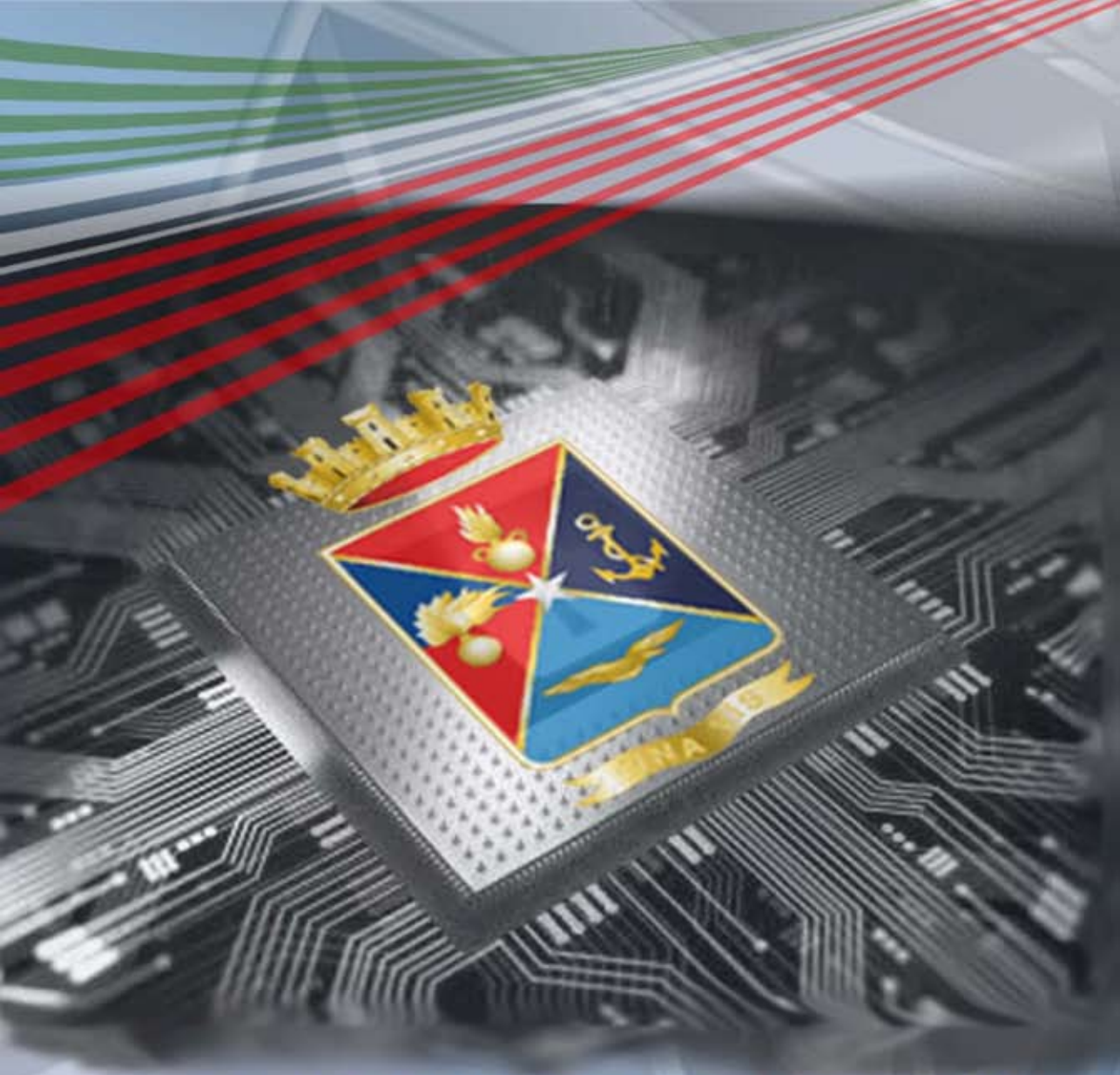


LO SPAZIO CIBERNETICO TRA ESIGENZE DI SICUREZZA NAZIONALE E TUTELA DELLE LIBERTA' INDIVIDUALI

"Cyberspace between national security and protection of individual freedom"

INFORMAZIONI DELLA DIFESA

Supplemento al n. 6/2014 di Informazioni della Difesa

CSSII
Centro interdipartimentale di Studi Strategici Internazionali e Imprenditoriali

ISPRI
ISTITUTO PER GLI STUDI DI PREVISIONE E LE RICERCHE INTERNAZIONALI
INSTITUTE OF FORECASTING STUDIES AND INTERNATIONAL RESEARCH
INSTITUT POUR LES ETUDES DE PREVISION ET LES RECHERCHES INTERNATIONALES
INSTITUTO PARA LOS ESTUDIOS DE PREVISION Y LAS INVESTIGACIONES INTERNACIONALES
INSTITUT FÜR VORAUSSICHTSSTUDIEN UND INTERNATIONALE FORSCHUNG

Realizziamo
sistemi complessi.
Perché il vostro lavoro
sia più semplice.

DEFENCE
HOMELAND SECURITY
SPACE & TRANSPORTATION
GOVERNMENT & INDUSTRIES

www.vitrociset.com

Supplemento al n. 6/2014 di
Informazioni della Difesa
Periodico dello
Stato Maggiore della Difesa
fondato nel 1981

Gli articoli investono la diretta responsabilità degli autori, di cui rispecchiano le idee personali
Chiuso in Redazione
Dicembre 2014 – Gennaio 2015

Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali

"C*yberspace between national security and protection of individual freedom*"

Sommario

SEZIONE I Lo spazio cibernetico e la sicurezza nazionale

Le nuove minacce cyber 5

I centri di eccellenza e la conoscenza condivisa 30

I Social Media, Cloud ed evoluzione da web 2.0 a web 4.0 – Opportunità e sfide per la sicurezza nazionale 39

SEZIONE II Lo spazio cibernetico e il diritto La legislazione internazionale, europea e nazionale

Il confronto in atto sul controllo e sulle regole di gestione di internet 47

O.S.C.E. Sicurezza Cibernetica, Sicurezza delle Tecnologie Informatiche e di Comunicazione (TIC): costruire la Fiducia 56

Il Garante Europeo per la protezione dei dati 61

Autorità per le garanzie nelle comunicazioni tra reti, sicurezza e *privacy* 68

L'identità nel cyber spazio e la normativa nazionale 76

NATO towards a more concrete approach to cyber challenges 91

SEZIONE III Lo spazio cibernetico e le imprese nazionali

Cyber EW defence capability: ELT approach to future warfare 96

Vitrociset - Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali 108

SEZIONE IV Lo spazio cibernetico nella visione dall'estero

Come garantire nella fase attuale la sicurezza informatica internazionale (Federazione Russa)..... 115

Lo Spazio Cibernetico tra Esigenze di Sicurezza Nazionale e Tutela delle Libertà Individuali (Australia)..... 127

Lo Spazio Cibernetico tra Esigenze di Sicurezza Nazionale e Tutela delle Libertà Individuali (Estonia) 135

Spazio cibernetico visto dall'estero: Strategia Nazionale per la Sicurezza Cibernetica (Repubblica Ceca) 141

Formulazione di una strategia nazionale della cyber sicurezza - Aspetti chiave (Cile)..... 154

Cyber sfide durante l'operazione "Margine Protettivo" (Israele) 161

La cyber-security in Spagna (Spagna) 170

WWW (World Wild West): the American New Frontier and the US Cybersecurity Dilemma (U.S.A.)..... 178

Il Cyber spionaggio cinese e le risposte di Washington e Taipei (Cina) 186

In-sicurezza cibernetica e strategie nazionali: nuove sfide, vecchi problemi..... 193

Testi consigliati..... 200

SEZIONE I
Lo spazio cibernetico e la sicurezza nazionale

Le nuove minacce cyber

Umberto Gori

(Professore emerito nell'Università di Firenze - Presidente, CSSII, Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università di Firenze)

Gli effetti di risorse e tecnologia sulle relazioni internazionali

E' un fatto, accertato storicamente, che l'acquisizione, il possesso o la perdita di determinate risorse (da intendersi questo concetto nella sua accezione più ampia) siano sempre stati all'origine dei mutamenti nelle gerarchie internazionali di potenza ed abbiano inciso, positivamente o meno, sulla sicurezza degli Stati.

In particolare, i progressi nei settori scientifico e tecnologico hanno promosso lo sviluppo economico e reso più affidabile la sicurezza nazionale. Se guardiamo indietro nei secoli, e più in particolare a partire dagli anni della prima rivoluzione industriale, vediamo come i grandi rivolgimenti nella politica mondiale siano stati originati da tre fattori: guerre, mutamenti nell'economia e sviluppi tecnologici. Tutto è stato condizionato dalla ricerca spasmodica di risorse, materiali e immateriali. Quando c'è un trasferimento importante di risorse, insomma, il sistema internazionale subisce mutamenti di rilievo, si modificano le alleanze, nascono nuovi avversari, processi consolidati diventano impossibili. Si pensi solo alla tecnologia nucleare che, finora, ha reso la guerra *"unthinkable".*

Nello stesso modo ed ancor di più, le tecnologie ICT stanno modificando in misura difficilmente quantificabile la dinamica delle relazioni internazionali: rimodellano l'architettura del sistema internazionale, ne cambiano i processi tradizionali (già è in funzione, ad esempio, la 'diplomazia digitale' che determina una radicale trasformazione nei processi di comunicazione), rivoluziona la

finanza, il commercio, la raccolta di dati sensibili per l'intelligence, crea nuovi problemi per la politica estera (si pensi a *WikiLeaks*), modifica ed accelera la percezione di eventi critici per la sicurezza.
La tecnologia, spesso *dual use*, avvicina il mondo e nello stesso tempo lo divide. I satelliti commerciali, il GPS, le immagini dallo spazio, le previsioni meteo, Internet, tutto ciò ha potenziali applicazioni militari. L'ICT inoltre, accessibile anche ad entità subnazionali e ad individui, rende questi ultimi possibili protagonisti del cambiamento, sottraendo agli Stati il tradizionale monopolio del controllo e della forza. Ne è prova, non lontana nel tempo, il ruolo avuto dalle comunicazioni via computer o *i-phones* sul contemporaneo scatenarsi delle sommosse, in un primo tempo interpretate come 'primavere', dell'Africa del Nord.

Ulteriori sviluppi nei settori della microelettronica, nanotecnologia, biotecnologia, robotica, intelligenza artificiale, etc. potranno ulteriormente modificare i rapporti di forza fra gli Stati, introducendo nuovi strumenti nella conduzione dei futuri conflitti. Si noti che tali sviluppi sono esponenziali (in qualche modo la legge di Moore), non lineari. Questo progresso impressionante porta ad un aumento di potenza a ad una diminuzione contestuale dei costi, con conseguenze facilmente immaginabili. Oggi un iPhone ha più capacità di calcolo di quella a disposizione della NASA cinquanta anni fa. Con i *Big Data* gestibili solo con tecnologie innovative si arriva ad una quantità di dati calcolabile in Exabyte (= 10 alla 18, ulteriormente espandibili). Oggi un computer costa un millesimo rispetto ai prezzi dell'inizio anni '70. E' stato osservato che se i prezzi delle automobili fossero calati come quelli dei semiconduttori, una macchina oggi costerebbe non più di 4–5 euro. Lo sviluppo della tecnologia, e dell'ICT in particolare, non avvantaggerà però tutti nella stessa misura. Gli Stati che riusciranno ad innovare maggiormente e prima degli altri fruiranno di vantaggi strategici importanti.

La tecnologia, insomma, resta, come sempre è accaduto nella storia, la più importante variabile esplicativa per comprendere le relazioni internazionali e i mutamenti negli assetti di potere. In un mondo globalizzato e in era cibernetica chi sarà più avanti nella

tecnologia dominerà il mondo, così come è successo nel XIX secolo con l'Inghilterra per il suo dominio dei mari e nel XX secolo con gli Stati Uniti per la loro superiorità aerea e di proiezione delle forze.

Cyberspazio e cyberpolitics

Fino a non molto tempo fa il cyberspazio era considerato una questione di *low politics,* e cioè di questioni attinenti a processi e decisioni di routine, in contrapposizione alla *high politics* che riguarda la sicurezza nazionale, gli interessi dello Stato, i suoi valori, etc. Ma quando gli effetti cumulativi delle attività normali modificano le dinamiche delle interazioni fra Stati e società, anche la *low politics* diventa importante e si trasforma in *high politics.*

Come è noto, il cyberspazio, l'ultimo dei *global commons* anche se alcuni contestano questo attributo, è l'unico spazio creato dall'uomo e da esso modificabile. Le sue caratteristiche offrono grandi possibilità e, insieme, presentano gravi rischi. Il suo utilizzo è a minimo costo, garantisce l'anonimato, permette di sferrare attacchi da lontano e da qualunque parte a velocità quasi infinita, aumenta di dimensione continuamente ogni volta che si attiva un nuovo internauta, e le operazioni che si svolgono al suo interno hanno una propria *metrica* che ne misura la *performance*.

Le caratteristiche del cyberspazio implicano anche grandi vulnerabilità per la sicurezza nazionale. Le interconnessioni rese possibili da esso mettono in crisi la comprensione tradizionale delle relazioni internazionali, della politica di potenza e di altri concetti fondamentali della politica.

Sette sono le caratteristiche di questa quinta dimensione della conflittualità (e della cooperazione): rimpiazza il tempo convenzionale con il *real time*; trascende i limiti geografici e della localizzazione fisica; penetra i confini e gli ordinamenti giuridici; è fluida, si modifica e si riconfigura in modo estremamente rapido; abbatte gli ostacoli all'attività e partecipazione politica; oscura l'identità degli attori e delle connessioni (problema c.d. dell'attribuzione); scavalca i meccanismi della responsabilità.

Il cyberspazio è quindi un'arena resa possibile dall'innovazione tecnologica che permette di operare su campi

elettronici, i domìni spaziali dei quali trascendono le limitazioni tradizionali di tipo territoriale, governativo, sociale ed economico. Tale spazio consente nuove opportunità di competizione e conflitto, di acquisizione di potere ed influenza.

Lo spazio cibernetico è un sistema a quattro strati con funzioni differenziate, ma tutte ugualmente importanti o necessarie. Gli strati sono: i fondamenti e le strutture fisiche; i blocchi logici che rendono possibili i vari servizi; il contenuto di informazioni inserito, trasmesso e trasformato; gli attori che interagiscono in questa arena in ruoli diversi.

Infine – e questo è un problema serio – il cyberspazio offre alle 'superpotenze', diversamente da come accadeva in epoca di guerra fredda quando i conflitti bellici erano demandati agli Stati *proxy*, la possibilità di scontrarsi direttamente.

E veniamo così alla *cyberpolitics*, alla politica cibernetica. Essa è la congiunzione di due processi: l'interazione umana (*politics*) e quelli resi possibili dall'uso dello spazio virtuale (*cyber*). La *cyberpolitics* è insomma il nuovo modo di fare politica nell'arena cibernetica. Le azioni degli Stati stanno diventando sempre più 'virtuali' e gli investimenti in conoscenza ed innovazione diventano la fonte fondamentale del potere. Ciò comporterà una 'rivoluzione negli affari diplomatici' che si baseranno sempre di più sul *soft power* e su strumenti sempre meno 'materiali'.

Quattro sono le caratteristiche della politica cibernetica: dematerializzazione, decentramento, denazionalizzazione, deterritorializzazione. L'accesso diseguale al settore cibernetico riflette ormai la distribuzione del potere e misura i fattori di potenza degli Stati a livello internazionale. Ma è anche vero che il potere del debole oggi sfida il potere del forte.

Del resto, Kenneth N. Waltz, in *Man, the State, and War* , dà risalto all'individuo nella sua costruzione ternaria delle relazioni internazionali. L'individuo – egli sostiene – è "the sole thinking, feeling and acting system in politics". Oggi ciò è ancor più vero per la possibilità che l'individuo ha di accedere al cyberspazio. Oltre ai classici *homo oeconomicus* e *homo politicus*, viene in evidenza - come sostiene Nazli Choucri - l'*homo cybericus.*

A livello statale tre appaiono essere i fattori fondamentali: la popolazione, la tecnologia e le risorse. Ora, se noi classifichiamo gli Stati in funzione di queste variabili, abbiamo sei profili che permettono di prevedere l'intensità della loro attività in campo cibernetico. I profili sono i seguenti:
Profilo 1 : risorse, popolazione, tecnologia - *Profilo 2 :* popolazione, risorse, tecnologia - *Profilo 3* : popolazione, tecnologia, risorse - *Profilo 4* : risorse, tecnologia, popolazione - *Profilo 5* : tecnologia, risorse, popolazione - *Profilo 6* : tecnologia, popolazione, risorse. L'analisi del peso di tali fattori, delle loro interazioni e della loro collocazione ci permette di capire chi sarà più influente anche nel cyberspazio (1).

La domanda ora è: in quale gruppo si situa l'Italia? Ad avviso di chi scrive, l'Italia si situa a metà strada fra il terzo e il sesto gruppo: nel terzo gruppo perché fortemente dipendente da importazione di risorse; nel sesto perché notevolmente dotata di tecnologia. Solo da poco tempo, però, il nostro Paese ha varato norme per la protezione delle infrastrutture critiche.

Minacce cibernetiche e sicurezza

Per capire come i cyber conflitti si siano evoluti nel tempo è necessario un approccio storico che troppo spesso è stato trascurato con la conseguenza che non vengono imparate alcune lezioni che potrebbero evitare la ripetizione di errori nel presente.

Il perché la storia sia in questo campo trascurata è dovuto probabilmente, in primo luogo, alla erronea convinzione che il settore, lanciato a velocità esponenziale verso il futuro, non abbia in realtà un grande retroterra. Idea sbagliata, questa, perché – a ben vedere – la storia della cyber conflittualità risale agli anni '80, e cioè a quasi un quarto di secolo fa: quasi niente per la storia delle guerre, moltissimo per quella dei conflitti cibernetici.

Una precisazione, fra parentesi: *cyber conflict* è un *genus; cyber war* è una *species*. Molti sono stati gli episodi di conflittualità cibernetica, ma mai si è ad oggi verificata una *cyber war*.

Ciò detto, un altro motivo del mancato esame del passato è probabilmente dovuto alla scarsa trasparenza, voluta o *de facto*,

degli avvenimenti verificatisi. A questo proposito, occorre certamente una 'declassificazione' delle informazioni relative ai precedenti cyber conflitti. Un terzo ed ultimo motivo dipende dal fatto che la dinamica di base di questi conflitti è rimasta pressappoco la stessa. Ciò che è mutata, semmai, è la tecnologia ad essi sottesa.

Se questo è vero per gli Stati Uniti d'America - come ha messo in evidenza Jason Healey (2) - ancor di più lo è per l'Italia che solo da poco tempo ha iniziato ad occuparsi con una certa organicità di cyber sicurezza. Come accade anche in altri settori, è vantaggioso seguire gli insegnamenti dei primi e doveroso non ripeterne gli errori che producono conseguenze controproducenti sui processi decisionali e sulle strategie di contrasto.

La storia della conflittualità cibernetica viene divisa in tre periodi: quello della *realizzazione* (anni '80), quello del *decollo* (1998) e quello della *militarizzazione* (2003). Ed è stato Jason Healey , nel suo libro – il primo sull'argomento - *A Fierce Domain: Conflict in Cyberspace, 1986- 2012,* che ha individuato sette campanelli d'allarme (*Wake-up Calls*), dal *Morris Worm* (1988) - il nome deriva dal primo studente condannato per pirateria informatica - a seguito del quale fu dato vita al primo CERT (Computer Emergency Response Team) - fino allo *Stuxnet.* In realtà, a conoscenza di chi scrive, i campanelli d'allarme furono più di sette. Ad esempio, viene omesso volutamente l'attacco denominato *Cuckoo's Egg* del 1986 perpetrato dal KGB tramite hackers tedeschi, definito molto importante (*critical*), ma non tale da aver dato luogo a nuove dottrine e a nuovi assetti organizzativi nel sistema politico americano.

Se in questa sede non vale la pena elencare tutti gli attacchi importanti, è però altamente istruttivo ricapitolare le 'lezioni' e le risultanze di ricerca che da essi si possono apprendere. Si citano qui solo quelle che sembrano più significative.

a) Le conseguenze degli attacchi cibernetici sono state spesso esagerate; al contrario, gli effetti delle cyber intrusioni sono stati sottovalutati. E' bensì vero che siamo in un'era di *cyber guerra fredda*, ma è altrettanto vero che gli Stati, almeno finora, si

guardano bene dal superare il tetto della *hot cyber war*, così com'era accaduto nel periodo del confronto nucleare;

b) la maggior parte dei cyber attacchi appartengono alla categoria dello spionaggio economico – industriale - militare;
c) in generale, anche l'uso della Rete da parte dei gruppi terroristici non mira tanto a distruggere, almeno per ora, quanto a far propaganda, reclutare, etc.;
d) quanto più i cyber conflitti hanno valenza strategica, tanto più sono simili ai conflitti che hanno luogo nei domini classici, con un'importante differenza, però, e cioè in essi ha un ruolo decisivo il settore privato che detiene nei nostri Paesi a democrazia liberale la proprietà della stragrande maggioranza delle strutture nazionali e quindi ha le maggiori capacità di gestire le crisi e di mettere in atto le misure di contrasto per la protezione delle infrastrutture critiche;
e) attacchi cd. SCADA possono essere effettuati solo da Stati tecnologicamente avanzati;
f) solo i cyber attacchi tattici si svolgono in *no time*; quelli strategici, normalmente, che si attuano in un contesto geopolitico di rivalità e di confronto, durano periodi di tempo variabili e spesso molto lunghi;
g) è particolarmente difficile individuare i responsabili di attacchi tattici; il problema dell'attribuzione si risolve molto più facilmente quando gli attacchi sono strategici;
h) secondo dati dello Strategic Studies Institute, le operazioni nello spazio cibernetico si svolgono con una velocità di oltre 20.000 volte maggiore di quelle nello spazio fisico, di oltre 200.000 volte maggiore di quelle nell'aria, e di 10 milioni di volte maggiore di quelle in terra ed in mare. Ciò ha conseguenze precise e difficili da gestire per quanto riguarda il ciclo OODA, tali da immettere gli operatori tattici in una dimensione che può essere definita 'ultra-tattica' e che rende pressoché inevitabile la conduzione autonoma di particolari operazioni militari che richiedano invece autorizzazioni specifiche dai superiori comandi;
i) il fatto di concentrare l'attenzione sugli attacchi tattici comporta

squilibri negli investimenti e nelle strategie a danno delle difese strategiche;

j) l'esistenza di un CERT nazionale è certamente importante, ma non evita i danni, come è dimostrato dall'attacco all'Estonia nel 2007, né la sua assenza impedisce di avere solide difese contro gli attacchi cibernetici, come è il caso del Regno Unito (che solo nel 2014 si è dotato di un CERT), o di Israele: tutti e due gli Stati hanno però investito miliardi di dollari nella difesa cibernetica. Impossibile difendersi a costo zero;

k) l'utilizzo di attacchi cibernetici è stato talora funzionale, e contestuale, a scontri cinetici (es. Israele v. Siria, Russia v. Georgia).

Parlare di dinamica dei cyber conflitti significa anche parlare della progressione, quantitativa e qualitativa, dei medesimi e cioè, in concreto, delle caratteristiche che i cyber conflitti debbono avere per transitare nella categoria della guerra cibernetica, con tutte le conseguenze, anche cinetiche, che ciò comporterebbe.

Dato per scontato che il termine *conflitto* è più generico e comprensivo del termine *guerra*, cerchiamo di capire qual è la linea divisoria fra i due concetti, anche per renderci conto del fatto che, finora, la storia degli attacchi cibernetici è stata caratterizzata, ad eccezione forse di un solo caso, dall'assoluta preminenza dei *conflitti.*

Sul punto si confrontano le seguenti posizioni, ognuna delle quali enumera specifici criteri.

1. I 14 criteri di Healey si focalizzano sul problema dell'attribuzione. Sono quindi molto utili, ma non danno garanzie di obbiettività e di certezza. Se ne citano solo alcuni:
   - gli indizi fanno risalire ad uno Stato?
   - L'attacco è tecnicamente sofisticato?
   - L'attacco è correlato con dichiarazioni pubbliche o con specifiche politiche nazionali?
   - C'è assenza di cooperazione durante le indagini post-attacco?
   - Non c'è traccia di benefici economici?
   - *Cui prodest*?
2. I criteri del Manuale di Tallin si concentrano sull'uso della forza:

- intensità (quanti danni?);
- immediatezza (quanto velocemente sono percepiti gli effetti e quanto tempo è necessario perché gli effetti diminuiscano di intensità);
- impatto diretto (l'azione è stata la causa diretta degli effetti?);
- invasività (sono stati colpiti networks sicuri? L'attacco è stato sferrato all'interno stesso del Paese bersaglio?);
- misurabilità degli effetti (è il calcolo delle conseguenze, più facile in caso di conflitto armato);
- carattere militare (le FF.AA. sono state il bersaglio dell'attacco?);
- coinvolgimento statale;
- legalità presumibile (*presumptive legality*): l'azione può essere vista come uso della forza? Come è stato osservato (M. Skerov), "meno un attacco cibernetico assomiglia ad una pratica accettata dagli Stati, più consistente è l'argomentazione che si tratti di un uso illegale della forza o un attacco armato".

Con tutto il rispetto per gli eminenti giuristi redattori del Manuale, con l'eccezione di un paio di criteri (intensità e, forse, carattere militare) tutti gli altri criteri sono opinabili.

3. I criteri di Jean Pictet, autore del Commentario alle Convenzioni di Ginevra, si concentrano saggiamente su *estensione, durata e intensità* degli attacchi.
4. I criteri sui quali si concentra Thomas Rid del King's College di Londra sono la *letalità* e la *finalità politica.*
5. Molti criteri di Michael N. Schmitt, infine, ispirano quelli del Manuale di Tallin ad eccezione del 'carattere militare' e del 'coinvolgimento statale', e con l'aggiunta, successivamente, del criterio della 'responsabilità'.

Senza necessariamente trascurare alcuni criteri esposti, le preferenze di chi scrive vanno a quelli citati da Pictet e da Rid, se non altro perché già oltre due anni fa scrivevo quanto segue (in: *Armi cibernetiche e processo decisionale,* 2013, pp. 19-20): "Secondo la classica definizione ispirata da Clausewitz, il concetto di guerra implica l'uso della forza fisica *organizzata*. Oggi, ciò non è più

necessariamente vero. Allora per determinare se un attacco cibernetico è cyber war quali fattori dovremmo logicamente prendere in considerazione? Anche ammettendo che l'analisi potrebbe di solito non essere così semplice, la mia opinione è che dovremmo innanzi tutto individuare la fonte, e cioè valutare:

- se dietro l'attacco non ci sia uno Stato (e qui /…/ l'esame del contesto situazionale e strategico può essere d'aiuto);
- le conseguenze (tipo dei danni, quanto gravi, per quanto tempo);
- la motivazione (l'attacco è politico ? Risponde, cioè, a logiche di *Realpolitik*?);
- la complessità di pianificazione e di esecuzione".

Anche per quanto riguarda la *letalità*, scrivevo (*ibidem*, p. 21): "perché si possa parlare dei molti strumenti cyber come di armi da guerra /…/ innanzitutto lo strumento deve essere letale (distruttivo di cose o persone)", unico elemento – questo – *oggettivo.*

La dottrina d'impiego delle cyber operazioni è naturalmente e tendenzialmente offensiva, la difesa dagli attacchi deve essere *proattiva* piuttosto che passiva. Qui s'innestano due problemi: quello della *cyber deterrenza* e quello della *resilienza* (v. *infra*).

Circa la linea di confine fra conflitto e guerra, sono convinto che ogni attacco contro le *infrastrutture critiche* debba essere considerato un attacco armato e dunque un atto di guerra. Sono infatti operazioni belliche tutti quegli attacchi che hanno effetti *cinetici.*

A proposito di guerra, da un punto di vista sostanziale e non formale, essa "si configura ad un tempo come una specie di conflitto, una specie di violenza, un fenomeno di psicologia sociale, una situazione giuridica eccezionale, ed un processo di coesione interna" (3). E' evidente che non siamo ancora a questo punto.

Le minacce cyber rappresentano un serio pericolo per la sicurezza nazionale e per la stabilità economica dei nostri Paesi. Ciò impone a ciascuno di noi - imprese e privati, e non solo alle istituzioni - comportamenti responsabili di continua attenzione. Le vulnerabilità più frequenti, infatti, sono attribuibili alle persone più

che alla tecnologia. La privatizzazione delle risposte, però, dovrà essere regolata ad evitare possibili abusi.

L'Italia, nell'arco degli ultimi due anni, ha compiuto i primi organici passi in avanti in tema di misure di contrasto. Ricordo il DPCM 24/1/2013 che si occupa dell'architettura istituzionale necessaria; il Quadro strategico nazionale per la sicurezza dello spazio cibernetico che elenca le principali minacce informatiche; il Piano nazionale per la protezione cibernetica e la sicurezza informatica che indica le priorità e gli obiettivi, oltre ad individuare i corsi d'azione necessari, ambedue adottati il 27 gennaio 2014 dal Governo Letta; e, infine, il National Strategic Framework for Cyberspace Security del dicembre 2013, redatto dalla Presidenza del Consiglio dei Ministri (DIS). Fra le disposizioni merita ricordare l'obbligo imposto ai 'soggetti economici', pubblici e privati, di informare il CERT nazionale di ogni violazione informatica.

Naturalmente siamo agli inizi e moltissimi sono i compiti da assolvere: *in primis*, investire nelle persone e in tecnologia e soprattutto assicurare unità decisionale. E tutto questo va fatto con estrema urgenza. Credo che oggi ci sia consapevolezza di ciò. E' lecito dunque sperare, ma la sola speranza non è una strategia.

Premesso che la sicurezza nazionale oggi dipende da: sicurezza esterna, sicurezza interna, sicurezza ambientale e sicurezza cibernetica e che uno Stato è sicuro solo quando tutte le dimensioni della sicurezza sono garantite, la capacità cibernetica consente, almeno in teoria, di assicurare la *sicurezza cibernetica*. Quest'ultima si riferisce alla capacità di uno Stato di proteggere se stesso e le proprie istituzioni contro minacce, spionaggio, sabotaggio, crimini e frodi, furto d'identità ed altre interazioni e transazioni cibernetiche illecite e distruttive. Quasi sempre le pressioni sono superiori alle capacità di difesa. Ciò è anche dovuto al fatto che la rivoluzione cibernetica ha velocizzato e aumentato esponenzialmente le interazioni nel sistema internazionale, nonché l'anarchia di detto sistema, così come intesa nelle relazioni internazionali. La sicurezza cibernetica, inoltre, ha una natura dinamica perché deve adeguarsi continuamente all'evoluzione, costante e veloce, delle minacce. La sua realizzazione non è solo un

problema tecnico, ma piuttosto di mentalità: essa, infatti, non è compatibile con strutture gerarchiche ed eccessivi formalismi (4).

Per quanto riguarda le minacce cibernetiche alla sicurezza nazionale, esse sono: disinformazione, intasamento di server (DoS e DDoS), criminalità organizzata, spionaggio, modifica occulta di dati sensibili, disattivazione di strutture critiche, cyber-terrorismo, cyber warfare, etc. In particolare, è da temere la militarizzazione del cyberspazio, in cui è probabile si verifichi la dinamica che ha caratterizzato nel recente passato la corsa agli armamenti cinetici. Tutto ciò implica che gli anni avvenire saranno caratterizzati da instabilità per fronteggiare la quale saranno necessarie forme di cooperazione internazionale, anche se gli Stati continueranno a competere fra di loro. I processi di globalizzazione, spinti dal sempre maggiore sviluppo della tecnologia, accresceranno inevitabilmente le interdipendenze con effetti non necessariamente sempre positivi.

Dal punto di vista della pericolosità, gli attacchi possono essere suddivisi, in misura crescente, in cinque livelli: 1) vandalismo cibernetico e *hacktivismo*, che si verifica in concomitanza di tensioni e crisi politiche. E' questa la forma più comune di *cyber conflict*, ma anche la meno permanente e dannosa; 2) crimine cibernetico, che ha come bersaglio principale il settore privato con danni economici imponenti; 3) cyber-spionaggio, da parte di concorrenti o di Stati, che colpisce in più larga misura obiettivi industriali e scientifici; 4) cyber terrorismo. Se terrorismo significa – come è naturale che sia – atto che provoca terrore, allora, almeno fino ad oggi, non si è verificata alcuna azione riconducibile sotto l'etichetta di *cyber terrorismo*; 5) guerra cibernetica, la forma più sofisticata che può assumere la guerra dell'informazione (*I-War*). Sembra logico far rientrare in questa categoria attacchi che utilizzino *malware* come Stuxnet o simili.

Gli attacchi sono sempre più numerosi e sofisticati e dunque sempre più difficili da contrastare. Fra quelli che riguardano in particolare le imprese, sono da segnalare le sempre più probabili intrusioni nei *device* personali e nella 'nuvola' (*cloud*), le e-mail sempre più ingannevoli e il blocco dei computer con richiesta di riscatto (*ransomware*).

A fronte di queste minacce vi è tutta una serie di misure di contrasto la cui attuazione ricade sotto la responsabilità di individui, di imprese e di istituzioni statali. A queste ultime spetta il compito di varare una strategia idonea ed una normativa capace di assicurare una reazione pronta ed efficace alle minacce, di impostare il necessario coordinamento fra pubblico e privato e di collaborare con altri Stati ed organizzazioni internazionali al fine di potenziare sinergicamente le difese. Ma ognuno, nella propria sfera ha l'obbligo, oltre che l'interesse, a proteggere con estrema attenzione ed ogni mezzo i propri *assets*.

Le disattenzioni - se di disattenzioni si tratta - capitano anche nel mondo istituzionale. Negli USA, ad esempio, un tragico 'errore' ha reso pubblico un documento riservatissimo di 800 pagine intitolato *Aurora Project* contenente la descrizione dettagliata di tutte le vulnerabilità esistenti nelle infrastrutture di utilità pubblica (luce ed acqua) statunitensi. Il documento che doveva invece essere divulgato aveva un nome simile, *Operation Aurora*, contenente notizie su un attacco cibernetico del tipo APT sferrato dalla Cina nei confronti di Google e di altre grandi compagnie americane, sfruttando presumibilmente vulnerabilità *0-day* in Internet Explorer.

Tali minacce sono in aumento in tutto il mondo (oltre il 70% delle minacce cibernetiche a livello mondiale sono azioni di spionaggio economico), evolvono continuamente, non possono di solito essere individuate, così come non possono essere individuati con certezza i responsabili. Tutto ciò ha una serie di conseguenze negative derivanti anche dal fatto che oltre l'80% delle imprese non ritiene di essere vulnerabile ad attacchi cibernetici, o non denuncia gli attacchi per non compromettere la propria immagine. Anche le imprese italiane sono ad altissimo rischio, ma continuano a sottovalutare il pericolo delle minacce nonostante le gravi perdite finanziarie e di contenuti cui vanno incontro. Un documento presentato in sede Unione Europea ci informa che le perdite causate da attacchi cibernetici alle imprese del continente ammontano ogni anno a circa 53 miliardi di euro. Occorre quindi diventare 'proattivi' ed impegnarsi sempre di più in procedure di intelligence economica

almeno a livello delle imprese maggiori che, più a contatto con le istituzioni governative, sono più a rischio delle altre.

Secondo valutazioni di istituti specializzati, il mercato globale delle 'armi cibernetiche' supererà, nel decennio 2014 – 2024, la cifra di 4.000 miliardi di dollari. Ovviamente qui si pone il problema di definire esattamente il concetto di *cyber weapon*. A giudizio di chi scrive - ripeto - può essere considerata a stretto rigore *cyber weapon* soltanto un dispositivo cibernetico direttamente *letale*, e cioè distruttivo di cose o persone. Ad oggi, salvo errori, solo Stuxnet, che si propaga tramite chiavette USB, può essere considerato tale (5). Comunque sia, il ricorso sempre più massiccio alle armi cibernetiche *offensive* è dovuto anche ai costi trascurabili di queste ultime rispetto a quelle tradizionali, oltre al fatto che garantiscono in pratica l'anonimato. Le armi cibernetiche *difensive*, invece, sono di gran lunga più costose.

In particolare, le infrastrutture critiche

Un settore particolarmente delicato è quello delle cd *infrastrutture critiche* il cui malfunzionamento o collasso causerebbe conseguenze catastrofiche per i servizi essenziali alla vita economica, sociale, alimentare, sanitaria, etc., nonché per la stabilità del sistema politico e la sicurezza statale. Secondo l'opinione di una notissima esperta in materia, con riferimento alla scala dei bisogni di Maslow, non rientrerebbero nelle risorse critiche quelle che soddisfano bisogni immateriali (6). Benché suggestiva e parzialmente convincente, questa opinione non sembra del tutto soddisfacente a giudizio di chi scrive in quanto, oltre all'istruzione ed alla ricerca, sono da considerarsi 'immateriali' quelle strutture puramente informative come i *databases* contenenti dati sensibili e la stessa Internet, infrastruttura in grandissima parte immateriale.

Diverse sono le minacce cui le infrastrutture sono soggette: esse possono essere interne od esterne, naturali o provocate, da terra o dallo spazio, puntuali o persistenti (APT). I *malware* sono per lo più quelli noti: *troyan, worms, sniffers, rootkits, bootkits, backdoor, defacement* (modifica o distruzione di dati), *DoS, Stuxnet*, etc..

Agli attacchi si può reagire in tre modi: accettare le perdite (apparentemente assurdo, questo tipo di reazione è tipico di molti Paesi e soprattutto aziende); rafforzare le infrastrutture per ridurre future perdite; abbandonare l'uso di strumenti cibernetici e ritornare ai sistemi tradizionali. Assicurare la resilienza delle strutture, che è il modo più intelligente di reagire, presuppone l'analisi e la correzione delle vulnerabilità che possono dipendere dal computer (es., utilizzo di *passwords* troppo semplici) dalla rete (es., mancata protezione dei punti di entrata), dal personale (es., errori o atti illeciti del personale) e dal contesto, anche fisico (es., zone non protette). In particolare, le contromisure possono essere fisiche, organizzative e processuali, cibernetiche e assicurative, ma è evidente che per valutare il rischio che ogni minaccia comporta occorre conoscere alla perfezione il sistema da difendere, in altre parole conoscere i propri punti deboli, dato che il grado di rischio è il prodotto del grado della minaccia per quello delle vulnerabilità (R=MxV). Ai fini della sicurezza cibernetica sono pertanto fondamentali programmi antivirus aggiornati continuamente, parole di passo complesse, programmi di codifica o criptaggio, programmi di protezione (*firewall*) e salvataggio dati (*backup*).

A livello internazionale sono stati individuati sette 'meccanismi attenuanti' il rischio, validi sempre e comunque. Essi sono: 1) creazione della consapevolezza; 2) riduzione delle dipendenze; 3) incremento della ridondanza; 4) sviluppo di soluzioni di *backup* alternative; 5) incremento della flessibilità; 6) trasferimento del rischio; e, 7) condivisione delle informazioni. In futuro, si prevede che le infrastrutture critiche saranno sempre più interdipendenti e capaci di diventare resilienti, traducendo in termini computazionali le strategie tipiche del sistema immunitario.

Sicurezza cibernetica e collaborazione Pubblico/Privato

Al fine di contrastare le minacce, sempre più frequenti e sofisticate, alle nostre infrastrutture critiche da parte di innumerevoli attori, individuali, sub-nazionali e statuali, è ovvio che si debba procedere ad individuare una strategia ed una organizzazione condivise fra Stato, Istituzioni varie ed Imprese. Il perché è presto detto:

1. la maggior parte delle infrastrutture critiche nazionali sono di proprietà del settore privato e da esso gestite;
2. le vulnerabilità afferenti ai *networks* privati debbono essere risolte a livello aziendale;
3. i bersagli degli attacchi sono molto spesso il patrimonio di *know how* e i dati significativi di operatori privati;
4. ai fini di incrementare la sicurezza cibernetica e ridurre i rischi lo Stato ha necessità di avere le informazioni sulle minacce le più varie che in gran parte sono rivolte alle strutture non statuali. Il problema è di sapere se la collaborazione fra il settore pubblico e quello privato debba essere volontario od obbligatorio. Su questo preciso punto c'è un dibattito in corso negli Stati Uniti d'America che pure sono un Paese di gran lunga avanti a noi anche in questo campo. Dico subito che, data la cultura e la psicologia prevalenti in Italia, ritengo che nel nostro Paese la collaborazione debba divenire obbligatoria a tutti i livelli, anche perché da una strategia basata sulla *cooperazione* sembra utile procedere verso una strategia basata sulla *partecipazione* pubblico/privato nel contesto della quale ogni soggetto sia titolare di diritti e di doveri. Dal punto di vista strutturale, il CERT nazionale dovrebbe diventare il centro operativo per tutte le parti coinvolte. La condivisione delle informazioni, pur nel rispetto di quelle aziendali protette, e lo sviluppo ed aggiornamento delle regole sembrano essere due dei compiti più urgenti. Ovviamente, ogni struttura critica dovrà relazionarsi con il proprio ente governativo di riferimento.

Mentre lo Stato ha il compito di emanare le direttive strategiche e di attivare l'architettura istituzionale finalizzata al perseguimento della sicurezza cibernetica, i dirigenti aziendali hanno il compito, fra l'altro, di approfondire la consapevolezza della sfida e di monitorare con continuità le minacce, cercando addirittura di prevenirle, e di sviluppare metriche per quantificare l'impatto di ogni intrusione. L'*intelligence di rischio*, oggi, è probabilmente più importante della *business intelligence* convenzionale. Tutto ciò implica un costo, ma il far niente avrebbe dei costi molto più alti. Lo stesso *caveat* vale per il Governo che dovrebbe sostenere finanziariamente e legalmente le piccole e medie aziende e le *start-up* che non sono in grado di provvedere da sole alla difesa dei propri *assets.*

S'impone una nuova *cultura della sicurezza* che dovrebbe minimizzare le disattenzioni e gli errori degli operatori. L'anello più debole della catena è infatti quello umano, come prova - ad esempio – il successo dello Stuxnet, dovuto o ad un infiltrato, o - più probabilmente - ad un ingegnere iraniano poco scrupoloso.

I sistemi SCADA (*Supervisory Control and Data Acquisition*), e cioè i sistemi computerizzati di controllo industriale, sono comunque punti di forte vulnerabilità perché la loro protezione non era stata considerata prioritaria. E' un po' ciò che succede oggi con l'*Internet delle cose*.

Secondo la Mc Afee, "la sicurezza deve essere prevista fin dalle fondamenta delle componenti di rete in fase di pianificazione e progettazione" Sempre secondo Mc Afee, sono in particolare le *smart grid* ad essere particolarmente vulnerabili a causa dell'interconnessione dei sistemi integrati, dell'automazione e dell'obsolescenza della rete energetica, collegata così com'è, ad Internet "senza utilizzare sistemi di cifratura".

C'è anche un altro problema che deve essere risolto. Di solito, gli operatori cercano di arginare gli attacchi analizzando e operando sui propri *networks*, ma questo approccio è defatigante, costoso e non può dare risultati positivi a fronte dell'incalzare di nuove tecnologie. E' necessaria una nuova strategia di difesa basata sull'analisi delle minacce, sia tentate che riuscite, ai propri dispositivi e, così facendo,

costruire degli *indicatori* per mezzo dei quali intravedere tendenze e modelli d'azione (6), anche perché molti attacchi cibernetici, soprattutto quelli di carattere spionistico, si sviluppano sui tempi lunghi. La condivisione fra imprese dei dati sulle minacce - fatte salve le informazioni riservate - è altamente raccomandabile in quanto permette una migliore comprensione delle tattiche d'attacco ed una maggiore capacità predittiva.

E' necessaria anche una stretta cooperazione a livello internazionale. Sul punto è da ricordare che l'ITU, l'Unione Internazionale delle Telecomunicazioni, ha promosso l'*International Multilateral Partnership Against Cyber Threats (IMPACT),* un partenariato pubblico/privato impegnato ad assistere gli Stati membri, a gestire piattaforme *online* per la condivisione delle informazioni e per allertare le competenti autorità su minacce imminenti.

Per chiudere sul punto: il problema della cyber security è che essa deve rincorrere continuamente la costante e velocissima evoluzione dei rischi e delle minacce. La sua natura è dinamica, non statica. La sua realizzazione mal si adatta a rigide classificazioni, a formalismi istituzionali, a strutture gerarchiche. Ecco perché assicurare la sicurezza nell'era cibernetica non è soltanto un problema tecnico, ma un problema di mentalità, richiede una rivoluzione culturale particolarmente difficile da ottenere soprattutto nel contesto statuale dove ogni organo difende strenuamente le proprie specifiche competenze, esige un radicale snellimento delle strutture. La gravità delle minacce richiede un sacrificio delle pur legittime prerogative. Le decisioni devono essere quasi sempre immediate, il che richiede un unico centro sovraordinato legittimato ad imporre misure di contrasto. I compiti ancora da assolvere sono moltissimi: investire nelle persone e in tecnologia e soprattutto assicurare strategie condivise. E tutto questo va fatto con estrema urgenza.

Strategia militare e tecnologia

Che relazione c'è fra strategia e tecnologia? Sembra logico affermare che è la tecnologia a dettare la strategia, anche se è nello stesso tempo vero che fra evoluzione tecnologica e strategie e dottrine esiste un rapporto processuale di interazione. È l'informazione, e la velocità con la quale essa si diffonde, la caratteristica dell'ICT, insomma, che consente di superare le asimmetrie nei fattori di potenza. Sono il livello tecnologico e la conoscenza dell'avversario che compensano anche l'inferiorità numerica e delle forze convenzionali. Premesso che finora - come già detto - si può parlare di cyber guerra fredda fra gli Stati, ma non ancora di *hot cyber war,* l'ICT permette fra l'altro l'integrazione fra le forze di terra, di mare e di aria, per non parlare dello spazio fisico e di quello virtuale, con la conseguenza di razionalizzare l'impiego delle forze e degli strumenti con conseguente riduzione dei costi. Tutto ciò, insieme con l'innovazione tecnologica nei sistemi d'arma, consentirà di parlare di 'rivoluzione negli affari militari' (RMA), filosofia sulla quale s'innesterà, per concretizzarla, la *Network Centric Warfare.* La NCW si sviluppa su tre livelli: quello strategico, con il controllo di tutte le dimensioni del terreno di scontro; quello tattico, con la capacità di superare in velocità l'avversario; e quello 'strutturale', con i sensori che consentono lo scambio dei dati in tempo quasi 'reale'. Con il documento *Joint Vision 2020* gli Stati Uniti promuovono le *joint operations* e l'interoperabilità soprattutto dei mezzi di comando e controllo. Due altri concetti seguiranno: l'*effect based operations*, operazioni militari miranti ad un preciso risultato, e il processo continuo di *trasformazione* delle forze armate necessario per conformarsi alla NCW con il progressivo sviluppo di una nuova cultura che deve tendere a rimettere in discussione gerarchie consolidate e a creare e anticipare il futuro.

In Europa gli Stati hanno reagito alla NCW in ordine sparso. Abbiamo così la *Network Enabled Capability* (NEC) britannica, la *Network Based Defense* svedese, le *operazioni net-centriche* francesi, etc. Anche in Italia la NCW ha assunto la forma, meno dispendiosa, della NEC che consente di rendere progressivamente net-centriche piattaforme e mezzi *già esistenti.* Il progetto di 'Forza

NEC' dell'esercito italiano è concepito per essere funzionale a tutti i tipi di conflitto, da quelli ad alta intensità alle forme di contrasto al terrorismo transnazionale (7). Insomma, anziché concepire la NCW come una filosofia per ottenere la superiorità militare come fanno gli Stati Uniti, gli Stati europei guardano alla NEC come ad un modo per accrescere l'efficacia degli strumenti bellici ed ottenere i risultati ricercati, combinando l'utilizzo di strumenti diplomatici e strumenti militari (*Effect Based Approach).*

Nonostante gli indubbi lati positivi, la NEC presenta alcune vulnerabilità fra le quali un'eccessiva dipendenza dall'informazione, maggiori rischi in caso di attacchi cibernetici e la mancanza di interoperabilità con alleati non attrezzati con gli strumenti della guerra in rete. A ciò si aggiungano le resistenze culturali delle forze armate, i costi e la maggiore complessità nell'acquisizione dei materiali necessari. L'armonizzazione fra gli Stati e la soluzione dei problemi viene ricercata dalla NATO che ha elaborato il concetto di *NATO Network Enabled Capability* (*NNEC*) più vicino alle concezioni europee che a quelle americane. L'Unione Europea è rimasta indietro , anche se ha iniziato da tempo un processo di valutazione delle vulnerabilità esistenti con l'*European Capability Action Plan* (*ECAP*), considerato un "approccio promettente", ma poco operativo, dato che consiste in un processo volontario e senza fondi che possano dargli concretezza, anche se non mancano i tentativi per farlo progredire (8).

Ai fini di raccogliere informazioni la guerra in rete si avvale delle attività di cui alle ultime tre lettere dell'acronimo C4ISR (*Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaisssance*), e cioè intelligence, controllo elettronico e ricognizione. Le prime quattro operazioni di cui alle lettere precedenti hanno lo scopo di trasmettere l'informazione raccolta e di organizzarne la distribuzione in funzione delle esigenze della linea di comando.

E' indubbio che per gli Stati europei la guerra 'in rete' ha costi molto alti, è complessa e sottostà al rischio di perdere efficacia in caso di neutralizzazione anche di una sola funzionalità. Come dimostrano le *lessons learned* dalle operazioni in Afganistan ed Irak,

alla fine il fattore umano fa la differenza. Nei conflitti a bassa intensità, inoltre, e soprattutto nel caso di conflitti asimmetrici, la tecnologia perde di valore, se non altro perché non è difficile fornire false informazioni a chi sull'informazione basa la propria superiorità. D'altra parte, è vero che anche chi combatte la superiorità tecnologica con strategie e tattiche asimmetriche utilizza almeno uno degli elementi di C4ISR, il computer. I danni maggiori, da questo punto di vista, possono venire da una progressiva 'statalizzazione' del terrorismo.

L'aspetto positivo è che gli strumenti della guerra cibernetica possono essere usati anche a fini civili, ad esempio per prevenire catastrofi naturali, etc. (9).

L'impatto del cyberspazio sulla geopolitica e sulla strategia

Molti ritengono che le tecnologie dell'informazione abbiano causato la 'fine della geografia' su cui la geopolitica tradizionalmente si appoggia (10). Sostenitori della RMA, come Libicki ed altri, hanno affermato che la natura del tempo, dello spazio e della distanza nelle interazioni hanno subito un'alterazione a causa della rivoluzione informatica. Se i confini spariscono nel cyberspazio, può esserci una geopolitica, sia pure virtuale? Lo spazio cibernetico è unico perché costruito dall'uomo a differenza degli ambiti terrestre, marittimo, aereo e spaziale e quindi è manipolabile a differenza di ciò che accade con la terra e gli oceani. Ciò significa davvero la fine della geografia e della geopolitica? Nonostante il ridimensionamento di tempo e spazio è pur tuttavia vero che il territorio resta un basilare principio organizzativo che definisce sia le relazioni sociali che quelle politiche ed umane. Del resto la geografia condiziona, ma non determina, la strategia. La geografia è una costante, ma la creatività politica ne può fare una variabile nel calcolo strategico.

Altro problema discusso da alcuni analisti militari è se la codificazione della guerra in uso dai tempi dell'industrializzazione in tre livelli, strategico, operativo e tattico, non sia stata messa a rischio dalle tecnologie ICT. Con le tecnologie '*comando e controllo*'

basate su computer, satelliti e sensori diventa possibile una *situational awareness* condivisa che metterebbe a rischio il livello 'operativo', facendo tornare in vita il legame diretto fra strategia e tattica. Anche qui - senza poter entrare nei particolari - sembra doversi concludere che i tre livelli della guerra manterranno, sia pure in contesti diversificati, la loro funzione.

Ulteriore questione riguarda la fattibilità di una *cyber deterrenza*. A parte la considerazione che l'applicazione della deterrenza strategica tipica del periodo della guerra fredda urta contro la difficoltà od impossibilità di identificare la fonte dell'attacco e di individuare gli obiettivi, si deve prendere atto della differenza esistente fra le due situazioni: il numero degli stati nucleari era ed è limitato; quello degli attori cibernetici, invece, è altissimo, in rapida espansione e in costante mutamento. Il periodo precedente era caratterizzato da relazioni bipolari simmetriche, mentre in quello presente le relazioni sono numerosissime e asimmetriche. In breve, le alternative alla deterrenza in campo cibernetico sono la *resilienza* e la flessibilità, le uniche strategie che possano assicurare una *deterrence by denial.* Comunque, la deterrenza può funzionare solo nei confronti degli Stati, ma non nei confronti di gruppi terroristi ed organizzazioni clandestine. La validità di una strategia di deterrenza, insomma, declina con il diminuire del livello di organizzazione formale del potenziale attaccante.

La protezione assoluta dagli attacchi cibernetici è impossibile, ma – come è stato detto – "la resilienza è il ponte fra il possibile e l'ideale".

Infine, le caratteristiche dell'era cibernetica restringono drasticamente i tempi del ciclo decisionale OODA (*Observe, Orient, Decide, Act*), con il risultato di dover prendere decisioni sotto stress e quindi non ottimali, o addirittura ad impatto negativo. Unico rimedio sono decisioni pre-programmate in risposta a scenari diversificati.

La cyber intelligence

La sicurezza del sistema economico è diventato un problema estremamente serio che deve preoccupare non poco gli Stati e gli ambienti imprenditoriali e finanziari. Purtroppo, è scarsa la consapevolezza della potenziale gravità delle conseguenze di attacchi sempre più sofisticati di spionaggio economico che costituisce oltre il 70% delle minacce a livello del pianeta. In particolare, le aziende italiane 'penetrate' hanno avuto un incremento del 57,2% dal primo semestre 2012 allo stesso periodo 2013 (11). Si sospetta che anche i sistemi SCADA siano già stati infiltrati per circa un terzo. Secondo dati di Symantec, inoltre, gli attacchi hanno cominciato a colpire anche i social media e i dispositivi mobili.

Le difese tradizionali, basate sul rilevamento delle 'firme' di codice dei virus non sono più sufficienti contro gli attacchi complessi e dinamici, multi-vettoriali e multi-fase di nuova generazione e contro l'impiego delle APT e il possibile sfruttamento delle vulnerabilità *zero-day.* (12). Occorre rendersi conto che la cyber sicurezza è un processo dinamico che deve essere gestito e controllato senza sosta.

L'intelligence, ed in particolare l'intelligence economica, ha assunto un'importanza ancora più grande per la difesa del sistema Paese in un mondo sempre più globalizzato. La definizione del concetto, però, muta a seconda delle culture e delle tradizioni dei vari Paesi. Mentre in Italia essa mette in risalto l'attività dei Servizi, nei Paesi di cultura anglosassone gli attori possono essere pubblici o privati. In Francia l'attività riguarda soprattutto le imprese (13).

Quanto alla cyber intelligence, essa si pone al vertice dei vari tipi di intelligence in quanto adotta un approccio olistico e multidisciplinare di integrazione e fusione delle informazioni. La correlazione di queste ultime rappresenta un netto vantaggio per i soggetti, pubblici e privati, che devono ormai analizzare e processare quantità sterminate di dati (*big data)* e di dati sui dati (*metadati*). In futuro, la *Big Data Analytics* permetterà controlli automatizzati in tempo reale e capacità previsionali con l'individuazione di correlazioni nascoste. Nello stesso tempo, però,

questa proliferazione incessante di dati potrà essere all'origine di seri problemi per quanto riguarda la democrazia e la *privacy.*

Strumenti giuridici e diplomatici per limitare i conflitti nel cyberspazio

In un contesto come quello che abbiamo cercato di descrivere è ovvio che si siano fatti tentativi di ricercare strumenti che possano regolamentare le azioni che gli Stati sono in grado di svolgere nel cyberspazio e limitare i danni che tali azioni comportano. Oltre alle indicazioni contenute nel Manuale di Tallin già evocato, si è fatto spesso riferimento alla Convenzione di Budapest del 2001, promossa dal Consiglio dell'Europa sul crimine cibernetico, che è il primo trattato internazionale concernente i reati compiuti tramite Internet e le reti di computer. A parte, forse, la necessità di rivedere alcuni punti della Convenzione stessa (14), che ha l'obiettivo di proteggere la società nei confronti dei reati informatici con l'adozione di una appropriata legislazione quanto più possibile uniforme e attraverso la cooperazione internazionale, sembra maggiormente possibile, ad oggi, l'affermazione di regole non cogenti stabilite tramite le Nazioni Unite od altre organizzazioni internazionali rispetto ad accordi giuridicamente vincolanti anche a causa di non risolti problemi relativi alla definizione di determinati concetti. In altre parole, un approccio diplomatico-politico (adozione di cyber CBMs ed eventualmente istituzione di *hot lines* fra Cyber Comandi) sembra per ora avere maggiori possibilità rispetto ad un approccio giuridico alla questione anche perché, oltre tutto, i soggetti interessati non sono soltanto gli Stati, ma anche le industrie IT ed il settore privato. Il dibattito, insomma, è in pieno svolgimento ed è considerato urgente pervenire ad una soluzione. In assenza di accordi, infatti, ci si può trovare a breve in situazioni definitivamente compromesse. Per alcuni sarebbe utile formulare nuove norme adatte all'ambiente cibernetico, mentre altri sostengono la necessità di estendere analogicamente le norme di diritto internazionale vigenti nel settore dei conflitti armati. Per il resto, l'attenzione si è concentrata piuttosto sui reati informatici e sul cyber-terrorismo,

area degli attori non-statali, sulla quale è ovviamente più agevole pervenire ad una cooperazione internazionale (15).

Note

(1) N. Choucri, *Cyberpolitics in International Relations*, MIT Press, 2012.
(2) J. Healey, *A Fierce Domain:* Conflict *in Cyberspace 1986-2012*, 2013.
(3) U. Gori, *Guerra*, in: "Dizionario di Politica", a cura di N. Bobbio, N. Matteucci e G. Pasquino.
(4) U. Gori, *La protezione cibernetica delle infrastrutture nazionali: solo un problema tecnico ?*, in: U. Gori e S. Lisi (a cura di)., "La protezione cibernetica delle infrastrutture nazionali", F. Angeli, Milano, 2014.
(5) *Amplius* in: U.Gori, *Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici*, in: U.Gori e S. Lisi (a cura di), "Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana", F. Angeli, Milano, 2011.
(6) L. Franchina e AA.VV., *Infrastrutture critiche: Direttiva Europea e ricadute sull'Italia*, Presidenza del Consiglio dei Ministri, s.d.
(7) G.Gagnon, *Why Business should share Intelligence about Cyber Attacks*, Harvard Business Review, 2013.
(8) Si veda, per un'accurata analisi, CeMiSS, *La Network Centric Warfare e l'esperienza italiana. Il processo di digitalizzazione dell'Esercito*, a cura di P. Batacchi, 2009.
(9) J.P. Maulny, *La guerre en réseau au XXIe siècle. Internet sur le champs de bataille*, Parigi, 2006. Si veda anche EU Institute of Security Studies, *European Capability Action Plan (ECAP),* a cura di B. Schmitt, s.d.
(10) J.P. Maulny, *op. cit.*
(11) Fonte Maglan-Information Defense Technologies.
(12) Si veda U. Gori, *Dall'intelligence economica alla cyber intelligence: sfide e problemi per le imprese, sot*to stampa.
(13) Per una trattazione più esaustiva dell'argomento si veda U.Gori, *Cyberspazio e relazioni internazionali: implicazione geopolitiche e geostrategiche*, in: U.Gori e S. Lisi (a cura di), "Armi cibernetiche e processo decisionale", F. Angeli, Milano, 2013.
(14) J. Saunders, *How to Avoid Conflict Escalation in Cyberspace*, in: "The RUSI Journal", 2013.
(15) cfr. P. Meyer, *Diplomatic Alternatives to Cyber-Warfare – A Near-Term Agenda*, in: "The RUSI Journal", 2012.

I centri di eccellenza e la conoscenza condivisa

Serena Lisi
(CSSII - Docente a contratto di Analisi e Pianificazione delle Operazioni di Pace dell'Università di Firenze)

Ventisette aprile 2007: una serie di attacchi cibernetici con DDoS (Distributed Denial of Services) colpisce l'Estonia, anche soprannominata E-stonia o @stonia per l'alto grado di informatizzazione delle strutture socio-economico-politiche.

L'attacco, probabilmente proveniente dalla Russia a seguito della disputa sulla riallocazione della statua bronzea del Soldato Sovietico (*Pronkssõdur* o *Bronzovyj Soldat)* di Tallinn, fu perpetrato contro siti di organizzazioni estoni, pubbliche e private, ivi comprese le maggiori banche ed il Parlamento. Dalla stessa Russia, in periodi successivi all'attacco, provennero *rumors* e conferme non ufficiali pur smentite dalle autorità (Corriere della Sera del 18 maggio: Dmitrij Peskov, portavoce del Cremlino, dichiarò «Le accuse formulate sono assolutamente prive di qualsiasi fondamento»). Per questo attacco, l'Estonia chiese l'applicazione dell'Articolo 5 del Trattato NATO, ossia l'applicazione della dottrina della *self-* e *mutual-defence*, così come anche citata all'art. 51 della Carta delle Nazioni Unite. L'articolo, infine, non fu applicato. Tuttavia, una simile richiesta costituì un precedente mai visto, nonché un monito per la comunità internazionale, i Paesi del Patto Atlantico e l'Unione Europea, tanto che il Presidente dell'UE, José Manuel Barroso, sempre il 18 maggio 2007, dichiarò che l'UE sarebbe stata compatta «nel difendere i suoi membri in uno spirito di solidarietà».

Da una parte, questa dichiarazione di intenti del Presidente UE è risultata veritiera in vista del successivo sviluppo dell'Agenda Digitale, tuttavia più incentrata su innovazione tecnologica, normativa sulla concorrenza e copertura dei territori con servizi in banda larga ed extra-larga (Wi-Max). D'altra parte, sia a livello europeo che globale, la prima e più strutturata iniziativa in risposta all'attacco all'Estonia è giunta dall'ambiente NATO, con la nascita del Tallinn NATO Cooperative Cyber Defence Centre of Excellence. In realtà, l'idea di creare un centro cooperativo di difesa precedeva di

diversi anni l'emergenza estone. Come si può leggere nello stesso sito del Centro (https://ccdcoe.org/history.html), sin dal 2002, con il Summit di Praga, la Cyber Defence aveva cominciato a far parte del Concetto Strategico della NATO. Nel 2004, l'Estonia aveva avanzato proposte in questo senso e, nel 2006, il Supreme Allied Command Transformation (comando per le trasformazioni, situato a Norfolk, in Virginia) aveva approvato tale idea ed il concetto strategico ad esso sotteso. Così, nel 2007, le *sponsoring nations* candidate, tra le quali figura anche l'Italia, avviarono i negoziati che, nel 2008, porteranno all'apertura delle attività del Centro. Tali attività iniziarono con la firma del Memorandum of Understanding ad opera di Estonia, Germania, Italia, Lettonia, Lituania, Slovacchia e Spagna e con l'accreditamento del Centro presso la NATO, quale Organizzazione Militare Internazionale, il 28 ottobre 2008. Oggi le *sponsoring nations* sono 14 e l'Austria ha lo status di Contributing Nation.

Ma come funziona il Centro di Eccellenza? Nel sito si legge che esso è *'NATO-accredited research and training facility dealing with education, consultation, lessons learned, research and development in the field of cyber security'* . In breve, il Centro funziona come polo di formazione, ricerca e sviluppo della dottrina, tanto che, nel 2009, è stato lanciato il progetto (detto Tallinn Manual Process) per il *Tallinn Manual on International Law Applicable to Cyber Warfare*, che oggi è una pubblicazione, cartacea e telematica, di 302 pagine, che cerca di raccogliere dottrina e conoscenza condivisa, al fine di porre alcuni punti fermi nel settore della cyber security e cyber warfare. Questo tentativo di regolamentazione è uno dei pochi – ma non l'unico – riguardante la cyber security. Ma prima di analizzare alcuni dei tentativi più rilevanti in questo senso, pare opportuno, in questa sede, proseguire con la descrizione delle attività del Centro di eccellenza e di altri centri con scopi affini. Come già spiegato, il Centro di Tallin offre formazione e consulenza. Per andare più nello specifico, il CCD COE ha le seguenti caratteristiche:

- è cooperativo, poiché lo scopo del Centro consiste nello sviluppare una conoscenza a tutto tondo e condivisa, nonché una capacità di interazione tra Paesi, alla luce di un bagaglio culturale comune, basato sulle cosiddette "lessons learned";

- sotto la guida di un Direttivo, è diviso in cinque sezioni, ossia "Law and Politics", "Technology", "Strategy", "Education and Exercise", "Support".

In base a queste caratteristiche, all'interno del Centro, hanno luogo le seguenti attività:

- "Legal & Policy Support to NATO and Nations", ossia attività di sostegno ed integrazione per le le politiche legali e strategiche nazionali;
- "Legal & Policy Research", ossia attività di studio e ricerca legate alle aree legali e politiche, sempre, ovviamente, sui temi cyber security, defence, warfare;
- "Strategy and Capability Development", ossia sviluppo di capacità, singole (afferenti ai singoli Paesi) ed integrate, con lo studio di scenari futuri e casistiche;
- "Military Doctrine and Capability Development", ossia sviluppo di capacità di analisi, prevenzione, contrasto e adattamento in collegamento con la dottrina ed il Concetto Strategico NATO;
- "External Exercise Support", ossia sostegno ad alcune delle più note esercitazioni multinazionali realizzate su tematiche cyber (a titolo esemplificativo, si ricordano i contributi a Cyber Coalition 2014 e Baltic Ghost);
- "Education and Awareness", ossia attività di sostegno alla creazione della cosiddetta *cultural* and *situational awareness*, fondamentale in tutti gli ambienti strategici, dalle Peace Support Operations (PSOs) ai conflitti sociali ed economici;
- "Technical Exercises", ossia esercitazioni tecniche per restare al passo con l'evoluzione esponenziale delle tecnologie e della loro applicazione;
- "Digital Forensics", ossia lo studio della nascente dottrina giuridica in materia cyber, nazionale ed internazionale;
- "Penetration Testing", ossia lo studio di resistenza e resilienza delle strutture cyber, in particolare delle infrastrutture critiche;
- "Monitoring and Situational Awareness", ossia, come nella precedente sezione "Educational", il sostegno allo sviluppo di attività di monitoraggio e comprensione della realtà circostante, in nome della già citata "cultural and situational awareness".

Il Centro di Tallinn non è l'unico Centro di Eccellenza della NATO, anche se è il solo interamente dedicato alla cyber security, nonché l'unico, anche al di fuori dell'ambiente NATO, a trattare la materia con un approccio sistematico ed olistico al tempo stesso. Molti sono i Centri accreditati in Europa, oppure in via di sviluppo. Ai fini dei temi legati alla cyber security, i centri NATO più interessanti da tenere in considerazione sono:

- il Centre of Energy Security in Lituania, la cui attività si basa sulla protezione di infrastrutture critiche energetiche, quali quelle legate a gas e petrolio ed elettriche;
- il costituendo Crisis Management and Disaster Response Centre in Bulgaria, incentrato proprio sulla risposta alle crisi, ivi comprese quelle provenienti da attacchi cyber;
- il Modelling Simulation Centre di Roma, che realizza esercitazioni quali la NATO Computer Assisted Exercise (CAX);
- il Counter Improvised Explosive Devices Centre of Excellence in Spagna, ove vengono realizzate anche simulazioni in ambiente elettronico e cyber;
- il Centre for Air Operations in Francia, ove, di recente, è stato dato spazio anche alla dottrina d'uso dei mezzi *unmanned*, come droni ed affini.

Questo elenco non è tassativo ed è costituito da meri esempi, ma può essere molto utile per comprendere la portata delle tematiche cyber, nonché il grado di compenetrazione tra mondo reale e virtuale, che riguarda tutte le realtà della vita, dagli ambienti civili a quelli militari, dalla vita quotidiana ai casi di emergenza.

Un simile scenario ha contribuito al proliferare di svariati centri di studio sulla cyber security, molti dei quali hanno acquisito, eventualmente ex post, l'etichetta di "Centro di Eccellenza". Tra i più noti figurano quello dell'Esercito Americano, United States Cyber Center of Excellence di Fort Gordon, il costituendo *Cybercrime Centres of Intelligence Network*, i 44 centri universitari di eccellenza designati dalla NSA (National Security Agency) e dal DHS (Department of Homeland Security) come National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD), il NIST (National Institute of Standards and Technology),

National Cybersecurity Center of Excellence e il Cyber Center of Excellence of San Diego.

Il centro di Fort Gordon è destinato alla formazione del personale militare e di una vera e propria cyber force, in linea con la dottrina statunitense della *cyber supremacy*, dichiarata in chiaro anche nello stesso sito del Centro. Il personale viene addestrato seguendo la cosiddetta filosofia DOTMLPF (Doctrine, Organization, Training, Material, Leadership, Personnel and Facilities), con un forte indirizzo verso la risposta agli attacchi cyber ed alla Electronic Warfare (EW), una delle sette tipologie di Cyber Warfare enumerate da Libicki. Il Centro è dotato di una Signal School ed una Cyber School e produce svariate pubblicazioni settoriali di carattere tecnico. La condivisione della conoscenza è estesa anche alla popolazione civile, che tuttavia resta parte terza, poiché coinvolta solo indirettamente nelle attività del centro.

Il *Cybercrime Centres of Intelligence Network* è un progetto finanziato con fondi europei, basato sulla collaborazione tra organismi civili, militari, accademici e del mondo dell'industria per realizzare studi, esercitazioni, raccolta di buone pratiche e formazione nell'ambito della cyber security. Il *core* del centro sarà un organo di coordinamento bicipite, formato da due centri con base in Francia ed Irlanda. Il centro di eccellenza francese vede la cooperazione dei seguenti soggetti: Università della Tecnologia di Troyes, Università di Montpellier 1, Gendarmerie Nationale, Police Nationale, Thales (avionica e *big data*), Microsoft France. Il Centro irlandese, invece, si avvale della cooperazione di: University College Dublin Centre for Cybersecurity & Cybercrime Investigation, An Garda Síochána (servizio nazionale di polizia irlandese), Microsoft Ireland, Irish Banking Federation, INFACT (Irish National Federation Against Copyright Theft), eBay. L'approccio olistico è, da un lato, simile a quello applicato a Tallinn, ma, nonostante la cooperazione civile-militare evidenziata nei partenariati, non ha ancora sviluppato un proprio concetto strategico, anche vista la fase di avanzamento lavori, ancora allo start-up. Inoltre, a differenza del Centro di Tallinn e nonostante la forza economica di alcuni partners commerciali, il destino del Network è strettamente legato all'andamento dei

finanziamenti europei, soggetti a rendiconto ed anche a revisioni semestrali ed annuali delle politiche monetarie.

Tra i 44 centri designati da NSA e DHS come National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD), figurano colleges (per la formazione sia biennale che quadriennale), dipartimenti specializzati all'interno di istituti universitari, centri universitari di studio e ricerca. Nel novero sono inseriti, ad esempio, l'Università della Pennsylvania, l'Università del Texas ed il suo Dipartimento di Digital Forensics, Princeton, la Syracuse University, l'Università della California a Davis. La designazione avviene sulla base di criteri accademici, ma anche sull'attinenza dei programmi di studi alla *mission* di NSA e DHS, nonché al tipo di profilo professionale creato per gli studenti che terminino correttamente il corso di studi. Il NIST (National Institute of Standards and Technology) National Cybersecurity Center of Excellence è stato creato nel 2012 con lo scopo di rafforzare gli standard di sicurezza tecnologica, nonché di creare professionalità nel campo della sicurezza cyber, attraverso metodi di lavoro e di gestione del *business* innovativi.

Il Cyber Center of Excellence of San Diego, invece, è una partnership pubblico-privata di natura economica. Questo centro ha un approccio a tutto tondo e multi-disciplinare in ambito economico, ma non omnicomprensivo come quello di Tallinn. Tuttavia, anche questo centro merita di essere menzionato, poiché, al giorno d'oggi, le nuove guerre sono spesso combattute senza armi tradizionali, sono conflitti asimmetrici e a "bassa intensità", come direbbe Mary Kaldor e, sempre più spesso, l'aspetto economico assume un ruolo primario. Scopo principale del Centro è promuovere l'allineamento e la collaborazione nella comunità cyber, tenendo in collaborazione tutti i settori economico-strategici delle attività svolte nel cyber spazio, dall'industria alla formazione universitaria, dalla comunicazione alle infrastrutture, dalle applicazioni civili a quelle militari. Inoltre, il Centro cura le politiche di tutela delle infrastrutture critiche, soprattutto economiche e quindi, pur con le dovute differenze rispetto alle altre realtà trattate, anche il Centro di San Diego può costituire un riferimento utile nel campo della cyber

security. Anche gli esempi sopra riportati non costituiscono un elenco tassativo, ma possono comunque fornire un quadro della situazione corrente. Tutti questi centri contribuiscono alla diffusione di una cultura della sicurezza cibernetica, alla conoscenza delle cosiddette "lessons learned" e di buone pratiche, che devono costituire un background comune. Si ricorda, infatti, che lo spazio cibernetico fa parte dei cosiddetti *global commons* ed è quindi un patrimonio comune. Uno dei problemi legato a questo patrimonio comune risiede nel farlo conoscere correttamente agli utenti e, tramite tale conoscenza, dare una regolamentazione (o una "guida per l'uso corretto") minima, riconosciuta a livello globale. Ad oggi, come è noto, non esiste una regolamentazione unica dello spazio cibernetico. Alcuni Paesi, come gli Stati Uniti e, seppur in maniera minore, i Paesi dell'Unione Europea, riconoscono la necessità di regolamentare lo spazio cibernetico e stanno operando in questo senso. Altri Paesi, come ad esempio la Federazione Russa, non riconoscono appieno questa necessità. Altri ancora, come la Cina, hanno un comportamento ambiguo, poiché, se da una parte non riconoscono alcuni principi minimi della sicurezza cibernetica, dall'altra applicano una normativa estremamente restrittiva al mondo web: si veda, ad esempio, lo stretto controllo operato su rete e *social networks* e la possibilità di operare delazioni anonime, proprio attraverso il web, a danno di presunti dissidenti ed oppositori politici, come evidenziato, tra gli altri, da Freedom House.

Negli ultimi anni, come già accennato sopra, ci sono stati tentativi di regolamentazione dell'ambiente cyber. Uno di questi tentativi è costituito dal *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, un *export control regime multilaterale* (MECR)che, fin dal 1996, classifica tutti quei beni e device che possono essere ritenuti dual-use, cioè passibili di usi per scopi sia civili che strategico-militari (quindi anche bellici). L'*arrangement* prevede l'inserimento di taluni prodotti e *device* in una lista composta da nove categorie, sette delle quali attualmente strettamente correlate con l'ambiente cibernetico: Special Materials and Related Equipment, Materials Processing, Electronics, Computers,

Telecommunications and "Information Security", Sensors and "Lasers", Navigation and Avionics, Marine, Aerospace and Propulsion. L'*arrangement* è sicuramente utile al fine di dar una dimensione, anche fisica e tangibile, a tutto ciò che riguarda l'operato nello spazio cibernetico. Tuttavia, non ha valore universale né cogente ed è vincolante soltanto per i Paesi firmatari.

Un tentativo più stringente di regolamentazione e creazione di uno spazio normativo condiviso è costituito dal già citato Tallinn Manual on International Law Applicable to Cyber Warfare. Anch'esso, però, non ha valore vincolante. Tuttavia, è interessante analizzane il contenuto ed in particolare alcune "rules", che si concentrano su concetti quali: la protezione dei civili e la protezione delle infrastrutture vitali, con particolare riferimento a quelle energetiche e sanitarie, e anche la ridefinizione di concetti basilari come sovranità (rules 1 e 4), uso della forza (rules 10-12), necessità e proporzionalità (rule 14), imminenza ed immediatezza (rule 15), atto di perfidia, *self-defense*. Sempre in una situazione *de jure condendo*, si colloca anche un tentativo russo-americano del 2011, nato in occasione dell'attuazione degli accordi START2, alla Conferenza di Monaco sul disarmo nucleare: in questo contesto, è stato presentato un documento di produzione russo-americana intitolato "Working Towards Rules for Governing Cyber Conflict", dal quale emergono alcuni concetti relativi a scenari e strategie applicabili al contesto cyber: necessità di individuare entità oggetto di protezione nel ciberspazio; applicazione delle Convenzioni di Ginevra anche al ciberspazio; riconoscimento di attori non statuali e riconoscimento di modalità conflittuali c.d. "other than war". Tutti questi tentativi di creare una conoscenza e coscienza comune, condivisa, fanno parte di un contesto internazionale che è globale e frammentato al tempo stesso: si vedano ad esempio le posizioni dell'ITU (International Telecommunication Union) e dell'ONU, che raccomandano di attuare approcci comuni. L 'ITU ha creato il cosiddetto Cyber Security Index e l'ONU, proprio in collaborazione con l'ITU, ha definito la cyber security quale "global issue demanding a global approach" ed ha operato attraverso il Consiglio Economico e Sociale (ECOSOC) ed altri organi. Tuttavia, né l'ONU né l'ITU (che ha

solo centri regionali, con funzione tecnica, negli Stati-membri), ad oggi, hanno creato un proprio centro di eccellenza o formazione esclusivamente dedicato, a livello globale e a tutto tondo, alla cyber security. La strada da percorrere, dunque, è ancora lunga.

Note bibliografiche e sitografia

- Umberto Gori, Luigi Sergio Germani (a cura di): "Information Warfare – Le nuove minacce provenienti da cyberspazio alla sicurezza nazionale italiana", Franco Angeli, Milano 2011;
- Umberto Gori, Luigi Sergio Germani (a cura di): "Information Warfare 2011 – La sfida della cyberintelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale", Franco Angeli, Milano 2011;
- Umberto Gori, Serena Lisi (a cura di): "Information Warfare 2012 – Armi cibernetiche e processo decisionale", Franco Angeli, Milano 2012;
- Umberto Gori, Serena Lisi (a cura di): "Information Warfare 2013 – La protezione cibernetica delle infrastrutture critiche", Franco Angeli, Milano 2014;
- Tallinn Manual on International Law Applicable to Cyber Warfare (http://www.ccdcoe.org);
- "Working towards rules for governing cyber conflict";
  http://silendo.org/2011/02/04/il-cyber-spazio-e-le-convenzione-di-ginevra/
  http://vialardi.org/nastrazzuro/pdf/US-Russia.pdf
  http://italian.ruvr.ru/2011/02/06/43096774/
- http://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm;
- http://www.cybersquared.com/wp-content/uploads/downloads/2013/03/Medical-Industry-A-Cyber-Victim-Billions-Stolen-and-Lives-At-Risk.pdf;
- http://www.internationalpolicydigest.org/2014/02/26/the-wild-west-of-cyberwarfare/;
- http://www.wassenaar.org/introduction/howitworks.html
- *sdccoe.org*
- http://www.nist.gov/itl/csd/nccoe-022112.cfm
- www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml
- www.2centre.eu/
- www.cybercoe.army.mil

I Social Media, Cloud ed evoluzione da web 2.0 a web 4.0 – Opportunità e sfide per la sicurezza nazionale

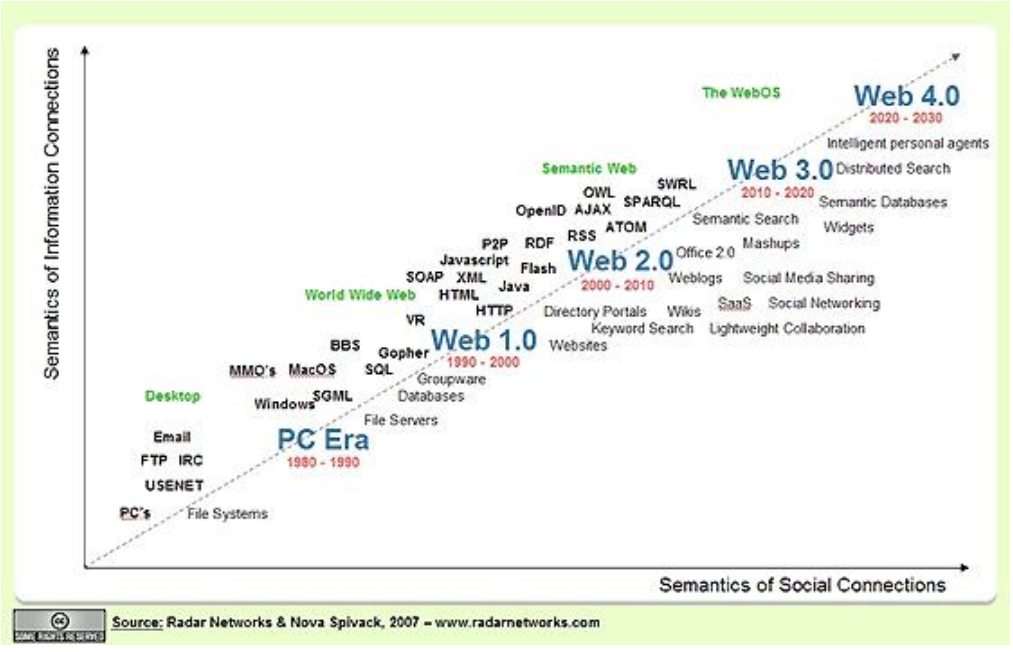
Luigi Martino
(CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, dell'Università di Firenze)

"Credo che alla fine del secolo l'uso delle parole e l'opinione delle persone di cultura saranno cambiate a tal punto che si potrà parlare di macchine pensanti senza aspettarsi di essere contraddetti".
Alan Turing

Secondo i coniugi Alvin e Heidi Toffler (futuristi americani), la storia dell'umanità va divisa in "ondate" e l'attuale "era dell'informazione" altro non è che il prodotto della "terza rivoluzione industriale". Passando dalla rivoluzione agricola alla rivoluzione industriale – scrivono i Toffler nel loro libro The Futur Shock (1) – si è giunti, ai nostri giorni, alla rivoluzione dell'informazione, appunto la "terza ondata". Le nuove scoperte tecnologiche, basate sull'utilizzo dell'informatica, hanno concesso l'opportunità agli individui di trasmettere le informazioni in tempo reale. Allo stesso tempo, le gerarchie burocratiche stato-centriche, investite da questa "tempesta di fuoco di mutamenti", perdono la loro egemonia soprattutto nell'ambito del dominio delle informazioni. Le radici dell'Information Revolution vanno fatte risalire a due distinti processi innovativi: la creazione della rete Arpanet, nata nel 1969 da un progetto congiunto sviluppato dall'agenzia del Pentagono DARPA con quattro università americane: Standford Research Institute, University of Utah, University Campus of Santa Barbara e University Campus of Los Angeles. Il secondo progetto pioneristico è legato alla creazione del World Wide Web (creato da Tim Berners-Lee a cavallo tra la fine degli anni '80 e i primi anni '90 nei laboratori del CERN di Ginevra). Arpanet, al contrario, è frutto di un progetto governativo che inizialmente aveva come ambito d'azione solo il dominio militare e successivamente divenne uno strumento civile. Viceversa, il CERN

il 23 agosto 1993 decise di rendere il World Wide Web dominio dell'umanità, rinunciando a qualsiasi diritto di proprietà intellettuale. Sono stati questi due processi, autonomi ma vincolati tra loro, che hanno dato vita a ciò che noi oggi chiamiamo Internet. Il Web, come vedremo nelle pagine successive, ha subito un enorme processo evolutivo. Infatti, si è passati dal Web 1.0 al Web 3.0 di oggi, con la prospettiva futuristica di giungere nei prossimi anni al Web 4.0.

L'immagine sottostante (ripresa dal sito lifeboat.com) spiega nel dettaglio le varie fasi che hanno interessato e che tuttora interessano l'evoluzione del World Wide Web.



I *social media*, come si può notare dalla lettura dell'immagine, fanno parte della tecnologia *Web 2.0*, la prima revisione ed evoluzione subita dal *World Wide Web*.

Se si prova a digitare su *google.it* la parola "*social media*", si ottengono circa *1.430.000.000* di risultati (dato aggiornato al 28 gennaio 2015). Secondo una definizione diffusa in ambito tecnico-informatico, per *social media* si intende: "qualsiasi servizio online attraverso il quale gli utenti possono creare e condividere una

varietà di contenuti" (2). In particolare, i *social media* vengono rappresentati come degli spazi adibiti per facilitare l'incontro tra le persone in modo "virtuale" e diretto. Sono inoltre utili per stabilire e proseguire lo scambio di comunicazioni tra individui e strumenti informatici. Questi "siti" permettono ai membri di fornire informazioni personali, condividere immagini e connettersi con altri utenti con interessi simili. In definitiva, si riesce tramite l'utilizzo dei *social media* "a propagare oltre il confine del reale la propria personalità". La possibilità di costituire degli spazi di incontro e discussione, dove è anche possibile *by-passare* la censura governativa, rende questi luoghi allo stesso tempo virtuali e virtuosi, al punto tale da costituire un utile forum adatto alla formazione dell'opinione pubblica del XXI secolo.

Come giustamente avverte Chris Hables Gray: "con l'era cibernetica si inaugura l'avvento di un nuovo tipo di cittadino, di un nuovo senso dell'umano", dove si assiste alla creazione del c.d. *cyborg citizen* che trova nello spazio cibernetico il suo ambiente naturale (3).

Contemporaneamente, come dimostrano anche gli ultimi avvenimenti internazionali, data la particolare conformazione del dominio cyber (ambiente anonimo e dinamico) nel quale operano i *social media*, questi strumenti si prestano anche ad azioni deleterie per la sicurezza nazionale. Ad esempio, negli ultimi anni si è accentuato sempre di più l'utilizzo dei *social media* da parte della criminalità e dei gruppi terroristici. Mentre la prima utilizza il *web* per fini puramente "economici" e "logistici" (per esempio per riciclare denaro di provenienza illecita, per cercare di eludere i classici sistemi di intercettazione etc.), i gruppi terroristici, sfruttando sempre di più le "maglie larghe" del *web*, riescono a utilizzare i nuovi mezzi di comunicazione come strumenti di propaganda a fini di reclutamento e proselitismo.

Proprio grazie al monitoraggio di *Second Life* (creato dalla società Linden Lab), il mondo virtuale dove l'utente crea il suo avatar simile al protagonista reale o del tutto inventato, il *Gchq*, l'agenzia di servizi segreti britannici per le telecomunicazioni, con l'"operazione Galizia" nel 2007 ha fermato un'organizzazione

criminale che trafficava dati di carte di credito servendosi degli avatar iscritti a *Second Life* (4). Sempre il servizio di intelligence britannico nel 2014 ha sottolineato come si stia diffondendo tra gli appartenenti allo Stato Islamico (noto in Italia come ISIS) sempre di più l'utilizzo di strumenti legati ai *social media* (o *network*) come WhatsApp e Facebook per inviare ordini logistici ai terroristi impegnati nei teatri di guerra (5).

Proprio questa consapevolezza che dal mondo virtuale si possano diffondere minacce alla sicurezza nazionale ha spinto i decisori politici americani a finanziare nel 2012 il programma *Reynad* (6). Il programma, alle dirette dipendenze dell'*Office of the Director of National Intelligence* (ODNI), ha come obiettivo la sorveglianza dei luoghi di socializzazione virtuali quali ad esempio *Second Life* e *World of Warcraft* (il più noto e popolato tra i giochi virtuali al mondo). Gli analisti di intelligence hanno il compito di utilizzare i metodi delle scienze sociali (quantitativi e qualitativi) "per predire le azioni portate avanti dagli avatar nel mondo virtuale, incrociando i dati con le caratteristiche delle persone reali che controllano i comportamenti degli stessi avatar". In altre parole, il programma *Reynad* è un raccoglitore di dati da cui poter tracciare dei profili standard e all'occorrenza, segnalare eventuali deviazioni dei c.d. *cyberborg*.

In questi casi, emerge sempre di più una dicotomia marcata tra la libertà degli utenti (libertà che sin dalle origini caratterizza il *Web*) e le necessarie contromisure adottate dagli Stati, per contrastare le minacce alla sicurezza nazionale che si propagano attraverso una dimensione ancora oggi *ungoverned*. In questo contesto agiscono i *social media* che, secondo la definizione data su *wikipedia* comprendono: forum di internet, blog, podcast, condivisione di file e messaggi. Esempi più comuni sono Facebook, Twitter, Linkedin, Blogger, Flickr, WordPress, Skype, YouTube, Google Chat. Tali strumenti, oltre ad avere le classiche caratteristiche di "catalizzatori", possiedono un'elevata capacità "virale" e di propagazione istantanea delle informazioni. In questo senso i *social media* possono essere definiti con il termine anglosassone "*mass self-communication*" (7) ovvero, la capacità

intrinseca dell'informazione inviata da un singolo individuo di raggiungere un pubblico di massa (capacità in passato detenuta solo dai mass media). Allo stesso tempo, l'informazione si avvale di un *feedback* (la risposta e la condivisione ricevuta dall'informazione) il quale, al di là dall'essere positivo o negativo, concede all'informazione la possibilità di entrare nel circuito mediatico-sociale attraverso un semplice "*like*" su Facebook, un "*twitt*" su Twitter o un video su Youtube. La condivisione non è certamente sinonimo di veridicità dell'informazione. Viceversa, nella quasi totalità dei casi l'attendibilità del contenuto non viene accertata. A tal proposito, si pensi ad esempio, alle ricadute negative che hanno le false notizie, catalizzate attraverso i *social media*, informazioni condivise per creare danni all'immagine di un potenziale avversario politico o un *competitor* finanziario o aziendale. Ancor più, si pensi ai sempre più diffusi casi di cyber-bullismo (termine utilizzato per descrivere le azioni di bullismo giovanile attraverso l'uso dei *social media*) che, nelle ipotesi estreme, hanno portato anche a casi di suicidi tra gli adolescenti colpiti. In questi casi emerge nitidamente il ruolo centrale ricoperto dai *social media* nelle interazioni umane, dove le informazioni non vengono per nulla regolate da un contraddittorio con la realtà dei fatti.

In definitiva, se il *Web 2.0* (attraverso anche i *social media*) ha favorito lo sviluppo delle relazioni orizzontali tra gli individui concedendo sempre di più la possibilità di espandere la rete della comunicazione e della condivisione delle informazioni indifferenti ai limiti dello spazio urbano e del tempo, contemporaneamente nasconde delle insidie per la sicurezza nazionale. L'attuale fase di evoluzione verso il *Web 3.0* ha favorito viceversa, un processo di verticalizzazione del *web*. In altre parole, le prime fasi della rivoluzione dell'informazione sono state interessate allo stesso tempo da un processo di "democratizzazione delle informazioni" e da un vero e proprio *data deluge,* un'esplosione di informazioni che ha dato vita a ciò che oggi definiamo con il termine *Big Data* (8). Il *Web 2.0* dunque, ha generato un *trade-off* tra informazioni e conoscenza e l'effetto di ciò è stato un processo produttivo continuo di informazioni e di dati, con la conseguenza che, pur essendoci

maggiori dati/informazioni, si è assistito ad una minore capacità di estrapolare notizie intese come "conoscenza specifica dei fatti".

Il *Web 3.0* intende correggere questo difetto imprevisto, attraverso la creazione di un *web* capace non solo di far interagire l'uomo e la macchina, ma di rendere lo stesso spazio virtuale *smart* (intelligente). Il primo passo di questa evoluzione 3.0 ha interessato il processo semantico dei dati trasmessi dagli utenti e dai sensori nel *web*. Gli smarphone, i tablet, così come le varie *App*, se da un lato facilitano l'utilizzo degli strumenti informatici perché li rendono sempre di più "intuitivi", dall'altro rivelano una mole di dati per i fornitori di servizi i quali, riescono a elaborarle e farle diventare notizie di valore soprattutto commerciale. Come spiegano i fautori del *web* di terza generazione, "il Web 3.0 sarà più connesso, aperto e intelligente, grazie alle tecnologie semantiche, ai database distribuiti, alle elaborazione del linguaggio naturale, all'apprendimento automatico".

Il *Web*, spazio dinamico e privo di limiti spazio-temporali, attraverso la tecnologia *cloud* assume l'aspetto ibrido di contenuto e contenitore trasformandosi in un *database* illimitato. Le caratteristiche principali del *Web 3.0* sono dunque legate alla sua capacità di fornire maggiori servizi "intelligenti" e corrispondenti alle esigenze dell'individuo (come ad esempio la possibilità di trovare i propri documenti in qualsiasi momento e di immagazzinarli in una "nuvola" sempre disponibile). Altro baluardo della terza rivoluzione del *web* sarà lo sviluppo dell'*Artificial Intelligence* (AI), capace di interagire *per l'uomo* con le macchine (nei casi in cui i *software* saranno chiamati ad assistere coloro che per problemi di salute non possono essere autosufficienti). Se il c.d. *cloud computing* fornisce una serie di vantaggi, inimmaginabili sino a pochi anni fa (si pensi ad esempio alla possibilità di costruire un archivio di documenti portatile senza doversi preoccupare del trasporto reale dei materiali), anche in questo caso alle innovazioni rivoluzionarie si affiancano dei rischi altrettanto marcati. Basti pensare ad esempio, che i documenti "collocati" sul *cloud* rispondono ad un servizio attivato sotto forma di architettura tipica di *client-server*. In altre parole, il servizio è offerto da un provider che detiene la proprietà

della struttura utilizzata per memorizzare i dati, la c.d. *Server Farm*.

Il data center utilizzato spesso ha sede in un Paese estero e risponde a regolamentazioni sulla *privacy* differenti rispetto all'ordinamento giuridico di riferimento del cliente detentore dei dati. In relazione all'*Artificial Intelligence* si prevedono scenari futuri alquanto innovativi ed inediti per le interazioni tra l'uomo e la macchina. Proprio in questo frangente, come dimostrano i vari progetti finanziati dalle grandi multinazionali, tra le quali Google, Microsoft e IBM, o dai centri di ricerca governativi come la Defense Advanced Research Projects Agency (DARPA) del Pentagono, si intravedono i vantaggi e i rischi dell'intelligenza artificiale. In particolare, si pensi al progetto *SyNAPSE* (Systems of Neuromorphic Adaptive Plastic Scalable Electronics) portato avanti dalla collaborazione tra DARPA e IBM che poco tempo fa ha svelato *TrueNorth*, il primo microchip in grado di imitare l'area destra e sinistra del cervello umano con l'obiettivo di far raggiungere alla macchina una propria capacità cognitiva. L'avvento dell'*Artificial Intelligence* e la diffusione dell'*Internet of Things* segneranno la futuristica affermazione del *Web 4.0*. A quel punto si passerà dalla primigenia idea di interazione (alla base del *World Wide Web*) alla nuova fase *dell'integrazione uomo-macchina*. In definitiva, i decisori politici e gli operatori preposti alla difesa della sicurezza nazionale, nel prossimo futuro, dovranno fare i conti con il concetto di responsabilità individuale delle azioni, nell'ottica in cui a commettere azioni illecite non saranno solo gli individui, ma anche gli automi.

Note

(1) Cfr. A. Toffler, *Lo choc del futuro*, Rizzoli Editore, Milano, 1971; Id., *The Politics of the Third Wave,* Andrew and McMeel, Atlanta, 1995; Id. *War and Anti-War: Survival at the Dawn of the 21st Century*, Little Brown and Company, Boston,1993. Per un'analisi dettagliata da un punto di vista filosofico sull'ampio concetto di *Information Age* si rinvia a L. Floridi, *La rivoluzione dell'informazione*, Codice edizioni, Torino, 2012. In questo saggio l'Autore per primo esprime l'ambiente nel quale si diffonde l'interazione tra individui e l'informazione, ovvero scrive che: "sotto molti profili non siamo entità isolate quanto piuttosto organismi informazionali interconnessi, o *inforg*, che condividono con agenti biologici e artefatti ingegnerizzati un ambiente globale costituito in ultima analisi dalle informazioni, l'*infosfera*" cit. p. 11.

(2) Cfr. A. M. Kaplan e M. Haenlein, *Users of the world, unite! The challenges and opportunities of Social Media*, Business Horizons, Volume 53, Issue 1, January–February 2010, pp. 59-68.

(3) Cfr. G. Hables Chris, *Cyborg Citizen. Politics in the PosthumanAge*, Routledge New York, 2001.

(4) Cfr. G. Pompili, *Tu giochi, io ti spio*, Il Foglio, 30 Gennaio 2014.

(5) Cfr. L. Martino, *Silicon Valley al servizio dei terroristi*, in Formiche.net, 05-11-2014.

(6) Office of the Director of National Intelligence, *Data Mining Report*, 15 February 2008, [Unclassified Document].

(7) Cfr. Appalayya M., Vani, H., Mutyalu N. M., *The Best Practices for Social Media, their Consumers, and Regulators*, in International Journal of Research in Computer Application and Management, Vol. 4, Issue No. 11 (November, 2014), p. 5-9.

(8) I Big Data sono porzioni di dati misurati in *petabyte*, *exabyte*, *zettabyte*, ovvero quantità gigantesche di dati che non possono essere memorizzati e gestiti dai *database* standard. Si pensi che la società informatica IBM ha dichiarato che: "Ogni giorno creiamo 2,5 quintilioni di byte di dati e il 90% dei dati è stato creato solo negli ultimi due anni. Questi dati vengono registrati ovunque: sensori per la raccolta di informazioni sul clima, post su siti di social media, video e immagini digitali, record delle transazioni di acquisto e segnali GPS dei cellulari, solo per fare qualche esempio. Questi tipi di dati vengono definiti big data" .

SEZIONE II
Lo spazio cibernetico e il diritto
La legislazione internazionale, europea e nazionale

Il confronto in atto sul controllo e sulle regole di gestione di internet

Costantino Moretti
(Analista indipendente)

Importanti tematiche legate alla gestione di internet sono affidate, oggi, ad un'organizzazione no-profit californiana, la *Internet Corporation for Assigned Names and Numbers* (ICANN) (1), sulla base di un Memorandum of Understanding stipulato nel 1998 tra la stessa ICANN e la *National Telecommunications and Information Administration* (NTIA), agenzia del Dipartimento del Commercio statunitense. Le decisioni dall'ICAAN sono assunte nel corso di riunioni nelle quali sono presenti, con pari diritti, i rappresentanti di tutte le categorie portatrici di valori ed interessi propri connessi con internet, secondo un modello partecipativo detto '*multistakeholder*'. Tuttavia, alcune attività permangono ancora in capo alla NTIA. Tra esse spicca il coordinamento nel sistema di assegnazione dei nomi ai dominii (*Domain Name System - DNS*).

A livello internazionale sin dal 1998 sono stati sollevati dubbi sulla validità di tale architettura amministrativa di internet e sono state avanzate proposte per sostituirla con una nuova impostazione, incidendo in particolare sul ruolo che il governo statunitense, unilateralmente, si era riservato nei confronti dell'ICANN.

Il confronto internazionale in corso in questi anni sulla *governace* di internet ancora non ha prodotto una posizione condivisa. Nel corso del *World Summit on Information Society* del 2005, organizzata dall'*International Telecommunication Union* (ITU) l'agenzia delle Nazioni Unite specializzata per le questioni che riguardano l'informazione e le tecnologie per la comunicazione, è stata adottata la c.d. Agenda di Tunisi (2). Al punto 34 dell'Agenda così testualmente è scritto: "A working definition of Internet

governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of Internet.".

Secondo alcuni studiosi la definizione di 'internet governance', riportata nell'Agenda di Tunisi, non si presta a rappresentare perfettamente il modello attuale e, quindi, hanno proposto delle differenti definizioni come, ad esempio, la seguente: "Internet governance is collective decisionmaking by owners, operators, developers, and users of the networks connected by Internet protocols to establish policies, rules, and dispute resolution procedures about technical standards, resources allocations, and/or the conduct of people engaged in global internetworking activities." (3).

Attualmente sono tre le posizioni che, a livello internazionale, godono di maggior seguito:

- la prima, propone la gestione di internet attraverso una struttura operante sul modello '*multi stakeholder*' similmente alle attuali modalità operative dell'ICANN;
- la seconda, propone il ricorso ad un modello di gestione di internet di tipo intergovernativo, con la creazione di un'apposita agenzia internazionale all'interno delle Nazioni Unite o con il trasferimento delle competenze all'ITU;
- la terza, partendo dall'assunto che le tematiche che riguardano la gestione di internet sono molto differenti tra loro, propone una *governance* a geometria variabile denominata *multi institutional*. Tale modello prevede la partecipazione degli *stakeholder* con un peso differente a seconda delle tematiche che di volta in volta vengono trattate (4).

Le differenze tra le citate posizioni ruotano, sostanzialmente, sulla funzione e, quindi, sul potere che i governi devono o non devono avere sulle tecnologie informatiche.

Dal 14 marzo di quest'anno, allorquando la NTIA ha comunicato la possibilità di cedere il proprio ruolo di coordinamento nel *Domain Name System – DNS* (5), non rinnovando il contratto che la lega all'ICANN in scadenza il 30 settembre 2015, il dibattito

sulle modalità di gestione della rete è diventato ancor più rovente, anche perché l'Agenzia governativa statunitense nel comunicato stampa, ha precisato che: "*NTIA will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution*".

Tra i contributi offerti al dibattito in corso, di particolare interesse è stato il discorso tenuto dal Presidente dell'Estonia Toomas Hendrik Ilves in occasione dell'apertura della 4ª conferenza annuale della *Freedom Online Coalition* (FOC) (6), svoltasi a Tallinn il 28 e il 29 aprile scorsi. Egli, grazie alla profonda competenza nel settore informatico (7), non ha rivolto ai partecipanti alla Conferenza un semplice saluto di circostanza ma ha illustrato la propria visione filosofica del concetto di libertà e di democrazia nel ciberspazio.

Oggi il mondo di internet, secondo il Presidente estone, è assimilabile allo 'stato di natura' tratteggiato dal filosofo inglese Thomas Hobbes, ovvero uno stato di belligeranza di tutti contro tutti. Se si seguisse fino in fondo l'impostazione hobbesiana, il passaggio dallo 'stato di natura' a quello 'civile' si avrebbe con la stipula di un contratto con il quale gli uomini, a fronte di una rinuncia autonoma ai loro diritti naturali, si sottomettono alla volontà di un potere superiore (persona fisica o persona giuridica) e si obbligano, nel contempo, a non opporgli resistenza. Ilves, conscio che dai tempi di Hobbes il concetto di democrazia e l'inquadramento dei rapporti tra cittadino e Autorità statale hanno subìto dei mutamenti significativi, auspica un nuovo contratto tra cittadini e governi sulla falsariga di quanto immaginato dal filosofo John Locke. Quest'ultimo, partendo da presupposti simili a quelli di Hobbes, riteneva necessario un potere superiore che però non annullasse i diritti che l'uomo aveva nello 'stato di natura'; tranne, naturalmente, il diritto di farsi giustizia da solo.

L'aspetto più interessante del discorso di Ilves è il passaggio ove egli ha paventato la possibilità di una "westphalizzazione della rete".

A questo punto si pone la domanda: qual è la connessione tra la Pace di Westphalia e internet?

Il termine "westphalizzazione della rete" è stato utilizzato per la prima volta nel 2012, nel corso di un seminario a latere del *World Summit on the Information Society* del 2012 (8) organizzato dall'ITU, per descrivere il fatto che l'ordine sociale, economico e politico del tradizionale sistema dei confini nazionali, derivante dalla Pace di Westphalia, non fosse applicabile al mondo di internet a causa della propria essenza virtuale e trans-nazionale. Ilves nel suo discorso ha voluto, invece, lanciare un monito sul rischio che internet possa essere 'westphalizzato', che vengano tracciati dei confini alla rete. Egli ha legato tale rischio all'iniziativa di alcuni paesi, da lui definiti autoritari, i quali vorrebbero sostituire l'attuale modello di governo di internet, fondato sul sistema '*multi-stakeholder*', con un sistema 'intergovernativo'.

I paesi che propugnano il ricorso ad una *governance* di internet sul modello 'intergovernativo', poggiano le loro motivazioni principalmente sul fatto che non vi sia una regolamentazione della rete condivisa internazionalmente e sulla necessità di prevenire e reprimere i reati commessi sulla e/o per mezzo della rete, attività quest'ultima di competenza esclusiva dei governi.

Ilves afferma che tali motivazioni, seppur pienamente condivisibili, nascondono in realtà la volontà di controllare e regolare il ciberspazio in modo da limitare anche la libera circolazione delle informazioni e delle idee. Egli aggiunge che, qualora si adottasse il sistema 'intergovernativo', ci sarebbe il rischio di arrivare ad applicare ad internet il principio giuridico del 'Cuius regio, eius rete', versione contemporanea del '*Cuius regio, eius religio*', stabilito con il Trattato di pace di Augusta del 1555 (9).

Secondo il Presidente estone, questa contrapposizione potrebbe dar luogo ad uno scontro fra civiltà. A fronteggiarsi sarebbero: da una parte quelle nazioni che vogliono sottoporre a censura e a restrizione internet e, dall'altra, le nazioni democratiche che reclamano una normativa universale che garantisca la libertà d'espressione e di circolazione delle idee. Da una parte gli stati che vogliono che internet venga regolato dai governi e dall'altra gli stati che auspicano che internet continui ad essere regolato da *relevant stakeholders*.

Per mostrare il rischio di ingerenze governative liberticide nella rete, qualora internet venisse regolato secondo il principio 'Cuius regio, eius rete', Ilves ha citato le iniziative poste in essere in Egitto per fronteggiare le dimostrazioni di massa del gennaio 2011 che sfociarono nella destituzione di Mubarak. In tale occasione le allora autorità egiziane arrivarono ad impedire alla popolazione, per ben cinque giorni, l'uso della rete internet e della messaggistica sui cellulari (10).

Per connessione d'argomento, non si può non fare cenno anche ad un altro principio informatore di internet, da alcuni anni al centro di serrati dibattiti i cui esiti possono avere ripercussioni sulla privacy degli utenti di internet. Il principio della neutralità della rete o, con termine anglosassone, quello della *net neutrality*.

Una fra le più chiare ed esaustive definizioni di neutralità della rete è quella riportata nella bozza della Dichiarazione dei diritti in internet (11), testo elaborato dalla Commissione per i diritti e i doveri in internet costituita presso la nostra Camera dei Deputati. L'articolo 3, titolato Neutralità della rete, così recita: "Ogni persona ha il diritto che i dati che trasmette e riceve in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuti dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone. La neutralità della Rete, fissa e mobile, e il diritto di accesso sono condizioni necessarie per l'effettività dei diritti fondamentali della persona. Garantiscono il mantenimento della capacità generativa di Internet anche in riferimento alla produzione di innovazione. Assicurano ai messaggi e alle loro applicazioni di viaggiare online senza discriminazioni per i loro contenuti e per le loro funzioni.".

Il dibattito sulla neutralità della rete è anche molto vivace oltre Atlantico tanto che sulla questione, il 10 novembre 2014, è intervenuto anche il presidente Barak Obama (12). Egli, con un discorso dai toni vibranti, si è rivolto alla *Federal Communications Commission* (13) auspicando che la *net neutrality* venga protetta con un regolamento quanto più vincolante possibile.

Secondo Obama, il regolamento dovrebbe contenere quattro principi, affinché i provider trattino tutti gli utenti di internet nella stessa maniera. Essi sono:

NO BLOCKING. Se un utente chiede l'accesso ad un sito o ad un servizio internet e il contenuto è legale, non deve essere permesso al provider di bloccarlo. Con l'inserimento di tale divieto si avrebbe, secondo Obama, un mercato totalmente libero e competitivo e non si avvantaggerebbero le società affiliate o 'vicine' agli *internet service provider* (ISP).

NO THROTTLING. Il divieto per gli ISP di velocizzare o di rallentare intenzionalmente alcuni contenuti in base al tipo di servizio o alle preferenze degli ISP stesso; ovvero in base ai loro interessi.

INCREASED TRASPARENCY. Allargare lo spazio di applicazione della regolamentazione attualmente valida solo per il cosiddetto 'ultimo miglio'.

NO PAID PRIORITIZATION. Vietare la possibilità per gli ISP d'instradare su connessioni più lente dei servizi poiché non sono state pagate a loro delle commissioni.

Sulla *net neutrality*, quindi sulla regolamentazione del traffico dei contenuti, è in corso una partita dai risvolti economici tra le tradizionali imprese di telecomunicazioni e i cosiddetti operatori *over the top* (OTT) (14).

Questi ultimi stanno assumendo un ruolo sempre maggiore nell'offerta di contenuti che transitano su internet, erodendo quote di mercato alle grandi imprese di telecomunicazioni, le quali hanno affrontato e continuano ad affrontare grandi investimenti per la realizzazione e la manutenzione delle infrastrutture e sulle quali si muovono poi trasversalmente gli stessi OTT, senza avere prospettive certe di adeguata remunerazione.

La distanza tra le parti è ancora molto ampia anche dal punto di vista filosofico; come ad esempio riguardo la pratica denominata *deep packet inspection*. Con tale termine si designa il controllo dei dati presenti nei pacchetti, effettuato dagli operatori/ISP, per verificare che i contenuti presenti nel singolo pacchetto siano conformi a determinati parametri da esso stesso stabilite. Nel caso il

pacchetto o il suo contenuto non rientri in detti parametri, esso può essere scartato, reindirizzato o ne possono essere modificate la priorità o la velocità. Secondo alcuni operatori/ISP, la *deep packet inspection* è una pratica utile per ragioni di sicurezza in quanto permetterebbe di bloccare la diffusione di *malware* e di proteggere gli utenti; i fautori della piena *net neutrality*, invece, vedono tale pratica come potenzialmente lesiva della *privacy* degli utenti.

Nell'attuale contesto storico-sociale, caratterizzato da uno spiccato ruolo svolto dall'informazione, le modalità di governo della rete internet necessitano sicuramente di una revisione. Ad oggi, come visto, la comunità internazionale non ha trovato una posizione univoca. Tenuto conto che gli esiti delle discussioni sul governo della rete avranno un impatto immediato sulla vita dei cittadini e delle imprese è di vitale importanza che l'Italia, con la propria componente pubblica e privata, in linea con l'Unione europea, continui ad essere presente e a non far mancare la propria voce nei vari fori internazionali. La posizione dell'Unione europea è sempre stata chiara e più volte ribadita in diversi contesti internazionali come, ad esempio, nel corso del *World Summit on the Information Society* organizzato dall'ITU a Ginevra dal 10 al 13 giugno scorsi dall'allora Commissario UE Neelie Kroes, responsabile per l'Agenda digitale (15).

Ma, sul tema del governo della rete, fondamentale è stato il lavoro svolto dall'Italia nel corso dell'attuale semestre di presidenza del Consiglio dell'Unione europea che ha portato, nella riunione in tema di trasporti, telecomunicazioni ed energia del 27 novembre 2014 presieduta dal Sottosegretario Antonello Giacomelli, all'adozione di una conclusione comune che impegna formalmente l'UE a supportare il modello multi-stakeholder in quanto lo stesso è quello che permette meglio di tutelare i diritti umani e i valori democratici degli utenti della rete.

Condividendo l'allarme lanciato dal Presidente dell'Estonia Toomas Hendrik Ilves, l'auspicio è che quando la gestione di internet sarà cristallizzata in una normativa internazionale, il nuovo impianto non metta in pericolo i diritti fondamentali degli utenti internet, tra i quali: la libertà di pensiero, la tutela della riservatezza, la protezione

dei dati personali, la sicurezza delle transazioni finanziarie e, non ultimo, il diritto di libero accesso al web.

Note

(1) Sul ruolo e sul modello funzionale dell'ICANN vedasi: http://archive.icann.org/tr/italian.html
(2) L'Agenda di Tunisi è reperibile sulla seguente pagina web: http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc
(3) M. Milton, J. Mathiason e H. Klein 'The Internet and Global Governance: Principles and Norms for a New Regime' in: Global Governance, vol. 13 (April-June 2007), pag. 245.
(4) Per maggiori informazioni riguardo l'operatività del modello multi institutional si rimanda all'articolo apparso sul numero 1/2013 di "Notiziario Tecnico" di Telecom Italia, a firma L. M. Pupillo dal titolo "Verso una nuova governance globale di internet" consultabile su: http://www.telecomitalia.com/content/dam/telecomitalia/it/archivio/documenti/Innovazione/NotiziarioTecnico/2013/n1-2013/NT1-8-2013.pdf
(5) Il comunicato stampa ufficiale della NTIA del 14 marzo 2014 è reperibile sulla seguente pagina web: http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions
(6) La FOC, lanciata nel dicembre 2011 nel corso di una conferenza internazionale organizzata a L'Aja dal Ministero degli affari esteri dei Paesi Bassi, è un foro di dialogo aperto che attualmente riunisce 23 Paesi, con lo scopo di valutare i modelli più rispondenti ad assicurare la libertà di espressione su internet nell'assunto che tale libertà possa contribuire alla promozione dello sviluppo sociale, culturale ed economico nel mondo.
(7) Toomas Hendrik Ilves è anche presidente di un Panel di esperti sul futuro della cooperazione globale su internet, costituito nel novembre 2013, con segretariato permanente presso l'ICANN. Il vice presidente del Panel è Vint Cerf, annoverato tra i fondatori di internet. Nel Panel, l'unico italiano presente è Francesco Caio, attuale presidente di Poste Italiane.
(8) Vds: http://groups.itu.int/LinkClick.aspx?fileticket=3T8l-8df8yw%3D&tabid=2103
(9) La Pace di Augusta, tra l'imperatore Carlo V e i principi tedeschi, sancì il diritto per quest'ultimi di scegliersi liberamente la confessione religiosa con il conseguente obbligo, per i loro sudditi, di abbracciare la medesima religione.
(10) Per una più attenta disamina degli avvenimenti egiziani si rimanda all'articolo del The New York Times del 15.02.2011 a firma J. Glanz e J. Markoff dal titolo: "Egypt leaders found 'off' switch for internet",

consultabile su: http://www.nytimes.com/2011/02/16/technology/16internet.html?_r=0

(11) La bozza della Dichiarazione dei diritti in Internet elaborata dalla Commissione di studio istituita presso la Camera dei deputati è reperibile sulla seguente pagina web: http://www.camera.it/application/xmanager/projects/leg17/attachments/upload_file/upload_files/000/000/187/dichiarazione_dei_diritti_internet_pubblicata.pdf

(12) Il discorso di Barak Obama è reperibile sulla seguente pagina web: http://www.whitehouse.gov/the-press-office/2014/11/10/statement-president-net-neutrality

(13) La Federal Communications Commission è l'agenzia governativa indipendente, vigilata dal Congresso, che sovrintende alle questioni relative alle telecomunicazioni. Ha potere anche regolamentare secondo il procedimento chiamato 'notice and comment'. Per maggiori informazioni riguardo la Commissione, si rimanda alla seguente pagina web: http://www.fcc.gov/what-we-do

(14) Gli operatori over the top sono quei soggetti che offrono servizi su internet e che sono soggetti terzi e indipendenti rispetto agli ISP, quali ad esempio: YouTube, Apple, Google, Facebook, ecc.

(15) Il discorso completo è consultabile sulla seguente pagina web: http://europa.eu/rapid/press-release_SPEECH-14-447_en.htm

O.S.C.E.
Sicurezza Cibernetica, Sicurezza delle Tecnologie Informatiche e di Comunicazione (TIC): costruire la Fiducia

Lamberto Zannier
(Ambasciatore Segretario Generale Organizzazione per la Sicurezza e la Cooperazione in Europa - OSCE)

Con l'adozione di misure volte a rafforzare la fiducia e ridurre il rischio di un conflitto derivante dall'uso delle tecnologie informatiche e di comunicazione (TIC), i paesi OSCE hanno stabilito un importante precedente.

Le infrastrutture che vanno sotto il nome di "Tecnologie Informatiche e di Comunicazione (TIC)" – le nostre linee telefoniche, le trasmissioni via cavo, le connessioni Internet, la "nuvola informatica" – sono il nuovo tessuto che ci unisce. Un tempo ci saremmo ritrovati nella stessa stanza per conversare, o avremmo inviato i nostri messaggi per lettera, via terra, mare o cielo. Nel mondo di oggi, queste interazioni sempre più spesso avvengono elettronicamente. Lo spazio cibernetico è diventato la scena su cui ormai si dispiegano le nostre vicende umane.

Il risultato di tutto ciò è chiaro: un attacco contro le nostre reti informatiche è ora un affare molto più personale. Quale che sia il luogo esatto in cui ci troviamo, si tratta di una minaccia che riguarda tutti, e una sfida che i governi non possono che affrontare, nessuno escluso. Le tecnologie informatiche e di comunicazione hanno il potere di unirci nella soluzione di un problema comune; al contempo hanno anche il potenziale di produrre profonde divisioni tra noi.

Possiamo dunque fidarci l'uno dell'altro? Abbiamo davvero altra scelta?

Gli attacchi cibernetici sono l'incarnazione perfetta delle sfide di sicurezza del ventunesimo secolo: globali nella loro natura, difficilmente rintracciabili, particolarmente facili da sconfessare, e spesso perpetuate da attori che potrebbero essere basati ovunque e

assumere le forme le più diverse, da un pirata informatico isolato a un'organizzazione vera e propria.

Forse ancora più rilevante è che le contromisure adottabili possono a loro volta produrre effetti potenzialmente destabilizzanti sulla sicurezza e la pace internazionali. A seconda del grado di intrusione in un network di un altro paese, esse possono infatti essere percepite come aggressive da parte di un altro Stato.

Ed è proprio qui che le misure volte a creare la fiducia ("confidence building measures") trovano la loro ragion d'essere.

Per i padri fondatori dell'OSCE – i leaders che organizzarono la prima Conferenza per la Sicurezza e la Cooperazione in Europea quaranta anni orsono – le confidence building measures rappresentarono un'innovazione volta a ridurre il rischio di guerra nucleare. Ora esse appaiono come il modo più efficace per affrontare problemi che sarebbero apparsi come pura fantascienza in quegli anni.

Di fatto queste misure contribuiscono ad allentare la tensione, consentendo agli stati di aprirsi gradualmente l'uno all'altro, iniziando a condividere informazioni sensibili e individuando problemi comuni che richiedono soluzioni comuni. Nel corso degli anni, l'OSCE ha accumulato un ricco bagaglio di esperienza in materia, e nell'aprile 2012 i paesi OSCE hanno deciso di fare tesoro di questa esperienza e applicarla alla minaccia della sicurezza cibernetica.

Decisi a intraprendere un viaggio ambizioso alla ricerca di strumenti per prevenire gli errori di percezione e ridurre il rischio che un attacco cibernetico possa sfociare in un conflitto armato vero e proprio, i paesi OSCE si sono impegnati in un negoziato culminato l'anno scorso nell'adozione di un accordo che fissa una prima lista di undici misure comuni.

Concentrandosi sul principio della trasparenza, queste misure rappresentano un significativo passo in avanti e costituiscono certamente "una prima" per l'area OSCE. Esse includono norme che dovranno disciplinare la condivisione di informazioni a livello dei governi e di esperti. All'OSCE si attribuisce la funzione di piattaforma per lo scambio di buone prassi. Preso atto dell'esistenza di molteplici

fori di discussione sulla sicurezza cibernetica, le misure adottate dai paesi OSCE intendono inserirsi in altri processi regionali e internazionali.

La maggior parte di queste misure prevede un'attuazione su base volontaria. Questo riflette il principio per cui la chiave di volta consiste nel cominciare a condividere ciò che è meno controverso per poi procedere gradualmente verso accordi più complessivi e stringenti, contestualmente al rafforzamento del livello di fiducia. Delle undici misure già adottate, quella con maggiore potenziale è probabilmente quella che prevede consultazioni per evitare errori di percezione. La difficoltà di individuare l'attore di un attacco cibernetico può creare il rischio che il sospetto ricada su di un paese confinante con cui i rapporti con il Paese vittima dell'attacco sono già logori. Il ricorso a consultazioni preliminari può dunque prevenire il rischio che una falsa attribuzione porti a tensioni o a un conflitto vero e proprio.

Un anno dopo l'adozione del primo insieme di misure, i paesi OSCE hanno completato il primo giro di scambio di informazioni. Senza dubbio sono stati raggiunti risultati importanti nonostante persistano sfide significative nello spazio OSCE – il che non fa che sottolineare l'importanza di tali misure. Oltre venti Stati hanno scambiato le proprie percezioni circa le minacce cibernetiche a livello nazionale e internazionale. Circa trenta Stati hanno deciso di discutere le rispettive strategie di sicurezza cibernetica. Diciassette hanno condiviso informazioni circa le proprie terminologie nazionali in materia e ventitré hanno fornito i recapiti dei loro focal point a livello nazionale.

Il 7 novembre 2014, la Presidenza svizzera dell'OSCE ha organizzato a Vienna una conferenza internazionale per fare il punto sull'attuazione delle norme esistenti e discutere possibili ulteriori misure.

Essenzialmente, le misure iniziali sono una chiara espressione della volontà degli stati OSCE – e rappresentano un invito ad "aprire le danze". Quando prevale un clima di insicurezza, il primo passo è generalmente il più difficile da fare. Dopodiché si tratta di conoscersi meglio e trovare un ritmo comune.

Per il futuro, mi attendo che gli stati OSCE si mostrino aperti a valutare misure ulteriori per ridurre in modo ancora più stringente gli errori di percezione e i rischi di escalation e conflitto. Ma la rapidità nell'attuazione e nell'individuazione di nuove misure dipenderanno come sempre dalla volontà politica degli Stati.

NOTA INFORMATIVA

Le misure in breve:

1. Gli Stati partecipanti forniranno volontariamente i loro pareri nazionali su diversi aspetti delle minacce nazionali e transnazionali alle TIC e all'uso delle stesse (…)
2. Gli Stati partecipanti faciliteranno volontariamente la cooperazione tra gli organismi nazionali competenti e lo scambio di informazioni in relazione alla sicurezza nell'uso delle TIC e del loro uso.
3. Gli Stati partecipanti terranno consultazioni su base volontaria e a livello adeguato al fine di ridurre i rischi di percezione errata e la possibile insorgenza di tensioni politiche o militari o conflitti che possono derivare dall'uso delle TIC, e di proteggere infrastrutture TIC nazionali e internazionali sensibili, compresa la loro integrità.
4. Gli Stati partecipanti condivideranno volontariamente informazioni sulle misure adottate per garantire una rete Internet aperta, interoperabile, sicura e affidabile.
5. Gli Stati partecipanti utilizzeranno l'OSCE come piattaforma per il dialogo, lo scambio di buone prassi, la sensibilizzazione e l'informazione sul rafforzamento delle capacità in materia di sicurezza delle TIC e del loro uso (…)
6. Gli Stati partecipanti sono incoraggiati a dotarsi di una legislazione nazionale moderna ed efficace per favorire la cooperazione bilaterale su base volontaria e lo scambio efficace e tempestivo di informazioni tra autorità competenti degli Stati partecipanti, comprese le agenzie preposte all'applicazione della

legge, al fine di contrastare il terrorismo o l'uso criminale delle TIC (…)

7. Gli Stati partecipanti condivideranno volontariamente informazioni sulla loro organizzazione, sulle strategie, le politiche e i programmi nazionali, nonché sulla cooperazione tra il settore pubblico e quello privato, rilevanti per la sicurezza delle TIC e del loro uso, nella misura da stabilirsi dalle parti che le forniscono.
8. Gli Stati partecipanti nomineranno un punto di contatto per facilitare le pertinenti comunicazioni e il dialogo sulla sicurezza delle TIC e del loro uso (…)
9. Al fine di ridurre il rischio di equivoci in assenza di una terminologia convenzionale e promuovere un dialogo continuo, gli Stati partecipanti, come primo passo, forniranno volontariamente un elenco nazionale di termini relativi alla sicurezza delle TIC e al loro uso accompagnato dalla spiegazione o dalla definizione di ciascun termine (…)
10. Gli Stati partecipanti scambieranno volontariamente le loro vedute avvalendosi delle piattaforme e dei meccanismi dell'OSCE, compresa la Rete di Comunicazioni dell'OSCE, gestita dal Centro per la prevenzione dei conflitti del Segretariato dell'OSCE, previa pertinente decisione dell'OSCE, al fine di facilitare le comunicazioni riguardanti le CBM.
11. Gli Stati partecipanti, a livello di esperti nazionali designati, si riuniranno almeno tre volte l'anno (…) al fine di discutere le informazioni scambiate ed esaminare sviluppi adeguati delle CBM

Questo articolo è stato originariamente pubblicato per Security Community:
The OSCE Magazine, numero 2, 2014
www.osce.org/magazine

Il Garante Europeo per la protezione dei dati

Pier Vittorio Romano
(Direttore responsabile ed editoriale di Informazioni della Difesa)

La figura del Garante europeo della protezione dei dati (GEPD) è stata istituita nel 2001 come un'Autorità di sorveglianza indipendente. Suo compito è quello di garantire il rispetto del diritto alla vita privata nel trattamento dei dati personali da parte delle istituzioni e degli organi dell'Unione Europea.

Il 4 dicembre 2014 sono stati nominati, per un quinquennio, Garante europeo della protezione dei dati (GEPD) e Garante aggiunto con Decisione Comune del Parlamento europeo e del Consiglio, rispettivamente Giovanni Buttarelli e Wojciech Wiewiórowski. I loro compiti e poteri e l'indipendenza dell'autorità di sorveglianza sono contemplati nel Regolamento (CE) n. 45/2001 pubblicato nella Gazzetta Ufficiale, Legge n. 8 del 12.1.2001.

La protezione dei dati personali è un diritto fondamentale del cittadino europeo ed è strettamente legato ad un altro diritto fondamentale: la privacy.

Possiamo far risalire al 1950, con l'adozione della "Convenzione Europea dei diritti dell'uomo" nell'ambito del "Consiglio d'Europa", la prima forma di tutela e rispetto per la vita privata. L'esercizio del diritto alla privacy si esercita nel regolamentare i poteri pubblici al fine di rendere meno invasive possibili le misure da adottare contemperandole in ragione delle finalità da perseguire.

È possibile far risalire al 1980 il periodo in cui il diritto alla protezione dei dati cominciava ad essere tutelato e ciò in ragione dello sviluppo tecnologico che, in quegli anni, iniziava ad interessare il settore della telematica.

Il Garante Europeo per la Protezione dei Dati – GEPD - ha come scopo principale la vigilanza sul rispetto della vita privata delle persone fisiche identificabili attraverso la regolamentazione di tutti gli aspetti relativi alla gestione dei dati che le Istituzioni e gli Organi dell'Unione Europea hanno necessità di "trattare".

Per "trattamento" si intendono tutte quelle attività volte alla raccolta, registrazione, conservazione, reperimento ai fini di

consultazione, comunicazione a soggetti terzi, blocco, cancellazione e distruzione dei dati appartenenti alla persona fisica identificabile.

Il Regolamento (CE) n. 45/2001, nel cui ambito il GEPD agisce, prevede una serie di compiti e poteri che distinguono i suoi tre ruoli principali: controllo, consulenza e cooperazione. Tali ruoli fungono tuttora da piattaforme strategiche per le attività del Garante e si riflettono sul mandato della sua missione.

In particolare il GEPD esplica la sua attività di controllo sia per garantire che le istituzioni e gli organismi dell'Unione Europea osservino le garanzie giuridiche esistenti quando procedono al trattamento di dati personali, sia per vigilare sulle nuove tecnologie che possono influire sulla protezione dei dati personali.

Altro compito del Garante è quello di fornire consulenza alle Istituzioni e agli organismi dell'Unione Europea su tutte le tematiche pertinenti, in particolare sulle proposte di legislazione europea che incidono sulla protezione dei dati personali.

A livello di coordinazione il GEPD coopera, inoltre, con le autorità nazionali di controllo e con altri organi pertinenti al fine di rendere più coerente la protezione dei dati personali. Interviene, inoktre, dinanzi alla Corte di Giustizia dell'Unione Europea per fornire consulenza sull'interpretazione della legge in materia di protezione dei dati personali.

Il GEPD ha elaborato un documento strategico 2013-2014, unitamente al suo regolamento interno e al piano di gestione annuale, al cui interno sono state fornite indicazioni preziose, articolando la visione e la metodologia necessarie per migliorare la sua capacità di lavorare in modo efficace in un clima di austerità.

L'Autorità ha ormai raggiunto la piena maturità, con obiettivi e indicatori di risultati chiari. Nell'ambito del controllo delle istituzioni e degli organismi dell'Unione europea, in relazione al trattamento dei dati personali, il GEPD ha interagito con numerosi responsabili della protezione dei dati appartenenti a organismi e istituzioni di diversi tipi, intrattenendo un numero di relazioni senza precedenti. Inoltre, ha portato a termine una serie di indagini che dimostrano come la maggior parte delle istituzioni e degli organismi dell'Unione europea, incluse varie agenzie, abbiano compiuto buoni

progressi in materia di conformità al regolamento sulla protezione dei dati, sebbene ce ne siano ancora alcuni che dovrebbero profondere maggiore impegno.

Nel settore della consultazione riguardante nuove misure legislative, la revisione del quadro giuridico dell'Unione, la protezione dei dati è rimasta al primo posto dell'agenda.

Tra i temi significativi del 2013 si segnalano l'agenda digitale e i rischi che le nuove tecnologie comportano. Tuttavia, anche l'attuazione del programma di Stoccolma in materia di libertà, sicurezza e giustizia e le questioni relative al mercato interno, come ad esempio la riforma del settore finanziario, e la sanità pubblica hanno inciso sulla protezione dei dati dei consumatori. Inoltre il GEPD ha potenziato la cooperazione su larga scala con le altre autorità di controllo, in particolare per quanto riguarda i sistemi relativi alla tecnologia dell'informazione (IT).

Nonostante i vincoli di bilancio, il 2013 ha visto un aumento del numero delle notifiche di controlli preventivi ed anche un aumento dei pareri derivanti dalle numerose notifiche pervenute. Allo stesso tempo il GEPD ha continuato a dar corso alle raccomandazioni formulate nei suoi pareri sui controlli preventivi già emessi ed è stato in grado di chiudere un numero considerevoli di casi.

Il GEPD, inoltre, nell'ambito della cultura della protezione dei dati al fine di garantire che le istituzioni europee siano consapevoli dei propri obblighi e della propria responsabilità, ha continuato a fornire orientamenti e formazione ai responsabili del trattamento dei dati, ai responsabili della protezione dei dati (RPD) e ai coordinatori per la protezione dei dati (CPD).

Tale attività è stata svolta prevalentemente sotto forma di orientamenti in materia di appalti pubblici, sovvenzioni ed esperti esterni, mediante una formazione di base per i nuovi RPD sulla procedura di controllo preventivo ed una formazione specifica. Le iniziative svolte dal GEPD finalizzate alla sensibilizzazione delle istituzioni e degli organismi dell'Unione Europea si sono realizzate attraverso workshop per responsabili del trattamento dei dati presso la Fondazione Europea per la Formazione Professionale (ETF) e l'Agenzia europea per la difesa (AED) e workshop mirati al campo

della comunicazione elettronica, sull'uso di dispositivi mobili sul luogo di lavoro e dei siti internet gestiti dalle istituzioni e dagli organismi dell'Unione Europea.

Riguardo l'attività di monitoraggio e politiche, nel 2013 il GEPD ha adottato la sua politica di ispezioni definendo gli elementi principali per la sua procedura ispettiva, fornendo orientamenti e garantendo la massima trasparenza a tutte le parti interessate. Sulla base dell'esperienza maturata dalle ispezioni precedenti è stato adottato un manuale interno per il personale del GEPD impegnato nelle ispezioni. L'attività consultiva del GEPD in ordine alle proposte legislative dell'Unione Europea e ai relativi documenti è aumentata con gli anni, anche se nel 2013 vi è stato un leggero calo - 20 pareri legislativi, 13 serie di osservazioni formali nonché 33 consulenze informali alla Commissione e altre istituzioni - dovuto ad un impegno delle proprie risorse sulle priorità strategiche per la riforma del quadro giuridico sulla protezione dei dati.

In ordine all'Agenda digitale e tecnologia, il GEPD ha affrontato più volte la questione dell'agenda digitale e di Internet, per esempio nel parere sulla comunicazione della Commissione "Agenda digitale per l'Europa - Le tecnologie digitali come motore della crescita europea", nel parere sul mercato unico europeo delle comunicazioni elettroniche e nel parere sul libro verde "Prepararsi a un mondo audiovisivo della piena convergenza: crescita, creazione e valori".

Per quanto riguarda lo spazio di libertà, sicurezza e giustizia, il GEPD ha pubblicato pareri sull'Europol, sulla strategia dell'Unione Europea per la cyber sicurezza e sulle frontiere intelligenti nonché relativamente all'accordo UE - Canada relativo ai dati delle pratiche passeggeri (Passenger Name Record, PNR) e sul modello europeo di scambio delle informazioni.

Nel settore della cooperazione con le autorità per la protezione dei dati, il GEPD ha contribuito attivamente all'attività del Gruppo di lavoro costituito ex Articolo 29 della direttiva 95/46, organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD, nonché da un rappresentante della

Commissione, in particolare, in qualità di relatore e correlatore, per la redazione di pareri.

A livello di controllo coordinato, nel 2013 il GEPD ha provveduto al segretariato per il nuovo gruppo di coordinamento della supervisione del SIS II ed ha continuato a presiedere i gruppi di coordinamento della supervisione di EURODAC, VIS e SID.

I cambiamenti verificatisi nell'ambito del controllo coordinato hanno portato con sé alcune sfide. Il nuovo regolamento EURODAC conteneva importanti modifiche, quali il possibile accesso ai dati di EURODAC da parte delle autorità di contrasto e, nel frattempo, il SIS II è divenuto operativo. Al fine di ridurre gli oneri finanziari, logistici ed amministrativi, il GEPD ha organizzato riunioni a catena tra i gruppi di coordinamento, puntando a garantire politiche di controllo coerenti e orizzontali, ove possibile, in materia di sistemi IT su larga scala.

Nel 2014 il modello dei gruppi di controllo coordinato si è espanso, comprendendo un nuovo gruppo di coordinamento della supervisione per il sistema d'Informazione del Mercato Interno (IMI). Il Garante ha consultato le autorità nazionali per la protezione dei dati e la Commissione per raccogliere notizie sullo status e sugli sviluppi del regolamento IMI.

Per quanto riguarda la politica in materia di IT (tecnologia dell'informazione), il GEPD ha contribuito alla redazione di diversi pareri riguardanti proposte della Commissione che sono d'importanza strategica per il futuro della società digitale in Europa.

Grazie alla sua competenza in materia di tecnologia dell'informazione, il GEPD ha condotto una visita presso l'Agenzia europea dei sistemi di informazione su vasta scala, nel contesto della migrazione al SIS II.

Nel settore della comunicazione il GEPD ha aumentato la propria visibilità a livello istituzionale mediante lo svolgimento delle sue attività nell'ambito dei ruoli di controllo, consultazione e cooperazione.

Il GEPD utilizza una serie di indicatori quali il numero delle richieste d'informazioni da parte dei cittadini, delle indagini dei media e delle richieste d'intervista (relazioni con la stampa), il

numero degli abbonati alla newsletter, dei follower dell'account del GEPD su Twitter ed il numero degli inviti a prendere la parola in occasione di conferenze, oltre ai dati sul traffico legato al sito Internet.

Quanto sopra conferma l'idea che il Garante europeo stia diventando sempre di più un punto di riferimento per le questioni relative alla protezione dei dati a livello di Unione europea. Le visite al sito internet del GEPD nel 2013 sono risultate il 63% maggiori rispetto all'anno precedente. È cresciuto anche il numero delle visite di studio: 17 gruppi nel 2013 rispetto ai due del 2012, e delle richieste di informazioni e di consulenza presentate dai singoli; 176 domande scritte, ossia un aumento pari al 51% rispetto al 2012. A dicembre 2013 è stata aperta una pagina aziendale su LinkedIn, un altro modo di promuovere il GEPD come istituzione, potenziarne la presenza online e aumentarne la visibilità.

Riassumendo, nel 2013 il GEPD ha adottato 91 pareri su controlli preventivi, 21 pareri senza controlli preventivi, ha ricevuto 78 reclami, di cui 30 ammissibili, ha posto in essere 37 consultazioni su misure amministrative, eseguito 8 ispezioni in loco incluse 2 visite di accertamento e 3 visite, ha pubblicato un orientamento in materia di trattamento dei dati personali nel settore degli appalti, ha formulato 20 pareri legislativi, 13 serie di osservazioni formali e 33 informali.

Il GEPD, nel suo documento strategico 2013-2014 a titolo "Towards excellence in data protection", ha individuato una serie di obiettivi strategici per aumentare l'impatto a livello europeo delle attività riguardanti la protezione dei dati.

Per misurare i progressi verso il raggiungimento di tali obiettivi, il GEDP ha identificato delle attività chiave. I relativi 10 Indicatori di Rendimento (ICR) servono per monitorare e adeguare, se del caso, l'impatto del lavoro e l'efficienza delle risorse impiegate. Gli ICR attuano i seguenti obiettivi strategici:

- perseguono una cultura della protezione dei dati in seno alle istituzioni e agli organismi dell'Unione Europea, in modo che siano consapevoli dei loro obblighi e responsabili della conformità ai requisiti della protezione dei dati;

- assicurano che il legislatore dell'UE (Commissione, Parlamento e Consiglio) sia consapevole dei requisiti della protezione dei dati e che questa sia integrata nella nuova legislazione;
- migliorano la cooperazione con le autorità nazionali per la protezione dei dati, in particolare il Gruppo dell'articolo 29, per garantire una maggiore coerenza nella protezione dei dati all'interno dell'Unione europea;
- sviluppano una strategia di comunicazione creativa ed efficace;
- migliorano l'impiego delle risorse umane, finanziarie, tecniche e organizzative del GEPD.

Il GEPD può garantire benefici al cittadino europeo poiché se ha motivo di credere che un'istituzione o un organo dell'Unione Europea abbia violato il suo diritto alla sua privacy, deve presentare denuncia alla persona responsabile dell'elaborazione dei dati in questione. Se non è soddisfatto del risultato della sua denuncia, ha la possibilità di contattare uno dei funzionari responsabili incaricati della protezione dei dati i cui nomi sono reperibili sul sito del GEPD.

Può inoltre presentare denuncia al Garante europeo della protezione dei dati, che prenderà in esame il reclamo e comunicherà al ricorrente, nel più breve tempo possibile, se è d'accordo con l'esposto e, in caso affermativo, in che modo intende porre rimedio alla situazione.

Il Garante europeo può decidere, per esempio, di trasmettere all'istituzione o all'organo interessato l'ordine di correggere, bloccare, cancellare o distruggere qualsiasi dato oggetto di trattamento illecito.

Se il ricorrente non è d'accordo con la decisone del Garante, può deferire la questione alla Corte di giustizia.

Fonti:

(1) European Data Protection Supervisor – The European guardian of personal data protection website;
(2) Strategy 2013-2014 "Toward excellence in data protection" of European Data Protection Supervisor;
(3) Relazione annuale 2013 del Garante Europeo della Protezione dei Dati.

Autorità per le garanzie nelle comunicazioni tra reti, sicurezza e *privacy*

Antonio Preto - Bruno Carotti
(Commissario e Consigliere del Commissario - AGCOM)

Introduzione

All'Autorità per le garanzie nelle comunicazioni (AGCOM) sono attribuite competenze dirette nei settori delle comunicazioni elettroniche, dell'audiovisivo, delle poste e, per alcuni aspetti, dell'editoria. È, dunque, un'autorità "convergente" (come lo è l'OFCOM britannica). È un'autorità indipendente – separata dal potere economico e politico – che gode di una particolare forma di autonomia, che si sostanzia nella potestà di adottare regolamenti per regolare i settori di propria competenza, di definire la propria organizzazione e di gestire le proprie risorse. È protetta dal diritto dell'Unione europea, che ne sancisce l'indipendenza (art. 3, direttiva n. 2002/21/CE), oltre che dalla normativa nazionale (leggi n. 481/1995 e n. 249/1997, ossia la legge istitutiva, il *Codice delle comunicazioni elettroniche*, il *Tusmar*).

Parlando dell'AGCOM, il tema della *privacy* può essere discusso in modo "trasversale". Infatti, l'Autorità non ha competenze "dirette" sulla *privacy*, ma le lambisce, in quanto incide sul mezzo per eccellenza di trasmissione delle informazioni: le reti, destinate per loro natura alla trasmissione dei segnali.

A questo riguardo, sembra esservi un "connubio" tra mezzo e contenuto. È questo il prisma attraverso cui guardare la realtà, in costante evoluzione, delle comunicazioni.

I profili generali della sicurezza

A seguito di tragiche vicende, come quelle francesi, sentiamo oggi la richiesta di maggiore sicurezza. Il tema richiede un'attenzione e un'analisi accuratissime. È certamente necessario assicurare la sicurezza. Gli strumenti di difesa però devono essere proporzionati alle minacce che purtroppo incombono. Nel binomio libertà/sicurezza, infatti, occorre assicurare un *balance of interest*

equilibrato, che non comprima in modo eccessivo la sfera individuale. Questo significa che, nell'equilibrio degli interessi, la *privacy* deve sempre essere tutelata. Sembra un controsenso, ma non lo è. Se vogliamo preservare le libertà che conosciamo e che proclamiamo, questi tasselli sono inamovibili.

Gli esperti mettono in guardia da un controllo eccessivo, che può avere un impatto negativo sul lavoro e sull'industria. Non dobbiamo sottovalutare le minacce, ma nemmeno mettere in discussione le libertà.

La sorveglianza di massa, come è stato efficacemente detto, "*is inherently an abuse of privacy*". Così, pochi giorni fa, si è espressa l'olandese Marietje Schaake, parlamentare europea che si è occupata della tutela dei diritti umani in ambito europeo e internazionale.

Il Garante europeo della *privacy* ha recentemente chiesto se possiamo "affidarci di più agli algoritmi" oppure "rilanciare *il fattore umano nelle investigazioni*" per combattere il terrorismo.

La proposta di direttiva per la registrazione dei dati dei passeggeri (PNR) ha aperto un dibattito acceso. Mentre Commissione e Consiglio UE sono a favore, il Parlamento europeo è preoccupato: la salvaguardia dei dati personali e della *privacy* dei cittadini è a rischio.

In questo scenario, è l'Europa a dover giocare un ruolo maggiore. Il Parlamento europeo, in questo senso, ha chiesto una risposta "tecnologica e politica" ai gravi fatti del *datagate*. Per il PE, combattere la sorveglianza di massa significa adottare la crittografia, le certificazioni e i sistemi *opensource*. Assieme a un "sistema europeo" di certificazione. Anche il Presidente *Juncker* vuole risollevare l'economia del vecchio continente, mediante il rafforzamento del mercato unico digitale e di una nuova autonomia dell'Europa, proprio in termini tecnologici.

L'Europa ha un ruolo fondamentale nel garantire sicurezza senza minare i diritti civili. Basti citare il nuovo regolamento sulla *privacy*, in corso di revisione, che cerca nuovi equilibri, correggendo lo sbilanciamento contrattuale delle parti, attenuando il principio del *one stop shop*, promuovendo un più efficace utilizzo dei *big data*,

ricercando forme di tutela della vita dei singoli adatte al nuovo ambiente digitale, alle sfide della profilazione e della *mass surveillance*.

Il discorso assume una vera e propria dimensione costituzionale, per la natura essenziale degli interessi coinvolti. In questo quadro a tinte variegate, dai contorni e sfaccettature plurimi, l'Unione insiste su un ambito che, come anticipato, interessa più da vicino: le reti e il loro utilizzo. Da qui si può partire per valutare l'ecosistema in cui ci troviamo, prima di ipotizzare possibili risposte ai problemi sollevati da risorse 'sconfinate'.

Rete, dati e giganti

Il *web* è dominato da poche grandi imprese. Secondo i dati dell'*Osservatorio Trimestrale AGCOM*, *Google* ha un quota del 90% nel mercato mondiale, mentre, tra i *social network*, *Facebook* copre il 79% della torta. Gli economisti chiamano questa tendenza "*winner-takes-all*": l'impresa vincente conquista tutto il mercato.

Il *World Economic Forum* ha stimato che nel 2020 la quantità di dati personali immagazzinati online sarà 44 volte maggiore rispetto al 2009. Nel 2013, la produzione media di dati di un impiegato d'ufficio in un anno era di circa 1800 GB (l'equivalente di 1200 film di due ore). Nello stesso anno, sono stati caricati 570.000 *tweet* al secondo.

Con questa mole di dati, i rischi sono molti. Una ricerca condotta da *Federprivacy* ha dimostrato che il 67% dei siti italiani tratta i dati in violazione al *Codice della Privacy*. Il *Global Privacy Enforcement Network* ha rilevato che appena il 15% delle "*app online*" fornisce un'informativa realmente chiara all'utente. L'ultimo rapporto del *Ponemon Institute*, infine, svela che anche gli attacchi informatici sono aumentati del 96% negli ultimi cinque anni.

L'assenza di regole adeguate si traduce in sfiducia e in maggiore diffidenza verso le attività *online*.

Con *ricadute sociali*, in termini di lesione della propria sfera individuale.

Con *ricadute economiche*, per il possibile impatto sull'utilizzo delle reti (soprattutto le NGN di cui si sta parlando moltissimo negli ultimi mesi).

Con, infine, *ricadute politiche*, se si considera che la *privacy online* è una sfida che interessa direttamente i delicati equilibri tra gli Stati che le autorità internazionali non possono più rimandare.

Di fronte a tali fenomeni, dunque, emergono sfide complesse, che toccano il pacifico svolgimento delle nostre stesse vite. Ci sentiamo illusoriamente protetti, poiché nessuno è in grado di controllare i contenuti, una volta immessi in rete. Il problema è in origine: i contenuti li immettiamo noi, ma la gestione è aliena da noi. La conducono altri, soggetti di cui spesso sappiamo poco.

La gestione dei dati (e dei mezzi su cui tali dati viaggiano) non rappresenta solamente un tema tecnico. È una questione di libertà. Occorre gestire consapevolmente le nuove frontiere della comunicazione, che si sviluppano attraverso la rete, per non soggiacere di fronte alle schiaccianti potenzialità del mezzo e continuare, invece, a tutelare dignità dell'uomo, anche dell'*homo digitalis*.

Diritto e istituzioni

Ci sono due strade maestre da seguire: il diritto e le istituzioni.

Da alcune parti si sostiene che non bisogna intervenire, pena la compressione delle libertà. È vero il contrario. È l'*assenza di regole* che pregiudica, se non elimina del tutto, le libertà di cui godiamo.

Le nuove tecnologie, per quanto sconvolgenti, cambiano i paradigmi, ma non gli elementi fondamentali della convivenza civile. In questo senso, i diritti fondamentali dell'uomo rimangono il punto di riferimento cui rivolgersi. Basti pensare alla *Guida ai diritti umani per gli utenti di Internet*, adottata dal Comitato dei ministri del Consiglio d'Europa nel 2014, la quale indica, correttamente, che occorre applicare *i diritti esistenti*.

Dobbiamo comunque coniugare diritti e doveri. In un importante seminario a settembre a Firenze, Joseph Weiler ha sostenuto che la dialettica dei diritti è sana. Ma che spesso si dimenticano i doveri correlati. Abbiamo una grande sete di diritti, anche nuovi, ma raramente sappiamo declinarli in misura ragionevole. Serve un punto di equilibrio che coniughi le potenzialità del mezzo con la difesa del singolo, tra libertà di espressione e protezione della sfera intima.

Questo tema conduce al discorso istituzionale. Per applicare diritti e assicurare doveri, infatti, servono soggetti specifici, con capacità provate. Di seguito, si illustreranno alcuni casi nuovi, di frontiera, per spiegare come un soggetto istituzionale come un'autorità indipendente possa – e debba – intervenire.

Gli ambiti di intervento

Il discorso qui svolto fa emergere aspetti molti rilevanti per l'AGCOM. Ai sensi del citato *codice delle comunicazioni elettroniche* (art. 4, comma 1, *lett. b*), la disciplina delle reti e dei servizi di comunicazione elettronica è infatti volta a salvaguardare "[l]*a segretezza delle comunicazioni, anche attraverso il mantenimento dell'integrità e della sicurezza delle reti di comunicazione elettronica*". L'art. 3, comma 3, dispone inoltre che nel settore "[s]*ono fatte salve le limitazioni derivanti da* […] [e]*sigenze di tutela della riservatezza e protezione dei dati personali, poste da specifiche disposizioni di legge o da disposizione regolamentari di attuazione*".

Come si vede, le comunicazioni elettroniche, presidiate da AGCOM, non possono mettere in secondo piano le esigenze di tutela della protezione dei dati personali.

Ne emerge un parallelismo tra settori, che devono spingere a considerare le tematiche nella loro globalità. Non è un tema secondario: basti citare la sentenza della Corte di giustizia, dell'8 febbraio 2014 (cause C-293/12 e 594/12) che ha annullato la direttiva europea n. 2006/24/CE sulla raccolta obbligatoria dei dati del traffico telefonico e telematico (*data retention*). È un ulteriore

esempio di come i confini tra dati e mezzi di comunicazione non siano così definiti. Sarà interessante sondarne le prospettive future.

Si può pensare anche a un argomento molto noto: il diritto all'oblio. La Corte di Giustizia ha compiuto un passo da condividere, ma ha lasciato aperta una questione fondamentale: il bilanciamento degli interessi, addossata a un soggetto privato. È una soluzione imperfetta, in quanto dovrebbe essere un'istituzione a sancire se sussiste un interesse pubblico che impedisce la rimozione di un determinato *link*. La prassi, d'altronde, è andata proprio in questa direzione, in quanto il Garante della *Privacy* si pronuncia contro le decisioni di *Google* circa il rigetto di un particolare *link* (nel 2014, peraltro, in sette casi su nove è stato ritenuto prevalente l'interesse pubblico).

Il Garante della *Privacy* ha certamente un ruolo primario in materia. Ma il discorso non può esaurirsi qui: le comunicazioni elettroniche siano sono più connesse alla tutela della riservatezza. Basti pensare alle nuove frontiere del *machine-to-machine*, in cui i dati relativi all'utilizzo di particolari macchine (veicoli, elettrodomestici) riveleranno sempre più aspetti della nostra vita, ma lo faranno partendo da un ambito tecnico, che è proprio quello su cui incide AGCOM (che infatti sta guidano uno studio di livello europeo sul M2M in seno al BEREC, l'organismo che riunisce i regolatori europei). La materia, dunque, potrebbe essere affrontata congiuntamente.

Un altro esempio concerne il tema dei nomi a dominio (*Domain Name System*, DNS) e, dunque, con la *governance* di Internet (con l'ICANN). I nomi a dominio sono risorse scarse e il loro utilizzo è gestito in ambito internazionale; in ambito nazionale sono previste forme di controllo affidate a organismi e istituzioni specifiche. Tra queste, seppure per pochissimi profili, vi è AGCOM. Poiché molti diritti vengono attuati anche mediante un sapiente utilizzo di tali nomi (ad esempio, analizzando non solo i domini .it, .fr, .eu, ma anche.com o .net), emerge la necessità di partecipare al dibattito internazionale: senza rinchiudersi nei propri confini, autorità con competenze specifiche possono contribuire ad affrontare problemi di natura globale.

Nell'economia digitale, i dati sono una risorsa economica, una componente centrale del *business model* dei principali attori del *web*. I giganti della rete, prima richiamati, raccolgono dati attraverso i propri servizi e li trasformano in informazioni utili per gli inserzionisti pubblicitari. Viste le loro posizioni di forza, i *big data* potrebbero considerarsi una *essential facility*. Se così fosse, occorrerebbe introdurre una forma di regolazione dell'accesso a tali informazioni, pensando anche a una forma di remunerazione dell'utente finale (che, di fatto, è il proprietario e "produttore" dei *big data*).

Infine, un tema fondamentale è quello della *net neutrality*, principio fondamentale – che negli USA si sta affermando in maniera sempre più netta – per assicurare un trattamento uguale delle informazioni. Allo stesso modo, si dovrebbe garantire anche una *platform neutrality*: oltre che nei confronti dei consumatori, le piattaforme devono restare neutrali anche rispetto al potere politico; i recenti scandali che hanno coinvolto i giganti del *web* e le agenzie di spionaggio (anche quelle private, che vendono i propri costosissimi servizi di nascosto, e dunque illegalmente) confermano il rischio di derive antidemocratiche che vanno contrastate.

Di fronte a tutte le questioni esaminate, l'approccio di un regolatore come AGCOM può fornire un contributo importante. L'Autorità da più di quindici anni si occupa di questioni simili a quelle descritte: dall'accesso all'infrastruttura alla concorrenza, fino alla tutela dei "cittadini". Inoltre, si occupa non solo di mercato, ma anche di persone, di cittadini (come indica l'art. 8 della direttiva n. 2002/21/CE). Dunque, la sua esperienza (l'*expertise*, come dicono i Giudici) potrebbe senz'altro essere un valore aggiunto.

L'azione del regolatore è improntata sulla tesi di enaudiana memoria: "*conoscere per deliberare*". È chiamato ad adottare decisioni informate e, per questo, deve conoscere a fondo il contesto di riferimento, dialogare con i soggetti che operano nel mercato, mantenere terzietà e indipendenza.

Viviamo in un momento in cui la cultura istituzionale è sempre più rarefatta. Occorre invece proteggere le esperienze acquisite nel settore, e conservare quelle migliori. Le autorità indipendenti sono

un fiore all'occhiello del Paese, e occorre proteggerle, aldilà delle facili retoriche, per affrontare con strumenti consolidati le nuove sfide.

Conclusioni

La rete diventa un veicolo di valori, quali la difesa dell'ambiente, la tutela dei lavoratori nelle imprese e, in generale, la libertà di informazione; allo stesso tempo, costituisce uno strumento di pervasività nelle vite di ciascuno.

Come ha ricordato il Parlamento europeo, è opportuno *integrare tali tecnologie dell'informazione e della comunicazione* sia nel panorama mediatico attuale sia in quello che sta evolvendo, insieme alle *condizioni essenziali dell'indipendenza, del pluralismo e della diversità*.

Non possiamo affrontare da soli, come singoli, l'intero flusso di informazioni. È l'organizzazione, la selezione, la comprensione degli effetti di tale mole ingentissima di informazioni a giocare la vera partita in cui i regolatori, come AGCOM, hanno un ruolo e una responsabilità enormi. L'indirizzo che dovrebbe seguirsi è quello di un approccio condiviso, in cui sia possibile sfruttare le conoscenze specifiche di ciascuna istituzione. Un metodo eclettico, che sappia coniugare la settorializzazione con un approccio globale e con una prospettiva d'insieme. Le moderne tecnologie spingono alla convergenza, generando un ecosistema nuovo; le risposte devono essere all'altezza, aprendosi ai nuovi scenari e cambiando, se necessario, paradigma. Per adeguarsi alla realtà in costante evoluzione ed evitare di rimanere ancorati a schemi superati o facilmente superabili.

Se le istituzioni sapranno essere all'altezza, utilizzando le loro competenze non a salvaguardia della loro specifica posizione, ma a vantaggio dei cittadini, potremo guardare con maggiore forza alle sfide che ci attendono.

L'identità nel cyber spazio e la normativa nazionale

Stefania Fini

Il rapido evolversi delle modalità di utilizzo delle tecnologie negli ultimi anni ha comportato la necessità di ordinare attraverso provvedimenti normativi un campo fino ad ora regolamentato solo in parte. Infatti in materia di cibernetica, fino al 2013, non si conosce una normativa unitaria che regoli la materia, ancora scarsamente sviluppata a livello nazionale. Si è stabilito di cominciare con la stesura più recente di un atto elaborato dagli organi parlamentari, il Decreto della Presidenza del Consiglio dei Ministri del 24 gennaio 2013, che racchiude al suo interno la disciplina di questa materia, ma anche riferimenti a Leggi emanate in anni antecedenti che rendono più esaustivo il suo contenuto.

Il DPCM 23 gennaio 2013 intitolata "Direttiva per la protezione cibernetica e la sicurezza informatica nazionale" consta di 13 articoli i quali trattano in maniera didascalica e puntuale le modalità di coordinamento della struttura istituzionale per far fronte alle minacce di cyber crime che provengono dall'esterno, sia considerando gli obiettivi sensibili quali infrastrutture critiche sia civili che militari, le minacce costituite dai tentativi di violazione di sistemi informatici e la sottrazione di dati riservati, riguardanti scambi di informazioni e il funzionamento di uno Stato ovvero a danno di aziende che erogano servizi essenziali per la Nazione e la società civile, o depositarie di know how, conoscenze industriali, scientifiche, tecnologiche, innovative o specialistiche; sia per contrastare ogni forma di terrorismo, che oltre ad attacchi informatici e capzione di dati riservati, alimenta le proprie attività quali finanziamento dei loro organismi, reclutamento e propaganda attraverso mezzi informatici e telecomunicazioni strettamente interconnessi tra loro. Oppure ancora, il settore della criminalità che utilizza questo strumento per compiere reati quali furti di denaro, truffe, a danno di privati cittadini o altri organismi diversi da questi. Infine vi è, non per ultima, la minaccia di guerra, intesa quale conflitto di ultima generazione, la cyber war, una serie di attacchi

informatici atti a paralizzare la capacità offensiva o di risposta degli avversari, ed arrecare attraverso questi interventi effettivi danni materiali.

Passiamo ad elencare le definizioni riportate nell'art. 2 del DPCM in esame: lo spazio cibernetico è definito l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi; la sicurezza cibernetica è una condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi; la minaccia cibernetica invece è intesa come il complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, in particolare, nelle azioni di singoli individui o organizzazioni, statuali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi; l'evento cibernetico è un avvenimento significativo, di natura volontaria od accidentale, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi; l'allarme è la comunicazione di avviso di evento cibernetico da valutarsi ai fini dell'attivazione di misure di risposta pianificate; la situazione di crisi è invece una situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale.

All'art. 1 del DPCM 24 gennaio 2013 viene stabilita l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativa alle infrastrutture critiche materiali e immateriali, per ciò che concerne la protezione cibernetica e la sicurezza informatica nazionali, indica i soggetti deputati a tale funzione, le loro competenze e le procedure di prevenzione dei rischi, tempestiva risposta alle aggressioni e ripristino nel più breve tempo possibile della funzionalità dei sistemi in caso di stato di crisi dovuta appunto ad azioni di hackeraggio.

I soggetti, o meglio le Autorità competenti nella direzione e nella responsabilità della politica di informazione della sicurezza, operano nel rispetto delle competenze attribuite dalla legge a ciascuno di essi, esse sono enunciate nella L. 124 del 2007 "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto" ; il Presidente del consiglio dei Ministri provvede al coordinamento delle suddette politiche impartendo direttive, ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento del Sistema di informazione per la Sicurezza nazionale, dopo aver consultato il Comitato Interministeriale per la sicurezza della Repubblica. Il Presidente può, in ogni caso, trasferire alcune di queste prerogative, che non sono attribuite ad esso in via esclusiva, all'Autorità Delegata, che, come descrive l'art. 3 della L. 124 del 2007, può ravvisarsi nella carica di un Ministro senza portafoglio oppure di un Sottosegretario di Stato; ma le funzioni sono solo quelle che vengono specificatamente attribuite, poiché il Presidente è costantemente informato delle attività e delle modalità di esercizio di queste ultime, potendo revocare in ogni momento l'esercizio di tutte o alcune di esse.

Al co. 3 dell'art. 1 il decreto delinea il modello organizzativo - funzionale che persegue l'integrazione con le attività di competenza del Ministro dello sviluppo economico e dell'Agenzia per l'Italia digitale, con quelle espletate dal Ministero della Difesa per la protezione delle proprie reti e sistemi e condotta delle operazioni militari nello spazio cibernetico, quelle del Ministero dell'interno, riguardo alla prevenzione dei crimini informatici e della difesa civile, e quelle della Protezione Civile.

L'art. 2 elenca i componenti del Sistema di informazione per la sicurezza della Repubblica che è composto dal Presidente del Consiglio dei ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'Autorità delegata di cui all'articolo 3, ove istituita, dal Dipartimento delle informazioni per la sicurezza (DIS), dall'Agenzia informazioni e sicurezza esterna (AISE) e dall'Agenzia informazioni e sicurezza interna (AISI).

Passiamo ad esaminare le competenze dei singoli organismi che, coordinandosi tra loro, attuano in sinergia tutte le misure necessarie per contrastare minacce e crisi di origine cibernetica, cominciando dal Presidente del Consiglio dei Ministri (art.3).

La lettera a) dispone, su proposta del CISR, di adottare il quadro strategico nazionale per la sicurezza dello spazio cibernetico, tenendo conto delle tendenze evolutive delle minacce cibernetiche e sulla vulnerabilità di sistemi e delle reti di interesse nazionale e l'individuazione degli strumenti e procedure da applicare nel settore della prevenzione e risposta ad attacchi di carattere cibernetico. Alla lettera b) invece, su deliberazione del CISR, adotta il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali con cui si stabiliscono gli interventi da conseguire e le linee di azione da perseguire nel quadro strategico nazionale; emana le direttive e ogni atto di indirizzo per l'attuazione del Piano, e, sentito il CISR, impartisce le direttive al DIS e alle Agenzie AISI e AISE (art.1 c.3 bis L. 124/2007)

All'art.4 esaminiamo le funzioni del Comitato interministeriale per la sicurezza della Repubblica, che indicheremo con la sigla CISR, in materia di sicurezza dello spazio cibernetico.

Al c.1 lettera b) delibera il Piano nazionale per la sicurezza dello spazio cibernetico, con la finalità di: proporre l'adozione del Quadro Strategico Nazionale da parte del Presidente del Consiglio dei Ministri; esprimere pareri sulle direttive emanate dal Presidente (art.3 c.1 DPCM 2013); è sentito per ciò che riguarda l'adozione di direttive agli Organismi di Informazione per la Sicurezza (DIS, AISI, AISE); esercita la sorveglianza sull'attuazione del Piano Nazionale; approva le linee di indirizzo per favorire l'efficace collaborazione tra soggetti istituzionali per il settore pubblico, e operatori privati

interessati alla sicurezza cibernetica, e la condivisione di informazioni per l'adozione di best practices e misure atte a raggiungere l'obiettivo della sicurezza cibernetica; elabora gli indirizzi generali e gli obiettivi fondamentali in materia di protezione da perseguire nell'ambito della politica dell'informazione per la sicurezza da parte degli organismi deputati, sempre all'interno delle rispettive competenze; promuove l'adozione delle iniziative che assicurino la partecipazione dell'Italia, il coordinamento ai consessi di cooperazione internazionali, bilaterali o multilaterali dell'unione Europea e NATO, per definire e adottare politiche e strategie comuni di prevenzione e risposta alle minacce cibernetiche; formula proposte di intervento normativo e organizzativo per il potenziamento delle misure di cui sopra e per la gestione di situazioni di crisi; ha funzioni di consulenza e proposta, e partecipa alle determinazioni del Presidente del Consiglio.

Per ciò che concerne le attività di consulenza l'art. 5 ci illustra che presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la sicurezza della Repubblica (CISR) con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. Al comma 2 dell'art. 5 il Comitato elabora gli indirizzi generali e gli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza, delibera sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza e sui relativi bilanci preventivi e consuntivi. (Funzioni del CISR art 4 DPCM). Al comma 3 dell'art. 5 sono elencati i componenti del CISR, il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia e dal Ministro dell'economia e delle finanze.

Al comma n. 5 dell'art. 5, il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, ma senza diritto di voto, altri componenti del Consiglio dei ministri, i direttori dell'AISE e dell'AISI, nonché altre autorità civili e militari quando sia ritenuta necessaria la

presenza in relazione alla tecnicità e specificità delle questioni da trattare.

Alle riunioni del CISR in materia di sicurezza cibernetica partecipa, senza diritto di voto, anche il Consigliere Militare del Presidente del Consiglio (art.4 c.2).

A svolgere le attività di coordinamento del CISR c'è l'organismo di supporto al CISR, un organo collegiale di coordinamento presieduto dal Direttore generale del DIS, a cui partecipa anche il Consigliere Militare (co. 2), la cui composizione è indicata nel DPCM 2 del 26 ottobre 2012 è stato adottato il "Regolamento che definisce l'ordinamento e l'organizzazione del Dipartimento delle informazioni per la sicurezza (DIS)". Ai sensi dell'art. 22, comma 2, del Decreto, le disposizioni ivi contenute sono entrate in vigore il 1° aprile 2013.

Le attività svolte dall'organismo collegiale di coordinamento sono quella preparatoria alle riunioni del CISR, predispone l'istruttoria per adottare gli atti e lo svolgimento delle attività del CISR esaminate in precedenza; espleta attività di verifica riguardo l'attuazione degli interventi previsti dal Piano nazionale per la sicurezza dello spazio cibernetico e l'efficacia delle procedure di coordinamento tra soggetti pubblici e privati che devono attuarli; coordina la formulazione di indicazioni necessarie allo svolgimento delle attività per l'individuazione delle minacce alla sicurezza cibernetica, delle vulnerabilità dei sistemi, l'adozione di best practices e misure di sicurezza, compiendo approfondimenti e acquisendo ogni utile valutazione.

Il Comitato Scientifico all'art. 6, è istituito presso la Scuola di Formazione, ed è costituito da esperti nel nostro campo di interesse, provenienti da enti di ricerca, università, dalle pubbliche amministrazioni e dal settore privato, con il compito di costruire ipotesi di attacco simulato per migliorare i livelli di sicurezza dei sistemi e delle reti per incrementare le condizioni di sicurezza del Paese, che assicuri ogni contributo necessario allo svolgimento delle attività dell'organismo collegiale di coordinamento e al Nucleo per la sicurezza cibernetica per la prevenzione e preparazione ad eventuali

stati di crisi. Il comitato formula proposte e progetti di promozione e diffusione della cultura sulla sicurezza cibernetica.

Passiamo agli Organismi di informazione per la sicurezza: l'art.7 stabilisce che il DIS e le Agenzie svolgono attività nel campo della cibernetica avvalendosi di mezzi adoperati secondo le modalità della Legge 124/2007 che li disciplina. Il DIS coordina le attività di ricerca e acquisizione delle informazioni utili ad incrementare la protezione cibernetica e la sicurezza informatica nazionale, secondo gli indirizzi generali e gli obiettivi fondamentali indicati dal CISR e le direttive impartite dal Presidente del Consiglio. Il Direttore del DIS è supportato dai propri uffici per svolgere le attività di coordinamento con il CISR e il Presidente del Consiglio. Il DIS sulla base dello scambio di informazioni acquisite formula analisi, valutazioni e previsioni circa le potenziali minacce cibernetiche, e provvede alla trasmissione delle informazioni rilevanti al Nucleo per la sicurezza cibernetica, alle pubbliche amministrazioni e ai soggetti privati interessati all'acquisizione di tali informazioni. Le Agenzie, nell'ambito delle loro attribuzioni, svolgono attività di ricerca e elaborazione informativa, sempre seguendo le direttive della Presidenza e le linee di coordinamento delle attività di ricerca stabilite dal Direttore Generale del DIS. Proprio per svolgere le attività previste, il DIS stipula convenzioni apposite con le università, enti di ricerca, le pubbliche amministrazioni e le aziende che erogano servizi di pubblica utilità; queste ultime due categorie consentono al DIS e alle Agenzie l'accesso ai loro archivi informatici, sempre secondo le procedure e le modalità disciplinate dalla legge. Inoltre il DIS, su indicazioni del Comitato scientifico, promuove attività di diffusione e informazione dei rischi derivanti dalla minaccia cibernetica e sulle misure di prevenzione.

Il Nucleo per la sicurezza cibernetica è istituito in modo permanente presso l'Ufficio del Consigliere Militare, da cui è presieduto, inoltre è composto rispettivamente da un rappresentante del DIS, AISE, AISI, del Ministero degli Affari Esteri, del Ministero degli Interni, del Ministero della Difesa, Ministero dello Sviluppo Economico, Ministero dell'economia e delle finanze, del Dipartimento della Protezione Civile e dell'Agenzia per l'Italia

digitale, e, per le azioni classificate, si avvale di un rappresentante dell'Ufficio centrale per la Segretezza.

Alle riunioni possono partecipare anche rappresentanti di altre amministrazioni, università ed enti di ricerca, oppure operatori privati che siano interessati alla materia. Il Nucleo si riunisce, su richiesta del Consigliere Militare o di un suo componente, una volta al mese ed è a supporto del Presidente per ciò che concerne la previsione e prevenzione dei rischi e situazioni di crisi e per porre in essere procedure di allertamento.

Il Nucleo, secondo l'art. 9 ha funzioni di raccordo fra tutte le componenti dell'architettura istituzionale, ciascuno nei propri ambiti di competenza attribuiti dalla legge. Per ciò che riguarda la prevenzione e la preparazione per affrontare eventuali crisi, promuove sulla base delle direttive impartite dal Presidente, la programmazione e pianificazione operativa di risposta a situazioni di criticità, da parte delle amministrazioni e dei privati interessati alle procedure di coordinamento interministeriale, raccordate con piani di difesa civile e protezione civile; mantiene attive le misure di allerta e le risposte alle situazioni di crisi, 24 ore su 24; promuove la condivisione di informazioni con operatori privati interessati per la diffusione di allarmi relativi agli eventi in questione e per gestire situazioni di crisi, in raccordo con le amministrazioni competenti per settori specifici di protezione cibernetica; acquisisce comunicazioni riguardo tentativi di violazione della sicurezza o casi di violazione o perdita della integrità indispensabili per il corretto funzionamento dei servizi e delle reti, attraverso il Ministero dello sviluppo economico, le Forze di polizia, le strutture del Ministero della Difesa e gli organismi di informazione per la sicurezza; il Nucleo promuove e coordina lo svolgimento delle esercitazioni interministeriali, in raccordo con il Ministero dello sviluppo economico e dell'Agenzia per l'Italia digitale, per i profili di loro competenza, e la partecipazione nazionale ad esercitazioni internazionali sulla simulazione di attacchi o situazioni di crisi cibernetica; è il punto di riferimento nei rapporti con UE, NATO, ONU, altre organizzazioni internazionali e Stati, ferme sempre le competenze del Ministero dello sviluppo economico, Ministero degli Affari Esteri, Ministero della Difesa, Ministero

dell'Interno e di altre amministrazioni previste dalla normativa vigente.

Per l'attivazione delle azioni di risposta e ripristino delle situazioni di crisi cibernetica il Nucleo riceve le segnalazioni di eventi cibernetici sia in ambito nazionale che dall'estero, e dirama gli allarmi alle amministrazioni e agli operatori privati per attuare le procedure di prevenzione che abbiamo trattato in precedenza; valuta se l'evento cibernetico può essere gestito in via ordinaria dalle amministrazioni competenti oppure vanno attuate decisioni coordinate a livello interministeriale e se l'evento assume una tale gravità da incidere sulla sicurezza nazionale, il Nucleo provvede a dichiarare la situazione di crisi cibernetica e a convocare ed attivare il NISP, il Tavolo interministeriale di crisi cibernetica, informando tempestivamente il Presidente della situazione che è in atto.

Dopodiché elabora appositi report sullo stato di attuazione delle misure di coordinamento per la preparazione e la gestione della crisi, per le finalità di cui al comma 5 co. 3 lettera c, (cioè espleta le attività necessarie a verificare l'attuazione degli interventi previsti dal Piano nazionale per la sicurezza dello spazio cibernetico e l'efficacia delle procedure di coordinamento tra i diversi soggetti, pubblici e privati, chiamati ad attuarli), e lo trasmette all'organo collegiale di coordinamento di supporto al CISR.

L'ultimo organismo da esaminare è il NISP, il Nucleo interministeriale situazione e pianificazione, il Tavolo interministeriale di crisi cibernetica, attivato dal Nucleo in caso di dichiarazione di stato di crisi cibernetica che incida sulla sicurezza nazionale. Il Tavolo è presieduto dal Consigliere Militare, dai rappresentanti dei vari Ministeri di cui all'art. 5 co. 3 e di un rappresentante del Ministero dello sviluppo economico e dell'Agenzia per l'Italia Digitale, che prendono decisioni che impegnano la loro amministrazione, e possono farsi accompagnare alle riunioni da altri funzionari della propria amministrazione; possono essere chiamati soggetti di cui all'art 5 co. 6 del DPCM 5 maggio 2010, gli operatori privati e altri soggetti interessati. Esso deve assicurare che tutte le attività di reazione e stabilizzazione delle Amministrazioni ed enti si svolgano in modo coordinato avvalendosi per gli aspetti tecnici di

risposta sul piano informatico e telematico del CERT nazionale, il *Computer Emergency Response Team*, istituito presso il Ministero dello Sviluppo Economico. Altri compiti non meno importanti del Tavolo sono: mantenere informato il Presidente del Consiglio sulla crisi in atto con aggiornamenti costanti, assicura il coordinamento a livello interministeriale, raccoglie i dati relativi alla crisi cibernetica, elabora i rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati, assicura i collegamenti per la gestione della crisi con omologhi organismi di altri Stati, NATO, UE e le organizzazioni internazionali di cui fa parte l'Italia.

Infine nel DPCM sono inclusi gli operatori privati, che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici, secondo quanto previsto dalla norma vigente o previa convenzione ad hoc, comunicano al Nucleo per la sicurezza cibernetica, anche per il tramite dei soggetti istituzionalmente competenti a ricevere le relative comunicazioni, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti; adottano le best practices e le misure finalizzate all'obiettivo della sicurezza cibernetica; forniscono informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza; collaborano alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

Per ciò che riguarda la tutela delle informazioni, lo scambio delle informazioni classificate si osservano le disposizioni di cui al DPCM 22 luglio 2011, n. 4, recante disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate. Il DIS, attraverso l'Ufficio centrale per la segretezza, assolve ai compiti relativi alla tutela dei sistemi omologati EAD delle pubbliche amministrazioni e degli operatori privati, che sono in possesso di

questa autorizzazione per trattare informazioni classificate con sistemi informatici, siano essi isolati, reti locali o geografiche.

L'applicazione del DPCM 24 Gennaio 2013 è stata attuata il 7 Febbraio del 2014 attraverso la pubblicazione sulla Gazzetta Ufficiale del "Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico", che detta le linee generali da adottare nel lungo periodo, nel caso del verificarsi di eventi che minacciano la sicurezza nazionale, sociale o industriale, e con la contestuale pubblicazione del "Piano nazionale per la protezione cibernetica e la sicurezza informatica", piano biennale da aggiornare quindi periodicamente, a causa del rapido evolversi delle minacce e della necessità di aggiornare le strategie di difesa e attacco nel caso del verificarsi degli eventi cyber. Per ciò che può dirsi del Quadro Strategico Nazionale, vengono confermati e ribaditi gli indirizzi sia strategici che operativi fondamentali già riportati nel DPCM 24 Gennaio 2013.

I primi sei indirizzi strategici consistono: nella formazione del personale e miglioramento delle capacità operative e tecnologiche degli attori istituzionali impegnati nel contrasto delle minacce del cyber; il potenziamento della difesa delle infrastrutture critiche a livello nazionale, assicurata anche per mezzo di una *compliance* con standard e protocolli di sicurezza internazionali; incentivazione della collaborazione tra settore pubblico e privato per meglio tutelare il patrimonio intellettuale, i settori della ricerca, e dell'innovazione del nostro Paese; promozione di una cultura della sicurezza, in collaborazione con le università e la ricerca, per educare i cittadini ad adottare misure di difesa, per quanto possibile, dalle minacce a cui potenzialmente rischiano di essere esposti quotidianamente; rafforzare la capacità di contrasto alla diffusione di contenuti e attività legali online; e, inevitabilmente, promuovere la cooperazione internazionale in materia cibernetica a livello UE e NATO.

Gli undici indirizzi operativi, descritti più specificatamente nel "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica", sono necessari per la realizzazione dei primi sei. Ricordiamo che essi sono: uno sviluppo delle capacità delle autorità competenti per una efficace prevenzione identificazione contrasto e mitigazione, nel caso siano inevitabili, degli eventi cyber e delle

conseguenze sui sistemi IT, sulle infrastrutture critiche nazionali e sul sistema Paese; individuazione di una Autorità nazionale NIS (Network and Information Security) che cooperi a livello internazionale con altre autorità omologhe per lo scambio di informazioni, favorire la cooperazione tra settore pubblico e privato costituendo tavoli di raccordo, o la pianificazione di esercitazioni periodiche, la segnalazione alle Autorità competenti degli incidenti informatici e la definizione di procedure operative per lo scambio di informazioni; la realizzazione di campagne di informazione nelle scuole di ogni grado per promuovere la cultura della sicurezza, e sviluppo di simulazioni ai fini della formazione e dell'addestramento; rafforzamento della cooperazione internazionale, considerando che la minaccia cyber è globale e non ha confini, potendo operare e provocare danni, reati o catastrofi, da una qualunque parte del mondo; dare attuazione al CERT Nazionale (*Computer Emergency Response Team*) con sede presso il Ministero dello Sviluppo Economico, e al CERT della Pubblica Amministrazione; fondamentale anche il punto 6, ovvero l'adeguamento normativo e organizzativo della legislazione, adattandola alla più rapida evoluzione della tecnologia; l'elaborazione delle norme tecniche per migliorare gli standard di sicurezza di prodotti e sistemi atti al contrasto degli eventi cibernetici; la cooperazione col settore industriale e le PMI, con la previsione di incentivi che siano utili a stimolare la competitività tecnologica ed industriale e il potenziamento delle attività di R&S; coerenza tra comunicazioni strategiche istituzionali e le attività di contrasto al *cyber space* per dissuadere potenziali azioni illegali; non da ultimi e comunque fondamentali gli ultimi due obiettivi, attribuire ai settori strategici della PA risorse umane, adeguatamente formate e preparate, risorse finanziarie, tecnologiche e logistiche per raggiungere gli obiettivi programmatici, e l'implementazione di un sistema integrato di *Information Risk Management* nazionale.

Certo, per la molteplicità degli organismi coinvolti e la fitta rete di correlazioni tra loro, la struttura è alquanto complessa e difficile da coordinare, in modo tale da attuare una sinergia che renda il sistema di difesa verso il cyber efficiente. In futuro forse si

troverà un criterio per snellire e rendere più rapide le procedure.

Altre criticità possono derivare effettivamente anche dalla difficoltà di reperimento delle risorse finanziarie per il funzionamento della struttura istituzionale, fondi che è difficile accantonare in periodi di recessione economica. Un altro aspetto di cui si discute è anche la resistenza dei privati nella comunicazione di eventuali attacchi cibernetici ai propri sistemi informatici, una mancanza di collaborazione che di certo non aiuta le Istituzioni nel contrasto ad accessi illegali e a specifici reati.

Dopo aver esaurito ampiamente la descrizione della struttura complessa che si avvia in casi di crisi cibernetica, ora possiamo passare ad esaminare ciò che può essere fatto per tutelare la privacy e i dati sensibili. Manca tuttora una classificazione completa dei reati e delle sanzioni applicabili, ancora molto va fatto in un campo che ormai può considerarsi globale, dove difficilmente si individua da quale parte provenga l'attacco, e ancor più arduo è l'impiego di mezzi e risorse per fronteggiare e difendersi da una minaccia non completamente prevedibile e controllabile, basti pensare agli eventi accaduti, l'ultimo in ordine di tempo l'attacco hacker presso conti correnti e alle stesse risorse di Banche a livello globale, realizzando furti e sottrazione di banconote per miliardi di dollari, o come attacchi ai sistemi del Pentagono per l'acquisizione di informazioni sensibili riguardo argomenti quali la difesa, o ancora informazioni riservate dello Stato, che siano militari o politiche, o di tentativi di violazione di sistemi di comunicazione, come accaduto per società di telefonia, al fine di acquisire, con pratiche illegali, intercettazioni di conversazioni o carpire contenuti di messaggi di testo, per danneggiare autorità e istituzioni con importanti funzioni nella politica del Paese, oppure acquisizioni a volte anche commissionate da Stati che adoperano le informazioni per spiare anche propri alleati, e per poi attuare politiche economiche mirate; o l'uso di internet e di social network e media, per raccogliere informazioni o promuovere propaganda, basti citare le ultime cruente e inquietanti vicende di terrorismo internazionale che si è sviluppato in Medio Oriente e che sta avanzando verso i Paesi Occidentali.

Attualmente sono state individuate alcune fattispecie di reati informatici: art. 494 c.p. furto di identità semplice che ricomprende tutti i tentativi di *phishing* attraverso l'invio di e-mail, e altri furti di identità, anche consumati, dai quali la persona offesa non ha ricevuto un danno; esercizio arbitrario delle proprie ragioni (art. 392 c.p.); attentato ad impianti di pubblica utilità (art. 420 c.p.); falsità in documenti informatici (art. 491-bis c.p.); accesso abusivo ad un sistema informatico (art. 615-ter c.p.) accesso illegittimo ad account di comunicazione, come caselle di posta elettronica sia personale, e sia aziendale; violazioni di centralini telefonici VOIP, attraverso i quali i sistemi di sicurezza e comunicazione di un operatore telefonico vengono attaccati e violati; violazione di piattaforme di commercio elettronico, vendite fittizie di beni con l'intento di non inviarli all'acquirente, ottenendo l'ingiusto profitto del prezzo che viene corrisposto con pagamenti elettronici prima dell'invio del bene; violazione o acquisizione indebita dell'account personale o di profilo relativo alle piattaforme di social network; detenzione e diffusione abusiva di codici di accesso (art. 615-quater c.p.); diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.); violazione della corrispondenza e delle comunicazioni informatiche e telematiche (art. 616, 617-quater, 617-quinquies, 617-sexies c.p.); rivelazione del contenuto di documenti segreti (art. 621 c.p.); trasmissione a distanza di dati (art. 623-bis c.p.); danneggiamento di sistemi informatici o telematici (art. 635-bis c.p.); art. 640 c.p. fraudolenta captazione di informazioni e dati riservati attraverso il *phishing* relativi a carte di credito, carte prepagate o conti correnti online e uso illecito di questi strumenti di pagamento da parte di terzi; frode informatica (art. 640-ter c.p.) attraverso "dialer", programmi autoinstallanti che disconnettono il modem e lo riconnettono a numeri a valore aggiunto o a codici internazionali satellitari che comportano costi elevati di chiamate o traffico internet. Riciclaggio elettronico di proventi illeciti, art 648 c.p. e 648 bis. La diffamazione *on-line* art.595 co. 3 c.p. in cui la persona offesa segnala una pubblicazione lesiva della propria reputazione e onore sulla rete internet, su blog o forum online, vengono escluse e-mail e sms che

non sono trattate dal pool reati informatici. In futuro ci si adoperi affinché lo strumento della prevenzione di detti reati, in scala più ridotta o su una più ampia, sia comunque contrastata efficacemente da una rete sempre più fitta e stretta di controlli, così da garantire tutela e sicurezza da minacce e attacchi cibernetici anche al singolo cittadino.

NATO towards a more concrete approach to cyber challenges

Emma Ferrero

(Nato Defence College Foundation Programme Manager)

"Inter-national" vulnerabilities

The protection of the critical infrastructures in a NATO framework is quite recent. The core business of the Alliance has always been strictly related to the protection of the territory and of the population of its member States from preview and conventional threats. The Strategic Concepts preceding the Strategic Concept 2010 were clearly focused on that kind of threats. Now, after the Lisbon Summit, something changed. The Strategic Concept elaborated after Lisbon sets an important precedent by establishing the new security threats, among which the protection of the critical infrastructures from cyber-attacks is an absolutely first.

The NATO New Strategic Concept is the result of a long process elaborated in many different steps among the last ten years. The NATO activities on the field (such as the intervention in Afghanistan) or the Russian-Georgian crisis in 2008, as well as the implementation of the NATO enlargement policy, have deeply influenced the idea behind the New Strategic Concept. Each member state has been involved in a complex internal process towards the definition of its own national strategic interests, able to fulfil the single national concern and the strategic interest of the Alliance as a whole.

The current Strategic Concept is more political and global. It is reaffirmed the value of the Article 5 of the Treaty of Washington, even though its aim is now globalized: the main purpose of the Alliance is to "protect and defend" its members from threats that transcend national boundaries, such as terrorism, proliferation of armaments and cyber-war. The main difference from the Strategic Concepts released in 1991 and 1999, is that the current one underline three key strategic objects which will be then extensively explained in several under-categories:

Collective defence: NATO members are committed in mutual assistance, as for the Article 5 of the Washington Treaty.
Crisis Management: NATO has a strong military and political will, able to react to any emerging crisis.

Cooperative Security: NATO can be influenced and influence itself the developments of security out of its borders. The partnership system is a tool in order to preserve international security.

The Alliance is not only oriented towards activities of defence and deterrence from any kind of threats, nowadays the NATO core business is to protect the allies and the Alliance from the emerging security threats. The meaning of "emerging security threat" is the capstone to understand the new role that NATO is going to take on. Even so, the New Security Concept clarifies that the conventional threats are still in place but they are not the first risks to deal with.

Not ignoring the old menaces, the Concept points out a heterogeneous classification of the potential threats that NATO is going to face in the very next future: international terrorism, nuclear proliferation, regional instability, weapon trafficking and - last but least – menaces from the cyber environment against vital communication, transport and strategic networks.

Given the importance of these emerging security threats, the institution of the Emerging Security Challenges Division at the NATO Headquarter in Brussels is a first approach towards the objectification of the determination expressed in the Strategic Concept. This Division embodies the backbone of the fight against the new unconventional threats at a NATO level. Indeed, it works as a container where all the NATO competencies and capacities are put together in order to monitor, analyse and define policies through ad-hoc working groups.

This issue is not a new element among the security responsibilities of a State. To provide the main basic services for the population has always been included into the core business of every governance policy. So, what is changing today? The factor that determines the step-forward in the protection of critical

infrastructures approach is the dimension in which this protection should be developed in order to be effective.

September 11th 2001 raised a different consciousness of the threat towards the vital systems of a State, which is more and more uncertain, unpredictable and hidden. The critical infrastructures of both United States and European Union have been subject of cyber-attacks during the last ten years. Most of the NATO member States key infrastructures came under attacks that neutralized huge logistic and storage networks for several days and hours. Railway lines, airports, communication hubs, sensitive data centres, city transports, military bases; this is only a short list of the potential targets of a cyber-attack.

The globalization process implies that the approach towards the protection of the national critical infrastructures cannot be limited only to a national level. On the contrary, the protection of the critical infrastructures requires an increasing awareness of the external dimension. The single States should understand that the protection of their own infrastructures calls for any kind of cooperative solution. International organizations such as NATO and European Union have the precise duty to enhance this cooperation. In spite of not having played a leading role on this issue since a few years ago, nowadays NATO and European Union are recognising the strategic relevance of the protection of critical infrastructure from cyber-threats.

Once a sensitive point of a State member of a political-military alliance is under attack, the whole alliance could be under attack. The principle at the base of the Article 5 of the Washington Treaty states: *"The Parties agree that an armed attack against one or more of them in Europe or North America shell be considered an attack against them all and consequently they agree that, if such armed attack occurs, each of them in exercise of the right of individual or collective defence […] will assist the Party or the Parties so attacked by taking […] such action as it deems necessary including the use of armed force, to restore and maintain the security of the North Atlantic area."* Considering this principle, the

analysis of the NATO approach towards the protection of critical infrastructures highlights three main critical topics:
In a cyber-security framework there is no clear boundary that establishes the red-line that must not be crossed in order not to trigger the Article 5 of the Washington Treaty;
NATO member States don't share a common definition of what a "critical infrastructure" is;

Despite the growing attention on the establishment of cooperation programmes among NATO and other national actors, both private and institutional, there is still a lack of focus and shared goals.

The Article 5 was defined during an historical period when the strategic threats towards the security of the NATO countries were deeply different from now. This could seem intuitive, but the hard work of evolution of the Strategic Concepts of the Alliance give evidence of the progresses made. Each Strategic Concept try to come across the menaces and the threats that NATO should deal with in the global strategic arena of its time. In the 50s, the meaning of "armed attack" was quite traditional and perfectly clear, consisting in a direct threat to the territorial integrity of a country by a physical attack from traditional armed forces. In the last twenty years, such a meaning has tremendously changed. The first time that the Article 5 was invoked was from the United States after the terroristic attacks at the World Trade Centre in 2001. This evidently implies that the notion of armed attack has evolved from its conventional meaning to a broader more shaded connotation. In the modern world, where the number and kind of threats is increasing and becoming less and less traceable and identifiable, at which stage a cyber-attack could be considered as an action of cyber-warfare able to trigger the reaction foreseen by the Article 5?

The absence of a mutual definition for "critical infrastructure" is not only a problem at a NATO level. To find such a coherent and agreeable definition should be the first step in order to define the tools and the competences that an organization (State or Alliance) has to put in action in order to protect these targets from a cyber-attack. Most of the NATO members do not have a National Action

Plan for the protection of the critical infrastructures, mainly because it is extremely difficult to define such a broad and wide-ranging category. At this stage, each State delineates its own classification of critical infrastructures following its own national security directives. This makes effective defence and coordination often a mirage, given the high level of interconnection among economies, societies and communications technologies.

The last key factor is related to the responsibility to protect the critical infrastructure. On one hand, this task is naturally assigned to the single nation that has been struck. On the other hand, in the vast majority of NATO countries this sector has been privatised, giving private actors the management of critical hubs that could be the target of terrorist attacks. Only by defining the criteria and instruments for a truly global governance it will be possible to effectively prevent cyber threats whether against governmental institutions or private companies.

This calls for a stronger cooperation, not only between national and international organizations, but among the public and private sectors as well. NATO indicates this activity as a crucial element in its policies against cyber menaces; even so, what is necessary right now is to finally define common and detailed regulations able to set a precise responsibility framework.

SEZIONE III
Lo spazio cibernetico e le imprese nazionali

Cyber EW defence capability: ELT approach to future warfare

Daniela Pistoia

(Company Chief scientist – Head of product innovation and advanced EW solution)

Preface

Modern systems (civil, national infrastructures, military) are today more and more based on communication networks without fixed infrastructure, interconnecting complex computing systems (1). The exchange of information and cooperation between these systems occurs by using, as the transmission medium, the Electromagnetic Spectrum (EMS), a resource which, by its nature, is not shielded.

Therefore, a system that makes use of this interface, provides a vulnerability that can be exploited in order to:

- collect sensitive information, which can be used for any operation within the network;
- force the access to the network, to take advantage of the services of the network itself;
- degrade the performance of the network, up to deny the whole service;
- degrade/modify the performance of one or more node of the network, by introducing dedicated data stream and inserting/activating malicious code in the computing system.

The nodes of networked systems physically reside in one of the traditional domains of warfare (air, land, sea, space), but the ability to achieve the objectives of an operational mission cannot be separated from the ability to control and to have freedom of action in cyberspace that, in this sense, is transversal to all other domains. Different wireless or wireless/wired networked systems, both military and civil infrastructures, require different frequencies to

operate effectively. They may use standard protocols and routing rules or ad-hoc infrastructures. Finally, the information exchanged can be clear or encrypted. In all the cases, they can be modeled as a network of computing systems. For a number of years, military operations have used electro-magnetic attacks to disrupt enemy radars on the battlefield, but today the access and manipulation of the EMS and/or the data and information carried by EMS let us foresee many additional capabilities.
In other words, EMS is an entryway for cyber.

Background

Electronic Warfare is a critical enabler for air, land, sea, space and cyber operations.

Cyber Electronic Warfare is warfare in the Cyberspace domain, which is defined as "a global domain within the information environment consisting of the interdependent network of computing systems and information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers."

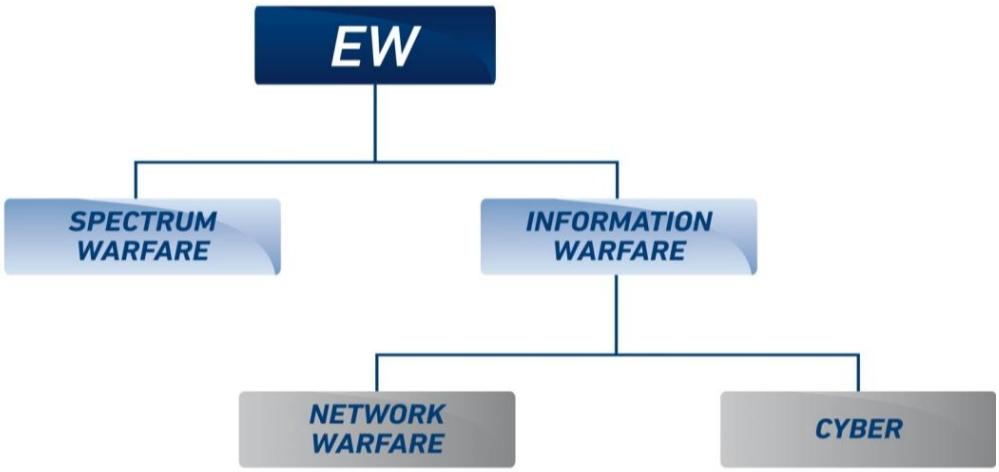


Figure 1 –The new domains of Electronic Warfare

Cyber Electronic Warfare (EW) encompasses Computer Network Operations (i.e., Attack, Defend and Exploit), Information Assurance, and the network operations that encompass Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) and Information Operations (IO) functions that occur within the Cyberspace domain. This includes Computer Network Operations (CNO) against automated systems (e.g. C4ISR), and the interaction between the physical, social and biological networks that define human-machine interaction.

Following the novelty of the concept of operation in this integrated cyber domain, any organization which aim to manage a complete Cyber EW is responsible for functions which include:

- mission analysis;
- assessment and development of technology base;
- continuous state-of-the-art research;
- demonstration of technology;
- engineering in support of production
- support to operating forces;
- supporting doctrine, policy, and strategy development;
- integration of numerous National and Tactical systems in the area of Cyber Warfare.

In the very next future, any Government customer (Ministry of Defense, Ministry of Critical Infrastructures, Ministry of Internal Affairs, etc.) will require advice, assistance, coordination and products necessary to support operational planning, assessment, integration and execution and technology development required to assure superiority for the war-fighter in the Cyberspace domain. Specific activities of interest required to achieve superiority in Cyberspace include, but are not limited to:

- Computer Network Operations (i.e., Attack, Defend and Exploit functions) as they relate to the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers. In particular:
  - Computer Network Attack (CNA) and Computer Network Exploitation (CNE) against automated systems, and the

interaction between the physical, social and biological networks that define human-machine interaction.
  - Information Assurance (IA) and Computer Network Defense (CND) measures to protect and defend Naval, Joint and National systems.
- Cyber Warfare Mission Assurance and Mission Planning.
- Understanding aspects of human behaviour and cognitive functions to influence adversary decision making (e.g. Psychological Operations (PSYOP) and Military Deception (MILDEC)).
- Spectrum Warfare to include Electronic Attack (EA) Electronic Support (ES) and Electronic Protect (EP) in the RF, millimeter wave, and optical environments.
- Monitoring, analyzing and mitigating Operations Security (OPSEC) vulnerabilities.
- Command and Control (C2) of Cyber Warfare capabilities.
- Intelligence, Surveillance and Reconnaissance (ISR) aspects of Cyber Warfare (including Space Operations).
- Ubiquitous Communications and Computing Environment.
- Countermeasures including the capabilities and expertise to develop cyber data management, and methodologies for object correlation and referencing
- Modeling, Simulation and Visualization of the future environment in which communications, computing, data, sensors and networks are interoperable, ubiquitous and transparent to humans.
- Understanding networks as a science and developing models which can provide clarity into how networks operate and resist or deter attack
- Convergence of physical, biological and social networks and how this will effect human interactions and decision cycles.
- Understanding of Cyber Warfare Doctrine, Tactics, Techniques and Procedures.

The work conducted by ELT will support the Italian Armed Forces and other Government agencies in creating capabilities and

providing technical services to support technical and operational activities in the Cyber EW domain.

Scenarios

The scope of Cyber attack is to break one or more of the principles of information security: **(1) Confidentiality, (2) Integrity, (3) Availability**. In this field of operation, **information** is the target and the **infrastructures** are the vehicles through which the information is disseminated.

The electromagnetic spectrum is essential for communications, lethality, sensors and self-protection. Traditional Cyber Warfare aims to achieve objectives in and through cyberspace, while traditional Electronic Warfare aims to control the electromagnetic spectrum or to attack the enemy by its use. These two disciplines may rely on the same information-related capabilities to accomplish these effects, so planners must synchronize and integrate them closely to ensure unity of efforts in words and actions, to:

- collect sensitive information, which can be used for any operation within the network;
- force the access to the network, to take advantage of the services of the network itself;
- degrade the performance of the network, up to deny the whole service;
- degrade/modify the performance of one or more node of the network, by (a) **introducing fake information** inside the network and/or (2) **activating malicious code** in one or more of the computing systems/nodes of the network and/or (3) **inserting malicious code** in one or more of the computing systems/nodes of the network.

Different policy of attack are possible and have to be considered. In general sense, three are the layers where an attack can occur:

- **Attack to the PHYSICAL layer**: the physical layer is the layer where information overlap with the physical world, i.e.

the spectrum itself. An attack to this layer elects the spectrum as the target and the operations in this layer are under the taxonomy of "Spectrum Warfare" (see Figure 1) . Traditional EW against radars or radio links (jamming/deception) is under this category of attack.

- **Attack to the INFRASTRUCTURAL layer**: the infrastructural layer is defined as the one where the information is collected, processed, disseminated and protected, i.e. the protocols and routing rules. An attack to this layer aims to degrade/destroy information flow and to delay/degrade the information quality. Operations in this layer are under the taxonomy of "**Network Warfare**" (see Figure 1).
- **Attack to the COGNITIVE layer**: the cognitive layer is defined as the layer where human decision making process takes place. An attack to this layer has the information itself as the target, aiming to break confidentiality, integrity and/or availability. The final goal is to interact with the decision making process, delaying or denying it. This can be done (1) sniffing information from the network, (2) introducing false information inside the network, (3) taking the control of one or more nodes of the network, by activating malicious sleeping codes or introducing malicious codes inside the computer/computing nodes of the network. Operations in this layer are under the taxonomy of "**Cyber Warfare**" (see Figure 1) .

Of course, the more an operation is conducted from the physical to the cognitive layer, the less is the power required, the smarter/sophisticated is the typology of attack, the higher is the technical/technological challenge. To perform an attack in the cognitive layer, the attacker not only has to be recognized as a node of the network, and this means to overpass the physical and the infrastructural layers, but also to exchange information with the nodes up to establish an interaction with their modes of operation. This last could require a strong effort in terms of cryptanalysis and

reverse engineering both at SW and HW level and a long phase of preparation of the attack.

The following table summarize the convergence of spectrum, network and cyber warfare in Cyber EW operations.

<table>
<tr><th colspan="2">CYBER ELECTROMAGNETIC SPECTRUM OPERATIONS</th></tr>
<tr><td colspan="2">Task: Conduct cyber electromagnetic activities as part of combined spectrum, network and cyber war-fighting operations

Purpose: To seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and across the electromagnetic spectrum, denying and degrading adversary and enemy use of the same and protecting friendly mission command systems</td></tr>
<tr><td>Cyber space Operation</td><td>Electronic Warfare Operation</td></tr>
<tr><td>Task: employ cyber capabilities

Purpose: to achieve objectives in and through the cyberspace</td><td>Task: use electromagnetic energy

Purpose: to control the electromagnetic spectrum or to attack the enemy</td></tr>
<tr><td>Cyber situational awareness: the knowledge of relevant information regarding activities in and through the cyberspace and the electromagnetic spectrum</td><td>Electronic Attack: use of electromagnetic energy to attack facilities or equipment</td></tr>
<tr><td>Network Operations: activities conducted to operate and defend the Global/National/Local Information Grid</td><td>Electronic Protection: actions taken to protect personnel, facilities or equipment from any effects of friendly or enemy use of the electromagnetic spectrum.</td></tr>
<tr><td>Cyber Warfare: warfare that extends cyber power beyond the defensive boundaries of the Information Grid to deny, degrade, disrupt, destroy and exploit enemies</td><td>Electronic Warfare Support: actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of of immediate threat recognition, targeting, planning and conduct of future operations</td></tr>
<tr><td colspan="2">Electromagnetic Spectrum Operations

Planning, coordinating and managing joint use of the electromagnetic spectrum through operational, engineering and administrative procedures</td></tr>
</table>

Table 1: Horizontal and vertical convergence of Cyber and EW operations

ELT response to the new requirements and expanded operational contest to Cyberwarfare, is based on the first command and control (C2) specifically developed for distributed electronic defense system, called LOKI ELT/950, which includes Cyber Electromagnetic Defence capabilities.

For specific Cyber-defense functionalities, LOKI identifies suspect behavior in networked platforms.

If an intrusion is detected, it verifies the identity of the suspect platform and, if necessary, removes it from the network while alerting EW management. LOKI can detect a compromised platform by monitoring data-flow integrity, timing and quantity and other parameters. Suspect behavior triggers additional security challenges to refine the analysis. The system provides a security layer when network is compromised, it identifies and insulates a threat when a breach occurs and reconfigures the network to operate, while bypassing isolated nodes.

Cyber EW Defence user requirements

Following the characteristics of the possible attacks previously described, an effective Cyber EW Defence is based on the capability of:

- monitoring the networks to be defended in the three layers (physical, infrastructural, cognitive) where the attacks could be performed;
- detecting and classifying the type of attack, identifying the nodes under failure;
- decide or suggest appropriate countermeasures

In other words, appropriate assets (HW and SW based) have to be foreseen to accomplish the goal of protecting the networked operations of the deployed platforms.

Typical communication networks and frequency range to be covered are:

- Combat Net Radio-communication systems: typically operating between 30 to 88 MHz, these type of communications are typically used by land forces;

- Radio-communications using airborne emitters (VHF-UHF): Typically operating in two main ranges:
  - 108 to 164 MHz (VHF)
  - 225 to 400 MHz (UHF)
- Radio-navigation systems, ATC in VHF band, radio up/down link used for command and control purposes with unmanned assets:
- Tactical narrowband communication in UHF band (225-450 MHz);
- Tactical data transmission systems or weapon systems: typically spread over 30 to 1300 MHz, in several dedicated bands;
- Tactical systems of transmission through radio relays: typically operating from 500 MHz to 2100 MHz;
- GSM /3G/4G networks (coupled with specific system);
- WiMAX networks

To ensure the defence of the proper wireless network, a comprehensive system of **Cyber Electromagnetic Situation Assessment (CESA)** should be foreseen, operating in the range of frequencies of wireless communication networks.

The primary functions of **CESA** should be:

- to guarantee the monitoring of data and information exchanged among systems and subsystems connected via wireless or wireless/wired networks in terms of integrity, availability and confidentiality; nodes of the monitored networks could be located on the same platform and/or on net-centric operating platforms (other vessels, UAVs, helicopters, maritime patrolling aircrafts, etc.) and could include (but are not limited to) sensors, actuators, command and control nodes, monitoring stations, etc.;
- to evaluate the authenticity of data and information exchanged among the nodes, both at the level of the protocols and of the payload (contents);
- to recognize in real time any anomalous behavior of the nodes belonging to the network under surveillance and/or

the unwanted presence of sources of data non homogeneous or inconsistent (intentional or not intentional);
- to perform a continuous/periodical diagnosis of the networks under surveillance, both passive and active, to evaluate their level of operation;
- to have a logging capability for purposes of post analysis and upgrade of the (Cyber EW) threat database;
- to elaborate different level of alarms, in relation to the event detected and classified, and to suggest (to the C4I, for example, or whatever is the authority designated for the purpose) a set of possible countermeasures (change in frequency management, selection of a different information/data coding, infected node isolation, etc., only as example)

In addition to the tactical assets needed to perform the continuous CESA functionalities, an additional strategic asset should be foreseen:

- **a Digital Laboratory (following the completion of NECTHAR project, already funded by Segredifesa)**, which (1) will support all the phases of the Project for analysis, numerical test and extensive numerical validation activities and (2) will be used by the Government agencies as the main numerical tool for Operational Support tasks in Cyber EW missions.

Conclusions & recommendations

In the next future, the availability of a National Cyber EW capability will have an organizational impact.

A new **Cyber EW Working Group/Command** has to be foreseen, able to integrate and synchronize information related to Cyber EW activity, to achieve desired conditions in cyberspace and the electromagnetic spectrum. The EW Working Group/Command seeks to **unify the offensive and defensive aspects of Cyber EW** (including cyber warfare, network operations, electronic attack, electronic protection, and electronic warfare support). The Cyber EW

Working Group/Command focuses on the commander's stated conditions to gain and maintain advantages for cyberspace and the electromagnetic spectrum.

To this end, the Cyber EW Working Group/Command:

- supports situational awareness related to cyberspace and the electromagnetic spectrum and continually assesses progress toward desired conditions;
- coordinates vertically and horizontally across echelons to achieve the best results from assigned and supporting information-related capabilities;
- integrates all appropriate capabilities (cyber electromagnetic and physical) to achieve these desired conditions

The Cyber EW Working Group/Command may perform the following **integration tasks**:

- Plan, integrate, coordinate, and assess the holistic employment of the full range of Cyber EW capabilities in unit operations;
- Plan and request offensive and defensive Cyber EW capabilities and actions to support the scheme of maneuver, including degraded operations;
- Synchronize and integrate offensive and defensive Cyber EW capabilities and actions into the scheme of maneuver;
- Facilitate and conduct Cyber EW vertical and horizontal integration and synchronization of operations across the war fighting functions (see Table 1);
- Synchronize operations with Cyber EW capabilities in the other domains of warfare (land, sea, air and space);
- Plan, assess, and direct friendly electronics security measures;
- Prioritize Cyber EW effects and targets;
- Deconflict Cyber EW with operations, including intelligence;
- Determine, adjudicate, and forward spectrum user requirements;
- Conduct frequency deconfliction and interference resolution for electronic attack;
- Integrate Cyber EW into the operations process;

- Identify and coordinate intelligence support requirements for unit Cyber EW operations;
- Assess offensive and defensive Cyber EW requirements;
- Maintain current assessment of Cyber EW resources available to the unit;
- Recommend and assess friendly protection measures related to Cyber EW.

A few of the **core capabilities** that must reside within the Cyber EW Working Group/Command to coordinate effectively Cyber EW consist of the following:

- Knowledge of network operations;
- Ability to access intelligence;
- Electronic Warfare;
- Electromagnetic spectrum management (also referred to as spectrum management);
- Employment of offensive Cyber EW and dynamic defense capabilities (such as cryptology capabilities);
- Ability to access support activities (for example, higher-level mission planning capabilities, test and simulation and vulnerability assessment);
- Synchronization and integration.

Note

(1) Following the definition by US DoD, a computing system is a system whose performed functionalities are mainly implemented and/or are enabled by means of programmable devices, which include DSP, FPGA, CPU, GPU and moreover, in terms of physical components, memory devices, interfaces, operating systems and application logics. Personal Computers in their various forms are icons of the contemporary Information Age and are what the most people think of as computing system or computers. However, the embedded computers found in many devices from MP3 players to radars to fighter aircrafts and from toys to industrial robot are the most numerous.

Vitrociset - Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali

Luisa Franchina – Alessia Valentini
(Senior Consultant Cyber Security - System Engineering Cyber Security - VITROCISET)

Introduzione

Durante l'Assemblea della Pennsylvania, dell'11 Novembre 1755, Benjamin Franklin rispose al Governatore dello stato con una frase destinata ad essere una delle citazioni più celebri sul tema dell'equilibrio fra libertà e sicurezza: "Chi è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza non merita né la libertà né la sicurezza".

Il monito di questo celebre giornalista, pubblicista, autore, scienziato, e diplomatico è ancora di grande attualità, perché l'aumento delle minacce legate al terrorismo e alle attività criminali e l'estensione al quinto dominio del cyberspazio, potrebbe indurre ad una cessione delle liberta individuali in favore di maggiori controlli finalizzati alla sicurezza e alla protezione; tuttavia sacrificare le proprie libertà per la propria sicurezza non è una equazione dal risultato certo. Ledere i diritti individuali non garantisce la copertura da qualsiasi minaccia e anzi il protrarsi di uno stato di controllo e di limitazione della popolazione potrebbe favorire lo sviluppo di minacce interne al sistema precostituito. Ricordiamo, infatti, che le recenti stime sul cyber-crime valutano la maggior percentuale di attacchi informatici e di danneggiamenti, quasi il 70%, ad opera dei cosiddetti "insider" ovvero individui che pianificano e attuano un attacco dall'interno della realtà di cui loro stessi fanno parte. E uno stato protratto di insoddisfazione causato dalla limitazione personale potrebbe scatenare simili conseguenze. Dunque il corretto bilanciamento fra tutela delle libertà personali e garanzia della sicurezza dello Stato è una condizione irrinunciabile di qualsiasi intervento di protezione. In sostanza si tratta di due facce della stessa medaglia che devono essere sempre viste come un sistema

unico in cui nessuna delle due facce deve mai essere completamente coperta.

Da queste considerazioni d'impostazione, discende un approccio orientato alla sicurezza capace di tutelare le persone e proteggerle allo stesso tempo e con esse anche i rispettivi dati personali, sensibili e privati. Sono necessari strumenti tecnologici adeguati, ma coadiuvati da una opportuna organizzazione, da procedure e processi e soprattutto dalla formazione poiché l'individuo è ancora e sempre considerato nell'ambito della difesa come "il primo sistema d'arma", ma opportunamente informato, equipaggiato e addestrato diventa "il primo sistema di difesa e prevenzione".

Il quadro Europeo

Dopo l'attentato a Charlie Hebdo, in Europa si distinguono due diversi orientamenti: da un lato, il primo ministro inglese J. Cameron che si batte contro il criptaggio delle app telefoniche, non consentendone il controllo ai Servizi Segreti. Cameron chiede anche un provvedimento di emergenza per continuare la conservazione dei dati (Direttiva del 2006) invalidata recentemente dalla Corte di Giustizia Europea proprio per non consentire più l'accesso delle informazioni da parte dei Governi. L'altro lato è costituito da tutte quelle figure che chiedono un maggior controllo democratico sui servizi di intelligence invocando lo stop alla sorveglianza.

Dopo il Datagate l'Europa è decisa a tutelare i dati dei suoi cittadini rinegoziando l'accordo Safe Harbor del 2000, grazie al quale le aziende americane riescono a trasferire i dati europei fuori confine, prestando di fatto il fianco alla sorveglianza. Sempre in linea con le tutele della privacy, la Corte di Giustizia ha anche emesso la sentenza sul "diritto all'oblio", che in sostanza garantisce di poter scomparire da internet e dai motori di ricerca che la interrogano. Nel 2015, infine, si dovrebbe concludere l'iter per rimpiazzare la vecchia direttiva 95/46/EC sostituita da un regolamento comune per la protezione dei dati, l'"European Data Protection Regulation". Nella nuova disciplina lo sforzo è quello di adeguare la legge agli sviluppi tecnologici, al mondo dei social e dei

big data, ma anche quello di rafforzare le tutele sui dati dei cittadini europei proteggendoli anche nei confronti delle compagnie e organizzazioni che non hanno sede nell'UE.

In conclusione l'Europa si è sempre distinta per la sua legislazione a tutela dei diritti, e proprio dalla Corte potrebbe arrivare la risposta: più sicuri non significa meno protetti.

In questo scenario assume un peso significativo la nona giornata della Privacy celebrata il Italia il 28 Gennaio 2015, e promossa dal Consiglio d'Europa con il sostegno della Commissione UE e di tutte le Autorità Europee per la protezione dei dati personali, in cui è stata ricordata l'importanza dei diritti legati alla tutela della riservatezza, della dignità della persona e delle libertà fondamentali. L'Italia, come gli altri paesi dell'Unione, dovrà adeguarsi alle nuove direttive a livello normativo e tenerne conto nelle implementazioni tecnologiche che sono necessarie alla transizione verso la PA Digitale. Questo significa che anche le aziende italiane chiamate a supportare il processo di innovazione delle Pubbliche Amministrazioni centrali e locali, compresi gli apparati della Difesa e delle PMI nazionali, dovranno adottare un approccio allineato con la legislazione, che sia anche rispettoso del bilanciamento fra gestione dei dati e loro protezione della RID (Riservatezza, Integrità, Disponibilità). In particolare nello scouting e adozione di prodotti innovativi esteri in tema di sicurezza informatica, è necessario preoccuparsi della localizzazione italiana poiché diversamente sarebbero implementate soluzioni troppo spinte sul versante del controllo ma lesive della normativa sulla privacy.

Approcci di altri paesi

Negli altri Paesi si è assistito a scelte diverse che seguono una delle tre linee di indirizzo: regolamentare, cooperativo o misto.
L'approccio regolamentare è basato su normative che prevedono l'obbligo di attività di analisi dei rischi, prevenzione e preparazione alla gestione di crisi. Le controindicazioni a questo tipo di approccio sono diverse e ad esempio gli Stati Uniti hanno risolto molti di questi problemi normando, a livello generalista, le richieste di sicurezza e protezione cui devono sottostare le infrastrutture "altamente

critiche" e "critiche": i livelli minimi non vengono riportati nella norma, bensì gli operatori sono obbligati ad attenersi agli *standard* elaborati dall'organismo federale di standardizzazione (NIST) preposto a studiare, confrontare e ideare standard di sicurezza e buona pratica (le regole d'arte e le tecniche più avanzate di qualità e di sicurezza nella realizzazione di prodotti e servizi) e a riportarne le relative descrizioni sotto forma di atti di riferimento pubblici.

L'approccio cooperativo si basa su assenza o comunque riduzione massiccia di regole generaliste in favore di meccanismi di cooperazione pubblico-privato e su standard *de facto*. La Gran Bretagna è pioniera di questo meccanismo organizzativo con il quale ha raggiunto ottimi livelli di co-investimento pubblico-privato ed efficacia nella protezione del Sistema Paese.

Infine, il sistema misto, integra meccanismi regolamentari (anche blandi o privi di sanzioni) e meccanismi di cooperazione (volontaria o parzialmente obbligatoria) pubblico-privata. Contrariamente a quanto può sembrare, tale scelta è la più articolata da realizzare. L'Unione Europea ha optato per questa scelta nella emanazione della direttiva 114/08CE: alla identificazione e designazione di infrastrutture critiche europee consegue, secondo la direttiva, una attività di controllo da parte delle Autorità competenti nazionali piuttosto "blanda" che, tuttavia, pone le basi per ulteriori attività di tipo cooperativo non obbligatorio, a scelta e discrezione dei singoli Stati membri.

DPCM e contesto italiano

Gli individui, le imprese e il governo usufruiscono dei molti vantaggi che il Ciberspazio offre e al contempo in questo nuovo "territorio" vengono esposti a nuove forme di strumenti di minaccia (e a nuove intrinseche vulnerabilità dello spazio medesimo): tale minaccia si concretizza in attacchi che possono essere perpetrati da individui, gruppi e stati per colpire valori come la sicurezza nazionale, la prosperità economica, il mantenimento della legalità e lo stile di vita.

Nel gennaio 2013 il Presidente del Consiglio pro-tempore ha emanato il DPCM recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

Il decreto realizza l'obiettivo di definire un'architettura istituzionale per la sicurezza delle Infrastrutture Critiche (IC) materiali e immateriali relativamente agli aspetti cibernetici ed informatici, con l'indicazione di compiti, meccanismi e procedure per ridurre le vulnerabilità, prevenire i rischi, dare risposta tempestiva ad aggressioni e ripristinare immediatamente le funzionalità dei sistemi in caso di crisi.

Con questo provvedimento e con la successiva adozione del Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico e del Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica nazionali (emanati a inizio 2014), l'Italia si confronta con una serie di nuovi scenari riguardanti lo spazio cibernetico, avendo chiaro l'obiettivo di perseguire *strategie ben definite*.

Tuttavia si fa notare che le linee guida del Quadro e del Piano Nazionale, finalizzate a fornire le priorità in termini di dotazioni di sicurezza e di azioni preventive sono perfettamente equilibrate fra l'esigenza di tutela e protezione dalle minacce e il requisito di salvaguardia della privacy.

L'Approccio di Vitrociset

Vitrociset è una azienda che da oltre quarant'anni opera in vari settori, Defence, Joint Operations, Homeland Security, Space, Transport, Utilities, Government, e ha una profonda conoscenza dei settori pubblico e privato. La sua mission è dedicata a sistemi mission critical, verso i quali ha una particolare gamma di soluzioni tutte basate sulla capacità di essere flessibile e custom oriented. È presente con 5 sedi in Italia e 9 all'estero (Belgio, Olanda, Germania, Turchia, Arabia Saudita, Kenya, Guyana Francese, Malesia).

L'azienda investe il 10 % del proprio utile in Ricerca e Sviluppo e nello scouting tecnologico di soluzioni innovative.

Per rispondere in modo pienamente conforme e ottimizzato alle richieste dei suoi clienti sia in ambito civile che in ambito militare, Vitrociset ha certificato la sua attività adottando diversi sistemi di gestione:

UNI EN ISO 9001:2008
QUALITY MANAGEMENT SYSTEM

QUALITY MANAGEMENT SYSTEM
NATO COMPLIANCE (AQAP 2110/160)

UNI EN ISO 14001:2004
ENVIRONMENTAL MANAGEMENT SYSTEM

PUBLIC SECTOR CONTRACTS AUTHORIZATION

UNI EN ISO 27001:2005
INFORMATION SECURITY MANAGEMENT SYSTEM

COMMUNICATION OPERATORS AUTHORIZATION

BS OHSAS 18001:2007
HEALTH AND SAFETY MANAGEMENT SYSTEM

CAPABILITY MATURITY MODEL INTEGRATION: LEVEL 2
(Level 3 expected in late 2013)

Vitrociset ha sviluppato competenze specifiche nell'ambito della sicurezza nazionale, grazie alla realizzazione di una serie di progetti atti a rispondere alle istanze espresse dal settore pubblico.
L'offerta in ambito sicurezza coinvolge tutte le Business Unit Aziendali, dalla Difesa all'Homeland Security, dallo Spazio e Trasporto al Government & Industries che adottano approcci e soluzioni in dual use. Gli ambiti applicativi riguardano la prevenzione dei rischi, l'identificazione delle minacce e la reazione agli attacchi proteggendo con la massima efficacia infrastrutture, luoghi, persone e informazioni.

Nella sfida per la sicurezza nazionale Vitrociset contribuisce alla gestione delle frontiere, alla difesa delle infrastrutture critiche, alla salvaguardia del territorio, alla tutela dell'ordine pubblico e alla sicurezza dei trasporti, perché nelle implementazioni progettuali adotta capacità di controllo ampio e capillare, supportata da moderne reti di comunicazione resilienti, sicure e multiservizio. Allo scopo sono state sviluppate soluzioni in grado di estendere le

potenzialità operative dei Clienti a ogni dominio, dalla terra al mare, dai cieli allo spazio, incluso il dominio cibernetico.

La sicurezza fisica non può, infatti, prescindere dalla sicurezza del Cyber Spazio perché nessuna minaccia può essere considerata, semplicemente, virtuale.

L'offerta di sicurezza informatica integra strumenti, metodologie e risorse per rispondere, in maniera efficace, innovativa e cost-effective, alle crescenti esigenze di sicurezza e difesa del Cyberspace preservando le esigenze di tutela della privacy a norma di legge e rispondendo pienamente agli orientamenti e alle linee guida espresse dalla Corte Europea.

Le soluzioni di sicurezza informatica riguardano la protezione contro minacce di tipo 0-day, la protezione di sistemi SCADA nell'ambito del tema più generale di protezione delle Infrastrutture Critiche, la Cyber Intelligence in ambito OSINT e un'ampia gamma di servizi professionali erogati da professionisti del settore.

Per il supporto alla formazione e all'addestramento per le esercitazioni di sicurezza informatica, in ambiente simulato e modellizzato, Vitrociset dispone anche di una specifica piattaforma customizzabile, grazie alla quale è possibile aumentare la human readyness ossia la consapevolezza, la conoscenza e la prontezza nella risposta ad attacchi mirati.

SEZIONE IV
Lo spazio cibernetico nella visione dall'estero

Come garantire nella fase attuale la sicurezza informatica internazionale (Federazione Russa)

A.V. Krutskikh

(Ambasciatore con incarichi speciali Rappresentante speciale del Presidente della Federazione Russa per la collaborazione internazionale nel campo della sicurezza informatica)

L'impiego di moderne tecnologie dell'informazione e della comunicazione (ICT) minaccia in maniera sempre più diretta la sicurezza di cittadini, società e stati e il danno che esse possono provocare può essere equiparato a quello degli armamenti più distruttivi. Tutti i paesi, senza eccezione alcuna, riconoscono la gravità delle minacce di natura criminale, terroristica e politico-militare nel cyberspazio. Molti si sono già scontrati con questa sfida sul piano pratico e hanno sperimentato la gravità delle conseguenze.

La situazione politico militare nel cyberspazio si sta aggravando. Si è assistito al passaggio a un nuovo livello tecnologico che consente l'uso delle ICT come armi offensive. Nel settembre del 2010 l'attacco agli impianti nucleari iraniani di Natanz e Bushehr, con l'impiego del virus Stuxnet ha dimostrato che le ICT sono di fatto utilizzabili per scopi bellici. Come è già avvenuto più volte, la comparsa di una nuova tecnologia fortemente innovativa, in grado di fornire vantaggi militari senza precedenti, altera l'equilibrio geopolitico consolidato. I possessori di tale tecnologia sono allettati dall'idea di utilizzarla nei confronti di un nemico che non disponga di tali strumenti. Quest'ultimo dunque sarà costretto a entrare nella corsa ai cyber-armamenti. Oltre 130 stati al mondo stanno incrementando il proprio potenziale per sostenere guerre informatiche o cyber-guerre. Questo significa che la militarizzazione del cyberspazio è in sostanza già iniziata.

In tale contesto assistiamo allo scontro tra due fondamentali concezioni politiche dell'utilizzo globale delle ICT: la prima, che in sostanza può essere definita "militarista", è rappresentata in maniera netta dagli USA e dai suoi più fedeli alleati,"pionieri" della colonizzazione militare dello spazio informatico. Essi stanno dando vita a reparti speciali di cyber-truppe stanziando fondi significativi per il settore ed elaborando i relativi fondamenti dottrinali.

Nel maggio del 2011 il Presidente degli Sati Uniti ha ratificato la "Strategia internazionale per il cyberspazio" nella quale si sostiene che gli USA reagiranno ai cyber-attacchi esattamente come a ogni altra minaccia diretta alla loro sicurezza nazionale e adotteranno quindi ogni tipo di iniziativa di risposta, ivi compresa quella militare. Nel 2013 è stata emessa una direttiva indirizzata al Cyber Command delle Forze Armate degli USA sulle norme di conduzione delle cyber-operations (rules of engagement) che prevede l'adozione di misure "proporzionali" in caso di cyber-attacco proveniente dall'estero. Con misure proporzionali, i vertici americani intendono una risposta al cyber-attacco con ogni tipo di arma.

Alcuni paesi si pronunciano già apertamente in merito alla propria transizione nel cyberspazio dalla difesa all'attacco. Nell'ottobre 2013 il Ministro della difesa britannico ha dichiarato pubblicamente l'intenzione del suo paese di incrementare il proprio cyber-potenziale offensivo al fine di svolgere operazioni elettroniche e azioni militari contro i nemici dell'arena internazionale.

Nella dichiarazione finale del summit NATO, svoltosi in Galles nel settembre 2014, sono già esposti in maniera sistematica i preparativi militari dell'Alleanza nell'ambito informatico delle azioni militari. Per la prima volta il blocco ha posto la questione dell'applicazione del principio della difesa collettiva (articolo 5 dell'Accordo di Washington) in risposta a un cyber-attacco, fatto che ci pare un esempio della logica della contrapposizione.

Tuttavia tali disposizioni della dichiarazione del Galles non sono state una sorpresa in quanto la NATO da tempo sta cercando di elaborare fondamenti teorici di questo approccio secondo la linea indicata dal Centro di Sperimentazione Avanzata nella Cyber-difesa di Tallin. Il "Manuale di diritto internazionale applicato alla

realizzazione di azioni militari nel cyberspazio" ("Tallin Manual") pubblicato nel 2013, costituisce un esempio di elaborazione del quadro giuridico di regolamentazione degli atti di aggressione nel cyberspazio. Di fatto non si tratta solo di un tentativo di legalizzare la militarizzazione dello spazio informatico (creare le norme di conduzione della guerra), ma anche di gettare le basi della contrapposizione tra blocchi, questa volta nella sfera delle ICT. Il suddetto documento pone l'accento sull'applicabilità nel cyberspazio delle norme del diritto valide in ogni altro ambito: marittimo, aereo e terrestre, e di conseguenza, si sostiene la tesi secondo la quale è ammissibile un'operazione di forza in risposta a un cyber-attacco.

In questo contesto sorge tutto un insieme di questioni che non hanno una risposta univoca. Infatti non tutte le azioni di forza, anche nel senso tradizionale del termine, danno il diritto a una risposta militare. Nell'ambito delle "cyber-guerre" è particolarmente complesso stabilire con certezza sia i motivi degli attacchi informatici, sia la fonte della minaccia (strutture statali, comunità di hacker, soggetti singoli), elementi essenziali a ingenerare il diritto all'autodifesa. A nostro parere il diritto al ricorso ad azioni militari può essere fondato solo nei casi in cui sia oggettivamente stabilita la partecipazione di un altro stato o di un gruppo terroristico all'attacco a seguito del quale si verifichino o possano inevitabilmente verificarsi grandi sciagure, distruzioni e vittime umane.

La reazione di difesa di uno stato nell'ambito dell'autodifesa deve essere sempre proporzionata e commisurata all'attacco ricevuto. Risulta quindi incomprensibile come questa proporzionalità possa essere garantita in caso di risposta a un cyber-attacco. Le azioni di risposta possono uscire dai confini del cyberspazio, la forza deve essere esercitata esclusivamente contro il responsabile (reti, server ecc.) oppure in misura più ampia?

È evidente che questa lacuna giuridica del diritto internazionale in merito ai cyber-conflitti può potenzialmente contribuire alla escalation dei cyber-incidenti in vere e proprie guerre o aggressioni con l'utilizzo praticamente di qualsiasi tipo di arma.

La Russia per parte sua contrappone all'approccio descritto il concetto di prevenzione dei conflitti in ambiente informatico e di rinuncia da parte degli stati all'uso della forza nel cyberspazio. A questo fine noi avanziamo una serie di concrete iniziative di pace, tra le quali la proposta di definire regole o principi di condotta responsabile degli stati nel cyberspazio. La loro messa a punto e adozione da parte della comunità internazionale sotto l'egida dell'ONU, costituirebbe il primo passo nella de-escalation della tensione nella sfera digitale.

Un significativo contributo è stato offerto alla costituzione di una base ideologica dell'attività di politica estera nell'ambito della sicurezza informatica internazionale. Nel luglio 2013 il Presidente della Federazione Russa ha ratificato le "Linee guida della politica statale della Federazione Russa nel campo della sicurezza informatica internazionale fino al 2020". Si tratta di un documento di pianificazione strategica che definisce gli obiettivi fondamentali, gli indirizzi e i parametri dell'attività degli organi federali del potere esecutivo per il rafforzamento della cyber-sicurezza nazionale russa e globale. Le "Linee guida" contengono una serie di determinazioni essenziali nell'ambito dell'utilizzo delle ICT. In particolare "la sicurezza informatica internazionale" viene definita come quella condizione dello spazio informatico globale che escluda la possibilità di violare i diritti delle persone, della società e dello stato nel cyberspazio. In conformità con le "Linee guida", l'obiettivo della politica statale della Federazione Russa consiste nel collaborare a stabilire un regime giuridico internazionale indirizzato a creare le condizioni per la formazione di un sistema di sicurezza informatica internazionale che non si basi sulla contrapposizione.

Le "Linee guida della politica statale" riflettono l'orientamento della Russia a prevenire l'utilizzo delle ICT per fini bellici a differenza di altre concezioni che contemplano la regolazione di conflitti nello spazio informatico e quindi, in sostanza, la loro legittimazione.

Una non meno importante iniziativa volta all'utilizzo pacifico dello spazio informatico è la concezione della convenzione per garantire la sicurezza informatica internazionale. Il documento è stato presentato dalla parte Russa all'incontro internazionale degli

alti rappresentanti responsabili per la sicurezza tenutosi a Ekaterinburg nel 2011. La Concezione della convenzione, così come le "Linee guida", costituisce materia di riflessione su come potrebbe essere redatto un trattato internazionale universale in questo settore. Al momento il documento è aperto a osservazioni e proposte da parte di tutti i paesi interessati ed è regolarmente discusso a livello dei consiglieri per la sicurezza nazionale.

La Russia sta costruendo con successo collaborazioni bilaterali nell'ambito della sicurezza informatica internazionale con una serie di partner internazionali strategici.

Nel giugno 2013 durante il summit del G8 di Lough Erne, per la prima volta nella storia delle relazioni russo-americane, è stata adottata una dichiarazione congiunta dei presidenti di Russia e USA su un nuovo campo di collaborazione per il rafforzamento della fiducia: l'utilizzo delle ICT. Contemporaneamente furono stipulati tre accordi bilaterali fortemente innovativi per portata che costituiscono un sistema di misure pratiche per il rafforzamento della fiducia nel cyberspazio. I nostri capi di stato definirono quegli accordi senza precedenti per il loro contenuto. I mass media internazionali battezzarono immediatamente quei documenti "patto sulla cyber-non aggressione" tra Russia e Usa. Tuttavia stupisce il fatto che, una volta stipulati quegli accordi importanti e utili per la sicurezza bilaterale e internazionale, Washington, attraverso l'imposizione ai suoi più prossimi alleati, ai partner europei - come da loro stessi riconosciuto - della nota politica delle sanzioni, esercita su di loro una pressione volta alla "salvaguardia" non solo dalla definizione di simili misure di fiducia con la Russia, ma anche dalla possibilità di instaurare con noi un vero dialogo bilaterale sulla problematica della sicurezza informatica. In questa maniera gli Stati Uniti incrementano la "inferiorità" politica dei propri satelliti dal punto di vista della garanzia della propria sicurezza e dell'elaborazione delle relative misure di fiducia.

A livello multilaterale, una delle iniziative chiave nell'ambito della sicurezza informatica internazionale è stata l'approvazione nel giugno del 2013 del Rapporto conclusivo del Gruppo degli esperti governativi dell'ONU sulla cyber-sicurezza internazionale. Il

Rapporto del Gruppo è un importante documento politico che sancisce il comune interesse delle nazioni all'utilizzo pacifico delle ICT. Il principale successo così ottenuto consiste nel fatto che il Rapporto è orientato alla prevenzione dell'utilizzo delle ICT per fini incompatibili con lo Statuto dell'ONU.

Durante la discussione nel gruppo di esperti si sono evidenziate con grande chiarezza le differenze tra due linee e cioè la prevenzione dei conflitti o la creazione di una base giuridica internazionale che li disciplini. La formulazione conclusiva del Rapporto in questo contesto prevede un ragionevole compromesso. Riconoscendo la generale applicabilità delle norme e dei principi del diritto internazionale, in primo luogo dello Statuto dell'ONU, agli atti commessi dagli stati nel cyberspazio, il gruppo di esperti ha sottolineato la necessità di un ulteriore approfondimento di come tali norme debbano essere applicate alla condotta degli stati nella sfera di utilizzo delle ICT. Con il tempo potranno essere elaborate norme supplementari.

Il documento stabilisce che la sovranità nazionale si estende alle azioni degli stati nella sfera di utilizzo delle ICT nonché alle infrastrutture delle ICT site sul loro territorio. Inoltre sancisce la responsabilità dello stato per le azioni commesse in questa sfera che siano in contrasto con il diritto internazionale, e l'obbligo ad adoperarsi per prevenire l'utilizzo delle ICT dal suo territorio per fini illegali.

I vertiginosi cambiamenti nello spazio informatico e la crescente minaccia della sua militarizzazione determinano la necessità di elaborare al più presto le regole per un comportamento responsabile degli stati nell'utilizzo delle ICT. Proprio per questo la Russia, insieme agli stati membri dell'Organizzazione di Shanghai per la Cooperazione (SCO) e ai partner di BRICS e CSI, promuove attivamente nell'arena internazionale le iniziative di pace volte a prevenire la contrapposizione politico-militare nella sfera di impiego delle ICT. Nel settembre 2011 quale documento ufficiale della 66° sessione dell'Assemblea Generale dell'ONU, i paesi membri di SCO diffusero, attraverso il Segretario Generale, un documento congiunto, sotto forma di progetto di risoluzione dell'Assemblea

Generale, intitolato "Regole di condotta nel campo della garanzia della sicurezza informatica internazionale". Scopo di questa azione era quello di stimolare un'ampia discussione internazionale su tale problematica a livello mondiale. In assenza di trattati internazionali universali che regolamentino le relazioni tra gli stati nella sfera della cyber-sicurezza il primo passo nella costruzione di un sistema internazionale di sicurezza in questa sfera potrebbe essere l'adozione di determinati principi o norme di condotta in forma di "soft law". Proprio questo è l'obiettivo che si sono posti i paesi SCO nell'elaborazione delle "Regole di condotta". Attualmente il documento è aperto a proposte ed emendamenti da parte di tutti i paesi coinvolti. Si è registrata la reazione interessata di molti dei nostri partner, la maggior parte dei quali appoggia l'idea fondamentale dell'iniziativa: prevenire i conflitti e le aggressioni nel cyberspazio al fine di conservarlo pacifico e libero.

Tali iniziative di prevenzione dei conflitti nel cyberspazio sono di giorno in giorno più attuali. La politica e i politici devono anticipare il progresso tecnico e trovare le necessarie soluzioni prima che le tecnologie generino una nuova realtà e conferiscano alla contrapposizione politica nuove forme tecniche ancora più distruttive.

Le misure di rafforzamento della fiducia sono una condizione importante per prevenire le situazioni di potenziale conflitto nella sfera di utilizzo delle ICT.

In questo campo l'OSCE sta svolgendo un lavoro prezioso. Il processo negoziale in tale direzione ha dimostrato la possibilità di raggiungere un compromesso nella formulazione di misure efficaci e fattive di reale fiducia e costruttiva collaborazione che tengano in considerazione le opinioni di tutte le parti coinvolte. Grazie al dinamismo della presidenza americana nel relativo gruppo di lavoro e al costruttivo contributo della Russia e di altri paesi, in ambito OSCE si è riusciti a progredire nel processo di elaborazione delle misure di rafforzamento della fiducia. Nel dicembre del 2013 nell'ambito del Consiglio dei ministri degli esteri dell'OSCE è stato adottato un documento consolidato: l'Elenco delle misure iniziali di rafforzamento della fiducia nell'impiego delle ICT.

È di essenziale importanza che la costruzione di misure per il rafforzamento della fiducia nell'utilizzo delle ICT da Vancouver a Vladivostok non susciti l'allarme di altri paesi, che queste misure siano compatibili con ciò che si sta facendo in questa direzione in altre regioni e nell'ambito delle organizzazioni e dei forum internazionali, in primis sotto l'egida dell'ONU. La "regionalizzazione" delle misure di fiducia, a nostro parere, ne impedirà l'efficacia e sarà controproducente dal punto di vista politico. Pur tuttavia il successo dei paesi europei nella formazione del meccanismo delle misure di fiducia nello spazio informatico ha già ispirato i nostri partner nell'Associazione delle Nazioni del Sud-est asiatico (ASEAN) nell'ambito della quale si sta svolgendo un lavoro analogo per elaborare misure di fiducia applicabili nella regione Asia e Pacifico.

Uno dei temi più attuali legati alla sicurezza informatica internazionale sostenuti attivamente nelle arene internazionali è il cosiddetto "incremento del potenziale". Non ci sono dubbi che sia necessario rispettare le necessità dei paesi in via di sviluppo di superare "il gap digitale", tuttavia l'attuazione di questa tematica richiede da tempo di essere concretizzata. A tutt'oggi non vi è certezza su come superare la preoccupazione dei potenziali paesi-riceventi rispetto alle condizioni di ricevimento dell'aiuto tecnologico e delle possibili conseguenze negative sulla loro sovranità e stabilità sociale. In questo senso è importante garantire che i programmi di "incremento del potenziale" non vengano usati per coprire l'ingerenza negli affari interni e la violazione della sovranità dei paesi riceventi il sostegno. D'altro canto, per i paesi donatori è importante assicurarsi che le tecnologie e le competenze trasferite non vengano in seguito usate contro loro stessi. Ecco perché anche il tema dell'incremento del potenziale nel campo della cyber-sicurezza richiede un attentissimo studio e un equilibrato approccio universale.

La correlazione tra gli elementi della triplice minaccia (militare, criminale e terroristica) nell'ambito dell'utilizzo delle ICT spiega in gran parte le difficoltà di cui è costellato il cammino della costruzione di una base giuridica di diritto internazionale per la lotta alla criminalità nello spazio informatico.

Negli anni '90 i paesi occidentali hanno preso l'iniziativa di elaborare un progetto di convenzione del Consiglio d'Europa sulla cyber-criminalità. Il documento è aperto alla firma dal 2011 ed è più noto con il titolo ufficioso di "Convenzione di Budapest". Oggi in una serie di paesi questo documento è considerato l'unico strumento di diritto internazionale nel campo della lotta alla criminalità nella sfera di utilizzo delle ICT ed è in atto un tentativo di globalizzarlo.

Negli ultimi anni è risultato evidente che la Convenzione del Consiglio d'Europa, elaborata ormai negli anni 1997-2001, quando il grado di evoluzione delle ICT era ancora piuttosto basso, è significativamente obsoleta. In quel periodo molti tipi di minacce in rete o erano sconosciuti oppure non ricevevano la dovuta attenzione. La Convenzione di Budapest individua solo 9 tipi di utilizzo illegale delle ICT, mentre ad oggi già si registrano più di 30 tipi di tali violazioni delle leggi. In particolare, la Convenzione non regolamenta le questioni legate all'utilizzo da parte di malfattori delle cosiddette "botnet (reti di computer infettate da malware che consentono la realizzazione remota di varie azioni illegittime). A titolo di esempio possiamo citare anche l'assenza nella Convenzione di qualsiasi riferimento all'adozione di misure contro lo spam, il "phishing" ecc… Nella Convenzione non viene neanche citato un fenomeno tanto pericoloso quale il cyber-terrorismo.

Tuttavia il problema fondamentale che rende impossibile l'adesione alla Convenzione di Budapest della Russia, dei paesi BRICS e del resto della stragrande maggioranza dei paesi del mondo (in oltre dieci anni di esistenza la Convenzione è stata ratificata solo da 39 paesi, essenzialmente occidentali, e neanche tutti, e dai loro satelliti più prossimi) consiste nell'inaccettabilità dell'approccio contenuto al punto "b" dell'Articolo 32 del documento. Infatti questo punto consente, con il pretesto di svolgere indagini, la possibilità di infiltrazione transfrontaliera nel cyberspazio dei paesi membri della Convenzione anche senza informare gli organi competenti di questi stati.

Le disposizioni della Convenzione di Budapest in questo modo fanno carta straccia del concetto stesso di sovranità nazionale e

creano un terreno fertile per la violazione dei diritti fondamentali e delle libertà dell'uomo e, in particolare, del diritto alla privacy.

Si tratta di un tema che acquisisce particolare attualità, tenuto conto delle rivelazioni fatte da E.Snowden di documenti segreti dell'Agenzia per la sicurezza nazionale degli USA che hanno fatto luce sulla portata e sul carattere delle attività illegali svolte dai servizi di intelligence americani, britannici, svedesi e di altre nazioni nel campo dell'utilizzo delle ICT. Di fatto hanno creato un sistema globale di rilevamento e trattamento dei dati personali degli utenti. Sorge il sospetto che la Convenzione di Budapest fosse di fatto deputata a legalizzare le azioni dell'intelligence americana nei confronti degli stati membri e dei loro cittadini. Infatti, nella concezione della Convenzione di Budapest l'unica condizione all'accesso ai dati dei cittadini di altri stati è il consenso del provider dei servizi di comunicazione o di qualsiasi altra società coinvolta nel trattamento dei dati. Come è emerso dalle rivelazioni di E.Snowden, i servizi americani per raccogliere informazioni nell'ambito del progetto "Prism", collaborano strettamente con le compagnie leader del settore. L'agenzia ha accesso ai server centrali delle società Microsoft (Hotmail), Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple. Questa collaborazione ha consentito ai servizi di intelligence di esaminare e analizzare la cronologia internet, le mail degli utenti e di seguire la trasmissione di file sia sul territorio degli USA sia al di fuori dei confini del paese. Alla luce della Convenzione di Budapest tali azioni nei confronti dei propri membri sono da considerarsi sostanzialmente legali.

Per la Russia il tema del rispetto dei diritti dei cittadini e della libertà di accesso a Internet è questione prioritaria. È necessario chiarire che il rispetto dei diritti della persona può essere garantito solo osservando rigorosamente i principi della sovranità nazionale e della non ingerenza negli affari interni di uno stato. La negazione di limiti legali in Internet, la trasformazione della libertà in Internet in un principio assoluto, creano un'atmosfera di "tutto è consentito" che a sua volta sortisce un effetto opposto e cioè porta alla crescita delle violazioni dei diritti della persona in rete. In questo contesto non perde di attualità il Patto Internazionale sui diritti civili e politici

del 1966, il cui articolo 19 prevede talune restrizioni dell'esercizio delle libertà al fine di rispettare i diritti e la reputazione altrui, tutelare la sicurezza nazionale, l'ordine pubblico, la sanità o la morale pubbliche.

L'approccio proposto dalla Russia consiste nell'elaborare sotto l'egida dell'ONU una Convenzione per il contrasto del crimine nell'utilizzo delle ICT che per contenuto e per geografia di impiego deve avere un carattere universale, considerare le realtà di tutti gli stati senza eccezione alcuna e deve fondarsi sui principi dell'uguaglianza sovrana delle parti e della non ingerenza negli affari interni degli stati.

Concepiamo la bozza di questa Convenzione come un documento multilaterale di diritto internazionale che rifletta la natura dei crimini nel campo dell'utilizzo delle ICT. Nell'elaborazione di tale documento è necessario tenere in considerazione in particolare la Convenzione dell'ONU contro la corruzione, la Convenzione dell'ONU contro la criminalità organizzata transnazionale, nonché una serie di convenzioni globali sull'antiterrorismo; e inoltre tenere presenti le disposizioni della menzionata Convenzione di Budapest escludendone i difetti e le odiose norme.

La Russia ambisce a sviluppare contatti bilaterali sulla questione della sicurezza informatica internazionale con tutti coloro che siano disponibili a tale dialogo. Oltre ai nostri partner in SCO, BRICS e CSI, collaboriamo da tempo e fruttuosamente con USA, Francia, Germania e Repubblica di Corea. Oltre a realizzare regolarmente consultazioni tra esperti, molti paesi europei sono interessati a stipulare con noi accordi pratici sulle misure di fiducia in questa sfera.

Russia e Italia possiedono un grande, ma non sfruttato, potenziale di collaborazione bilaterale nel campo della sicurezza informatica internazionale rispondente agli interessi della sicurezza nazionale di entrambi i nostri paesi. In questo contesto Russia e Italia hanno già maturato un'esperienza positiva di collaborazione nell'ambito del G8: nel 2010, grazie fra l'altro all'attiva partecipazione e al contributo costruttivo della delegazione italiana,

si è riusciti a definire nella dichiarazione di Dauville del G8 il problema della gestione e dell'utilizzo politico di Internet. La Russia per parte sua è tradizionalmente incline a stabilire un dialogo reale e plurisettoriale con l'Italia per tutta la gamma dei problemi della sicurezza informatica nonostante la contro produttiva politica sanzionatoria imposta da Washington e la dottrina da tempi di "guerra fredda".

Lo Spazio Cibernetico tra Esigenze di Sicurezza Nazionale e Tutela delle Libertà Individuali (Australia)

Mike Rann

(Ambasciatore d'Australia in Roma)

L'Australia è all'avanguardia nel dibattito sullo spazio cibernetico grazie ad un'economia tecnologicamente avanzata e all'attuazione della rete nazionale a banda larga (National Broadband Network), un progetto volto ad aggiornare l'attuale infrastruttura di telefonia fissa,e facilitare la transizione dell'Australia verso un futuro digitale. Il ritmo veloce dello sviluppo tecnologico a livello mondiale ha portato la questione della sicurezza informatica alla ribalta negli ultimi dieci anni. L'Australia, data la sua vasta dimensione geografica, è uno dei paesi che può beneficiare maggiormente di un'economia digitale con reti ad alta velocità, ma anche uno dei più esposti a minacce dello spazio cibernetico, data l'economia aperta e la promozione di investimenti esteri.

La storia recente della sicurezza dello spazio cibernetico in Australia

Il primo importante riconoscimento ufficiale di come la sicurezza nello spazio cibernetico fosse una questione di sicurezza nazionale vi fu nel 2000, con il Libro bianco della Difesa, in cui veniva trattata la questione della 'nuova sfida per la sicurezza' contro gli attacchi cibernetici alle principali infrastrutture informatiche in Australia. Successivamente venne lanciata l'iniziativa E-Security, per proteggere tali infrastrutture. Gli istituti principali coinvolti nell'iniziativa erano: l'Australian Security Intelligence Organisation (ASIO), l'Australian Signals Directorate (ASD), la Polizia Federale Australiana (AFP) e l'Attorney-General's Department (AGD).

Il Libro bianco della Difesa del 2009 "Difendere l'Australia nel secolo dell'Asia e del Pacifico: Forza 2030» ha evidenziato il

potenziale impatto di una guerra informatica contro gli interessi nazionali australiani. Secondo il Libro bianco gli attacchi cibernetici alle infrastrutture informatiche di difesa, sicurezza, governative e civili potrebbero seriamente minacciare la sicurezza nazionale australiana. In risposta, l'allora governo istituì il Cyber Security Operations Centre (CSOC), che opera nell'ambito dell'ASD, individuando eventuali intrusioni informatiche perpetrate ai danni del governo australiano e contro le sue infrastrutture fondamentali e coordinando una risposta operativa.

A novembre del 2009 è stata pubblicata la strategia per la sicurezza informatica (Cyber Security Strategy), che definiva le priorità strategiche del Governo per rendere sicura l'infrastruttura informatica in Australia, prevedendo l'istituzione del Computer Emergency Response Team (CERT Australia). CERT Australia ha avviato l'attività a gennaio del 2010 offrendo informazioni e pareri in merito alla sicurezza informatica alla comunità australiana. Si impegna anche con altri centri CERT a livello globale per condividere informazioni e migliori prassi.

Valutazione della minaccia

Non ci deve essere nulla di più insopportabile per un imprenditore australiano (o italiano) che trovare la propria nuova invenzione brevettata in vendita in un altro paese senza permesso, per via di un attacco di pirateria nei confronti del suo progetto: anni di ricerca e duro lavoro palesemente rubati.

Il Rapporto ASIO del 2012-13 presentato in Parlamento ad ottobre del 2013 ha rilevato l'aumento nel numero dei casi e nel livello di sofisticatezza dello spionaggio cibernetico contro sistemi informatici del settore privato e del Governo australiano, ed ha evidenziato come "l'attività cibernetica può essere la manifestazione più visibile di attività di spionaggio estero nei confronti dell'Australia, sottolineando l'interesse e il valore per entità straniere di accedere ad informazioni australiane protette o sensibili e utilizzarle".

Nel giugno del 2013 è stato reso noto che il CSOC aveva rilevato o segnalato 1790 casi di incidenti di sicurezza informatica verificatisi nel 2012 nei confronti del Governo australiano. In 685 casi si era reso necessaria una 'risposta di livello superiore' da parte del CSOC. È stato inoltre osservato come 'le parti sponsorizzate dallo stato costituiscano la fonte più attiva' di minaccia ed il 65% di tutte le intrusioni informatiche prende di mira informazioni commerciali nei settori energetico e minerario, bancario e finanziario, della difesa, delle telecomunicazioni e della tecnologia.

Al fine di coordinare al meglio la risposta del Governo australiano agli attacchi cibernetici nei confronti degli interessi australiani, nel 2013 l'allora Primo Ministro Gillard annunciò, nell'ambito della strategia di sicurezza nazionale, l'istituzione dell'Australian Cyber Security Centre (ACSC). Il Centro situato nella nuova sede dell'ASIO comprende funzionalità di sicurezza informatica di ASD, ASIO, AGD, AFP e dell'Australian Crime Commission.

Cooperazione Internazionale

Nel 2002 l'Australia ha firmato un memorandum d'intesa con Canada, Nuova Zelanda, Regno Unito e Stati Uniti, per istituire il Coordination Working Group (ICCWG) dell'International Computer Network Defence (CND). L'ICCWG, tra le altre cose, facilita la condivisione di informazioni e la risoluzione dei problemi relativi al CND.

Secondo il Libro bianco della Difesa del 2009 il Governo avrebbe finanziato la Defence Science and Technology Organisation (DSTO) per studiare opzioni di sicurezza informatica avanzate, tramite il Technical Cooperation Program. Il DSTO interagisce anche con le forze armate di altri paesi su questioni come la guerra cibernetica.

A settembre del 2011 è stato convenuto che il Trattato di Sicurezza tra Australia, Nuova Zelanda e Stati Uniti (Trattato ANZUS) potesse essere invocato in risposta ad un attacco

cibernetico ed il Libro bianco della Difesa del 2013 ha ribadito tale posizione.

L'Australia partecipa anche ad un'esercitazione di sicurezza informatica multilaterale guidata dagli Stati Uniti, nota con il nome di Cyber Storm. A marzo del 2013 l'Australia ha partecipato ad un'esercitazione internazionale sponsorizzata dagli Stati Uniti nell'ambito di Cyber Storm IV.

L'Australia è attivamente impegnata nelle questioni cibernetiche a livello tecnico. Ha presieduto, ad esempio, il gruppo di esperti governativi delle Nazioni Unite sulla cibernetica, che nel 2013 ha pubblicato un rapporto di riferimento che, per la prima volta nell'ambito dell'attenzione data dalle Nazioni Unite alla cibernetica, ha confermato che il diritto internazionale, in particolare la Carta delle Nazioni Unite, si applica all'utilizzo dello spazio cibernetico da parte degli stati.

L'Australia cerca anche di condividere la propria esperienza nel settore dello spazio cibernetico, ad esempio nell'ambito del Forum Regionale dell'ASEAN o a favore dell'Unione Internazionale delle Telecomunicazioni, sviluppando standard e capacity building, in particolare nei paesi in via di sviluppo. Infine, sostiene il lavoro dell'ICANN, l'Internet Corporation for Assigned Names and Numbers. A marzo del 2014 l'Australia ha lanciato il programma di ricerca Strategy and Statecraft in Cyberspace, che riunisce ricercatori provenienti da cinque università australiane, statunitensi e britanniche e crea un quadro integrato di modellazione per esplorare le sfide nel settore dello spazio cibernetico. Permetterà agli studiosi di discipline umanistiche, scienze sociali e naturali di lavorare insieme per creare e testare ipotesi sulla sicurezza nell'era cibernetica.

Nel corso della sua durata triennale il programma svilupperà un quadro politico per la valutazione critica delle conoscenze convenzionali in materia di conflitti dello spazio cibernetico e di sicurezza informatica, alimentando il dibattito pubblico sulle minacce dello spazio cibernetico e le sfide per la politica di sicurezza e la strategia nazionale.

Cosa dice il Governo australiano

I vari governi australiani che si sono succeduti nel tempo hanno considerato la sicurezza cibernetica come una questione d'importanza nazionale, che tuttavia deve anche essere valutata in un contesto di crescita e prosperità. Sebbene in Australia sia il Ministero per le Comunicazioni ad occuparsi delle questioni di spazio cibernetico, con responsabilità che vanno dall'internet governance alla privacy, dal controllo dei dati alla libertà di espressione online, molti altri rami del Governo sono coinvolti nell'elaborazione delle politiche in materia, tra cui l'Australian Signals Directorate, l'Attorney-General's Department, il Department of Prime Minister and Cabinet e il Ministero degli Affari Esteri e del Commercio.

L'era informatica ha avuto enormi ripercussioni in Australia. Il Ministro australiano della Comunicazione, Malcolm Turnbull, durante un discorso a marzo del 2014 in cui lanciava il programma di ricerca sullo spazio cibernetico già citato, ha dichiarato: "La nostra capacità di fare, trasmettere, archiviare ed elaborare grandi quantità di dati crea un'enorme vulnerabilità, ma anche enormi opportunità. Ciò ha offerto a chi cerca di proteggerci e a coloro che vogliono danneggiarci, la capacità di scavare sempre più a fondo nelle nostre vite". Il Ministro Turnbull ha inoltre identificato una limitazione fondamentale da parte di qualsiasi governo nel tentare di disciplinare lo spazio cibernetico: " Lo spazio cibernetico... è stato costruito, viene gestito ed è quasi interamente di proprietà del settore privato ed è in gran parte al di là del controllo di qualsiasi governo, la cui giurisdizione è limitata dal fattore geografico".

Alcuni critici, sottolineando il fatto che la crescita e la regolamentazione dello spazio cibernetico è stata guidata in gran parte dai privati, hanno richiesto ai governi di assumere un ruolo più diretto nella gestione dello spazio cibernetico, pensiero che il Governo Abbott non condivide e, nuovamente, il Ministro Turnbull affronta l'argomento in modo diretto nello stesso discorso: "mantenere un sistema di gestione dello spazio cibernetico che sia aperto, globale e non dominato dai governi, è una delle questioni strategiche fondamentali del nostro tempo e rappresenta un obiettivo che il Governo australiano si è impegnato a perseguire.

L'Australia sostiene l'attuale approccio multilaterale all'internet governance, che si è evoluto organicamente e positivamente. Secondo tale modello il settore privato, i governi e tutti gli utenti partecipano a plasmare l'evoluzione e l'utilizzo di internet. Gli accordi multilaterali massimizzano l'accesso e le opportunità a beneficio di tutti".

Protezione degli australiani dagli attacchi cibernetici

Il Governo ha sviluppato diversi programmi per proteggere persone, imprese e infrastrutture australiane da minacce informatiche. L'obiettivo è di trovare sempre il giusto equilibrio nell'affrontare la minaccia, proteggendo e mantenendo al contempo le libertà individuali.

Le azioni volte ad aumentare la consapevolezza dei cittadini sui problemi cibernetici sono iniziate da tempo, come dimostra Cybersmart, un programma nazionale di educazione alla sicurezza informatica gestito dall'Australian Communications and Media Authority (ACMA). Il programma è specificamente progettato per soddisfare le esigenze di bambini, giovani, genitori, insegnanti e bibliotecari. L'obiettivo è di creare "*cittadini cybersmart*". Un'importante parte di questo programma affronta il fenomeno del bullismo cibernetico. L'attuale Governo australiano ha annunciato un finanziamento di $10 milioni nell'ambito della politica di miglioramento della sicurezza online per i bambini, di cui $7.5 milioni saranno destinati ad assistere le scuole per accedere a programmi di sicurezza on-line riconosciuti.

Le misure adottate nell'ambito del programma Cybersmart sono dirette anche alle comunità indigene e ai bambini. Il programma educativo sullo spazio cibernetico dal nome "Be Deadly Online" agisce a favore delle comunità indigene, affrontando il bullismo cibernetico, la messaggistica con riferimenti sessuali e la gestione digitale delle impronte, rispondendo alle preoccupazioni dei leader delle comunità indigene. L'impatto dei mezzi di comunicazione sociale sulle relazioni familiari e comunitarie e sugli stessi giovani rappresenta un problema serio in molte comunità

indigene e il programma offre consigli pratici e positivi su come navigare in modo intelligente.

Le iniziative per i bambini sono ulteriormente supportate da programmi interattivi "Budd:e" (*ndt:* associato al termine *buddy*= amico del cuore), sviluppati per le scuole primarie australiane. Questi programmi spiegano ai bambini, attraverso giochi e attività online, i rischi in cui si può incorrere navigando su internet e le possibili conseguenze di tali rischi. Si tratta di uno strumento interattivo che permette ai bambini di costruire e personalizzare un "Budd:e", che impersonifichi le buone pratiche di sicurezza informatica e di condotta online.

A livello più generale il Governo fornisce consulenza sulla sicurezza informatica ai privati e alle aziende attraverso il sito 'Stay Smart Online', che offre suggerimenti pratici sulla sicurezza informatica. Alle imprese, ad esempio, consente l'accesso ad efficaci pratiche di sicurezza online. Offrire un ambiente sicuro per le transazioni online è fondamentale per costruire e mantenere la fiducia dei clienti, fattore chiave per aumentare il numero di transazioni online, riducendo così i costi per imprese e consumatori e, in modo particolare in un grande paese come l'Australia, riducendo in parte l'impatto ambientale del consumismo. Nell'ambito di questa iniziativa l'Australian Signals Directorate offre una "Top 35 Mitigation Strategies", che sottolinea l'importanza di mantenere i software aggiornati per contrastare gli attacchi online.

Proteggere le imprese australiane dagli attacchi cibernetici

Come già accennato, CERT Australia rappresenta l'organizzazione che risponde a livello nazionale alle emergenze informatiche ed è il punto di riferimento nel Governo sulle questioni di sicurezza informatica che riguardano le grandi aziende australiane. CERT condivide informazioni e lavora a stretto contatto con l'Australian Security Intelligence Organisation, l'Australian Signals Directorate, e la Polizia Federale Australiana. Collabora inoltre in modo diretto ed ha accordi con il Governo e con altre

organizzazioni che affrontano le emergenze informatiche nelle aziende a livello internazionale. Ciò significa che CERT è in una posizione ideale per aiutare le aziende a proteggersi dagli attacchi informatici.

CERT offre consulenza e sostegno ai proprietari e ai gestori di importanti infrastrutture in Australia e di altri sistemi informatici di interesse nazionale per far fronte alle minacce cibernetiche e gestire le aree di vulnerabilità. Se venissero compromessi tali sistemi potrebbe esservi un impatto significativo sulla prosperità economica, il benessere sociale, la difesa e la sicurezza nazionale dell'Australia.

La Trusted Information Sharing Network (TISN) rappresenta le principali infrastrutture identificate come cruciali ai fini della sicurezza nazionale. Tra queste i settori bancario e finanziario, delle comunicazioni, dell'energia, alimentare, della salute, dei trasporti e dei servizi idrici. CERT Australia lavora a stretto contatto con TISN, per dare consigli ed assistenza sulle strategie per proteggersi contro eventuali attacchi cibernetici.

Conclusioni

Questo documento offre soltanto una breve panoramica sui vari programmi adottati dai governi australiani succedutisi negli ultimi anni per affrontare la questione delle minacce da e verso lo spazio cibernetico. La protezione dello spazio cibernetico rappresenta uno dei sempre più numerosi problemi globali, per cui non ha più senso per un paese pensare a livello locale o agire in maniera isolata. Ecco perché l'Australia ha posto particolare enfasi sulla collaborazione con altri paesi e cerca di condividere la propria competenza ed esperienza in materia. Il Governo australiano, inoltre, incoraggia attivamente le imprese, che si tratti di banche, miniere o imprese ad alta tecnologia, a rafforzare le proprie difese contro gli attacchi cibernetici. L'Australia continuerà a lavorare con i partner internazionali per garantire che la governance dello spazio cibernetico offra un adeguato livello di protezione della sicurezza nazionale, evitando di minacciare, allo stesso tempo, quella libertà individuale che il mondo della rete incarna.

Lo Spazio Cibernetico tra Esigenze di Sicurezza Nazionale e Tutela delle Libertà Individuali (Estonia)

Johannes Kert
(Ambasciatore)

Cyber Difesa oggi

Gli Attacchi cyber esistono e sono destinati ad evolversi e a trasformarsi finché l'uomo continuerà ad utilizzare Internet. Oggi ci troviamo in una situazione nuova, in cui i nostri interessi di sicurezza impongono nuove soluzioni. Per orientarci e adattarci alle nuove circostanze, dobbiamo essere flessibili e cominciare a pensare fuori dagli schemi.

È perfettamente chiaro che l'avvento di minacce cyber e la necessità di rispondere ad esse risulta essere un allontanamento significativo dal modello classico della guerra come descritto da Clausewitz. Tuttavia, i funzionari e capi militari persistono ad aggrapparsi a un modello obsoleto. Anche i politici della NATO e dell'UE non sono preparati a riconoscere la nuova situazione sul panorama della sicurezza e per molti anni hanno nascosto la testa sotto la sabbia. Tuttavia, siamo assistendo sempre più anche a punti di vista più progressisti che ammettono la gravità della nuova situazione e cercano soluzioni ad essa.

La situazione sembra essere leggermente migliore in Estonia. Il nuovo ambiente minaccia colpisce i paesi più piccoli e con risorse limitate - per ragioni comprensibili, non hanno il lusso di sovrapporre capacità di ministeri e agenzie, come fanno alcune superpotenze. È essenziale essere consapevoli dei cambiamenti nel modello di rischio e saper rispondere adeguatamente ad essi. Per fare ciò, la divisione dei ruoli tra agenzie e comando coordinato e di controllo deve essere preparata già in fase di formazione ed esercitazioni.

Le minacce

Regioni e paesi diversi percepiscono le minacce cyber in modi diversi. Negli Stati Uniti e nella maggior parte dell'Unione europea, le minacce cyber sono viste soprattutto in termini di attività ostile all'*intelligence* (spionaggio) e di potenziale furto di proprietà intellettuale. Ciò minaccia la pianificazione strategica e si traduce in un vantaggio economico ingiusto, e ha un effetto a catena sugli atteggiamenti sociali e le politiche del governo.

Molte altre regioni, invece, vedono il crimine cyber come la minaccia cibernetica principale.

I potenti paesi totalitari, che sono l'origine della maggior parte degli attacchi cyber, tentano di garantire la loro sicurezza limitando la libertà on-line delle loro popolazioni e controllando il cyberspazio.

Non troppo tempo fa, gli Stati Uniti, un paese che sta conducendo la guerra contro il terrorismo globale e chiaramente patrocina valori democratici, si è trovata in uno scandalo riguardante *snooping* on-line. Ma la totalitaria Russia, che gongolava per una telefonata intercettata tra il capo della politica estera dell'Unione europea Catherine Ashton e il ministro degli Esteri estone Paet, non è stata ampiamente vista come una minaccia cyber, almeno non in Europa.

Per i paesi ex sovietici confinanti con la Russia, le minacce cyber sono spesso percepite specificamente come strumento di influenza politica. Un certo numero di attacchi cyber hanno avuto luogo in questo spazio geopolitico, e o hanno rappresentato le reazioni ad alcuni eventi politici o sono state volte a influenzare la politica - in altre parole, rappresenterebbero la continuazione della politica con altri mezzi. Gli attacchi cyber che hanno avuto luogo nella regione geopolitica post-sovietica sono stati spesso combinati - e col passare del tempo, anche orchestrati - con pressioni economiche, rivendicazioni politiche o, come la guerra in Georgia del 2008 ha dimostrato, con l'azione militare convenzionale.

Nel cyberspazio, una vasta gamma di tattiche sono state utilizzate per ottenere vari effetti. Oltre agli attacchi *denial of service* utilizzati per tagliare l'accesso alle comunicazioni, è stata utilizzata la manipolazione dei dati (ad esempio il *defacement*) tra le molte

altre tattiche. Ad esempio, un attacco cyber è stato utilizzato per manipolare i tassi di cambio presso la Banca della Georgia, il cui obiettivo era quello di seminare il panico finanziario e ridurre la fiducia al governo. Varie *cyber*-operazioni con tattiche diverse possono anche essere viste come una componente nelle operazioni di *intelligence* anti-ucraina, in combinazione con l'uso di forze irregolari e regolari in Crimea e nell'Ucraina orientale. L'emergere di guerrieri cibernetici ha ulteriormente aumentato la complessità e l'ampiezza del campo di battaglia di oggi. Allo stesso tempo, a coloro che sono abbastanza ingenui per insistere su una visualizzazione della guerra cibernetica come fantascienza o minaccia futura deve essere ricordato che anche le asce di pietra degli uomini del paleolitico rimangono un'arma mortale, insieme a tutto il resto che si trova tra questi due estremi.

Sul campo di battaglia moderno, con una componente cyber attiva, non vi è alcun modo di sperare che le infrastrutture civili in qualche modo non siano nel mirino. Ciò che vediamo è che la logica di funzionamento sta trasformando la visione di quello che un tempo era il teorico della forza aerea di bombardamento strategico, l' italiano Giulio Douhet, - praticata avidamente da tutti i principali belligeranti nella seconda guerra mondiale - in una strategia di attacco cyber. Alcuni paesi stanno inoltre utilizzando i propri cittadini per realizzare i loro obiettivi nazionali nel cyberspazio.

Il meccanismo per prendere decisioni nella NATO e l'UE si basa sul consenso. Da un lato, questo è un bene per queste organizzazioni in quanto la cultura di prendere decisioni basate sul consenso risulta gradevole per i paesi europei, e ha portato alla situazione in cui molti membri della NATO hanno fatto volontariamente una grande quantità di lavoro necessario per adottare i principi democratici necessari per aderire alla NATO e l'UE. I paesi che hanno aderito alla NATO e l'UE hanno notevolmente aumentato la quantità di territorio, stabile in Europa.

Le risposte a minacce cyber potrebbero rappresentare una sfida per il sistema in termini di velocità pura, nonché l'identificazione del l'attaccante vero e proprio.

Gli attacchi cyber possono essere utilizzati anche da altri gruppi politici - spesso gruppi internazionali che non sono entusiasti di NATO e UE, e spesso operano su principi religiosi comuni o interessi economici o attributi ideologici ed etniche condivise. Gli esempi includono Al Qaeda, i talebani, lo Stato islamico, e gruppi di criminalità organizzata sponsorizzati dagli Stati.
NATO e l'UE sono un bene per i paesi europei, poiché hanno mantenuto la maggior parte dell'Europa libera dalla guerra o hanno portato la pace nelle regioni. La cooperazione e l'unione delle nostre forze sono diventati una priorità importante per combattere e respingere le nuove minacce subdole, che richiedono la cooperazione e l'impegno.

L'esperienza estone

Gli estoni di oggi si riferiscono alla loro società cablata chiamandola "*e-lifestyle*". La convinzione degli estoni nei confronti dei servizi elettronici e la connettività non è stato scossa dagli attacchi cyber del 2007 - al contrario, il discreto successo della neutralizzazione di quegli attacchi cyber ha fornito esperienza e fiducia in se stessi e nella correttezza delle nostre decisioni.

L'uso diffuso di servizi pubblici elettronici, la carta d'identità elettronica e la firma digitale ci hanno dato opportunità senza precedenti per integrare la stragrande maggioranza dei servizi. Oggi il 99% dei trasferimenti bancari in Estonia sono elettronici, così come lo sono il 94% delle dichiarazioni dei redditi, che richiedono una manciata di minuti. Possiamo anche parlare di una sempre più ampia affluenza popolare per le votazioni elettroniche per il governo e le elezioni locali, sistemi di prescrizioni mediche digitali, e-scuola, servizi di polizia elettronici, governo senza carta e molto altro.

È del tutto chiaro che i paesi situati in zone geo-politicamente complessi devono fare molteplici compiti al fine di ridurre le vulnerabilità e prevenire gli attacchi.

Il CERT nazionale è in funzione dal 2006. Oggi il CERT-EE è parte del sistema di informazioni dell'autorità estone (RIA). Il RIA è responsabile di tutti gli aspetti dello sviluppo dei sistemi cyber statali e la disponibilità di servizi elettronici pubblici, nonché per

l'organizzazione di protezione delle infrastrutture di informazioni critiche a livello nazionale. Inoltre, garantisce il funzionamento del sistema delle misure di sicurezza dei sistemi di informazione statali in un ambiente in continua evoluzione così come la gestione degli incidenti di sicurezza attraverso operazioni CERT, e controlla lo stato di attuazione dei fornitori di servizi pubblici ai sensi della normativa.
Il centro corrispondente alle forze di difesa - il CIRC - garantisce la sicurezza cyber nella giurisdizione del Ministero della Difesa estone. Corsi di formazione pertinenti ed esercitazioni si svolgono regolarmente allo scopo di aumentare l'efficacia della protezione delle reti delle forze di difesa.

In tempo di pace, ossia in un periodo in cui la frequenza e la natura degli incidenti corrispondono a una routine, le istituzioni responsabili per le nostre forze civili e di difesa cyber sono in grado di gestire correttamente le persone in servizio permanente, ma se dovesse cambiare il modello di rischio e la situazione si dovesse aggravare, potremmo avere bisogno di una riserva ben preparata.

A tal fine, la *Estonian Defense League* sta preparando un sistema di formazione sulla difesa cyber che è stata anche chiamata *Cyber Defence League*. La *Cyber Defence League* è composta da volontari, cittadini estoni che hanno qualifiche di alto livello e un forte senso di responsabilità. Tiene corsi di formazione e di esercizi per i suoi membri, e i membri aiutano a trasmettere questa formazione al grande pubblico. Per i membri della *Cyber Defence League*, il più grande valore aggiunto di questa organizzazione è quello conferito dall'esperienza.

Poiché i membri della *Cyber Defence League* hanno esperienza in istituzioni diverse che si occupano di difesa cyber - per esempio, banche, telecomunicazioni, istituzioni della infrastruttura di informazione critica, università, sviluppatori di software, e forze di difesa – lo scambio di esperienze è reciprocamente vantaggioso. La *Cyber Defence League* può essere coinvolta in modo flessibile esattamente dove è necessaria assistenza e nella misura in cui è necessaria assistenza.

Un *hub* per la difesa cyber è il *cyber defense range* finanziato dallo stato e istituito su iniziativa della *Cyber Defence League*. Esso

permette esercizi di difesa cyber che si tengono a livello organizzativo, statale e internazionale. La possibilità di organizzare una formazione moderna e utilizzando un ambiente di formazione moderno sostiene la motivazione dei volontari in quanto aumenta le loro qualifiche e la loro competitività agli occhi dei loro datori di lavoro. Il più grande e internazionale degli esercizi si tiene ogni anno in questo *range* ed è costituito dal *Locked Shields* e dalla *Cyber Coalition*.

Il *Locked Shields* è detenuto dal *Cooperative Cyber Defence Centre of Excellence* della NATO (NATO CCD COE) e la Cyber Coalition è detenuta dall'unità strutturale di riferimento, al quartier generale della NATO.

È negli interessi vitali dell' Estonia - e spero, di tutti gli Stati membri - che la NATO sia il più moderna ed efficace possibile. Per questo motivo, l'Estonia e altri paesi sponsor si sono impegnati a creare e sviluppare il NATO CCD COE a Tallinn.

Il CCD COE è un *think tank* che offre alla NATO, e ai suoi membri, servizi nel settore della difesa cyber, le basi giuridiche e il quadro normativo, la formazione e le soluzioni tecniche. Del CCD COE fanno parte 15 Stati e un certo numero di parti coinvolte, tra cui la *Cyber Defence League*. Vi è un interesse costante nel CCD COE da potenziali nuovi soci e stiamo lavorando nell'interesse di un allargamento costante e di prestazioni migliori.

Posso riassumere l'esperienza dell'Estonia nel settore della difesa cyber notando che quando si tratta di attacchi cyber, non c'è scelta tra le soluzioni buone e cattive ma tra soluzioni cattive e pessime. L'unica buona soluzione è quella di organizzare in modo continuo l'aggiornamento della formazione e delle esercitazioni con scenari il più possibile aggiornati. Abbiamo bisogno di vedere ogni esercizio come un esperimento ed essere pronti per una flessibilità strutturale e organizzativa degli sviluppi che ci saranno.

Spazio cibernetico visto dall'estero: Strategia Nazionale per la Sicurezza Cibernetica (Repubblica Ceca)

Daniel P. Bagge M.A. – Roman Pačka

(Responsabile Sezione di supporto teorico della formazione e della ricerca, Centro Nazionale di Sicurezza Cibernetica - Analista Sezione di supporto teorico della formazione e della ricerca, Centro Nazionale di Sicurezza Cibernetica)

Introduzione

Garantire la sicurezza cibernetica dello Stato è una delle sfide principali dell'epoca attuale. La dipendenza dei settori pubblico e privato dalle tecnologie di informazione e di comunicazione diventa sempre più evidente. La condivisione e la protezione delle informazioni è al momento attuale fondamentale per la tutela degli interessi dello Stato e dei suoi cittadini nei settori di sicurezza, dell'economia e della finanza. Mentre i cittadini temono innanzitutto le perdite nel campo finanziario oppure quelle dei propri dati e l'utilizzo indebito dei dati personali, la realtà di tutta la problematica della sicurezza cibernetica è molto più vasta. I rischi significativi consistono in particolare nello spionaggio cibernetico (sia industriale che militare, politico o altro), dietro il quale vi sono sempre più spesso i governi, ovvero le strutture di sicurezza di uno Stato concreto, attività della criminalità organizzata nello spazio cibernetico, hacktivism ovvero attivismo informatico, diffusione intenzionale delle disinformazioni allo scopo dell'ottenimento degli obiettivi politici e militari, o nel futuro anche il terrorismo cibernetico. Il rischio attualmente è rappresentato non solo da frequenti attacchi cibernetici effettuati ad esempio allo scopo dell'ottenimento dei profitti economici, ma anche da casi di violazione della sicurezza e dell'integrità delle reti, causate non intenzionalmente, ad esempio da un errore umano, da una calamità naturale e simili.

Lo Stato deve essere in grado di garantire una reazione efficace a tutte le sfide attuali e future in un ambiente di continui

cambiamenti di pericoli cibernetici che possono arrivare dall'ambiente cibernetico ad evoluzione dinamica, e di garantire così uno spazio cibernetico sicuro e affidabile.

Vista la natura aperta e accessibile al pubblico dell'internet, caratterizzato dall'assenza delle frontiere geografiche, la sua tutela e messa in sicurezza richiedono non solo le iniziative dello Stato ma anche la collaborazione dei cittadini. Lo Stato crea e amplia in modo costante le capacità nazionali in questo settore, ma in assenza di cooperazione con il settore privato e con il mondo accademico e in assenza di una intensa collaborazione internazionale ed in particolare in assenza del coinvolgimento degli stessi utenti, non può essere garantita la dovuta efficacia di tali attività.

Sicurezza cibernetica nella Repubblica Ceca

In riferimento a quanto detto sopra è evidente che l'importanza del settore di sicurezza cibernetica continua a crescere e già oggi rappresenta uno degli aspetti determinanti dell'ambiente di sicurezza della Repubblica Ceca. In concreto, il concetto della sicurezza cibernetica rappresenta nella Repubblica Ceca un insieme di misure organizzative, politiche, giuridiche, tecniche e formative e di strumenti volti a garantire nella Repubblica Ceca lo spazio cibernetico sicuro, protetto e resiliente, sia per quanto riguarda i soggetti pubblici e privati, che per tutta la popolazione. La sicurezza cibernetica aiuta a identificare, valutare e risolvere i pericoli dello spazio cibernetico, diminuire i rischi cibernetici e eliminare conseguenze di attacchi cibernetici, di criminalità elettronica, di cyber-terrorismo e di spionaggio cibernetico rafforzando la confidenzialità, l'integrità e l'accessibilità dei dati, dei sistemi ed di altri elementi dell'infrastruttura di informazione e di comunicazione.

Alla fine del 2011 il Governo ceco ha istituito l'Ufficio Nazionale per la Sicurezza come gestore e contemporaneamente come autorità nazionale nel campo della sicurezza cibernetica. Nell'ambito delle sue attività la detta autorità ha aperto ufficialmente nel 2014 a Brno il Centro Nazionale per la Sicurezza Cibernetica che svolge il ruolo fondamentale nel garantire la sicurezza cibernetica nella Repubblica Ceca. Esso rappresenta quindi

una componente organizzativa dell' Ufficio Nazionale per la Sicurezza, composta da CERT governativo (GovCERT.CZ) e dalla Sezione del supporto teorico della formazione e della ricerca.

Dopo il suo predecessore in questa funzione (il Ministero dell'Interno) l'Ufficio Nazionale per la Sicurezza ha acquisito la Strategia per la sicurezza cibernetica della Repubblica Ceca per gli anni 2011 – 2015, che ha aggiornato nel 2012 e successivamente implementato e realizzato con successo. Con il prossimo termine della validità e del raggiungimento di tutti gli obiettivi fondamentali di questa strategia, nell'ultimo periodo il Centro ha iniziato a sviluppare una nuova strategia nazionale per la sicurezza cibernetica che risponderebbe pienamente alle attuali sfide e necessità della Repubblica Ceca nel campo della sicurezza cibernetica. Al momento attuale dunque sta in attesa di approvazione la nuova Strategia nazionale per la sicurezza cibernetica della Repubblica Ceca per gli anni 2015 - 2020 (di seguito solo „Strategia"), che rappresenterà il documento fondamentale concettuale del Governo della Repubblica Ceca per il relativo settore e sarà in armonia con gli interessi di sicurezza e punti di partenza definiti nella Strategia per la sicurezza della Repubblica Ceca. Servirà come documento di riferimento per la redazione di relative norme giuridiche, politiche o standard, direttive e altre raccomandazioni nell'ambito della protezione e della messa in sicurezza dello spazio cibernetico nella Repubblica Ceca.

Quadro fondamentale strategico e concettuale della sicurezza cibernetica della Repubblica Ceca

"La Strategia per la sicurezza della Repubblica Ceca" dichiara i fondamentali valori, interessi, approcci, ambizioni e strumenti della Repubblica Ceca nel garantire la propria sicurezza e formula i principi, su cui fonda la politica di sicurezza della Repubblica Ceca. Nella strategia vengono definiti gli interessi vitali, strategici ed altri interessi importanti della Repubblica Ceca, lo spazio di sicurezza ceco e la descrizione del sistema di sicurezza ceco. La Strategia per la sicurezza rappresenta così il documento fondamentale della politica di sicurezza della Repubblica Ceca, che nel suo testo al

livello generale pone accento ovviamente anche sulla sicurezza cibernetica. In base a tale strategia poi vengono sviluppate altre sottostrategie e concetti.

Nell'ambito della tutela della sicurezza cibernetica, più importanti sono due strategie/concetti con essa collegati. Si tratta da una parte del "Libro bianco della difesa" che nel settore della difesa dello spazio cibernetico definisce principali compiti del Ministero della Difesa e dall'altra parte, attualmente ancora valida, la "Strategia per il settore della sicurezza cibernetica nella Repubblica Ceca negli anni 2012 – 2015", che dal 1 gennaio 2015 viene sostituita da qui presentata "Strategia Nazionale per la Sicurezza Cibernetica per gli anni 2015 - 2020". Tale nuova Strategia rispetto alla versione precedente, che si muoveva piuttosto in contorni generici e cercava fondamentalmente di creare i mezzi, le capacità ed il quadro legislativo/strategico atti a garantire la sicurezza cibernetica, tratta la problematica di sicurezza cibernetica in modo molto più completo e sistematico.

Valutazione della strategia precedente e i motivi di una Strategia nuova

La Strategia per il settore della sicurezza cibernetica nella Repubblica Ceca per gli anni 2012 – 2015 doveva migliorare il livello della sicurezza cibernetica per le istituzioni governative, infrastrutture a rischio e sfera commerciale, dunque anche per i cittadini della Repubblica Ceca. In concreto, nella Strategia 2012-2015 sono stati definiti nove obiettivi, concretizzati nei 17 punti del Piano d'Azione, di cui alcuni sono stati già raggiunti mentre gli altri sono in via di compimento progressivo.

Si può sottolineare innanzitutto:

- la presentazione al Governo della Repubblica Ceca di un disegno di legge sulla sicurezza cibernetica e sulla modifica delle leggi con essa collegate. Il disegno di legge è stato successivamente approvato dal Governo e dal Parlamento della Repubblica Ceca ed il Presidente della Repubblica lo ha firmato il 13 agosto 2014 (Legge sulla Sicurezza Cibernetica entrerà in vigore alla data

della sua pubblicazione nella Gazzetta Ufficiale della Repubblica Ceca e sarà efficace dal 1 gennaio 2015);

- il coinvolgimento attivo della Repubblica Ceca nelle esercitazioni internazionali sulla sicurezza cibernetica. L'Ufficio Nazionale per la Sicurezza, tramite il suo dipartimento specializzato Centro Nazionale per la Sicurezza Cibernetica ha partecipato a tutta una serie di esercitazioni nel campo della sicurezza cibernetica sia da solo che in collaborazione con ad esempio CIRC militare, Ministero della Difesa, Ministero degli Affari Esteri, Polizia della Repubblica Ceca, Servizio d'informazione e sicurezza, CZ.NIC ed altri (ad esempio esercitazioni: Cyber Coalition, CMX, Locked Shield, Cyber Europe, esercitazione CECSP);
- l'istituzione del Centro Nazionale per la Sicurezza Cibernetica, e dunque di un organo che provvede al coordinamento della collaborazione al livello nazionale e internazionale nell'ambito della sicurezza cibernetica e mette in opera un sistema di rivelamento, analisi, soluzioni e previsioni degli attacchi cibernetici efficace e di alta qualità. Fa parte di questo Centro anche GovCERT.CZ, il cui compito consiste nel monitoraggio dello spazio cibernetico e nel rilevamento e nella soluzione degli attacchi cibernetici, nella loro prevenzione etc.;
- la collaborazione attiva con università selezionate con le quali l'Ufficio Nazionale per la Sicurezza ha firmato gli accordi quadro sulla collaborazione che permettono la realizzazione di progetti comuni nell'ambito della sicurezza cibernetica;
- la partecipazione attiva della Repubblica Ceca all'elaborazione della legislazione internazionale, delle norme, etc. e la partecipazione ad altre attività, concernenti la sicurezza cibernetica nell'ambito dell'UE e al di fuori delle sue frontiere.

In conclusione bisogna sottolineare che i due obiettivi strategici principali, che supportavano la Strategia (la realizzazione di un quadro legislativo in materia della sicurezza cibernetica e l'istituzione del Centro Nazionale per la Sicurezza Cibernetica e dell'ufficio governativo CERT), sono stati raggiunti con successo ed anche il resto dei compiti, e cioè degli obiettivi principali della Strategia, sono stati compiuti oppure stanno in via di compimento

progressivo. La realizzazione della Strategia in base alla valutazione qui presentata può essere considerata compiuta e si può costatare che nella Repubblica Ceca a partire dal 2012 il livello della sicurezza cibernetica è considerevolmente accresciuto. In considerazione di tale esaurimento ovvero raggiungimento degli obiettivi e dei compiti, e del termine della validità della strategia, è stata elaborata una strategia del tutto nuova per gli anni 2015 – 2020.

Strategia nazionale di sicurezza cibernetica della Repubblica Ceca per gli anni 2015 – 2020

Struttura della Strategia

Dal punto di vista della struttura e dell'articolazione del testo della Strategia viene in primis presentata la visione della Repubblica Ceca riguardante il settore della sicurezza cibernetica, che va oltre il quadro temporale di questa Strategia (2015 – 2020). In seguito sono definiti principi fondamentali che lo Stato segue nel garantire la sicurezza cibernetica del Paese. Si tratta di una prima parte, piuttosto generica. Segue poi il capitolo sulle sfide concrete nel campo della sicurezza cibernetica sia per la Repubblica Ceca che per l'ambiente internazionale in cui si colloca la Repubblica Ceca. In conclusione sono presentati i principali obiettivi strategici, che affrontano tali sfide e in base ai quali è stato elaborato il concreto Piano d'Azione della sicurezza cibernetica della Repubblica Ceca per gli anni 2015 - 2020 (di seguito solo il Piano d'Azione).

Sfide più importanti

Nella Strategia sono definite esattamente 19 sfide che la Repubblica Ceca identifica al momento attuale come fondamentali. Si tratta di problemi e tendenze che la Repubblica Ceca ed i suoi cittadini affrontano ed ai quali lo Stato deve in un certo modo reagire (stabilendo gli obiettivi principali e passi fondamentali nel Piano d'Azione). Si tratta ad esempio di:

- Repubblica Ceca come possibile oggetto da testare
  La Repubblica Ceca come il paese che al fine di garantire la sicurezza utilizza le tecnologie moderne, utilizzate anche da altri Stati, può servire agli eventuali attaccanti come un oggetto da

testare prima di sferrare un attacco contro i nostri alleati, o contro altri Stati di una maggiore importanza strategica, che usano le stesse tecnologie e meccanismi e processi di sicurezza come la Repubblica Ceca.

- Con il crescente numero di utenti delle piattaforme mobili cresce anche la quantità di malware mobile
  Solo una piccola parte della società usa almeno elementi protettivi di base (ad esempio programmi antivirus) nei loro tablet e cellulari intelligenti. Ne approfittano gli attaccanti come si vede dall'incremento annuale di malware e degli attacchi sferrati contro tali dispositivi.
- Possibilità dell'uso illecito delle backdoor dell'hardware per il prelievo delle informazioni
  Con l'aumento del numero degli utenti e fornitori delle tecnologie cresce il rischio dell'inserimento delle backdoor nell'hardware che possono essere successivamente utilizzate in modo illecito ad esempio per monitorare e acquisire i dati strategicamente importanti o personali e sensibili.
- Big data, immagazzinamento dati negli ambienti nuovi
  La protezione e la difesa dei dati è per la Repubblica Ceca molto importante, in particolare di quei dati che sono di interesse pubblico, ad esempio importanti dati relativi alle infrastrutture informatiche critiche (KII) e ai sistemi informatici importanti (VIS). Negli ambienti pubblico e privato cresce il volume dei dati, oggetto di elaborazione, che devono essere di seguito immagazzinati. Per questo motivo si è iniziato a utilizzare nuove forme d'immagazzinamento dati, ad esempio cloud storage. L'utilizzo incrementato di questo tipo di servizi online e di cloud porta spesso a una soluzione di protezione non trasparente, la cui affidabilità è come minimo discutibile.
- Protezione dei sistemi di gestione industriale e dei sistemi informatici nella sanità
  Dalla sfera di un profitto economico diretto degli attaccanti gli attacchi si spostano ad esempio nella zona dello spionaggio cibernetico industriale, del vandalismo cibernetico e della ricerca della vulnerabilità dei singoli elementi delle infrastrutture critiche

e dei sistemi informatici importanti. Gli attaccanti mirano sempre di più su elementi di struttura informatica come ad esempio sistemi energetici, condotti di prodotti e sistemi informatici nella sanità. Questi sistemi, il cui fallimento potrebbe avere conseguenze fatali, sono caratterizzati di un'alta eterogeneità di soluzioni tecniche, direttamente connesse con la difficoltà tecnica di qualunque analisi ex post.

- Crescente dipendenza degli organi di difesa dello Stato dalle tecnologie di informazione e di comunicazione
  Le tecnologie di informazione e di comunicazione penetrano sempre di più nei sistemi, nelle reti e nella stessa tecnica degli organi di difesa dello Stato (ad es. veicoli delle forze armate, tecnica militare aeronautica). La vulnerabilità di queste tecnologie e il pericolo della loro violazione e distruzione, compresi gli effetti degli attacchi cibernetici, accrescono notevolmente i rischi di un impatto negativo al compimento di competenze fondamentali degli organi di difesa dello Stato e al mantenimento degli impegni, risultanti in particolare dalla partecipazione alla NATO e all'UE. Gli organi di difesa dello Stato devono essere capaci di reagire in modo efficace alle minacce, provenienti dallo spazio cibernetico, e partecipare attivamente alla loro neutralizzazione.
- Malware è sempre più sofisticato
  I software dannosi e gli stessi attaccanti sono sempre più sofisticati. Per questo motivo sono fortemente limitate le ricerche della fonte dell'attacco, e cioè le possibilità di reverse engineering e forensic analysis. Tali procedimenti analitici saranno oggetto di formazione degli esperti in materia di sicurezza cibernetica.
- Botnet e attacchi DDoS/DoS
  Le botnet, tramite le quali si effettuano sempre più spesso attacchi DDoS/DoS, acquisiscono la robustezza, resistenza e crescente segretezza. E' necessario perciò accrescere il subconscio della popolazione su come difendersi dagli attacchi DDoS/DoS.

- Mancanza di esperti in sicurezza cibernetica e necessità della revisione di attuali programmi di studio nelle scuole
  Il modello ceco di istruzione e di formazione così come è concepito non risponde, al giorno d'oggi, alle richieste che vengono dal settore di sicurezza cibernetica e delle tendenze attuali. Esso perciò non riesce a fornire agli alunni delle scuole elementari e medie un'istruzione e una formazione adeguata. Inoltre, l'offerta di programmi universitari, che formerebbero specialisti in campo di sicurezza cibernetica, è largamente insufficiente nonostante la richiesta di tali esperti sia elevatissima.

Ed inoltre:

- Insufficiente fiducia dei cittadini nello Stato;
- Numero sempre crescente di utenti di internet, di tecnologie di informazione e di comunicazione, e aumentata criticità del loro fallimento;
- Reti energetiche intelligenti;
- Aumento della criminalità nel settore informatico;
- Minacce e rischi connessi con l'uso delle reti sociali sull'internet;
- Bassa alfabetizzazione digitale degli utenti finali;
- Concetto dell'"internet delle cose";
- Rischi di sicurezza collegati con il passaggio dal protocollo IPv4 a quello IPv6;
- Rischi di sicurezza collegati con l'informatizzazione dell'amministrazione pubblica (eGovernment);
- Insufficiente garanzia delle piccole e medie imprese.

La strategia inoltre definisce obiettivi principali che reagiscono alle sfide e forniscono un quadro per la soluzione. Tali obiettivi principali sono elaborati nei passi concreti in un ulteriore documento, chiamato Piano d'Azione. Tale piano d'Azione, che sarà presentato nel corso del primo semestre 2015, concretizza i passi, necessari per il raggiungimento degli obiettivi principali, fino al livello di singoli dicasteri con le scadenze del compimento dei compiti chiaramente definito.

Obiettivi principali più importanti:

- Assicurare l'efficacia e rafforzare tutte le strutture, processi e collaborazione nel garantire la sicurezza cibernetica
  - Creare un modello efficace di collaborazione al livello nazionale tra i singoli soggetti della sicurezza cibernetica – centri tipo CERT e CSIRT, soggetti KII e simili, e rafforzare le loro strutture e processi attuali.
  - Creare un procedimento coordinato nazionale per la gestione di eventuali incidenti, che definisce il modello di collaborazione, conterrà la formula di comunicazione, il protocollo del procedimento e definirà i ruoli di singoli attori.
  - Creare la metodologia per la valutazione dei rischi nella Repubblica Ceca al livello dello Stato.
  - Osservare la posizione unica della Repubblica Ceca nei confronti di altri Paesi. Tale posizione deve essere coordinata con altri dicasteri, impegnati nell'ambito della sicurezza cibernetica.
  - Considerare in modo adeguato la problematica della minaccia cibernetica, che sta in continua evoluzione, nell'abito della realizzazione e dell'aggiornamento dei materiali importanti, relativi alla strategia ed alla sicurezza della Repubblica Ceca (Strategia di sicurezza della Repubblica Ceca ed altri).
- Cooperazione internazionale attiva
  - Nell'ambito della propria adesione all'UE, alla NATO, all'ONU, all'OSCE, all'Unione internazionale delle telecomunicazioni e ad altre organizzazioni internazionali, la Repubblica Ceca prenderà parte attiva alle discussioni internazionali sulle attività in occasione dei seminari, convegni, programmi, iniziative etc.
  - Nello spazio centroeuropeo agire come promotore della sicurezza cibernetica e del dialogo tra gli Stati della regione.
  - Istituire e approfondire la collaborazione bilaterale con altri Stati.

- Partecipare alle esercitazioni internazionali e alla loro organizzazione.
- Collaborare sulla realizzazione di un modello efficace della collaborazione e costruire la fiducia tra i centri tipo CERT e CSIRT al livello internazionale, tra le organizzazioni internazionali e i centri accademici.
- Collaborare nella formazione del consenso nell'ambito dei canali ufficiali e non ufficiali riguardo le norme giuridiche e il comportamento nello spazio cibernetico, nel garantire l'apertura dell'internet, i diritti umani e la libertà.

– Protezione delle infrastrutture informatiche critiche (KII) e dei sistemi informatici importanti (VIS) nazionali
  - Proseguire una costante analisi e monitoraggio della messa in sicurezza dei sistemi KII e VIS nella Repubblica Ceca tramite una metodologia definita con chiarezza.
  - Sostenere l'istituzione di altri centri di tipo CERT e CSIRT nella Repubblica Ceca.
  - Incrementare in modo continuo la resistenza, l'integrità e l'affidabilità dei sistemi e delle reti KII e VIS.
  - Effettuare una continua analisi e monitoraggio delle minacce e rischi nella Repubblica Ceca.
  - Condividere in modo efficace le informazioni tra lo Stato ed i soggetti KII e VIS.
  - Incrementare capacità e possibilità tecniche del Centro Nazionale per la Sicurezza Cibernetica, ovvero GovCERT.CZ, e al livello del personale formare e aggiornare regolarmente i dipendenti/gli esperti di tale centro.
  - Proteggere in modo perfetto e affidabile l'ambiente per l'immagazzinamento e per il lavoro con i dati dei soggetti KII e VIS, che istituirà e gestirà lo Stato.
  - Effettuare regolari controlli, rilevamento degli errori e della vulnerabilità dei sistemi di informazione e delle reti che utilizza lo Stato, fondati sul principio dei test di penetrazione nei KII e VIS.

- Incrementare costantemente presupposti tecnici e organizzativi al fine di respingere (reprimere) gli attacchi cibernetici.
- Incrementare possibilità, capacità e potenzialità nazionali nell'ambito della predisposizione di una protezione attiva e nell'adozione delle contromisure contro gli attacchi cibernetici.
- Formare i professionisti specializzati, che si concentreranno sulla problematica e sulle possibilità di adozione di contromisure efficaci nel garantire la sicurezza cibernetica e la difesa e sulla concezione generalmente offensiva di sicurezza cibernetica.
- Elaborare il procedimento per il passaggio tra lo stato del pericolo cibernetico dichiarato ai sensi della legge sulla sicurezza cibernetica e gli stati, definiti dalla Legge costituzionale n. 110/1998 della Raccolta, sulla sicurezza della Repubblica Ceca.

Fanno parte degli obiettivi principali inoltre le seguenti sfere:

- Collaborazione con il settore pubblico
- Ricerca e sviluppo / Fiducia degli utenti
- Sostegno della formazione, della conoscenza e dello sviluppo della società d'informazione
- Rafforzamento delle capacità della polizia della Repubblica Ceca di indagare e punire i reati cibernetici
- Norme per la sicurezza cibernetica (realizzazione di un quadro giuridico). Partecipazione sulla redazione e sull'implementazione delle norme europee e di quelle internazionali.

L'Ufficio Nazionale per la Sicurezza e il suo centro specializzato Centro Nazionale per la Sicurezza Cibernetica seguirà, discuterà e valuterà regolarmente il raggiungimento di singoli obiettivi in collaborazione con altri soggetti coinvolti. Nell'ambito della "*Relazione annuale sullo stato della sicurezza cibernetica nella Repubblica Ceca*" viene elaborato ed allegato alla stessa il Rapporto sullo stato di attuazione del Piano d'Azione. La Relazione informerà il

Governo ed i cittadini dell'efficacia delle misure adottate e dell'esecuzione dei compiti definiti dalla Strategia.

CONCLUSIONE

Dal 2011, quando l'Ufficio Nazionale per la Sicurezza ha assunto la gestione della problematica riguardante la sicurezza cibernetica nella Repubblica Ceca, il livello di sicurezza cibernetica nel Paese è aumentato considerevolmente e tutti i principali obiettivi della Strategia precedente sono stati raggiunti oppure sono in via di un progressivo compimento. Lo conferma in particolare l'istituzione del Centro di Brno (Centro Nazionale per la Sicurezza Cibernetica) o l'approvazione della legge sulla sicurezza cibernetica.

Come si evince dal testo, la strategia per gli anni 2012-2015 serviva innanzitutto per definire un modello efficace e le possibili garanzie della sicurezza cibernetica nella Repubblica Ceca. Qui presentata la nuova Strategia per gli anni 2015 – 2020 amplia considerevolmente questo modello, va più in profondità, considera la complessità delle soluzioni della sicurezza cibernetica e in generale si può dire che, rispetto alla strategia precedente, pienamente soddisfa l'attuale moderna concezione delle strategie nazionali per la sicurezza cibernetica nel mondo.

La Repubblica Ceca si dirige così speditamente verso la situazione in cui il Paese diventa uno dei luoghi più sicuri in Europa per le attività imprenditoriali nello spazio cibernetico, sarà sempre più resistente nei confronti degli attacchi cibernetici, e lo Stato sarà così in grado di difendere meglio i propri interessi nello spazio cibernetico, e di aiutare a mantenere lo spazio cibernetico aperto, dinamico e stabile, e, non per ultimo, garantirà una continua acquisizione di conoscenze, abilità e capacità nel campo della sicurezza cibernetica nella Repubblica Ceca.

Formulazione di una strategia nazionale della cyber sicurezza - Aspetti chiave (Cile)

Esteban Maurín
(Capitano della Forza Aerea del Cile e S.Capo Analisi Vulnerabilità CSIRT)

Il Cyberspazio, come nuovo dominio, secondo il parere di molte pubblicazioni, insieme a quelli già noti: terra, aria mare e spazio, attrae sempre di più diversi attori da distinte prospettive. Alcuni per interessi commerciali, altri per fini militari, (come nuovo dominio della guerra), altri per avvicinare sempre di più il cittadino ai molteplici servizi della pubblica amministrazione.

Senza dubbio, la base comune è essere immersi in una vera "Società Digitale", con tutti i vantaggi e gli svantaggi che questo implica. Paragonando quello che è successo con l'evoluzione dei domini tradizionali, come ad esempio nell'ambito marittimo, è stato necessario definire regole, norme, codici di navigazione, modelli di segnaletica, sicurezza navale, linee di comunicazione; lo stesso è accaduto come per lo spazio aereo, nel quale è stato necessario regolare il suo utilizzo, principalmente per evitare incidenti, le rotte aeree, i procedimenti di aeronavigazione, i piani di volo. Cosa è successo nel caso del Cyberspazio?

Ci sono autori che considerano "Internet" il principale strumento di uso e gestione del cyber-spazio, e che senza Internet questo dominio non avrebbe ragione di esistere. Ci sono ovviamente Protocolli di Rete, norme dettate da organismi come la IEEE, codici di buona condotta o guide di buona pratica, *standard* internazionali come la famiglia delle ISO 27000, pubblicazioni del NIST, una serie di studi e raccomandazioni riguardanti la Sicurezza della Rete, tuttavia si evidenzia che non esiste un vero o reale "Ordine stabilito", e non si percepisce tra i diversi attori di questa Società Digitale una chiarezza di comportamento nel Cyberspazio. Non accade come nel caso della "Sicurezza Stradale o di Transito" che è disciplinata da parametri comuni e logici per gli attori coinvolti. Alcuni esempi quasi ovvi e riconosciuti dalla maggior parte delle

persone a livello mondiale sono: l'uso delle cinture di sicurezza, il rispetto della segnaletica stradale, nel caso dei pedoni, guardare su entrambi i lati della strada prima di attraversare, guidare nella corsia giusta, non guidare sotto gli effetti dell'alcool; la maggior parte di queste regole sono diventate ormai "norme di comportamento" e non dipendono dal pese, dal luogo, dal tipo di automobile, dalla strada, dalla tecnologia applicata, etc. e sono rispettate a livello mondiale.

Nella maggior parte dei casi, inoltre, il mancato rispetto di queste norme viene sanzionato in base alla legislazione vigente di ogni paese. Questo esempio denota senza dubbio un ordine, dei protocolli, una cultura e dei codici di comportamento.

Perché costa tanto arrivare a qualcosa di simile nel caso del Cyberspazio? A quanto pare, questi "veicoli e rotte cyberspaziali" necessitano di qualche meccanismo di controllo o di cyber-polizia". Possiamo inoltre chiederci o dirigere lo sguardo verso le Forze Armate e il loro ruolo, visto che sono concepite per difendere una nazione da qualsiasi minaccia, proveniente dall'aria, dal mare, da terra e allora anche da minacce provenienti dal Cyberspazio.. Questo in tempo di crisi e/o guerra, ma in tempo di pace, chi ci difende da queste minacce?

Le riflessioni esposte nei paragrafi precedenti su questa problematica, mettono in evidenza quanto sia difficile capirla, spiegarla e ancora di più risolverla. Da qui nasce la necessità di poter contare su una "Strategia Nazionale di Cyber- …"
e dico "Cyber- ...", perché persino nella terminologia non c'è consenso. Per alcuni si tratterà di Cyber Sicurezza, per altri di Cyber Difesa, per altri ancora di Cyber Guerra. Quello che è chiaro è il suo contributo essenziale alla Sicurezza Nazionale, indipendentemente dalla sua denominazione, e la sua relazione diretta con l'evoluzione delle tecnologie dell'informazione e delle comunicazioni.

Questa strategia deve tener presente alcuni fattori comuni, secondo l'opinione di chi scrive, di seguito indicati.

- Prima di definire la Strategia, bisogna individuare le minacce alla cybersicurezza nazionale, successivamente gli obiettivi che si vogliono raggiungere insieme alla misure da applicare. Alcuni

autori definiscono questo punto una adeguata "Analisi del rischio tecnologico", dove si stabiliscono tra le altre cose, le minacce, le vulnerabilità, le probabilità di impatto, gli indicatori, il calcolo del rischio.

- La Strategia deve integrare tutti gli attori di questa "Società Digitale", come il settore pubblico, privato, Forze Armate e cittadino.
- Deve considerare la protezione dell'Infrastruttura Critica Nazionale.
- Deve essere realizzabile, vale a dire che non serve a nulla tenerla sulla carta se non esiste una struttura organizzativa e gerarchica che ne garantisca l'applicazione.
- Deve tener conto della formazione di una "Cultura della Cybersicurezza" di tutti gli attori coinvolti.
- Si deve tener presente che la nazione si riflette nella citata Strategia con tutta la sua cultura e le sue tradizioni.
- Deve chiarire e standardizzare concetti, termini, linee d'azione ed essere una vera guida o quadro di riferimento, giacché dovrà essere la base di altri documenti normativi e regolamentari.
- Deve raggiungere un equilibrio tra il livello Strategico, Operativo e Tattico. Per questo non deve essere troppo generica e nemmeno eccessivamente tecnica, in modo da coprire un ampio spettro affinché tutti gli attori siano beneficiati da questa pubblicazione.
- Deve includere gli strumenti per prevenire, individuare, neutralizzare, rispondere e/o reagire alle cyberminacce, il che significa prendere decisioni giuste e tempestive oltre a valutare la dovuta Gestione del Rischio tecnologico inerente. Nell'elaborazione della Strategia si debbono considerare tutte quelle norme e/o disposizioni sia a livello nazionale che internazionale che riguardano questo dominio ed essere coerenti e integrative rispetto a queste.
- Deve rispettare la *privacy* dei cittadini e la riservatezza dei loro dati, rispettandone i diritti e le libertà.

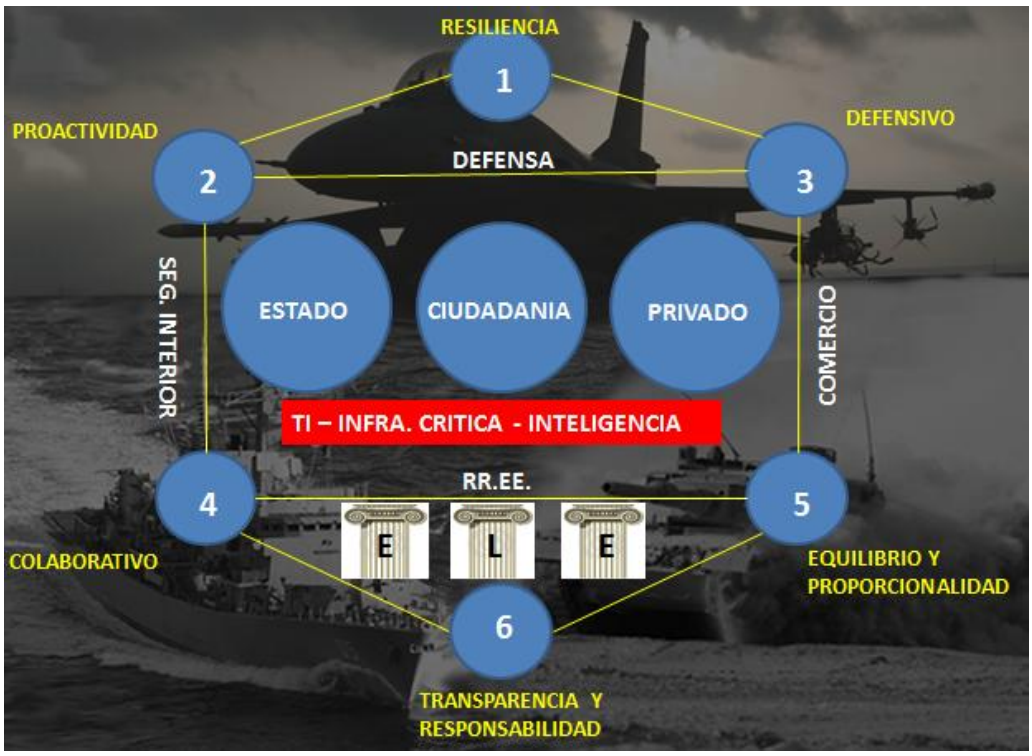
Nel caso del Cile esiste una Strategia Nazionale sulla Sicurezza e la Difesa, che riguardo all'area del cyberspazio, e si segnalano di seguito alcuni aspetti rilevanti.

- Riconosce che le minacce attuali alla sicurezza delle nazioni sono di diversa natura e che, nella maggior parte dei casi hanno carattere transnazionale ed includono tra le altre, il narcotraffico, la criminalità organizzata, il traffico di armi e i "Cyberattacchi".
- Segnala che per far fronte a queste nuove minacce si deve potenziare la presenza internazionale del Cile nella regione (Sudamerica) e nel mondo.
- Mette in evidenza il fatto che la sicurezza e la prosperità di molte nazioni dipende sempre di più da eventi che accadono fuori dalle loro frontiere e che in molti casi sfuggono ad un controllo diretto.
- Sottolinea come il divario tra paesi innovatori e consumatori di tecnologia può far si che la dipendenza tecnologica abbia un impatto sempre maggiore sulla sicurezza di questi ultimi.
- Fa notare come il Cyberspazio viene sempre più spesso utilizzato per compiere azioni ostili e/o criminali da parte di attori istituzionali e non istituzionali, e segnala anche come i metodi intrusivi che vengono impiegati – come gli attacchi informatici, i blocchi di sistemi, i furti di informazioni sensibili, lo spionaggio e la frode informatica – siano aumentati notoriamente nel mondo e anche in Cile, negli ultimi anni.
- Il cyberattacco è ritenuto una minaccia alla sicurezza del paese perché nella misura in cui il Cile continua ad evolversi, le attività commerciali, finanziarie, economiche, statali e strategiche prevedono un utilizzo sempre più intensivo del cyberspazio, con il conseguente aumento da parte di entità, pubbliche e private, di subire attacchi che possono incidere sulla loro sicurezza e su quella del paese.
- È necessario contare su competenze informatiche affidabili destinate a neutralizzare gli atti di ostilità contro i sistemi vitali della difesa nel cyberspazio.
- La Cyber-sicurezza inizialmente ha avuto una impostazione reattiva, per poi evolvere verso un approccio basato sull'anticipazione e il contenimento delle Cyber-minacce. A

questo punto, è importante sottolineare che in America Latina il Cile è tra quei paesi con una maggiore penetrazione digitale, in cui l'uso della tecnologia informatica è molto diffuso. L'Indicatore Società dell'Informazione (ISI) nel 2011, attribuisce al paese 5,70 punti su un massimo di 10, situandolo al primo posto per l'accesso ad Internet tra i paesi della regione.

Tuttavia, la citata Strategia, secondo l'autore, può essere migliorata negli aspetti relativi alla Cyber-Sicurezza e Cyber- Difesa, compresa la attuale nel cui capitolo "Mezzi della Difesa", si citano solo le forze terrestri, marittime ed aeree, e non si menziona la componente cyber spaziale.

Infine, per elaborare questa Strategia, occorre strutturare un Quadro Concettuale di principi, attori, linee d'azione, come quello proposto nella seguente figura, che può servire da base per la formulazione della "Strategia Nazionale per la Cyber – Difesa del Cile":



Nella figura, si delineano sei principi fondamentali: resilienza, proattività, difensivo, collaborativo, equilibrio e proporzionalità e infine, trasparenza e responsabilità, i quali danno un quadro per i settori Difesa, Commercio, Relazioni Internazionali e Sicurezza Interna, avendo come base le Tecnologie per l'Informazione e le Comunicazioni nonché il rafforzamento del Sistema di Intelligence Nazionale.

Inoltre, i pilastri di questa proposta di Strategia, considerata come esempio da questo autore per gli effetti della presente pubblicazione, sono: "Estructura (Struttura), Legislazione ed Educación (Istruzione)", coinvolgendo direttamente gli attori principali: "Stato, Cittadini e Settore Privato".

All'interno di questo modello di Strategia si possono prevedere inoltre iniziative per ogni linea o asse di azione, che questo autore denomina "Avvicinamenti Strategici per Pilastro", come per esempio per il Pilastro Struttura si può "rafforzare la capacità dello stato di affrontare le cyberminacce garantendo Riservatezza, Integrità e Disponibilità delle informazioni che vengono trattate nei Sistemi Critici di Informazione". Tutto ciò, contando su un modello efficace di risposta, in caso di incidenti informatici, da parte delle strutture preposte (CSIRTs, CERTs, Ministeri e Servizi Pubblici, Forze Armate, Settore Privato, Agenzia Nazionale di Intelligence, Multisettoriale).

Inoltre, per il Pilastro Legislazione, si può: "rafforzare la legislazione nazionale vigente in materia di Reati Informatici, Cybersicurezza e Cyberdifesa, con la formulazione di iniziative nel Congresso Nazionale, la modifica del nostro Codice Penale e tra le altre cose, l'analisi della Regolamentazione Internazionale.

Per il Pilastro Educación (Istruzione), l'Avvicinamento Strategico può essere: "fornire formazione, istruzione e competenze specifiche, per sensibilizzare la Sicurezza nel Cyberspazio" con gli appropriati programmi di sviluppo delle capacità rivolti ai funzionari pubblici e privati responsabili del TI, incentivi in ambito accademico per favorire lo scambio di conoscenze, attività di ricerca, innovazione e sviluppo tecnologico nell'ambito della Cybersicurezza

e della Cyberdifesa, così come realizzare campagne di Sensibilizzazione.

Per concludere, si può evidenziare che ogni paese ha la propria realtà che riguarda diversi fenomeni e tendenze che sono presenti ogni giorno nello sviluppo delle nazioni e dei suoi cittadini insieme alle relative minacce che ciò comporta, come è il caso dell'uso e lo sfruttamento del cyberspazio. Nonostante ciò, è importante elaborare un quadro normativo per queste azioni, che consenta la libertà d'azione nel Cyberspazio, seguendo però determinate norme di buona condotta e di uso adeguato di questo dominio. È importante inoltre essere capaci di definire in modo chiaro e semplice quale sarà la struttura organizzativa e procedurale per gestire i rischi di sicurezza cibernetici esistenti. Non possiamo aspettare che i nostri sistema tecnologici collassino o che i nostri sistemi critici di infrastrutture subiscano un cyberattacco per incominciare ad occuparci del problema.

Senza dubbio è indispensabile avere una visione multisettoriale, istaurare forme di cooperazione sia nazionale che internazionale su queste materia, definire chiaramente i diversi soggetti interessati, compreso il ruolo specifico delle Forze Armate, insieme alle linee d'azione ed ai relativi pilastri fondamentali sui quali la Strategia debba basarsi.

Infine, è opportuno constatare che deve trattarsi di un documento flessibile, che evolva nel tempo, come avviene per le Cyberminacce. Altro fattore importante è il contributo che può derivare dallo studio e dall'analisi di modelli e strategie di altri paesi, però bisogna tener presente che copiare strutture e modelli senza aver fatto precedentemente un' analisi adeguata del rischio nella nostra realtà non garantisce il successo.

Traduzione a cura dell'Ufficio per la Difesa, l'Esercito, la Marina e l'Aeronautica del Cile in Italia

Cyber sfide durante l'operazione "Margine Protettivo" (Israele)

Daniel Cohen e Danielle Levin
(Ricercatore associato e assistente di ricerca presso l'Istituto per gli Studi sulla Sicurezza Nazionale - INSS dell'Università di Tel Aviv)

La cyber guerra è diventata un'importante fonte di potere per le nazioni, e, allo stesso tempo, è una minaccia strategica per le infrastrutture critiche di una nazione, dato che la comunicazione, i media, la finanza, e molti altri settori si basano ormai sul dominio del cyberspazio. I militari, in particolare, sono diventati fortemente dipendenti dalle tecnologie avanzate del cyberspazio. A livello nazionale, Israele è in fase di creazione di un sistema integrato di cyber difesa nazionale, che richiede la cooperazione tra il settore civile (pubblico e privato) ed establishment di sicurezza e militari.

L'operazione "Margine Protettivo", condotta nella Striscia di Gaza da Israele nel luglio 2014, è un ulteriore esempio di scontro asimmetrico, non solo in termini di uso della forza, ma anche in termini di rispettivi fini strategici da entrambe le parti nella campagna. Conclusa la campagna militare di 50 giorni, è difficile determinare se i combattimenti ingaggiati da Hamas e altri gruppi palestinesi fossero il prodotto di una pianificazione anticipata (in particolare poiché nessuna delle due parti sembrava avere interesse in un conflitto). Analizzando gli aspetti cyber del conflitto si può rilevare un collegamento diretto tra il forte aumento del numero di attacchi contro obiettivi nello Stato di Israele contestualmente all'ingresso delle forze di terra dell'esercito israeliano nella Striscia di Gaza. Alcuni di questi attacchi possono essere attribuiti a cyber campagne organizzate di gruppi di hacker amatoriali, mentre altri attacchi informatici vertevano su un livello più sofisticato concentratosi sui network di comunicazione israeliani. Una volta terminata l'operazione di terra, il numero di attacchi è diminuito in modo significativo.

Attacchi alle infrastrutture finanziarie di una nazione hanno gravi ripercussioni, che potrebbero provocare pesanti danni finanziari, turbando l'abituale attività finanziaria di imprese commerciali e famiglie allo stesso modo. Anche se le capacità dell'esercito israeliano di gestire minacce cinetiche ha raccolto gran parte dell'attenzione durante l'operazione Margine Protettivo, è chiaro che Israele è stato anche costretto ad affrontare delle sfide informatiche.

Il focus dell'offensiva informatica, durante l'operazione, è stato la rete internet civile. Il sistema di difesa israeliano contro gli attacchi informatici durante l'operazione Margine Protettivo ha testato l'utilizzo di Israele della policy di governo in ambito informatico, e ha segnato un significativo miglioramento del coordinamento tra le organizzazioni di cyber difesa di Israele, compreso il funzionamento dei sistemi di sicurezza IT di Israele e la crescente cooperazione tra settore civile e settore della difesa. Quest'articolo esamina gli attacchi informatici avvenuti durante l'operazione Margine Protettivo, analizzando tre fattori principali: il volume di attacchi, gli attori dietro gli attacchi, e i progressi di Israele in materia di sicurezza informatica.

Volume di attacchi informatici contro Israele

Un grande attacco informatico durante l'operazione si è concentrato sui fornitori di comunicazione e di internet, con lo scopo di sovraccaricare il sistema e causare il collasso della rete israeliana. Più in generale, le azioni comprendevano attacchi DDoS (Distributed Denial of Service) e DNS (Domain Name Service), divulgazione di database e di informazioni personali di israeliani, come credenziali di accesso. Uno degli attacchi informatici iniziali contro Israele ha violato oltre 1.000 siti web israeliani, anche se la maggioranza di essi è stata considerata non cruciale, avendo così poco o nessun impatto significativo, dato che la maggior parte dei siti è stata ripristinata in poche ore e le informazioni erano già state pubblicate in attacchi precedenti. Inoltre, i provider Internet israeliani sono stati reindirizzati e gli IP stranieri sono stati bloccati per diverse ore. Ancora, sono stati divulgati gli indirizzi IP ed e-mail di impiegati

ministeriali israeliani; anche se i dati si sono rivelati essere vecchi e scaduti.

Ogni episodio ha generato ulteriori opportunità per Hamas di raccogliere ulteriori dati, essendo stati identificati nuovi potenziali bersagli. Inoltre, sono stati sviluppati metodi adeguati e mezzi di approccio a questi obiettivi, come ad esempio quando Hamas ha effettuato invii di massa di messaggi di testo agli israeliani in cui si affermava di essere della Security Agency israeliana (ISA), di Haaretz, o di Hamas.

Altri attacchi si sono concretizzati nell'interferenza con un satellite televisivo privato, che ha permesso che un messaggio di propaganda pro-Hamas andasse in onda momentaneamente sui canali 2 e 10 (Hamas aveva già lanciato un attacco simile contro i canali commerciali durante l'operazione Pilastro di Difesa). Il blog e l'account Twitter del portavoce dell'IDF hanno subito un grave attacco informatico condotto dalla Syrian Electronic Army (SEA), con messaggi postati in inglese e in arabo. Inoltre, grandi gruppi di hackeraggio hanno coordinato numerose cyber proteste contro Israele, sotto il nome di "OpIsrael". Queste operazioni hanno spinto i principali gruppi informatici a lavorare insieme, durante tutta l'operazione, per la causa palestinese.

Gli attori dietro gli attacchi

Vari sono stati gli attori che hanno coordinano gli attacchi contro Israele durante l'operazione Margine Protettivo. Molti erano legati a gruppi informatici con collegamenti a stati che sponsorizzano il terrorismo, e con qualche affiliazione al gruppo cyber Anonymous. Anonymous è un gruppo "hacktivisti" senza leader, suddiviso in decine di cellule, che volge l'attenzione su una causa sociale o politica attraverso l'hackeraggio. Per quanto riguarda gli attacchi contro Israele, Anonymous può essere divisa in tre celle: arabi, musulmani, e il restante insieme. In termini di capacità e abilità, i primi due gruppi di solito si fondono, mentre il terzo può essere costituito da hacker d'élite, ma l'operazione Margine Protettivo si è distinta in quanto questo calibro di hacker ha deciso di non partecipare. L'operazione Margine Protettivo ha

segnato un cambiamento nella percezione delle posizioni e delle azioni di Anonymous, inducendo l'opinione pubblica a chiedersi se Anonymous e altri gruppi di "hacktivisti" siano infiltrati e sfruttati da Hamas e altri affiliati di organizzazioni pro-terrorismo. Nel corso di Margine Protettivo è stato organizzato un certo numero di cyber proteste, anche se queste proteste informatiche sono diventate sempre più ripetitive, risultando in una esigua circolazione mediatica. Un esempio importante si è registrato verso la fine di luglio, quando Anonymous ha implorato gli hacker d'élite di unirsi alle iniziative, ma non è stato rilevato alcun grande attacco e la rete israeliana ha continuato a funzionare regolarmente.

Durante l'operazione, l'IDF ha collaborato con l'ISA per sventare gli attacchi pianificati dall'Iran in occasione dell'al-Quds Day (la "Giornata di Gerusalemme", dal nome arabo della città. N.d.t), un evento annuale organizzato dai leader iraniani contro Israele. L'attacco ha coinvolto hacker di tutto il mondo, che hanno tentato di disattivare i siti web israeliani. Gruppi di cyber terrorismo sponsorizzati da Stati, come l'Iranian Cyber Army (ICA) e il SEA hanno sferrato attacchi informatici durante l'operazione Margine di Controllo e, in generale, l'IDF afferma che l'Iran ha avuto un ruolo importante nell'incremento di attacchi informatici mirati a strutture civili israeliane durante l'operazione. Negli ultimi anni, i principali gruppi terroristici come Hamas e Hezbollah, con l'assistenza dell'Iran, hanno mostrato un crescente interesse nel campo del cyber terrorismo.

Un alto ufficiale del Corpo C4I israeliano ha osservato che, nel corso della campagna, elementi iraniani hanno lanciato una diffusa offensiva informatica contro obiettivi israeliani, inclusi i tentativi di danneggiare reti di sicurezza e finanziarie. Questi tentativi sono stati neutralizzati in modo relativamente semplice e veloce dalla difesa informatica israeliana, ma sembra che l'Iran stia investendo ingentemente nello sviluppo di efficaci capacità offensive contro i sistemi di infrastrutture, e possa quindi costituire una seria sfida per la difesa israeliana nel prossimo futuro. Nel 2013, una serie di attacchi contro i siti web delle principali banche e istituzioni finanziarie americane fu attribuito all'Iran. Un esperto di sicurezza

delle informazioni ha descritto questi attacchi, che comprendevano tecniche sofisticate mostrando capacità di agire in ambito importante contro obiettivi di alta qualità, come attacchi senza precedenti in termini di grado ed efficacia.

I progressi di Israele nella Cyber Security

Israele ha adottato un approccio cyber proattivo con una strategia di difesa pre-programmata, con capacità operative avanzate che hanno fornito un'ottima resa in security defense. Sia l'IDF sia l'ISA sono stati in grado di sventare qualsiasi tentativo di danneggiare le reti del governo israeliano e delle infrastrutture critiche. L'ISA ha confermato di essere stata in grado di mettere in sicurezza tutte le reti e i sistemi governativi israeliani contro gli attacchi informatici. Uno dei metodi di difesa è stato quello di bloccare gli IP stranieri per due ore, all'inizio dell'operazione Margine Protettivo. L'ISA, attraverso la sua divisione informatica, ha agito in coordinamento con gli imprenditori privati, il Ministero israeliano delle Comunicazioni e i media, adottando misure preventive contro gli attacchi.

L'IDF ha lavorato con una rete di comunicazione integrata d'intelligence militare e di aziende informatiche legate al Ministero della Difesa, che hanno contribuito a individuare ed eliminare tutte le minacce informatiche che giungevano da attacchi esterni. Inoltre, tutti questi sforzi contro tali attacchi sono stati coordinati dall'Israel Cyber Bureau.

Il capo dell'unità di cyber-defense dell'IDF ha affermato che vi sono stati anche tentativi di infiltrazione nelle reti dell'IDF, e che le già alte capacità tecnologiche di Israele sono state ulteriormente elevate al fine di assicurare che tali violazioni non si verificassero.

Risultati

Finora, non vi è stata alcuna dimostrazione di elevate capacità tecnologiche e di intelligence in attacchi informatici contro le reti israeliane da parte di unità informatiche indipendenti di organizzazioni terroristiche (come Hamas). Per riuscire a realizzare

un attacco informatico è necessario determinare gli obiettivi, e servono coordinazione dell'attacco e strumenti informatici. Le organizzazioni terroristiche devono ancora superare le soglie operative e tecnologiche indipendenti, per condurre una guerra informatica indipendente contro Israele e altri paesi. Organizzazioni terroristiche come Hamas e Jihad islamica palestinese possiedono capacità e risorse tecnologiche molto limitate. Mentre ci sono gruppi di cyber terrorismo affiliati a Stati, come il SEA e l'ICA, che sono in grado di condurre operazioni informatiche più avanzate.

L'analisi dell'attività cyber dell'Iran durante l'operazione Margine Protettivo indica una crescente maturità nelle capacità operative della Repubblica Islamica e dimostra che essa è in grado di condurre una vasta cyber-operazione militare contro una serie di obiettivi, utilizzando un'ampia gamma di metodi. Inoltre, l'attenzione dell'Iran per il cyberspazio durante l'operazione Margine Protettivo può indicare l'inizio di un processo in cui la guerra cibernetica sostituirà il terrorismo classico come uno dei principali strumenti della dottrina iraniana di guerra asimmetrica. La guerra cibernetica, che offre a chi compie l'attacco distanza e possibilità di negare, due caratteristiche che gli iraniani considerano estremamente preziose, consente di inferire gravi danni al fronte civile di un nemico che goda di superiorità militare e geostrategica. Finora le capacità dell'Iran nel cyberspazio rimangono inferiori a quelle d'Israele e a quelle delle principali potenze tecnologiche, ma la Repubblica Islamica sta rapidamente ed efficientemente colmando il divario.

Nel frattempo, le manifestazioni pro-Gaza hanno comportato un incremento degli episodi di antisemitismo, soprattutto in Europa, tanto da indurre un importante handle Twitter di Anonymous a commentare l'allarmante situazione. Anche se Anonymous non ha cessato le proprie proteste, è incontestabile che i principali attacchi informatici furono ampiamente ridotti. Gli esiti antisemiti di troppe delle manifestazioni pro-Gaza hanno indotto gli "hacktvisti" all'interno della comunità a sollevare dubbi sull'iniziativa pro-araba di Anonymous; molti hanno sostenuto che il perseguimento della giustizia propugnato da Anonymous avesse preso un taglio pro-

palestinese, e il suo coinvolgimento nel conflitto israelo-palestinese ha portato ad accuse di antisemitismo.

Quando i membri della comunità di Anonymous si sono trovati di fronte all'ipotesi che dei gruppi terroristici potessero essersi infiltrati in alcune divisioni di Anonymous per portare avanti la propria agenda, molti hacker hanno risposto affermando che chiunque può unirsi ad Anonymous; tuttavia, coloro che sfruttano la comunità di Anonymous per ottenere visibilità avranno difficoltà a sostenere attacchi informatici a lungo termine. Inoltre, alcuni membri credevano che il concetto di cyber-terroristi all'interno di Anonymous fosse una vaga minaccia piuttosto che una questione reale. Di fronte alla crescente ondata di antisemitismo, molti membri si sono discostati concentrandosi su Israele o spostando l'indice sull'identità del "vero" nemico.

Ciò fornisce potenzialmente una spiegazione per la distinzione avutasi fra le operazioni Pilastro di Difesa e Margine Protettivo, per quanto riguarda l'identità di chi ha compiuto gli attacchi. Nell'operazione Pilastro di Difesa, il governo israeliano ha fronteggiato oltre 100 milioni di attacchi informatici in otto giorni, con indirizzi IP riconducibili a siti in tutto il mondo, prevalentemente in Europa e Stati Uniti. Mentre durante l'operazione Margine Protettivo, il rapporto di una società di sicurezza informatica ha stimato che il 70% degli attacchi informatici contro i siti governativi israeliani era riconducibile al Qatar e ad altri paesi del mondo musulmano.

Conclusione

Le cyber cellule delle organizzazioni terroristiche non sono state finora in grado di compiere attacchi informatici strategici contro Israele, cosa che richiede elevati livelli di intelligenza e di capacità tecnologiche. Le organizzazioni terroristiche stanno presumibilmente migliorando e sviluppando le proprie capacità informatiche avanzate, che potrebbero in futuro costituire una minaccia alla sfera informatica. Questa minaccia è interconnessa alle organizzazioni terroristiche e al terrorismo sponsorizzato da Stati, che include l'inganno tramite gruppi di "hacktivisti". La prospettiva

della difesa per la cybersecurity israeliana dovrebbe riconoscere questo legame come una minaccia alla sicurezza nazionale.

Il legame tra le organizzazioni terroristiche, il terrorismo sponsorizzato da Stati, e lo sfruttamento di gruppi di "hacktivisti" dovrebbe essere ammesso e riconosciuto come una minaccia nazionale. Le organizzazioni terroristiche che s'infiltrano in gruppi di "hacktivisti" come Anonymous dovrebbero essere affrontate con misure governative preventive. Un'azione preventiva deve prendere di mira anche le risorse dell'operatore, dai siti web alle finanze. Le parti coinvolte, inoltre, devono essere denunciate, accusate e condannate per atti terroristici.

Il cyber case study durante l'operazione Margine Protettivo mostra la necessità della spiegazione applicata a comunità di "hacktivisti" in tutta la rete Internet come parte della percezione di difesa nazionale. Questo case study è importante anche per i partecipanti attivi nella sfera non-virtuale, indica la necessità di spiegazione nei network dei social media e in manifestazioni fisiche, e può essere uno strumento contro i raggiri e gli inganni in rete. I cyber difensori israeliani sono riusciti a sventare attacchi condotti da elementi sponsorizzati da Stati, ma non vi è alcuna certezza di poter ripetere l'impresa in futuro. Israele deve ancora stabilire un approccio globale di preparazione.

Il successo ottenuto nel prevenire il recente attacco è più indicativo di cooperazione e lavoro coordinato a livello professionale. L'intensificazione della cyber potenza e degli attacchi da parte di Iran e di altro terrorismo sponsorizzato da Stati sta procedendo a ritmo sostenuto, e presto potrebbero essere in grado di sfidare le capacità difensive di Israele in misura maggiore rispetto quanto mai in passato. Inoltre, le misure difensive non sono sufficienti, e quindi Israele deve lanciare attacchi preventivi e di rappresaglia. L'attuazione di regolamenti informatici e azione preventiva mira a rendere la difesa informatica una necessità intrinseca per proteggere lo stato di Israele, compreso il settore civile (pubblico e privato). In primo luogo, per aumentare la consapevolezza della possibilità che gli operatori possono essere ritenuti responsabili di favoreggiamento di attacchi di hackeraggio o informatici, è indispensabile riconoscere

questi settori come parte dell'infrastruttura della sicurezza nazionale.

C'è stato un miglioramento significativo nel coordinamento delle organizzazioni di cyber difesa di Israele durante l'operazione Margine Protettivo, compreso il funzionamento dei sistemi di sicurezza IT di Israele e la crescente cooperazione tra settore civile e settore della difesa. Questa esperienza sottolinea la necessità immediata di formulare un protocollo per la difesa del cyberspazio civile. Altre misure comprendono azioni esplorative preventive.

In secondo luogo, è necessario identificare gli operatori degli attacchi informatici. Come sottolineato, in molti casi gli autori degli attacchi informatici sono stati ingannati ed erano completamente ignari del fatto che venissero manovrati da organizzazioni terroristiche sponsorizzate da Stati. È quindi possibile che queste azioni possono ridurre la portata del fenomeno.

La cyber-security in Spagna (Spagna)

Carlos De Palma Arrabal
(Colonnello Addetto per la Difesa, Militare, Navale ed Aeronautico del Regno di Spagna in Italia)

Ringraziamo la Direzione della Rivista "Informazioni della Difesa" per l'invito a collaborare con questo articolo, destinato a condividere esperienze nell'appassionante ambito della Cyber Security, nel quale l'Italia e la Spagna mantengono una stretta relazione bilaterale, sempre aperta alla cooperazione.

È noto che una delle potenzialità dei paesi sviluppati è l'uso intensivo e trasversale delle tecnologie e infrastrutture, civili e militari, relazionate con i sistemi informativi e di telecomunicazione. In effetti, l'interazione e l'interdipendenza rispetto alla nuova dimensione transazionale, denominata Cyberspazio, è sempre maggiore, coinvolgendo ogni attività della nostra vita quotidiana ed esigendo l'attenzione di tutti gli organi governativi, sociali ed economici connessi in un mondo globale.

Pur tuttavia, ogni moneta ha una doppia faccia e insieme agli attuali benefici derivati dallo sviluppo tecnologico e sociale legato al Cyberspazio, vi sono anche i rischi e le vulnerabilità dei nostri sistemi e delle nostre infrastrutture. Tali vulnerabilità sono state evidenziate in numerose occasioni, sia per cause tecniche o disastri naturali, che per attacchi cibernetici di varia provenienza e a carattere intenzionale, di cui ogni giorno milioni di persone sono vittime e che provocano gravi danni e perdite economiche calcolate in centinaia di miliardi di euro. Pertanto è essenziale disporre di un'adeguata capacità di Cyber Defence per mantenere l'uso ed il controllo dei nostri sistemi informativi e disporre di libertà di azione e di uso nel Cyberspazio.

Secondo quanto si riassumerà di seguito, in Spagna si stanno sviluppando diverse iniziative a livello nazionale, coordinate sia nei campi civile e militare, che in ambiti bilaterali e multilaterali, con l'Unione Europea e la NATO, in modo da garantire la sicurezza

nazionale e contribuire alla stabilità internazionale e all'uso legittimo del Cyberspazio.

Normativa spagnola sulla cyber security

Tutti i cittadini e le organizzazioni devono prevenire e proteggersi dagli attacchi cibernetici (cyber criminalità, cyber terrorismo, cyber spionaggio, attivismo sovversivo nella rete, ecc.). La crescente richiesta nel campo della Cyber Security va di pari passo con i casi rilevati e intenzionali di attacchi cibernetici che si susseguono ogni giorno. Si può notare ad esempio il crescente aumento delle offerte di posti di lavoro per persone specializzate in Cyber Security, le iniziative contro gli attacchi cibernetici di stampo militare, le analisi forensi, la tutela della proprietà intellettuale, la sicurezza industriale e le nuove precauzioni nell'uso di computer, database, telecomunicazioni fisse e mobili, internet, sistemi cifrati e di identificazione, reti ferroviarie ed aeree, infrastrutture critiche e sistemi di controllo remoto.

Per sviluppare questo campo, in Spagna si sono prese le seguenti iniziative:

- la Direttiva della Difesa Nazionale del luglio 2012 considera gli attacchi cibernetici una minaccia globale, che potrà essere affrontata solo da un insieme di forze, coordinate dalla NATO e dall'Unione Europea, ma che dovrà contare altresì sull'appoggio di altri paesi ugualmente interessati al controllo di questa minaccia. In questo ambito, la Spagna partecipa e favorisce una gestione integrale e multilaterale della Cyber Security.
- Per raggiungere tali obiettivi, la Strategia Nazionale di Sicurezza del 31 maggio 2013 identifica dodici minacce/rischi: conflitti armati, terrorismo, cyber minacce, crimine organizzato, instabilità economica e finanziaria, vulnerabilità energetica, proliferazione delle armi di distruzione di massa, flussi migratori irregolari, spionaggio, emergenze e catastrofi, vulnerabilità dello spazio marittimo, vulnerabilità delle infrastrutture critiche e dei servizi essenziali. Molte di queste minacce sono collegate tra loro e con il Cyberspazio. Considerando che le Cyber minacce sono al terzo posto della classifica, questo ci fa supporre che devono

essere affrontate con la "Cyber Security", stabilendo, allo stesso tempo, alcune Linee di Azione strategiche che sono state sviluppate nella "Strategia di Cyber Security Nazionale".

- La Strategia di Cyber Security Nazionale è stata approvata il 5 dicembre 2013 e si prefigge come obiettivo principale un uso sicuro delle Reti e dei Sistemi Informativi e di Telecomunicazione, attraverso il rafforzamento delle capacità di prevenzione, difesa, rilevazione e risposta agli attacchi cibernetici. In Spagna, per raggiungere questo risultato, la Strategia stabilisce sei obiettivi specifici (pubbliche amministrazioni, imprese e infrastrutture critiche, ambito giuridico e di polizia, sensibilizzazione, formazione e collaborazione internazionale) e otto Linee di Azione:
    - capacità di prevenzione, rilevamento, risposta e recupero di fronte alle cyber minacce.
    - Sicurezza dei Sistemi Informativi e di Telecomunicazione utilizzati dalle Pubbliche Amministrazioni.
    - Sicurezza dei Sistemi Informativi e di Telecomunicazione utilizzati dalle Infrastrutture Critiche.
    - Capacità di Investigazione e persecuzione del cyber terrorismo e della cyber criminalità.
    - Sicurezza e resilienza delle Tecnologie dell'Informazione e delle Comunicazioni nel settore privato.
    - Conoscenze, competenze e ciclo di Ricerca, Sviluppo e Innovazione.
    - Cultura della Cyber Security.
    - Impegno Internazionale.
- Per vigilare sulla corretta applicazione della già citata Strategia di Sicurezza Nazionale, il 25 febbraio 2014 è stato creato il Consiglio di Cyber Security Nazionale, dipendente dal Consiglio di Sicurezza Nazionale e formato da consiglieri permanenti di dieci Ministeri, del Centro Nazionale di Intelligence (CNI) e del Dipartimento di Sicurezza Nazionale (DSN). Per il Consiglio di Cyber Security Nazionale lavorano due Comitati Specializzati: Cyber Security e Situazione. Quest'ultimo Comitato Specializzato di Situazione è unico ed è

supportato dal Centro Situazioni del Dipartimento di Sicurezza Nazionale, al fine di garantire il suo collegamento con il resto dei centri operativi nazionali e di favorire le decisioni e risposte in situazioni di crisi. I due Comitati Specializzati agiscono in modo complementare con la direzione strategica e politica del Consiglio di Sicurezza Nazionale e del Presidente del Governo.

- La ripartizione delle responsabilità sulla Cyber Security tra i principali Ministeri è la seguente:
  - MINISTERO DELL'INTERNO: per le Infrastrutture Critiche, attraverso il Centro Nazionale di Protezione delle Infrastrutture Critiche (CNPIC), il Cyber crimine ed il Cyber terrorismo.
  - Centro Criptologico Nazionale (CCN): per le Pubbliche Amministrazioni, in collaborazione con il Computer Emergency Response Team (CCN-CERT).
  - MINISTERO DELL'INDUSTRIA, ENERGIA E TURISMO: per sostenere gli sviluppi tecnologici e le imprese pubbliche e private.
  - MINISTERO DELLA DIFESA: per la difesa dei sistemi informativi e delle reti di comunicazione del Ministero e per la protezione dei sistemi di interesse nazionale ad esso assegnati.
- Tra le varie iniziative, vi è anche il Programma di Esercitazioni di Simulazione di Incidenti di Cyber Security, al fine di assicurare il coordinamento tra gli organismi interessati e, in particolare, tra il CCN-CERT della Pubblica Amministrazione, il Comando Congiunto di Cyber Defence (MCCD) ed il CERT di Sicurezza e Industria. I CERT delle Comunità Autonome Regionali, quelli degli enti privati e degli altri importanti servizi di Cyber Security si coordinano con i suddetti a seconda delle competenze di ognuno di essi.

IL COMANDO CONGIUNTO DI CYBER DEFENCE IN SPAGNA (MCCD)

Esigenza Operativa ed evoluzione del MCCD

L'esigenza operativa del MCCD si basa sulla dipendenza delle Forze Armate dal Cyberspazio, sia per l'organizzazione delle operazioni militari che per la loro direzione ed esecuzione. Qualsiasi conflitto moderno implica azioni congiunte nel Cyberspazio, essendosi costituito come quinto ambito, dopo quello terrestre, marittimo, aeronautico ed aerospaziale.

La creazione del Comando Congiunto di Cyber Defence è la scelta più efficiente per la ripartizione delle responsabilità tra le Forze Armate o per creare un nuovo Esercito. Per la fine del 2014 il MCCD disporrà di circa 70 esperti e si incaricherà delle tre competenze principali: Difesa, Utilizzo e Risposta.

Per quanto riguarda la capacità di Difesa, il MCCD dispone di un suo proprio Centro di Risposta (CERT), tra le cui funzioni vi sono il coordinamento, la direzione ed il supporto all'attività dei centri relazionati con la sicurezza informativa dell'Esercito, della Marina e dell'Aeronautica e, in quest'area, si arricchisce di tutti i metodi e strumenti disponibili sul mercato, basati su tecnologie a doppio uso, ossia valide per uso civile e militare. All'interno di ogni Forza Armata esiste un'autorità di sicurezza, responsabile di ogni sistema o rete specifica che si occupa della sua protezione, della disponibilità e del controllo dei requisiti necessari ad ottenere la certificazione di sicurezza, in conformità alle disposizioni e agli standard stabiliti dal MCCD. D'altro canto, le competenze di Utilizzo e Risposta sono una responsabilità esclusiva del MCCD che, in questo ambito, collabora con il settore industriale e le Università nella ricerca delle tecnologie, mezzi, procedure e strumenti specifici, che offrano soluzioni alle necessità specifiche delle operazioni militari.

Il MCCD si occupa altresì delle forze militari rischierate in operazioni internazionali, essendo più esposte e sottomesse ad un maggior livello di rischio. E' previsto inoltre che il MCCD collabori nella protezione di reti e sistemi di interesse strategico nazionale nel caso in cui avessero bisogno di supporto, così come con altri centri

di risposta militare alleati. La Spagna è stata socia fondatrice e svolge un ruolo attivo, attraverso il MCCD, nelle attività didattiche, nel foro di ricerca e nelle cyber esercitazioni del Centro d'Eccellenza nel Cyber Defence di Tallìn (Estonia). In Spagna, così come in altri paesi o nell'UE, la normativa giuridica applicabile alla Cyber Security è una parte fondamentale nello sviluppo delle sue attività, pertanto il MCCD si avvale del Gabinetto Giuridico dello Stato Maggiore della Difesa, incaricato di applicare la legislazione generale alle specificità del Cyberspazio, assistendo il suo Comandante in ogni situazione gli si presenti.

Il MCCD ha i seguenti compiti:

- Protezione di reti e sistemi congiunti delle Forze Armate.
- Coordinare le attività di difesa delle Forze Armate.
- Rispondere ai cyber attacchi in forma legittima e proporzionata.
- Dirigere la sensibilizzazione e la formazione della Cyber Defence nelle Forze Armate.
- Assumere la rappresentanza Nazionale ed Internazionale del Ministero della Difesa nei temi di Cyber Defence.
- Prestare assistenza se necessario nei casi in cui vengano compromessi gli interessi nazionali.

Gli obiettivi a breve e medio termine del MCCD sono:

- Operare in coordinamento con il Comando delle Operazioni (MOPS) ed il Centro di Intelligence delle Forze Armate (CIFAS), secondo l'organizzazione di base delle Forze Armate in Spagna (Decreto Reale 872/2014 del 20 ottobre 2014, che altresì coordina il Comando Congiunto delle Operazioni Speciali, il Comando di Vigilanza e Sicurezza Marittima, il Comando di Difesa e Operazioni Aree e l'Unità Militare di Emergenze).
- Potenziare la sensibilizzazione e attuare il Piano ed i Programmi di Formazione e Addestramento per tutto il Ministero della Difesa.
- Dirigere e coordinare le capacità difensive delle Forze Armate.
- Adeguare le risorse del personale alle esigenze operative.

- Raggiungere la Capacità Operativa Finale nella Difesa, Utilizzo e Risposta.
- Ottenere l'approvazione del Bilancio annuale.
- Collaborare nel raggiungimento degli obiettivi preposti dalla Strategia di Cyber Security Nazionale.
- Collaborare in stretta relazione con gli organismi della Pubblica Amministrazione.
- Favorire il progresso industriale e rafforzare il ciclo di Ricerca, Sviluppo e Innovazione, collaborando con imprese ed Università.
- Aumentare la cultura di Cyber Defence.
- Promuovere e appoggiare l'impegno internazionale con le organizzazioni internazionali e con le Nazioni alleate.

Gli obiettivi a lungo termine (Obiettivi Permanenti) del MCCD sono:

- Sviluppare le capacità di Difesa, Utilizzo e Risposta.
- Perfezionare il Piano ed i Programmi di sensibilizzazione, formazione e addestramento.
- Collaborare nel raggiungimento degli obiettivi stabiliti nella Strategia di Cyber Security Nazionale in vigore.

Considerazioni finali

La Spagna ha fatto importanti passi in avanti nell'utilizzo libero del Cyberspazio a fini pacifici e nel tenere il passo mantenendo l'iniziativa per prevenire ed affrontare gli attacchi cibernetici sempre più frequenti, intensi, sofisticati e gravi.

Per riassumere e trattare in modo adeguato la nuova dimensione del Cyberspazio e dei suoi nuovi sistemi, infrastrutture e procedure, è necessario prendere in considerazione alcuni aspetti:

- considerare il Cyberspazio come parte integrante delle nostre vite e attività generali, sia in ambito civile che militare, per contribuire alla sicurezza nazionale ed internazionale.
- Favorire lo sviluppo di tecnologie industriali e della ricerca scientifica ed universitaria che offrano soluzioni, strumenti, sistemi e procedure di qualità sempre più sicuri, visto che

nell'hardware, nel software e nella gestione dei sistemi e reti si trova immerso il primo baluardo della Cyber Defence.

- Potenziare la sensibilizzazione, la formazione e l'addestramento specifico di ogni tipo di utente sulla vulnerabilità e difesa dei sistemi e reti di informazione, essendo il fattore umano uno degli anelli deboli della catena.
- Contare su conoscenze specialistiche e su personale tecnico che conosca profondamente la tecnologia propria dei sistemi informativi e reti di telecomunicazione. Questa conoscenza specializzata permetterà di disporre delle abilità di prevenzione, utilizzo e risposta, garantendo il libero uso del Cyberspazio ed il suo sviluppo efficace nelle attività e missioni civili, nelle operazioni militari e nell'impiego efficiente di tutte le risorse.
- Sviluppare le strategie, i regolamenti, gli accordi di cooperazione, le esercitazioni e lo scambio di informazioni ed esperienze a livello locale, regionale, nazionale ed internazionale con paesi alleati, essendo tutti i soggetti connessi globalmente (la Spagna è coordinata con la NATO e la UE).
- Aggiornare ed adattare la base giuridica nazionale ed internazionale, affinché si possa agire contro gli individui, i gruppi e le organizzazioni che intraprendono attacchi cibernetici intenzionali ed illeciti.
- Organizzare e dotare con risorse economiche adeguate le forze con capacità di reazione nazionali ed alleate (di polizia, militari, CERT, ecc.) affinché risultino interoperabili, siano supportate da una specifica intelligence e siano capaci di prevenire, contrastare e, nel caso, rispondere agli attacchi cibernetici.

Per concludere, occorre essere consapevoli dell'esigenza di tenere il passo e l'iniziativa nel Cyberspazio, per concorrere alla tutela delle libertà individuali, ispirare fiducia nella popolazione, proteggere il legittimo sviluppo economico e difendere i valori universali della nostra società. Pertanto, si deve investire adeguatamente nelle risorse umane, nei mezzi materiali, nella legislazione internazionale e nelle procedure convenute con i nostri alleati.

Traduzione della Dott.ssa Antonella Di Lorenzo

WWW (World Wild West): the American New Frontier and the US Cybersecurity Dilemma (U.S.A.)

Cristiana Era

(Analista indipendente)

The United States is the country of birth of the greatest technological revolution bridging the 20th and the 21st centuries: internet. Its potential and its implications might not have been entirely understood at the onset of the '60s, when the net was still at his embryonic stage, and it certainly took few decades before it could develop into an international network, an open space with literally no frontiers. But once the net bypassed the closed academic and military environment, it was just a matter of – not too much – time before it could become an overlapping system redefining our daily life: from social relations to business, from politics to communications.

The United States was obviously the first to get the most out of this revolution and today it is still the leader of anything related to internet and pc technology. As the net expanded beyond American boundaries, the US high tech private sector could reach out to the global market operating in a monopoly system. The need for constant innovation spurred the American society to become the most technologically advanced of our times.

However, high standards of computerization came with a significant vulnerability to hacking and to any type of cyberthreat.

While in the last decade of the century basically all government agencies - the intelligence and the military in the first place - adopted the net for their regular activities, the security issue was largely underestimated and little was done by either the American institutions or by the private sector. The proliferation of hackers, from bored teenagers to individual criminals, from disgruntled employees to hostile State actors or terrorist groups in cyberspace, did change the situation. Moreover the number of internet users skyrocketed in a short time, which led to the creation

of a new, virtual world, where any sort of activity could be put in place: institutional, cultural, social, political campaigning, banking, trade, communication, all of them irreversibly interconnected to the real world. The demand for internet security increased accordingly, but the growing dependence of sensitive areas (like military operations, energy infrastructures, etc.) on cyber technology also significantly contributed to raise political attention towards online threats.

By the turn of the century, many top officers and officials inside government's agencies became finally aware of the risks posed by the fifth domain, as cyberspace is also known. The first to plan an ad-hoc body specifically committed to cyberdefense and security was the American Air Force (AF) in 2006 following the inclusion of cyberspace in the AF Mission statement, which, by the end of 2005, read: "The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in air, space and cyberspace". Supremacy in the new dimension was then considered a matter of utter importance, mostly from a military perspective. In the words of the AF Cyberspace Task Force Director, Lani Kass:

> *"Cyberspace is something on which, as a technologically advanced nation, the United States is hugely dependent. You use your ATM card, you use your cell phone and you go to an Internet cafe. If somebody is pregnant, they go have a sonogram. If they are sick, they have an X-ray or an MRI. All those things are in cyberspace. Our life has become totally bounded, dependent on cyberspace. Therefore, the importance of that domain is not only for how we fight, but also for our way of life (…) Cross-domain dominance means being able to deliver effects in all domains at the same time, at the speed of sound and at the speed of light. We cannot afford to allow an enemy to achieve cross-domain dominance before us. This is the nature of the transformational mission the chief and the secretary gave us. Enemies who cannot match us on land, at sea, in the air, or in space, are exploiting the fact that in cyberspace you have a very low entry cost"* (1).

Unfortunately, the AF Cyber Command maintained a provisional status and was never brought into permanent activation. Only in 2009 a unified military Cyber Command (USCYBERCOM) was created, becoming fully operational in 2010 under the direction of Lt. Gen. Keith Alexander who headed the National Security Agency (NSA). The dual role of the NSA Director who is also the USCYBERCOM chief guarantees coordination between the primary security agency and the unit, which however is subordinated to the US Strategic Command (StratCom). Its core mission is to manage and protect the Pentagon's 15,000 computers' network across 4,000 military bases in 88 countries and to conduct military cyberspace operations.

Some experts at the time argued that USCYBERCOM was a response to increased activity in the fifth dimension, one of the most relevant having been the Russian cyber attack against the Georgian government's communication and banking system in the summer 2008 (2). But this is a unit devoted to the protection of military systems, the "dot-mil" domain. Clearly national security in cyberspace could not be limited to the military, due to the dual nature of most of the so-called critical infrastructures (3), including – among others - telecommunications, electrical power systems, banking, finance, and transportation. The defense of the "dot-gov" domain was left under the competence of the Department of Homeland Security (DHS), which unfortunately proved - according to its critics – to be unable to implement defense policies because of inefficiency and ineffective leadership (4).

Filling the gap?

From 2009 onwards, the quick escalation of hacking, criminal and spying activities in American websites (including those of the Pentagon and the DHS) and failure by the US Congress to approve significant cybersecurity legislation forced the Obama administration to undertake further steps for the improvement of critical infrastructures' defense. Only on February 12, 2013, though, the White House released the Executive Order (E.O.) 13636: Improving Critical Infrastructure Cybersecurity, a comprehensive approach that

recognizes the need for increased coordination and cooperation between private and public sectors and for information sharing in the protection of key assets against cyberthreats.

To this purpose the E.O. 13636 charged the National Institute of Standards and Technology (NIST) of the Department of Commerce with the development of a framework to reduce cyber risks to critical infrastructures, and provided for the inclusion of privately owned critical infrastructures in the Enhanced Cybersecurity Services program (5). The Cybersecurity Framework was issued one year later, in February 2014, establishing a set of standards, guidelines and best practices to coordinate public agencies and private entities addressing cyber risks. However their adoption by non-governmental companies and organizations is entirely on voluntary basis and that's why the E.O. 13636 refers to specific incentives and benefits programs for all those who implement the Framework.

Both the E.O 13636 and the Framework have been considered a step forward in the protection of vital infrastructures and networks, and in the promotion of a nation-wide coordinated effort to address cybersecurity, but they are also deemed insufficient in the face of rapidly evolving threats. Experts note that Obama's Order lacks the necessary authority to impose the implementation of common rules and standards by private stakeholders. Besides, the Framework does not provide for new standards and practices; on the contrary, it refers to existing rules of conduct and procedures (6).

The E.O. and the Framework's regulatory nature and absence of funds allocation in the text - in addition to the assignment of responsibilities to DHS and to NIST instead of NSA and CYBERCOM - led some observers to question their ability to produce concrete results (7), calling for the adoption of a comprehensive legislation that might include key components like education and training, cybersecurity liability, international cyber engagement, and the development of a cyber workforce.

As a matter of fact, several attempts to pass a nationwide legislation on cybersecurity were made in the past without success.

One of the bills submitted to the Congress, the Cyber Intelligence Sharing and Protection Act (CISPA), has been reintroduced several times since it was initially proposed in 2011 by House Representative Michael Rogers. After the setbacks at the Senate, the House of Representatives reintroduced it in January 2015 for the third time, in the aftermath of last November's cyberattack against Sony Pictures, initially attributed to North Korea's hackers.

Since the beginning, the bill spurred a fierce debate in the American public opinion: opposition groups, mostly civil rights organizations and movements, argue that, if passed by the Congress, CISPA would affect key democratic principles by allowing government departments like DHS and DoD (Department of Defense) to legally spy on citizens and to access to private data and information without effective accountability measures. Privacy and civil liberties advocates have found a staunch supporter in the current Administration: the White House had threatened several times to veto the bill, while strong corporate lobbies, like the powerful American Chamber of Commerce, are pressing for the adoption of CISPA.

The ongoing tug-of-war on cybersecurity legislation and the slow pace of any regulation that might offer pre-emptive measures and rapid reaction to cyberattacks to counterweight the damage inflicted to vital national networks unveil what is probably the thorniest dilemma underlying the cyberspace issue: security vs. freedom and civil rights protection. The debate involves the Administration, the corporate sector and the entire American society and has assumed, at times, harsh overtones as in the Snowden case, which revealed the surveillance – some would say "spying" – activities by the NSA over millions of internet users thanks to the data access from web giants like Microsoft, Google, Facebook, YouTube and Skype. Aside from international indignation, the summer 2013 Prism scandal - as the surveillance program was known - sparked off outrage among civil liberties groups and increased public mistrust against the introduction of any regulation or act, like the aforementioned CISPA, that might legally legitimate

the government's violation of citizens' privacy. Fears of restrictions over internet freedom also widened and President Obama, who authorized the NSA's program, had a difficult time in publicly addressing the issue amid great embarrassment and loss of credibility.

Looking ahead: squaring the circle

The mounting pressure by privacy advocates has somehow slowed the development of a comprehensive policy. But after another year marred by hundreds of cyberattacks against companies and federal networks, cybersecurity has surged to a top priority in the presidential agenda, and for the first time it was included in the State of the Union speech of January 20, 2015 (8). The President also announced a legislative proposal promoting information sharing, laying the grounds for liability protections for companies, and safeguarding privacy and civil liberties protection (9), and launched key policy initiatives (10) on consumer protection and privacy.

The proposal, which is an update of the DHS Cybersecurity Authority and Information Sharing, of the Law Enforcement Provisions Related to Computer Security, and of the Data Breach Notification, addresses three key issues: enhancing cyber threat information sharing within the private sector and between the private sector and the Federal Government; protecting individuals by requiring businesses to notify consumers if personal information is compromised; strengthening and clarifying law enforcement's ability to investigate and prosecute cyber crimes (11).

Although experts welcomed this renewed effort by the Administration to engage private and public entities in the defense of national interests in cyberspace and to keep the issue on top of the government's agenda, doubts remain on whether these are sufficient steps to hold back cybercrime. Defense of personal rights and freedoms continues to come into conflict with the need of tightening controls over the net and restrict its openness, which is at the same time the core of its *raison d'être* and its main vulnerability. Unlike political debates, which are time-demanding, threats evolve

rapidly in a fast-pace environment like internet. And so do the actors behind the attacks. If until now most cyberattacks were confined to criminal activities, industrial espionage and disruptive actions by hostile nations, last January's breach of the US Central Command's network by hackers linked to ISIS (Islamic State of Iraq and Syria, known also as the Islamic Caliphate) was a reminder that cyberterrorism is on the rise and that radical religious groups are rapidly filling the technological gap in the fifth dimension. International developments in the past few years indicate that cyberattacks will play a significant role in future military affairs, with unpredictable implications due to the underlying attribution problem, that is, the difficulty of identifying the attack's source and nationality: an issue which is becoming even more delicate as the technique of the so-called false flagging is increasingly employed.

The asymmetrical nature of the cyberconflict, moreover, will certainly shift the balance of power, mostly in favor of non-State actors, who might operate without any real cyber-structure against which to retaliate, thus weakening deterrence strategies.

On these grounds, it looks like a sound cyberdefense strategy that might effectively offset the challenges from cyberspace is far from being implemented, but it is also clear that resilience – a feature which the federal government is missing – and some compromise on the civil liberties issue might be soon needed in order to preserve the smooth running of our technology-based societies.

Note

(1) As reported in: http://www.spacedaily.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html.

(2) See quote by Nigel Inkster, Director of Transnational Threats and Political Risk at the International Institute for Strategic Studies (IISS), in: http://news.bbc.co.uk/2/hi/technology/8511711.stm.

(3) As defined by the Executive Order 13010—*Critical Infrastructure Protection*. Federal Register, July 17,

1996. Vol. 61, No. 138. pp 37347-37350 and in John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets:*
Definition and Identification, CRS Report for Congress, October 1, 2004, Order Code RL32631.
(4) See Jaikumar Viajyan, *DHS bears brunt of criticism at House Cybersecurity hearing*, March 11, 2009, available on: http://www.computerworld.com/article/2531881/security0/dhs-bears-brunt-of-criticism-at-house-cybersecurity-hearing.html; Stephanie Condon, Critics: Homeland Security unprepared for cyberthreats, December 7, 2008, available on: http://www.cnet.com/news/critics-homeland-security-unprepared-for-cyberthreats.
(5) See http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
(6) Markus Rauschecker, "*Thinking Ahead – Implementing the NIST Cybersecurity Framework to Protect from Potential Legal Liability*", in: *United States Cybersecurity Magazine*, Summer 2014
(7) See Abraham R. Wagner, *Cybersecurity: New Threats and Challenges*, in: The American Foreign Policy Council, Defense Technology Program Brief, n.1, September 2013; Stephen p. Bucci, Paul Rosenzweig and David Inserra, *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace*, in: The Heritage Foundation, *Backgrounder*, No. 2785, March 28, 2013.
(8) Available at http://italy.usembassy.gov/news-events/sotu-2015.html.
(9) See Remarks by the President at the National Cybersecurity Communications Integration Center, January 13, 2015, available at: http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent.
(10) The highlights: the forthcoming White House Cybersecurity Summit to be held at Stanford University on February 13, 2015.
(11) See Letter from the Director of Management and Budget Office – Executive Office of the President, Shaun Donovan, to the House of Representatives Speaker, John A. Boehner, January 13, 2015, available at www.whitehouse.gov.

Il Cyber spionaggio cinese e le risposte di Washington e Taipei (Cina)

Rodolfo Bastianelli
(Analista indipendente)

La questione della cyber – sicurezza rappresenta oggi uno dei temi più importanti per la difesa nazionale di tutti gli Stati ma in particolare per quella di Stati Uniti ed a Taiwan, vista la crescente capacità di effettuare attacchi informatici sviluppata dalla Cina Popolare. E proprio questa attitudine negli ultimi anni ha iniziato seriamente a preoccupare le forze militari e d'intelligence di Washington e Taipei per i gravi rischi che pone alla loro sicurezza.

I primi segnali che dimostrano la capacità di Pechino a portare avanti attacchi informatici risalgono al 1999, quando in risposta al bombardamento compiuto per errore dalle forze aeree statunitensi nel corso delle operazioni contro la Serbia, *hackers* cinesi misero fuori servizio alcuni siti istituzionali di Washington e degli altri Paesi della coalizione. In seguito, nell'Aprile 2001, in occasione della collisione avvenuta sopra l'isola di Hainan tra un ricognitore dell'USAF ed alcuni aerei militari cinesi, si registrò un'ulteriore azione di disturbo ai danni di siti governativi incluso quello della Casa Bianca che venne reso inattivo per breve tempo. Tuttavia, pur non producendo danni significativi alla rete Internet statunitense, le azioni rappresentavano il primo attacco informatico compiuto da cittadini della Cina Popolare e mostravano in maniera evidente come i rischi per la sicurezza nazionale non provenissero più soltanto da minacce convenzionali. Da parte cinese invece gli attacchi confermavano quello che ormai da un decennio i vertici politici e militari del Paese stavano sostenendo, ovvero la necessità di ammodernare i sistemi difensivi nazionali adattandoli alle nuove capacità tecnologiche ed informatiche. Avviati a partire dalla seconda metà degli anni Novanta, i programmi di rafforzamento militari di Pechino poggiano essenzialmente su una riduzione del numero di effettivi uniti ad un miglioramento qualitativo delle Forze Armate, miglioramento che ha proprio nello sviluppo di un adeguato

sistema tecnologico e di difesa informatica uno dei punti salienti. Un programma che ha portato notevoli risultati visto che, stando a quanto riportato dal Dipartimento della Difesa statunitense, già nel 2009 le Forze Armate cinesi avevano sviluppato sia una serie di *virus* capaci di attaccare i computer degli altri Paesi che un sistema di difesa per proteggere i propri sistemi informatici da eventuali aggressioni esterne. La questione della cyber – sicurezza è stata così al centro dell'attenzione da parte dell'Amministrazione Obama fin dal suo insediamento alla Casa Bianca, come dimostra l'istituzione nel 2010 dello *"U.S. Cyber Command",* un sotto – comando all'interno del Dipartimento della Difesa incaricato di coordinare tutte le cyber – operazioni di interesse militare.

Ed è in questo scenario che vanno inquadrate le tensioni sorte negli ultimi dieci anni tra Washington e Pechino in merito alla crescente attività degli *hackers* cinesi ai danni di siti industriali ed istituzionali statunitensi. Secondo gli analisti e gli esperti militari americani, la Cina avrebbe reclutato una serie di *hackers* specializzati nel portare a termine azioni che vanno dall'attacco delle reti informatiche di Paesi stranieri, al cyber – spionaggio fino ad un'azione di controllo della dissidenza interna, operazioni che non possono essere classificate come compiute dal governo di Pechino in quanto gli *hackers* ufficialmente non sono collegati in alcun modo al regime cinese. Sul piano strettamente militare, le Forze Armate cinesi hanno invece istituito delle unità operative, alle quali è stato aggiunto anche personale specializzato proveniente dal Ministero della Sicurezza di Stato e dalle varie industrie elettroniche di proprietà statale, incaricate di pianificare e sviluppare una vasta serie di azioni offensive, mentre una particolare attenzione è stata data allo sviluppo di sistemi di controllo capaci di monitorare la rete Internet ed essere così in grado di censurare e contrastare l'attività dei diversi gruppi di opposizione presenti nel Paese (1). Sul piano operativo, è opinione condivisa da diversi analisti che gli Stati Uniti si trovino oggi nel settore della cyber – sicurezza in una situazione di svantaggio nei confronti della Cina la cui causa va ricercata essenzialmente in due elementi. Il primo è che mentre Pechino dispone di un stringente controllo governativo su Internet così da

poter intervenire immediatamente qualora si prospettino potenziali rischi per la sicurezza nazionale, negli Stati Uniti invece la rete è gestita da operatori privati ed il governo per proteggerne la sicurezza può soltanto attuare delle misure di regolamentazione, senza dimenticare come della stessa manutenzione dei *networks* informatici del Pentagono siano incaricate compagnie private. Il secondo è l'estrema dipendenza di Washington dai sistemi elettronici. Come ha sottolineato l'Ammiraglio Mike Mc Connell, ex – Direttore della *"National Security Agency"* (NSA) e della *"National Intelligence",* gli Stati Uniti costituiscono il Paese più informatizzato al mondo e per questo si presentano come i più vulnerabili in caso di cyber – attacchi alla reti governative, industriali e finanziarie. Al contrario la Cina non appare così dipendente, in quanto la stragrande maggioranza degli uffici governativi, delle infrastrutture e dell'apparato industriale non poggia sui sistemi informatici e la loro operatività può essere ristabilita attraverso controlli manuali. Tuttavia, per altri esperti proprio la progressiva informatizzazione a cui stanno andando incontro le Forze Armate cinesi potrebbe in futuro annullare questo vantaggio di cui attualmente gode Pechino, visto che il sempre maggiore apporto della tecnologia renderà Pechino dipendente dai computer e quindi vulnerabile ai cyber – attacchi dall'esterno.

Se quindi gli Stati Uniti conservano tuttora un considerevole vantaggio rispetto alla Cina vista la superiorità qualitativa e tecnologica dell'apparato militare americano, Pechino per contrastare questo *gap* punterebbe allo sviluppo di adeguate capacità nel portare a termine attacchi informatici, una strategia che rientra in una sorta di *"guerra asimmetrica"* grazie alla quale le Forze Armate cinesi potranno infliggere notevoli danni ad Eserciti qualitativamente più forti sfruttando proprio i punti deboli che questi ultimi presentano (2). Questa tattica era già stata esposta in un breve volume redatto nel 1999 da alcuni ufficiali superiori dell'Esercito cinese ed intitolato *"Unrestricted Warfare"*, dove si sosteneva che per sconfiggere i Paesi dotati di maggior forza militare era necessario ricorrere a mezzi non convenzionali, quali inondare il territorio nemico di stupefacenti, favorire la sovversione

interna ed, ovviamente, procedere ad attacchi informatici. Appare evidente come i programmi di guerra cybernetica portati avanti da Pechino rientrano sia nella visione di *"Guerra di Popolo"* enunciata a suo tempo da Mao Tse – Tung che in quella di *"stratagemma",* un concetto tipico della cultura cinese e che nell'ambito militare può riassumersi come la ricerca di mezzi e la messa in atto di azioni capaci di ingannare il nemico (3). A rendere poi più complicato il contrasto all'azione di cyber – spionaggio contribuisce anche il fatto che gli *hackers*, pur essendo la loro azione tollerata dal governo cinese, non hanno nessun collegamento diretto con le autorità di Pechino, trattandosi di figure spesso oscure che ruotano intorno al regime se non addirittura di veri e propri elementi criminali. Ed anche per questo la Cina si oppone a qualsiasi accordo con gli Stati Uniti teso a fissare delle regoli comuni per chi opera nel mondo informatico, vedendo nel cyber – spionaggio non solo uno strumento di difesa nazionale, ma anche un mezzo per rafforzare l'economia del Paese, visto che attraverso l'acquisizione di informazioni scientifiche ed industriali Pechino punta a diventare non più solo un produttore di merce a basso costo ma anche una potenza tecnologica globale (4). Gli obiettivi su cui in questi ultimi anni si sono concentrati i cyber – attacchi cinesi sono stati principalmente gli Stati Uniti e Taiwan, ma l'azione cinese si è anche indirizzata contro i dissidenti tibetani, tanto che gli *hackers* di Pechino si sarebbero infiltrati nei computer di oltre cento Paesi per ottenere informazioni. Inoltre, durante le recenti proteste scoppiate ad Hong Kong, non solo i telefoni cellullari dei manifestanti avrebbero ricevuto messaggi di *"Phishing"* così da *"infettare"* con un *malware* il sistema operativo *"Android",* ma sarebbe apparso anche un sofisticato software in grado di attaccare la piattaforma iOS usata dalla *"Apple"* per gli iPads e gli iPhones, un sistema che fino a quel momento si riteneva essere pressoché immune da attacchi informatici (5). Stando ad un'informativa recentemente rilasciata dell'agenzia di cybersicurezza *"Mandiant",* l'*"Unità 61398"* dell'Esercito cinese sarebbe responsabile dei numerosi attacchi informatici subiti dagli Stati Uniti negli ultimi anni, attacchi che avrebbero coinvolto oltre un centinaio di aziende alle quali sarebbero

state sottratte informazioni di estrema importanza sui processi tecnologici e di produzione industriale, risultati di tests e documenti finanziari (6).

Di questi, il più importante è stato sicuramente quello compiuto nel 2010 ai danni di *"Google"* di altre importanti aziende statunitensi. Indicata con il nome di *"Operazione Aurora"* l'azione, condotta con sistemi ultrasofisticati, sarebbe stata effettuata dalla *"Lanxiang Vocational School"* di Jinan nella provincia dello Shandong e dalla *"Shanghai Jiaotong University"* (7). Successivamente, una nuova importante azione di hackeraggio è avvenuta nel 2011 con l'attacco alla *"Lockheed Martin",* un'azienda la cui attività è legata al settore della difesa. L'altro obiettivo degli attacchi informatici cinesi è appunto Taiwan, l'isola considerata da Pechino come una sua provincia ma *"de facto"* indipendente e da quasi settant'anni causa di forti tensioni politiche e militari in Asia orientale. Stando a quanto riportato lo scorso anno dal capo del *"National Security Bureau"* (NSB) di Taiwan Tsai Der – Sheng nel corso di un'audizione davanti allo *"Yuan Legislativo"* e da un rapporto del Ministero della Difesa, la Cina starebbe pianificando le sue forze militari così da raggiungere nel 2020 la piena capacità per sferrare un attacco al territorio dell'isola. E' chiaro infatti che mentre un'eventuale invasione cinese potrebbe essere rilevata tempestivamente dando alle Forze armate taiwanesi il tempo di intervenire, un cyber - attacco difficilmente potrebbe essere prevenuto e, data l'estrema dipendenza di Taiwan sui sistemi informatici, questo cambierebbe radicalmente l'equilibrio strategico tra i due Paesi rendendo così più agevole un'eventuale successiva azione militare. Ed è in questo contesto che vanno inquadrati i timori taiwanesi per le sempre più frequenti azioni di cyber – spionaggio da parte di Pechino. Per l'intelligence taiwanese, che stima in oltre centomila il numero di effettivi incaricati delle azioni di guerra cybernetica all'interno delle Forze Armate cinesi le quali disporrebbero di due unità preposte esclusivamente allo spionaggio informatico nei confronti di Taiwan, la minaccia è *"molto severa"* tanto che l'isola è stata l'obiettivo del maggior numero di cyber – attacchi da parte di Pechino (8). Iniziati nel 1999 con un sabotaggio dei siti informatici universitari e commerciali dell'isola

avvenuto subito dopo che l'allora Presidente Chen Shui – bian affermò come i rapporti tra Pechino e Taipei dovessero intendersi *"tra Stato e Stato",* gli attacchi sono andati intensificandosi negli anni seguenti, tanto che già nel 2003 gli esperti informatici americani e taiwanesi esprimevano tutta la loro preoccupazione sul fatto che la *"Microsoft"*, fornendo al governo cinese i codici del suo nuovo software *"Windows XP"*, poteva favorire lo sviluppo di sofisticate tecnologie informatiche che sarebbero state poi utilizzate a scopo militare (9). E la conferma di come il problema costituisca oggi uno dei temi più importanti per la sicurezza di Taiwan e degli stessi Stati Uniti è venuta dalle recenti dichiarazioni del Ministro della Scienza e della Tecnologia taiwanese Simon Chang, il quale avrebbe affermato come l'isola sia ormai continuamente oggetto di attacchi informatici e che la Cina consideri Taiwan una sorta di *"laboratorio"* per sperimentare le tecniche di cyber – spionaggio da usare in seguito contro il territorio americano (10).

Note

(1) Una delle misure di monitoraggio informatico più efficienti sviluppati dalle forze di sicurezza di Pechino è la possibilità di *"isolare"* la rete Internet cinese da quella internazionale attraverso un controllo delle informazioni in entrata od in uscita dal Paese effettuato per mezzo di *"server farms"* strettamente sorvegliate, così da impedire immediatamente, qualora vi fosse la necessità, l'accesso ai siti stranieri.

(2) Sull'attività di cyber – spionaggio di Pechino vedi GEORGE PATTERSON MANSON III, *Cyberwar: The United States and China Prepare for the Next Generation of War,* apparso su *"Comparative Strategy",* Vol. 30, No. 2, 2011, pagg. 121 – 133.

(3) Sulla dottrina militare cinese per la guerra cybernetica vedi l'analisi di BARRINGTON M. BARRETT JR., *Information Warfare: China's Response to U.S. Technological Advantages,* pubblicato su *"International Journal of Intelligence and Counterintelligence",* Vol. 18, No. 4, 2005, pagg. 682 – 706.

(4) Vedi su questo l'analisi di ADAM SEGAL, *Chinese Computer Games: Keeping Safe in Cyberspace,* apparsa su *"Foreign Affairs",* Council on Foreign Relations, New York, Vol. 91, No. 2, 2012, pagg- 14 – 20.

(5) *China Declares Cyber-War on Hong Kong Protesters,* Voice of America English Service, 6 Ottobre 2014.

(6) Vedi sull'argomento *China's Military Behind Cyberattacks,* Investor's Business Daily, 21 Febbraio 2013.

(7) Su questo vedi *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence,* apparso su *"Journal of Strategic Security",* Vol. 4, No. 2, Estate 2011, pagg. 1 – 24.

(8) Sulla posizione di Taiwan riguardo al cyber – spionaggio di Pechino vedi l'analisi *Critical Node: Taiwan's Cyber Defense and Chinese Cyber-Espionage,* The Jamestown Foundation, China Brief, Vol. 13, No. 24, 5 Dicembre 2013.

(9) Vedi in proposito *China's Cyberwarriors,* apparso su *"Foreign Policy",* Sett./Ott. 2006, pag. 93.

(10) Vedi su questo *Taiwan Complains of "Severe" Cyber Attacks From China,* apparso su *"The Diplomat"* il 15 Agosto 2014.

In-sicurezza cibernetica e strategie nazionali: nuove sfide, vecchi problemi

Cristiana Era

(Analista indipendente)

Sin dal 1989, internet – forse la più grande rivoluzione del XX secolo – ha stravolto i criteri della comunicazione, del commercio, del settore militare e della governance. Ai suoi esordi negli anni '60, la rete (allora conosciuta come ARPAnet) permetteva solamente la connessione fra un numero estremamente limitato di computer, tra l'altro accessibili in termini di spazi e costi solo a determinate istituzioni (per lo più in ambito accademico e militare). Come sottolinea *Abraham R. Wagner,* c'era dunque poco da rubare o da "attaccare" e la cyber security concettualmente non esisteva. La progressiva accessibilità del World Wide Web alla società civile ha creato nuove opportunità di sviluppo nel settore economico, ma anche nelle relazioni sociali. Oggi è impossibile pensare di poter fare a meno di internet.

Con lo sviluppo del mondo virtuale, tuttavia, si sono diffusi in rete anche fenomeni negativi già conosciuti nel mondo reale: attività criminali, spionaggio industriale, terrorismo, sabotaggio e attacchi di varia natura spesso sponsorizzati da Stati ostili. Secondo quanto riportato dallo *Special Report* del *Council on Foreign Relations* (CFR) americano, i costi annuali della criminalità online hanno raggiunto i mille miliardi di dollari nel 2010, mentre pochi mesi fa la nota azienda di sicurezza informatica McAfee ha rilasciato un rapporto che ridimensiona in parte i dati del CFR, stimando le perdite dovute alla cyber criminalità e al cyber spionaggio in circa 445 miliardi di dollari.

Una stima approssimativa, come riconosce l'azienda, risultando difficile quantificare con precisione i danni perché l'industria stessa è restia (anche per una questione di immagine) ad ammettere di aver subito perdite a seguito di violazioni dei propri sistemi informatici. Si tratta comunque di cifre impressionanti e,

come rilevato anche da altre aziende del settore (Symantec, HP, ecc.), in forte crescita.

Oltre al crimine, diciamo di "tipo comune", la cui ragion d'essere è per lo più finalizzata a profitti illeciti, vanno considerate le azioni coordinate di gruppi di hacker al servizio, diretto od indiretto, di uno Stato e che riescono talvolta a paralizzare Paesi interi, come è stato nel caso di Estonia, Georgia e Kirghizistan; queste ultime azioni attribuite alla Russia che naturalmente ne nega la paternità e continua ad invocare un uso non offensivo della tecnologia internet.

Il tema della conflittualità nella quinta dimensione, il cyber space, e le minacce derivanti al sistema Paese e alla sicurezza nazionale sono arrivati all'attenzione generale di praticamente tutti i governi.

Alcuni, quelli tecnologicamente più avanzati, si sono mossi prima rispetto ad altri, cercando di innalzare il livello dei propri sistemi di difesa contro eventuali attacchi cibernetici alle infrastrutture nazionali (più o meno critiche), creando altresì un quadro normativo interno di riferimento, identificando le strutture idonee e investendo sia sullo sviluppo dell'high tech che su strategie non solo difensive ma anche offensive.

Negli ultimi 2-3 anni molti Stati membri dell'Unione Europea e della Nato (come Spagna e Repubblica Ceca) hanno seguito la scia, in tempi più o meno rapidi, almeno per ciò che riguarda lo sviluppo di una normativa nazionale sulla cyber security ed una struttura adeguata per fronteggiare le nuove sfide e le nuove minacce.

I Paesi che hanno colmato in fretta il gap cibernetico sono quelli al di fuori dell'area occidentale: Cina, Russia e Iran hanno messo in piedi strutture ad hoc tecnologicamente avanzate con potenzialità offensive, gestite da personale altamente qualificato, tanto da spingere alcuni osservatori a parlare di cyber-esercito e cyber soldati. Il gruppo di hacker "di Stato" che nell'ultimo anno è salito alla ribalta delle cronache internazionali per le sue intrusioni nell'industria americana aerospaziale, dei satelliti e della comunicazione è l'Unità 61398 dell'Esercito Popolare di Liberazione.

Recentemente un nuovo e più sofisticato gruppo di hacker, anch'esso legato alla Cina secondo le aziende di sicurezza

informatica, denominato Axiom, sembra aver rubato la scena all'Unità 61398 e ha fatto innalzare il livello di allerta all'FBI americana. Ma un'intensificarsi di attività ostili nel cyberspazio negli ultimi mesi sembra provenire anche dalla Corea del Nord.

In Italia solo recentemente le istituzioni sono arrivate a riconoscere l'impatto dirompente di un eventuale attacco cibernetico al sistema paese colpendo le cosiddette "infrastrutture critiche": con l'approvazione del decreto della Presidenza del Consiglio del 24 gennaio 2013 si è dato il via alla definizione di una strategia nazionale di difesa, dopo un anno, il 2012, definito dagli esperti "disastroso" per la crescita esponenziale di attività del cyber crime.

Il decreto presenta ancora molte lacune, non ultima l'assenza di un elenco delle infrastrutture critiche nazionali. Manca inoltre di una razionalizzazione degli organi che dovrebbero fare fronte ai rischi, alle minacce e ad una eventuale risposta agli attacchi della criminalità dello spazio virtuale, dai malware alle attività di cyber spionaggio, dal furto di dati ai cosiddetti "*Denial of Service*" (DoS) in grado di compromettere l'attività di un sito o addirittura di una nazione (l'attacco all'Estonia nel 2007 è diventato ormai un case-study in cui si evidenziano gli effetti del DoS).

Si fanno salve, inoltre, tutte le prerogative dei vari dipartimenti, ministeri ed enti che lavorano nel settore della sicurezza. Quest'ultimo aspetto, ossia la pluralità degli enti coinvolti, rappresenta forse la maggiore vulnerabilità della pianificazione della difesa cibernetica italiana. La natura stessa della quinta dimensione è dinamica ed immediata, con uno stravolgimento dei concetti di spazio e tempo: la presenza di più organi decisionali rappresenta in sé un ostacolo a qualunque attività cibernetica ostile che richiede tempi infinitamente ridotti rispetto alle farraginose macchine burocratiche istituzionali.

E' chiaro dunque che per essere efficace ed effettiva, una strategia di cyber defense deve poter rispondere in tempi rapidi, almeno per ciò che riguarda il contenimento dei danni provocati da un attacco cibernetico.

Le vulnerabilità della rete sono ulteriormente amplificate dalla disattenzione istituzionale nei confronti di programmi educativi sulla

sicurezza cibernetica. Considerando che l'uso della rete è ormai quotidiano per centinaia di milioni di persone in tutto il mondo (tramite pc, tablet o smart phone), la mancanza di una chiara consapevolezza dei rischi e delle contromisure minime da adottare da parte degli utenti facilita la diffusione delle attività criminali, soprattutto per quelle collegate al furto di dati e di identità.

Le password, facilmente eludibili, costituiscono per la stragrande maggioranza dei cittadini la sola barriera all'intrusione nei propri sistemi telematici. L'Australia, rispetto ad altri Paesi, ha avviato da tempo programmi di educazione alla sicurezza informatica, come "Cybersmart", volti ad incrementare la consapevolezza dei pericoli da parte della popolazione. Ma per altri governi la discussione è ancora limitata alla protezione degli spazi istituzionali o aziendali di particolare importanza e ai rischi della cyber warfare (guerra cibernetica). La collaborazione con privati ed università, che dovrebbe essere uno dei perni su cui ruota una strategia di difesa nazionale, rimane anch'essa un argomento di dibattito ma senza effetti concreti di rilievo, almeno per quanto riguarda l'Italia.

Le minacce, però, si evolvono molto più rapidamente delle strategie governative. E' chiaro che c'è una impellente necessità di sviluppare, e in fretta, sistemi adeguati di protezione che non solo garantiscano la riduzione dei danni provocati dagli attacchi ma che possano in qualche modo risultare un deterrente agli attacchi stessi, nella consapevolezza che comunque non potranno essere evitati al 100%. Da un certo punto di vista, l'evoluzione del cyberspazio è vittima del suo successo: tanto più la rete è diventata sofisticata ed il mezzo di comunicazione di massa più diffuso, tanto maggiori sono diventate le sue vulnerabilità. Dai contributi delle rappresentanze estere risulta inoltre evidente che l'*information-sharing*, ormai considerata da tutti come un elemento importante di contrasto alle minacce, rimanga ad oggi lettera morta. In nessuno degli interventi si forniscono, infatti, notizie che non siano limitate all'elenco della normativa nazionale o che riguardino il contenuto (sia pur generico) di attività svolte dagli organi preposti alla cyber defense.

Nonostante da più parti, formalmente anche a livello istituzionale, si chieda a gran voce maggiore concertazione tra i governi, e tra il governo e l'industria, gli organi istituzionali rimangono restii a condividere le informazioni necessarie per attuare una strategia globale e nazionale di difesa contro gli attacchi cibernetici. In parte questo si spiega con il retaggio culturale del segreto di Stato e in parte dal fatto che numerosi governi sponsorizzano hacker di Stato e dunque non hanno interesse a condividere informazioni rilevanti con le parti avverse: un riflesso di quanto già avviene sul piano internazionale al di fuori del cyber space.

E' difficile infatti pensare che in questo momento, ad esempio, in cui i rapporti tra Russia e Stati Uniti sono ai minimi storici dalla fine della Guerra Fredda, questi due Paesi possano dar seguito ad una qualsiasi iniziativa concreta mirante a mettere un po' di ordine nel Far West cibernetico dove in mancanza di una autorità internazionalmente riconosciuta regna la legge del più (tecnologicamente) forte. Così come resta difficile ipotizzare di riuscire a mettere d'accordo nazioni come Israele e Iran da sempre in aperto contrasto, diffidenti e poco inclini alla collaborazione.

Il panorama della quinta dimensione rimane frammentato. In alcuni Paesi non democratici ma tecnologicamente avanzati, come Russia e Cina, permane un forte controllo statale su internet.

In paesi più liberali, il controllo è limitato, per la natura stessa del regime democratico, e molte criticità e limiti derivano dalla presenza di più centri decisionali spesso in competizione e attenti a preservare le proprie prerogative più che ad inserirsi in un sistema integrato di difesa, per non parlare del settore privato che spesso è solo marginalmente coinvolto nel processo di formazione strategica di cyber defense.

Nei regimi democratici, inoltre, è estremamente forte la resistenza a qualunque regolamentazione della rete che limiti le libertà individuali o che implichi un controllo governativo sul cittadino, in primis la violazione della privacy.

Il mondo virtuale è la nuova frontiera del XXI secolo: ha aperto nuove prospettive e nuove opportunità di sviluppo, di

socializzazione e di comunicazione. Ma ha anche riprodotto - senza i limiti di spazio, di tempo e di costi – i pericoli che le società affrontano nel mondo reale.

Mentre però in quest'ultimo esiste già a livello nazionale ed internazionale un sistema di contrasto ad attività illegali, nel cyber spazio la minaccia è arrivata con largo anticipo rispetto alle capacità di reazione dei governi che trovano un ostacolo anche nel limite geografico delle loro giurisdizioni laddove in un sistema virtuale geografia e confini sono annullati, tanto da modificare molto più facilmente e rapidamente equilibri e rapporti di forza.

Si vedrà nei prossimi anni se gli Stati attualmente più avanti sul piano della difesa cibernetica riusciranno a creare un regime internazionale cibernetico, in cui esistano delle regole certe e i mezzi per farle rispettare. Al momento attuale sembra poco probabile che i governi siano disposti ad accettare i limiti che una sovrastruttura internazionale, anche solo normativa, comporterebbe.

Molto più realistico è lo scenario in cui ogni Stato continuerà a dare seguito alle proprie strategie nazionali di difesa (e di offesa), magari nell'ottica di una concertazione con altri paesi alleati in ambito regionale. Resta il punto interrogativo sul grado di sofisticazione che le minacce in rete saranno in grado di raggiungere mettendo in serio pericolo le normali attività quotidiane delle nostre comunità.

RIFERIMENTI

- Umberto Gori, "*Cyberspazio e relazioni internazionali: implicazioni geopolitiche e geostrategiche*", in: "*Information Warfare 2012. Armi cibernetiche e processo decisionale*", a cura di Umberto Gori e Serena Lisi, FrancoAngeli editore, 2013.
- Umberto Gori, "*La protezione cibernetica delle infrastrutture nazionali: solo un problema tecnico*?", in: "*Information Warfare 2013. La protezione cibernetica delle infrastrutture nazionali*", a cura di Umberto Gori e Serena Lisi, FrancoAngeli Editore, 2014.
- Cristiana Era, "L'ultima *sfida: la protezione delle infrastrutture e la quinta dimensione*", giugno 2013, in: www.argilnews.eu.
- Cristiana Era, "*La difesa contro la minaccia cibernetica: il nuovo decreto governativo*", 14 giugno 2013, in: *Informazioni della Difesa Online*.
- Cristiana Era, "*Cyber spazio e multidimensionalità*", marzo 2013, in: www.argilnews.eu.
- Cristiana Era, "*Cyberdefense, la nuova frontiera della sicurezza nazionale*", luglio 2012, in: www.argilnews.eu.
- Cristiana Era, "*Cyberintelligence: le sfide della realtà virtuale al mondo reale*", novembre 2011, in: www.argilnews.eu.
- Lorenzo Franceschi-Bicchierai, "*Researchers reveal new Chinese hacking group*", 28 ottobre 2014, in: www.mashable.com.
- Joey Cheng, "*Cyber conflict escalates: Second Chinese PLA hacking group accused*", 10 giugno 2014, in: http://defensesystems.com/home.aspx
- Robert K. Knake, "*Internet Governance in an Age of Cyber Insecurity*", Council on Foreign Relations Special Report N. 56, September 2010.
- Symantec, "*Internet Security Threat Report 2014*".
- "*Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cyber crime II*", Center for Strategic and International Studies, June 2014.
- McAfee Labs, "*Threats Report*", November 2014.
- DPCM 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, in: GU n.66 del 19-3-2013.

Testi consigliati

Per coloro che vogliano approfondire gli argomenti sulla *Information Warfare*, oltre ai libri di cui alle Note, si segnalano le seguenti pubblicazioni:

Invisible Threats: Financial and Information Technology Crimes and National Security, (U. Gori e I. Paparela , a cura di), the NATO Programme for Security through Science, IOS Press, Amsterdam, Berlin, Oxford, Washington, DC, 2006.

Modelling Cyber Security: Approaches, Methodology, Strategies, (U. Gori, a cura di), The NATO Science for Peace and Security Programme, IOS Press, 2009.

Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana, (U. Gori e L.S. Germani, a cura di), F. Angeli, Milano, 2011.

La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale, (U. Gori e L.S. Germani, a cura di), F. Angeli, Milano, 2012.

Questi volumi costituiscono gli Atti di Conferenze internazionali e nazionali promosse dal Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII) dell'Università di Firenze e dall'Istituto per gli Studi di Previsione ISPRI), d'intesa ed in collaborazione con Maglan-Information Defense Technologies. Alcune volte la collaborazione si è estesa anche a Link Campus University, al Centro Studi "Gino Germani" e al CIS Sapienza. Un altro volume, contenente gli Atti delle Conferenze di Roma e di Milano tenutesi nel 2014, è attualmente sotto stampa.

Si consiglia anche la lettura del *2014 Italian Cyber Security Report*, sulla consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione italiana, redatto dal Cyber Intelligence and Information Security Center dell'Università di Roma 'La Sapienza', diretto dal prof. Roberto Baldoni.