattutto non può portare a conquiste territoriali[31]. Ciò non di meno la visione strategica che si è imposta è quella che considera l'integrazione di tutti i cinque domini del *warfare* terra, mare, aria, spazio extraatmosferico e spazio cibernetico, in un'ottica della conduzione del potere militare nella politica internazionale.

Partendo da quest'ultima considerazione e cioè che la forza nel mondo *cyber* non può essere inteso come un potere militare "decisivo in solitaria" per una guerra ma una componente dello stato di belligeranza, gli stati hanno ridefinito il loro approccio alla guerra introducendo nuove strategie e armi tanto che si è cominciato a parlare di militarizzazione del *cyberspazio*[32].La prima formalizzazione di questa dinamica si è avuta, non a caso, negli Stati Uniti; nel febbraio del 2003 l'amministrazione Bush junior emanava il

30 Maertin Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, 2009; pag 117; documento reperibile all'indirizzo internet http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf consultato il 03/07/2017.

31 Ibiden pag. 176.

32 Cfr. Alain. Joxe, L'impero del caos. Guerra e pace nel nuovo disordine mondiale, Sansoni editore, Milano 2003.

documento "*National Strategy to Secure* Cyberspace"[33] che riconosceva il cyberspace come un nuovo teatro per le operazioni militari.

Nel 2010 venne istituito l'*US Cyber Command* con il proposito di organizzare e centralizzare il controllo delle operazioni nello spazio *cyber* e sincronizzare la difesa delle reti militari statunitensi[34]. Gli altri paesi non sono rimasti a guardare e sulla scorta delle scelte americane hanno istituito organismi omologhi. La corea del nord ha ufficializzato la creazione di una unità speciale dedita alla guerra cibernetica che ha provocato la risposta del governo del Sud della penisola che si è dotata di un "*Cyber warfare Command*". Alla fine del 2009 si ha notizia della prima attribuzione di una attività del Unita 61398 dell'Esercito Popolare Cinese, reparto dedicato alle azioni di *cyberspionaggio* e *cyber defence*[35]. Ad oggi si ha notizia che tutti i maggior paesi, Russia, Francia, Germania, Regno Unito, Israele Iran, India, Pakistan, Australia a titolo di esempio, dispongono di unità militari preposte a questo nuovo scenario di combattimento[36].

Come era facile aspettarsi questa militarizzazione del *cyberspazio* ha portato negli ultimi anni a una vera e propria fase di "proliferazione" di armi cibernetiche[37]. La relativa economicità, il facile reperimento sul mercato civile degli strumenti informatici "malevoli", e le tecnologie *dual-use capability* hanno indotto numerosi esperti a ipotizzare il loro utilizzo indiscriminato contro una serie di bersagli plausibili. I maggiori dei quali sono stati individuati nei sistemi di difesa aerea; nei depositi di armi convenzionali e non; nei sistemi di comando e controllo; nelle infrastrutture civili essenziali quali le reti elettriche, gli acquedotti, le dighe, le centrali nucleari; il sistema finanziario e in quello dei trasporti e delle comunicazioni[38]. Tramite un attacco del mondo *cyber* è possibile causare seri danni economici, distruzione di infrastrutture fisiche o addirittura la perdita di vite umane. Quindi affinché si possa definire arma *cyber* bisogna che lo strumento utilizzato debba essere letale, distruttivo di cose o persone. Tenendo conto di questa precisazione bisogna aggiungere che esistono altri strumenti che, pensate nel contesto di un conflitto militare convenzionale, concorrono a formare "l'arsenale militare" cibernetico; sono quelle armi

33 Cfr. The National Strategy to Secure Cyberspace, Washington DC, Febbraio 2003, documento reperibile all'indirizzo https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf; consultato nel maggio 2017.

34 U.S. Department of Defence , Cyber Command Fact Sheet , 21th May 2010 documento reperibile sul sito http://www.stratcom.mil/factsheets/Cyber_Command/ consultato nel gennaio 2017.

35http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html consultato il 10/07/2017.

36 Una disamina completa si trova in Shmuel Even, and David Siman-Tov, Cyber Warfare: Concepts and strategic Trend, Memorandum No. 117, May 2012 documento reperibile sul sito https://www.files.ethz.ch/isn/152953/INSS%20Memorandum_MAY2012_Nr117.pdf consultato nel maggio 2017

37 Nicola De Felice, Le sfide della cyber-war al processo decisionale in materia di politica della Difesa, in Information Warfare 2012, Franco Angeli,2013, pp. 39-46

38 Shmuel Even, and David Siman-Tov, Cyber Warfare: Concepts and strategic Trend, Memorandum No. 117, op.cit.

che, in grado di interferire con l'*hardware* del nemico sono capaci di provocare danni rilevanti o rendere inutilizzabile i sistemi di difesa. Esempio accademico di uso di questo tipo di armi è rappresentato dall'Operazione Orchar:. Il 6 settembre 2007, l'esercito israeliano, prima di procedere al bombardamento di un impianto nucleare in Siria, ha utilizzato un aereo armato di un disturbatore elettronico (*jamming*) che ha permesso di emettere falsi segnali e inserire false informazioni nella rete di difesa aerea siriana così che gli operatori del comando e controllo del paese mediorientale furono indotti a credere che non ci fossero penetrazioni nello spazio aereo controllato. In questo modo i caccia israeliani pur non godendo di tecnologia *stealth* (invisibilità ai radar) sono riusciti a eludere i sistemi di tracciabilità e portare a compimento la missione di bombardamento; il tutto senza che vi fosse la prova evidente del coinvolgimento israeliano nell'esplosione del sito nucleare[39]. Pur non rientrando nel novero specifico della guerra cibernetica, l'esempio appena citato rende l'idea della potenziale vulnerabilità a cui sono soggetti gli asset militari una volta inglobati in un sistema *netcentrico* e soprattutto, richiamano l'attenzione sulla poliedricità delle minacce provenienti dallo spazio cibernetico[40]. E tale minaccia non si realizza solo nella capacità di inibire sistemi come quello radar, ma troverà perfetta applicazione nella manipolazione delle comunicazioni causando gravi danni alla catena di comando e controllo.

Un altro particolare tipo di attacco, considerato però alla stregua di una forma ibrida fra un attacco puramente informatico, e quello che coinvolge lo spettro dei protocolli di comunicazione è quello portato avanti secondo la tecnica del *Distribuited Denay of Service* (DDoS) dove attraverso una rete di computer sotto controllo dell'attaccante (*botnets*) si mandano richieste di servizi a reti pubbliche o private impedendogli di fatto di funzionare, come è accaduto in Estonia nel 2007 e in Georgia nel 2008 poco prima degli scontri con le truppe russe.

Da questo ampliamento concettuale degli strumenti militari *cyber* deriva che le dottrine la guerra elettronica (EW) già ampiamente sviluppate e le azioni ibride utilizzate ai fini bellici, rientrano nell'alveo della guerra cibernetica.

Per concludere l'argomento relativo alle armi cibernetiche la caratteristica più importante da evidenziare è quella della relativa alla facilità della loro creazione e dispiegamento. Questa caratteristica, riducendo il differenziale di forza fra gli attori presenti nel *cyberspazio* e fornisce un forte potenziale agli attori più deboli, sia essi statali

39 Daniele Pistoia, La Guerra Elettronica nella quinta dimensione in Information Warfare 2012, Franco Angeli,2013, pp. 65-72.

40 Umberto Gori, Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici, in Information Warfare 2010. FrancoAngeli, Milano, 2011, pp. 31-38.

o organizzazioni più o meno organizzate. Ed è proprio da questi ultimi soggetti che provengono i rischi maggiori dell'utilizzo di *cybearmi*, perché scontando un'inferiorità operativa negli armamenti convenzionali sopperiscono sfruttando le vulnerabilità presenti nell'ambiente cibernetico sottovalutando o volutamente trascurando le reazioni degli attaccati.

L'intelligence.

L'intelligence è un'attività delicatissima di cui qualsiasi organizzazione statale non può fare a meno. Con l'avvento dell'era digitale tutti i principali Stati hanno avvertito la necessità di riorganizzare i loro Servizi Segreti poiché la loro materia prima, l'informazione, ha trovato piena sistemazione nel *cyberspazio*.

Molti stati ed organizzazioni internazionali hanno sentito la necessità di dare una chiara definizione al *cyberspionaggio* e circoscrivere lo spazio di intervento delle rispettive agenzie. Cosi nel manuale di Tallin[41], elaborato in ambito NATO, si definisce come "qualsiasi azione intrapresa clandestinamente o con l'inganno che utilizza le capacità informatiche per raccogliere (o tentare di raccogliere) informazioni con l'intenzione di comunicarle alla parte avversa". In un documento strategico predisposto dalla Germania nel 2011 si parla di spionaggio informatico nei termini di "un attacco IT nel cyberspazio diretto contro uno o più altri sistemi IT e finalizzato alla compromissione della sicurezza degli stessi[…] Gli attacchi informatici diretti contro la riservatezza di un sistema informatico, che vengono lanciati o gestiti dai servizi segreti stranieri costituiscono azioni di *cyberspionaggio*; gli attacchi informatici contro l'integrità dei sistemi IT costituiscono azioni di *cybersabotaggio*[42].

In ogni caso, anche se esercitate nel nuovo mezzo digitale le operazioni di intelligence restano comunque le stesse che hanno impegnato per secoli gli operatori del settore. A parte i servizi speciali[43] che, pur facendo parte a pieno titolo dei compiti delle agenzie di intelligence, nel mondo del *cyberspazio* sono diventate prerogative delle forze armate, i loro compiti istituzionali si possono sintetizzare nella raccolta di informazioni e

41 Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit.

42 Cybersecurity strategy for Germany 2011, documento reperibile all'indirizzo https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile consultato il 05/07/2017.

43 Cfr Francesco Cossiga, Abecedario; Catanzaro; Rubbettino, Roma, 2002. Nel suo libro il presidente emerito Cossiga definisce servizi speciali offerti dall'intelligence come azioni operative che si distinguono dalla ricerca delle informazioni, quali ad esempio, sabotaggi, esfiltrazioni, arresti non convenzionali, eccetera.

nella elaborazione delle stesse al fine di fornire ai decisori politici/militari le istruzioni necessarie per interpretarle correttamente e dare loro un significato che sia utile ad elaborare previsioni verosimili[44].

Nel mondo del cyberspazio, quindi, gli agenti segreti compiono le stesse operazioni dei loro colleghi con la differenza che agiscono in un ambiente dominato dai *computer* e dai dispositivi elettronici. Sia che si tratta di spionaggio attivo, ricerca di bersagli e raccolta di informazioni, che attività di *conuterintelligence* i nuovi agenti dovranno essere degli esperti di tecnologie oltre a possedere le altre competenze che contraddistinguono gli operatore del settore[45].

In ogni caso l'oggetto del lavoro degli operatori dell'intelligence resta comunque l'informazione sia essa *cyber* o meno. Ma nel mondo informatico la quantità di informazioni è tale da essere costretti di parlare di "big data" in termini di volume, velocità e varietà. Tale modello di riferimento, indicato come schema delle "3V", richiede tecnologie e metodi analitici specifici. Lo scopo della collezione e analisi di così tanti dati, si parla dell'ordine dei *Zettabyte* cioè miliardi di *Terabyte*, è quello di poter estrarre informazioni per conoscere la situazione attuale e cercare di predire future evoluzioni[46]. Big data non sono soltanto le informazioni strutturate e catalogate in appositi database ma sono anche, e soprattutto, dati provenienti da fonti eterogenee e non strutturati, come immagini, email, dati GPS, informazioni prese dai social network, eccetera. Una applicazione importantissima per l'intelligence deriva dalle tecniche di analisi di big data (*big data analytics*); questa permette di ottenere risultati finalizzati alla prevenzione di minacce di tipo APT, Advanced Persistent Threat, che rappresentano minacce molto gravi alla sicurezza delle informazioni. Gli APT sono gestiti da attaccanti altamente qualificati, ben finanziati e motivati, che agiscono su periodi medio lunghi, persino anni. L'obiettivo ultimo di questo tipo di attività, è quello di penetrare e restare il più a lungo possibile all'interno delle reti di una organizzazione al fine di avere un accesso costante a informazioni strategiche. Utilizzando un sistema big dati, elaborando, un miliardo di messaggi, pari ai log di un intero giorno di un medio server di posta elettronica, si sono ottenuti ottimi risultati nell'individuazione di APT. Un altro campo in cui l'elaborazione corretta dei Big Data da risulta utile è quello della ricerca dei cosiddetti "terroristi isolati" (*lone wolf terrorist*). Come noto sono persone che agiscono in maniera autonoma senza prendere ordini o essere direttamente connessi a organizzazioni specifiche. I terroristi isolati sono

44 Ibidem.

45 Crf. Salvatore Di Giovanni, L'Open Source Intelligence quale ruolo nell'attività dei servizi di informazione e sicurezza, Roma, 2006.

46 Cfr. Alec Ross , Il nostro futuro. Come affrontare il mondo dei prossimi vent'anni, Feltrinelli, Milano, 2016.

difficili da individuare con le tecniche tradizionalmente usate per il terrorismo organizzato, ma lasciano spesso tracce digitali che, se individuate e correlate, possono essere usate come indicatori di un comportamento da "attenzionare". Gli studi dimostrano infatti che il processo di radicalizzazione di un *lone wolf* avviene quasi totalmente su Internet; nelle sue pagine *web* o nei suoi account di *social network* compaiono segnali specifici quali ammissioni di voler colpire un obiettivo, interesse ossessivo verso qualcosa o qualcuno, esaltazione di un gruppo o di una causa. La sfida è quella di poter continuamente tracciare e monitorare le pagine *Web* e gli account di *social network* alla ricerca dei possibili soggetti interessanti.

Nell'*intelligence* strategica il compito è quello di anticipare le opportunità e le sfide, analizzare le loro implicazioni e fornire ai decisori tutti gli elementi per lo sviluppo di una strategia in modo da trarre il maggiore vantaggio competitivo per il Paese. Per poter ottenere risultati attendibili l'osservazione dei dati deve avvenire in maniera orizzontale cioè devono riguardare tutti gli aspetti della società; solo così si può essere in grado di evidenziare i cambiamenti ed interpretare le cause. Nelle applicazioni statistiche tradizionali, gli studiosi dividono l'analisi dei dati in statistica descrittiva, analisi dei dati esplorativa e analisi dei dati per confermare le ipotesi. Viceversa, nell'analisi predittiva ci si concentra sull'applicazione di modelli statistici-strutturali per una funzione predittiva. Se da un lato lavorare su grandi quantità di dati per scopi descrittivi o comunque per confermare ipotesi pre-formulate è comunque possibile anche se complesso, dall'altro i modelli e tecniche predittive devono ancora essere migliorate per arrivare a livelli di affidabilità soddisfacenti. Altro elemento di complicazione della funzione predittiva consiste nella necessità di pervenire a tesi valide in tempi ristretti. Spesso questo significa che non si è in grado di eseguire un processo di analisi completo, ma vanno trovati dei meccanismi per ottenere approssimazioni rapide dei risultati

Le funzioni sopra descritte condividono la stessa caratteristica di dover scorgere e collegare pochi elementi nascosti in una grandi quantità di informazioni e richiedono l'analisi di enormi volumi di dati dinamici ed eterogenei che non possono essere effettuate se non con l'ausilio di *computer* molto potenti.

Così come per le attività di *cyberguerra* lo strumento tecnologico non può essere considerato esclusivo e risolutivo in se e per se. Un esempio di attività di *intelligence*, nato e cresciuto sul *web* e portato a soluzione nel modo reale e il caso del potenziale terrorista francese Reda Hame. Soluzione che come vedremo forse non è riuscito ad evitare attentati sanguinosi ma rappresenta comunque una vittoria per i servizi d'oltralpe. Si parla

di vittoria perché, bisogna sempre tenere a mente che quando le agenzie di *intelligence* assurgono agli onori della cronaca è solo quando hanno fallito nei loro compiti; ma al fianco di un fallimento non è dato conoscere quante operazioni sono andate a buon fine e quanti attentati siano stati sventati e quante vite salvate. Il caso di studio riguarda la vicenda di Reda Hame, raccontata in un articolo del *New York Times*[47]; informatico della società *Airbus Defence and Space* di Parigi parte per la Siria dopo aver aderito allo Stato Islamico inviando un *application form* come per una normale richiesta di lavoro. Il suo scopo è contribuire ad abbattere il regime di Assad, ma dopo un rapido addestramento viene indirizzato verso il "settore" ISIS degli attentati in Occidente. Il nostro uomo possiede un passaporto francese e competenze informatiche che non possono essere sprecate per gli scontri in Siria. Hame torna in Europa facendo un giro complicato per simulare un viaggio di piacere ma tornato a casa, grazie alla soffiata di un compagno arrestato in Spagna, viene prelevato dalla polizia francese e decide di collaborare con le autorità. A Raqqa, in Siria, aveva appreso un preciso protocollo per comunicare con il quartier generale dell'ISIS. Tutte le comunicazioni da inviare dopo essere state criptate utilizzando Truecrypt[48] dovevano essere caricate su un servizio *cloud* turco. Niente telefonate, niente email, niente chat, niente reti sociali. Si tratta di un sistema di comunicazione semplice ma efficace, che soprattutto lascia pochissimi metadati[49]: niente ora di invio e ricezione, nessun indirizzo di email, nessuna reti di contatti social, nessun numero di telefono. Una volta catturato Hame parla di attacchi ad obiettivi civili, in particolare sale da concerto. Ciononostante, qualche mese dopo la strage del Bataclan ha luogo ugualmente, ma che questa sia in qualche modo legata a quanto confidato da Hame è palesato dal fatto che il

47 Rukmini Callimachi, How ISIS Built the Machinery of Terror Under Europe's Gaze, New York Time, 29/03/2016, articolo reperibile all'indirizzo https://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html consultato il 06/07/2017

48 Si tratta di un programma per cifrare cartelle o un intero disco rigido. E' un programma *open source*, e il suo codice sorgente ha subito un vero e proprio processo di *code auditing*, un controllo da parte di ingegneri del software ed esperti di crittografia indipendenti, durato oltre un anno, in cui non sono state trovate vulnerabilità di rilievo, e se usato correttamente, anche un ente come l'NSA avrebbe serie difficoltà a decifrare dei documenti da esso criptati. Il gruppo di sviluppo di Truecrypt è sempre rimasto anonimo; il software sembra si basasse inizialmente sul codice di E4M, un programma analogo il cui autore, Paul Le Roux, è diventato trafficante di armi e droga e mandante di svariati omicidi e poi, dopo l'arresto, un collaboratore della DEA (v. E. Ratliff, *The Mastermind*, https://mastermind.atavist.com/). Infine, alla fine di maggio 2014 il software viene ritirato dai suoi autori, che annunciano senza alcuna motivazione ragionevole di non voler più proseguire nel suo sviluppo e consigliano di passare a soluzioni proprietarie per Windows e Mac. Nel frattempo sono apparsi diversi suoi *fork*, delle modifiche basate sul codice originale, tra i quali *Veracrypt*, che corregge tutti i piccoli problemi evidenziati nel *code auditing*.

49 Un **metadato** (dal greco μετὰ "oltre, dopo, per mezzo" e dal latino *datum* "informazione"), letteralmente "(dato) per mezzo di un (altro) dato", è un'informazione che descrive un insieme di dati. In riferimento al contesto dell'informazione elettronica in rete: i metadati sono un'amplificazione delle tradizionali pratiche di catalogazione bibliografica .

suo mentore (*handler),* colui che aveva gestito il suo addestramento in Siria, non era altri che colui che ha poi organizzato gli attacchi di Parigi, e cioè Abdelhamid Abaaoud.

L'ISIS non ha teorici che fanno convegni per discutere se il *cyberspazio* sia o no un quarto dominio militare o una nuova via per lo spionaggio. Ciononostante, a supporto delle sue attività, ha trovato il modo di sfruttare lo spazio *cybe* ed utilizzarlo per i suoi propositi sia per azioni di propaganda[50] sia per le comunicazioni operative senza che queste possano essere scoperti dai servizi di intelligence dei paesi occidentali.

Il settore maggiormente in difficoltà nel *cyberspazio* è comunque quello della difesa dagli attacchi altrui; cioè il settore che nel mondo delle "barbe finte" è noto come controspionaggio. Le minacce a cui si deve far fronte sono abbastanza complesse da individuare poiché sono complesse anche le finalità spesso sensibilmente diversi e distanti dall'evento dannoso provocato: si possono rubare dati commerciali per poi rivenderli o infiltrarsi in sistemi per decrittare dati su carte di credito o segreti industriali per favorire una particolare realtà nazionale o conoscere in anticipo informazioni sensibili dal punto di vista economico o militare.

La maggior parte degli attacchi perpetrati ai sistemi informatici viene effettuata grazie a una componente: il fattore umano. La componente umana può essere sia di natura consapevole sia di natura inconsapevole, ma in entrambi i casi è decisiva per portare a termine un attacco con successo. È chiaro che le soluzioni tecnologiche non possono da sole assicurare la sicurezza di un sistema; occorre infatti alimentare una cultura della sicurezza informatica, in modo tale che siano scongiurati comportamenti inappropriati. Uno degli aspetti più importanti del fattore umano è la cosiddetta Ingegneria Sociale (*Social Engineering*, SE): un insieme di tecniche atte a raggirare l'essere umano al fine di ottenere informazioni riservate. Queste possono essere poi utilizzate per portare a termine un attacco utilizzando strumenti e tecnologie idonee. Dal punto di vista psicologico, il *social engineering* si basa sulla consapevolezza che, in determinati contesti, il comportamento umano mostra una certa tendenza alla fiducia verso gli altri. Tuttavia, ciò si somma alla abilità tecnica dell'attaccante di impersonare il ruolo di entità fidata ed al livello di vulnerabilità della vittima che a sua volta dipende dalla percezione della pericolosità nei confronto del mondo *cyber*. Gli obiettivi finali di questo tipo di attacchi sono quelli tipici del *cyberspionaggi*o, quindi, in generale, la compromissione dei requisiti di confidenzialità, integrità o disponibilità di un sistema, spesso attuato attraverso la strutturazione di un

50 L'ISIS, ad esempio, ha una rivista in inglese che si configura con un vero e proprio organo di propaganda. Fino al 2016 si chiamava *Dabiq,* dal nome della città siriana che in una visione profetica islamista sarebbe il luogo della battaglia finale contro gli infedeli. Quando la città di Dabiq è stata liberata da ribelli e truppe turche l'anno scorso la rivista ha cambiato nome in *Rumiyah*, e cioè "Roma" in arabo.

attacco di tipo APT (*Advanced Persistent Threat*). L'attacco di SE è cioè spesso solo la prima fase di un attacco o di una serie di attacchi complessi che si possono protrarre nel tempo e solitamente progettati per una specifica vittima, intesa come singola persona o come organizzazione. Un esempio di attacco di questo tipo è lo *spear phishing*, in cui la vittima riceve una e-mail fortemente personalizzata, contestualizzata rispetto a dettagli reali della sua vita. L'apertura dell'e-mail comporta l'installazione di un *malware* che a sua volta può controllare l'ulteriore installazione di *malware* attraverso opportuni *download*. L'obiettivo è spesso quello di installare *backdoors* multiple all'interno della rete dell''organizzazione bersaglio che possano garantire all'attaccante l'accesso anche nel caso in cui i precedenti attacchi venissero rilevati e contrastati. Attraverso le *backdoors* l'attaccante ha quindi la possibilità di effettuare prelievi abusivi di informazioni, scaricare *account*, *password*, codici di accesso e, addirittura, di costruire una base per realizzare attacchi ad altri soggetti sfruttando la copertura e spesso la credibilità del primo bersaglio.

Vittima illustre di questo tipo di attacco è stato il nostro ministero della difesa; da un articolo di Repubblica.it[51] siamo venuti a conoscenza che l'importante dicastero è stato penetrato da un gruppo di *hacker* russi conosciuti con il nome di battaglia Apt28. Dall'ottobre del 2014 al maggio del 2015 un flusso continuo di notizie riservate è stato dirottato sui server dei pirati dietro i quali, secondo attendibili ricostruzioni di intelligence e le attività della Procura militare di Roma, che indaga con l'ipotesi di spionaggio internazionale, ci sarebbe direttamente il Cremlino. Da quanto è emerso si è trattato di un attacco persistente (APT) portato avanti da molto tempo che ha visto coinvolti anche altri paesi europei. Si presume infatti che il vero obiettivo di tale attacco fossero documenti riservati della NATO.

In conclusione può affermarsi, che le capacità difensive nel *cyberspazio* sono importanti tanto quanto quelle offensive; questo perfetto bilanciamento ha causato negli ultimi anni una colossale proliferazione di strutture specificatamente impiegate in attività di difesa informatica sia private che pubbliche e non ha visto i servizi di intelligence semplici spettatori degli eventi.

51M. Mensurati e F.Tonacci, Hacker Russi nei server del ministero della difesa italiano, reperibile in http://www.repubblica.it/cronaca/2016/02/17/news/hacker_russi_ministero_difesa_italiano-155988416/?ref=search

Il piano di sicurezza Nazionale

A livello nazionale, l'Italia già nel 2003 creava, in seno al Ministero per l'Innovazione Tecnologica, un gruppo di lavoro sulla protezione delle Infrastrutture Critiche delle Comunicazione. Con il decreto legge n. 155 of 31/7/05 (legge Pisanu), la responsabilità di tale protezione veniva affidata alla Polizia di Stato e in particolare al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC). Con il DCPM del 24 gennaio 2014 dal titolo "Strategia nazionale per la sicurezza cibernetica" il nostro paese ha avviato un percorso di strutturazione del *cyberspazio* nazionale, e con due pubblicazioni allegate al decreto ha definito i presupposti teorici e le strutture istituzionali per affrontare le problematiche relative alla sicurezza. Il primo documento intitolato "quadro strategico Nazionale per la sicurezza dello spazio cibernetico" ha posto l'attenzione sul fatto che la principale minaccia dello spazio virtuale è rivolta alla sicurezza del potenziale industriale nazionale rappresentato dal *know-how* scientifico, tecnologico ed aziendale con inevitabili ripercussioni sul benessere sociale ed economico nazionale. Il secondo documento "Piano nazionale per la protezione cibernetica e la sicurezza informatica" ha definito gli organismi incaricati di individuare azioni congiunte tra il settore pubblico e privato finalizzate ad un'idonea capacità di prevenzione, reazione, contrasto e contenimento.

Entrambi i documenti hanno mostrano che il legislatore ha interiorizzato il concetto che la minaccia *cyber* è in continua evoluzione sia sotto il profilo tecnologico e sia sotto il profilo delle conseguenze e della varietà degli attori in campo, non solo minacce terroristiche ma anche e soprattutto attività mirate ad azioni di sabotaggio e/o spionaggio. Si parla quindi di minacce alla capacità di funzionamento delle nostre strutture critiche che può essere contrastata attraverso lo sviluppo di potenzialità di prevenzione assicurando al contempo una efficace azione di contenimento in caso di attività ostili. Si è altresì intuito che tali capacità possono essere espresse solamente attraverso una adeguata formazione, sensibilizzazione e responsabilizzazione del personale e mediante l'adozione di misure di sicurezza fisiche, logiche e procedurali.

Il quadro strategico precisa la nuova minaccia che il nostro paese si trova ad affrontare; attraverso i dati relativi all'impatto della minaccia, offre maggiore comprensione circa la vera entità del problema. Per fare questo individua alcuni strumenti per il potenziamento delle cosiddette "capacità cibernatiche". In primo luogo si sofferma sulla necessità di migliorare le capacità tecnologiche operative e di analisi al fine di potenziare

le capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema paese. Auspica la cooperazione tra istituzioni ed imprese nazionali e internazionali promuovendo la diffusione della cultura della sicurezza cibernetica;

Tra gli elementi di assoluta novità e di particolare interesse, vi è quello di individuare nelle Università e negli istituti di ricerca, gli interlocutori privilegiati per quel che riguarda la diffusione della cultura della sicurezza di modo che questa possa entrare a far parte del bagaglio formativo degli studenti e dei ricercatori.

Accanto al quadro teorico sono stati identificati alcuni indirizzi operativi, contenuti nel "Piano nazionale per la protezione cibernetica e la sicurezza informatica". Si è, quindi, predisposto il potenziamento della capacità di *intelligence*, di polizia e di difesa civile/militare implementando modalità di coordinamento sia a livello nazionale, tra soggetti pubblici e privati, che internazionali promuovendo anche la realizzazione di esercitazioni e protocolli si sicurezza condivisi. Il piano ha previsto anche la operatività di un CERT[52] nazionale da affiancare hai CERT-PA e ai CERT già presenti nei vari dicasteri.

Per quanto riguarda la struttura occorre sottolineare che l'architettura istituzionale individuata nel decreto si sviluppa su tre livelli di intervento: uno politico per l'elaborazione degli indirizzi strategici affidati al Comitato interministeriale per la sicurezza della Repubblica, uno di supporto operativo ed amministrativo e uno puramente operativo che ha dato via a due organismi distinti: il nucleo per la sicurezza cybernetica presieduto dal Consigliere militare del Presidente del Consiglio e un Tavolo interministeriale di crisi cibernetica per la gestione delle crisi in atto.

Allo stato attuale, l'approccio interministeriale sembra essere l'unico possibile, anche se la partecipazione in egual misura dei vari Ministeri si configura come un elemento di dispersione delle forze; infatti in caso di attacco ad una infrastuttura il primo referente che si fa carico di gestire la crisi sarà il Ministero di riferimento anziché un Comando integrato Difesa/*intelligence*.

Un aspetto certamente migliorabile è quello della istituzione di un unico CERT in grado di rilevare le minacce che si originano nel *cyberspazio*, rispondere prontamente agli attacchi informatici e ripristinare le funzioni dei servizi eventualmente compromessi; la realizzazione di una simile struttura consentirebbe anche un'azione di indirizzo e coordinamento anche attraverso il dialogo con omologhe strutture europee ed internazionali.

52 Acronimo di *Computer Emergency Response Team*.

Come accennato, Il decreto ha invece previsto la coesistenza di tre CERT: il CERT Nazionale; il CERT della pubblica amministrazione presso l'Agenzia per l'Italia Digitale, il Nucleo di Sicurezza Cibernetica presso l'Ufficio del Consigliere Militare alla Presidenza del Consiglio dei Ministri. Il CERT nazionale è inquadrato presso il ministero dello sviluppo economico. Si tratta di una struttura destinata a potenziare i meccanismi di risposta agli incidenti informatici e gli strumenti di rilevazione e contrasto alle minacce. In ambito internazionale, il CERT nazionale ha già avviato forme di dialogo con il CERT EU dell'unione europea sostenuto dall'Agenzia europea per la sicurezza ENISA ed è già attivo un significativo scambio di informazioni. Il CERT_PA è una struttura che opera all'interno dell'Agenzia per l'Italia Digitale ed è preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle pubbliche amministrazioni. Il CERT difesa è un team creato presso lo stato maggiore difesa con lo scopo di fornnire supporto agli utenti della difesa nel campo della difesa delle reti telematiche promuovendo al contempo la divulgazione di informazioni a scopo preventivo nel campo della sicurezza informatica. Un attività divulgativa di cultura informatica generale viene poi condotta attraverso la redazione e relativa distribuzione alle forze armate del periodico "bollettino di sicurezza informatica" liberamente consultabile on-line.

In ogni caso il DCPM del 24 gennaio ha una grossa problematica relativa ai finanziamenti indispensabili per le finalità attuative proposte; al riguardo l'art 13.1 stabilisce che "dal presente decreto non derivano nuovi oneri a carico del bilancio dello Stato".

Così disponendo, l'intera struttura, pensata e voluta, soffre della necessità concreta di disporre di un adeguato *budget* per poter attuare quanto richiesto.

Seppure siano trascorsi soltanto pochi anni dall'emanazione delle direttive sopra riportate, è opportuno rivedere certi aspetti ed adeguarli ad una realtà in rapidissima evoluzione, occorre che vi sia una maggiore consapevolezza dei rischi ed è indispensabile una più incisiva cultura della *cyber* sicurezza nei cittadini e nel settore privato; settore quest'ultimo che stenta ad adeguarsi alle esigenze.

Bisogna peraltro individuare metodologie che consentono la trasformazione delle leinee guida predisposte dalle autorità politiche, in modelli strutturali ed efficacemente applicabili. Un primo passo in tal senso è stata la creazione di *framework* nazionale per la *cyber security* predisposto in ambito CIS/CINI consorzio interuniversitario Nazionale per l'informatica.

Conclusioni

L'espansione del *cyberspazio* ha determinato un totale stravolgimento delle istituzioni politiche e sociali dell'era post-industriale, ed ha imposto la trasformazione dalla politica internazionale che da un sistema basato su una concentrazione del potere, in mano a poche super potenze, si è orientato verso una conformazione con forze distribuite di tipo orizzontale. L'avvento di *internet* e la conseguente nascita di molteplici centri di potere rischiano di generare, nelle relazioni internazionali odierne, un'anarchia tale da rendere vani qualsiasi modello di dissuasione e deterrenza, sistema che, nel bene o nel male, ha scongiurato grandi conflitti e mantenuto una certa stabilità e un lungo periodo di pace dalla seconda metà del secolo scorso ad oggi. La possibilità di condurre una guerra con strumenti non militari, che garantiscono l'anonimato, l'istantaneità e assicurano l'immunità da azioni di rappresaglia punitiva si configurano come un incentivo all'uso delle armi cibernetiche specialmente da parte di piccoli stati che potrebbero agire per assecondare il senso di frustrazione di fronte alla potenza militare dei paesi più sviluppati. La *dual-use capability* conferita dall'*Information Technology* ha reso la guerra economica ed ha esteso la quantità di bersagli potenzialmente utili, spesso di valenza civile. Esempio emblematico è quanto è avvenuto con il virus Stuxnet in grado di colpire un sistema SCADA indipendentemente che sia connesso a internet o meno. La consapevolezza che la maggior parte delle Infrastrutture Critiche, dighe, acquedotti, centrali elettriche, centrali nucleari, gasdotti, ferrovie, porti, aeroporti, eccetera poggiano su questo tipo di sistema di comando e controllo informatico, ci fa capire quanto la società moderna sia vulnerabile di fronte hai rischi provenienti dal *cyberspazio*.

E considerando la tendenza ad "internettizzare" tutte le cose e facile comprendere come l'esposizione ai rischi e la necessità di sicurezza aumenteranno in maniera esponenziale. Le nuove frontiere della tecnologia saranno la realtà virtuale, l'automazione di servizi più o meno essenziali quali gli automezzi senza pilota o l'assistenza a bambini ed anziani, e la telemedicina[53]. Lo sviluppo di queste tecnologie procede a passi da gigante: centri di ricerca, multinazionali e start-up sono al lavoro per produrre soluzioni che porteranno significativi progressi in questi settori.

Compresa la situazione e inquadrate le tendenze bisogna interiorizzare la consapevolezza che esiste il rischio reale che un qualsiasi attore dotato di una certa

53 Cfr. Alec Ross , Il nostro futuro. Come affrontare il mondo dei prossimi vent'anni, op.cit.

competenza informatica sia in grado di provocare un evento distruttivo capace di provocare vittime o addirittura paralizzare un intero Paese.

Verrebbe da chiedersi se tale diluizione del potere e l'interdipendenza data dalla interconnessione di tutte le infrastrutture hardware, non potrebbe portare ad una sana cooperazione internazionale fra tutti gli attori presenti nel cyberspazio o se questo aumenti il rischio di una guerra che partendo dal mondo *cyber* si estenda agli scontri fra eserciti. Il perdurare del "sacro egoismo nazionale", l'affollamento e il caos dell'arena internazionale, nonché la scarsa sensibilità degli attori privati verso i rischi alla sicurezza, fanno propendere maggiormente sulla seconda ipotesi.

Non è un caso se emerge, anche negli Studi Strategici, la necessità di rivoluzionare le stesse dottrine difensive basate sulla massa e sulla forza, e favorire modelli più malleabili, più elastici, più resilienti, con la perfetta cooperazione tra settore pubblico e privato. In questa breve ricerca, si è cercato di porre l'accento sulla rilevanza strategica del *cyberspazio* e i rischi che provengono da esso, nella consapevolezza che il rischio peggiore, nelle previsioni strategiche, è dato dal diniego di riconoscere il problema. Mai come adesso appaiano attuali i consigli che Macchiavelli dava al suo principe virtuoso quando affermava che il buon governante deve saper predisporre nei "tempi quieti" gli strumenti necessari per affrontare le difficoltà future[54].

54 Cfr. N. Machiavelli, Il Principe ediz. integrale, Feltrinelli, Milano 1991

Bibliografia

Autori vari, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press 2013.

Davide Bennato, Il computer come macroscopio. Big data e approccio computazionale per comprendere i cambiamenti sociali e culturali, Franco Angeli, 2015.

Iacopo Chiarugi, Nicolò De Scalzi, Luigi Martino, Marco. Mayer, La politica nell'era digitale. Dispersione o concentrazione del potere?, in Umberto Gori, Luigi Martino (a cura di), Intelligence e Interesse nazionale, Aracne, Agosto 2015.

Francesco Cossiga, Abecedario; Catanzaro; Rubbettino, Roma, 2002.

Nicola. De Felice, Le sfide della cyber-war al processo decisionale in materia di politica della Difesa, in Information Warfare 2012, Franco Angeli, Milano, 2013.

Salvatore Di Giovanni, L'Open Source Intelligence quale ruolo nell'attività dei servizi di informazione e sicurezza, Roma, 2006.

Shmuel Even, and David Siman-Tov, Cyber Warfare: Concepts and strategic Trend, Memorandum No. 117, Tel-Aviv May 2012.

Cristiano Giorda, Cybergeografia. Estensione, rappresentazione e percezione dello spazio nell'epoca dell'informazione, Tirrenia Stampatori, Torino, 2001.

Umberto Gori, Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici, in Information Warfare 2010. FrancoAngeli, Milano, 2011.

Alain. Joxe, L'impero del caos. Guerra e pace nel nuovo disordine mondiale, Sansoni editore, Milano 2003.

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

Nicolò. Machiavelli, Il Principe ediz. integrale, Feltrinelli, Milano 1991.

Daniele Pistoia, La Guerra Elettronica nella quinta dimensione, in Information Warfare 2012, Franco Angeli, Milano, 2013.

Alec Ross , Il nostro futuro. Come affrontare il mondo dei prossimi vent'anni, Feltrinelli, Milano, 2016.

Francesco Vitali, La geopolitica economica dei dati e il futuro del dominio. Dal controllo alla previsione. Il potere tra social media e manipolazione dell'azione sociale, in Nomos & Khaos. Rapporto Nomisma 2011-2012 sulle prospettive economico-strategiche, Agra 2012.

William Gibson, Neuromancer, Ace Books, 1997.

Sitografia

BSI.BUND.de
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

Rukmini Callimachi, How ISIS Built the Machinery of Terror Under Europe's Gaze, New York Time, 29/03/2016 https://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html

Commissariato di P:S. online, https://www.commissariatodips.it/profilo/cnaipic.html

European Commission http://europa.eu/rapid/press-release_IP-13-94_it.htm
http://europa.eu/rapid/press-release_IP-13-13_en.htm

Shmuel Even, and David Siman-Tov, Cyber Warfare: Concepts and strategic Trend, Memorandum No. 117, Tel-Aviv May 2012 https://www.files.ethz.ch/isn/152953/INSS%20Memorandum_MAY2012_Nr117.pdf

Luigi. Martino, La Quinta Dimensione della Conflittualità. La rilevanza Strategica del Cyberspace e i Rischi di Guerra Cibernetica, CSSI - Centro Universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII) ttp://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf.

M. Mensurati e F.Tonacci, Hacker Russi nei server del ministero della difesa italiano, http://www.repubblica.it/cronaca/2016/02/17/news/hacker_russi_ministero_difesa_italiano-155988416/?ref=search

New York Times, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Rand Organization,
http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Securelist, https://securelist.it/it-threat-evolution-q1-2017-statistics/62536/

Autori vari, Tallinn Manual on the International Law Applicable to Cyber Warfare ,
https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

Treccani, la cultura italiana http://www.treccani.it/enciclopedia/cyberspazio_%28Lessico-del-XXI-Secolo%29/; 25/giugno/2017

Sistema di informazione per la sicurezza della repubblica, https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html

E. Ratliff, *The Mastermind*, https://mastermind.atavist.com/

US The White House,
https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf;

U.S. Department of Defence , Cyber Command Fact Sheet,
http://www.stratcom.mil/factsheets/Cyber_Command/.

Wikipedia, https://it.wikipedia.org/wiki/Silk_Road