Alma Mater Studiorum - Università di Bologna

SCUOLA di SCIENZE POLITICHE
Sede di Forlì

Corso di Laurea in

Scienze Internazionali e Diplomatiche (LM-52)

TESI DI LAUREA
in Studi Strategici

"*National Cyber Approach: analisi dell'ecosistema difensivo nazionale rapportato alle minacce cibernetiche". Il caso di Estonia e Israele*

CANDIDATO
Matteo Gramaglia

RELATORE
Prof. Filippo Andreatta

CORRELATORE
Prof. Gian Piero Siroli

Anno Accademico 2012/2013
Sessione III

A mio padre, ai miei padri.

يد وحدها ما بتصفق.

Ringraziamenti

Vorrei ringraziare tutti coloro che hanno reso possibile questo mio elaborato di tesi. Innanzitutto il mio relatore Filippo Andreatta, entusiasta sostenitore del progetto, e il correlatore Gian Piero Siroli, mentore e amico. Inoltre, vorrei ringraziare l'International Centre for Defense Studies di Tallinn, l'Institute for National Security Studies e il Yuval Ne'eman Workshop di Tel Aviv, per avermi concesso l'opportunità di approfondire le tematiche del mio elaborato presso le loro sedi. In particolare, uno speciale ringraziamento va a di Emmet Thouy e Piret Pernik, fondamentali nell'aiutarmi a carpire le dinamiche estoni, Gabi Siboni, Daniel Cohen, Lior Tabanski e Isaac Ben-Israel, miei riferimenti in Israele.

Vorrei poi poter dare un personale ringraziamento a tutti coloro che mi hanno concesso delle interviste in questi mesi: tra gli altri Stefano Mele, Sandro Bologna, Giampiero Giacomello, Mihkel Tammet, Rain Ottis, Patrik Maldre, Kristjan Prikk, Kadri Kaska, Toomas Viira, Priit Laaniste, Siim Alatalu, Nir Tordjman, Ram Levi, Cameron Brown, Meir Elran, Gil Baram e l'indimenticabile Martin Van Creveld.

Vorrei inoltre menzionare UNIDIR, Cyber Tech, Isodarco, AIIC, IPRED, DiploHack, per avermi dato la possibilità di prendere parte ad eventi estremamente rilevanti per la costruzione della mia tesi. Altresì, vorrei ringraziare l'Università di Bologna e il Ser.In.Ar. per il sostegno finanziario, necessario a intraprendere le mie ricerche.

Vorrei infine inevitabilmente consegnare il ringraziamento principale alla mia famiglia per il sostegno e l'affetto. E a Roberta, pazientissima compagna di viaggio.

INDICE

INTRODUZIONE

Questo elaborato di tesi è il frutto di un intenso lavoro di analisi e ricerca riguardo al cyber-spazio. Il suo obiettivo è quello di ricercare le caratteristiche principali di questo nuovo dominio militare, evidenziandone attori e modalità di interazione. Lo spunto che ha portato a questa ricerca è stato certamente fornito dalla crescente attenzione internazionale riguardo la questione. Infatti, se è vero che tra i militari di tutto il mondo la consapevolezza che si potesse militarizzare l'arena digitale è un'informazione ormai datata di almeno vent'anni, la comunità internazionale degli studiosi di materie militari sembra essersi accorta solo con Estonia 2007 e con Stuxnet dell'esistenza di una concreta minaccia bellica all'interno del cyber-spazio.

Da alcuni anni a questa parte, perciò, il cyber-spazio viene guardato con occhio differente sia dagli esperti di settore che dalla comunità internazionale nel suo complesso, ed è diventato improvvisamente *attraente*[1] e capace di scatenare un fervente dibattito tra scettici e assidui sostenitori della sua natura rivoluzionaria. La mia esigenza di ricerca prende le mosse proprio da questa diatriba e intende fare luce sulla reale dimensione che la questione cibernetica ha assunto, e potrà assumere in un futuro prossimo, nel mondo delle relazioni internazionali, degli studi strategici e nel panorama della Difesa.

Pe questo motivo, ho iniziato a investigare innanzitutto cosa sia in concreto il cyber-spazio e quali siano le modalità di interazione che si sviluppano al suo interno tra i principali attori, così da ridimensionare sia i timori di coloro che vedono nelle minace cibernetiche un altro possibile olocausto, sia gli scetticismi di chi non ritiene rilevanti gli odierni sviluppi offensivi apparsi nel cyber-spazio. Così analizzando le principali vicende

[1] Rid, T. (2011) *Cyber War Will Not Take Place*, The Journal of Strategic Studies, Vol.35, No.1, 5-32

internazionali riconducibili a *cyber-warfare* (partendo dalle primordiali forme di spionaggio elettronico e arrivando sino al rivoluzionario Stuxnet), mi sono reso conto che la rilevanza della questione sta crescendo, e che attorno ad essa vi è una profonda confusione concettuale e tematica. Così ho deciso di approfondire le ricerche e offrire la mia interpretazione su alcuni degli aspetti più importanti relativi alla dimensione cibernetica: le entità, la conflittualità e le modalità di protezione. Sono così arrivato ad occuparmi delle entità statali in quello che viene considerato il più asimmetrico dei domini bellici, destrutturando molte delle credenze più diffuse sulle potenzialità catastrofiche del cyber-spazio.

Ho cercato di mantenere un approccio misto nello studio della questione. Da una parte, un approfondito studio di documenti, analisi e report mi ha permesso di utilizzare delle forti basi teoriche, dall'altra l'interazione coi policy-makers e coloro che si occupano di implementare le politiche nazionali a livello di sicurezza cibernetica, mi ha permesso di mantenere uno sguardo pragmatico alla questione. Questo soprattutto grazie alle due esperienze fatte a Tallinn e Tel Aviv, durante le quali mi è stato possibile interagire con esperti, rappresentanti delle istituzioni e tecnici. Questo duplice approccio mi ha permesso anche di mantenere un occhio critico su entrambi gli aspetti relativi al cyber-spazio, quello tecnico e quello politico, che troppo raramente vengono considerati contemporaneamente quando si studia la questione cibernetica, soprattutto in termini di difesa.

Nello specifico, il progetto di tesi, è suddiviso in cinque capitoli. Nel primo si delineano in modo dettagliato la storia delle tecnologie e della terminologie relative al cyber-spazio, per lasciare poi spazio alla descrizione del ruolo degli stati nazione in questo contesto. Si analizzerà sinteticamente la possibilità di sviluppare trattati internazionali per la regolamentazione di questo dominio, prima di spostare l'attenzione alla dimensione interattiva attuale, ossia quella conflittiva. Sarà appunto questo lo scopo del secondo capitolo che si occuperà di scandagliare il dibattito dottrinale sull'esistenza e l'entità della guerra cibernetica. Successivamente verrà presentato un *excursus*

di tutte le principali vulnerabilità e possibilità di attacco che possono essere modulate nel cyber-spazio, corredata da un elenco dei più rilevanti incidenti conosciuti. Il terzo capitolo sarà l'antitesi del precedente, in quanto saranno analizzate le principali modalità difensive adottate dagli stati nazionali, osservate anche da un punto di vista delle Strategie Nazionali, pubblicate da ciascun paese. Con la rappresentazione del ruolo di ognuno degli agenti coinvolti nell'amministrazione della sicurezza cibernetica, si delineerà infine il modello olistico di ecosistema che verrà comprovato dai due *case studies* (Estonia ed Israele) presentati negli ultimi due capitoli.

Al di là della ricerca condotta, credo di aver imparato tre concetti fondamentali frequentando gli ambienti degli studiosi del cyber-spazio. Innanzitutto, mi è parso che siano davvero pochi coloro che hanno un'idea chiara e precisa di cosa sia rilevante nell'universo cibernetico. La maggior parte di coloro che ne scrivono o che lo studiano ne hanno una visione al più parziale. Militari, politici, multinazionali, tecnici, sono tutti attratti ed interessati ad un'unica dimensione del cyber-spazio, così da tralasciare le altre, perdendosi l'immagine d'insieme e cadendo spesso in drammatiche rappresentazioni iperboliche.

In secondo luogo, *cyber is not bad.* È importante riconoscere che la necessità di incrementare la sicurezza informatica sia una problematica urgente, perché le perdite economiche e le minacce tangibili provenienti dallo spazio cibernetico sono una realtà che non si può sottovalutare, ma non si può trattare una meravigliosa invenzione, quale è la rete, come se fosse un'entità intrinsecamente malvagia. Pur nella piena consapevolezza che sia un meccanismo difensivo proprio della mente umana, quello di temere l'ignoto, trovo insano e distruttivo che anche nell'ambito della ricerca prevalga questo tipo di impostazione.

Infine, mi preme sottolineare che il cyber dominio non è onnipotente, onnipresente e Primo Motore Immobile[2]. Nel senso che, non si può attribuire ogni tipo di dinamica umana (sociale, economica,

[2] Nel pensiero di Aristotele, il concetto di Primo Motore Immobile rappresenta la causa ultima del divenire dell'Universo.

militare) alle conseguenze prodotte dal cyber-spazio, semplicemente perché è erroneo e riduttivo. Un esempio estremamente chiaro, a mio modo di vedere, sono gli avvenimenti degli ultimi tre anni nei paesi dell'Africa del Nord e del Medio Oriente. Per quanto sia stato considerevole l'impatto che hanno avuto i social media, il blocco della rete e la persecuzione degli *hacktivists* nello svolgimento della storia, non si possono investire questi fenomeni di effetti causali che non gli corrispondono.

Tutte e tre queste ragioni conducono alla stessa risultante: studiare la materia è una necessità per rimuovere i timori, ampliare la visione del fenomeno e per creare un sostrato di conoscenze spendibile per la gestione degli affari militari, ma soprattutto per quella della vita sociale più in generale.

Questo studio si rivolge principalmente alla dimensione strategica, ma come si può notare scrutando il modello (eco)sistemico, avverte l'esigenza di comprendere anche altre aree tra cui l'etica, la sociologia e le scienze politiche (intese come studio della gestione delle società civili). Mi piacerebbe dunque consigliare a tutti coloro che si interesseranno alla questione di non limitarsi a un solo punto d'analisi, ma di approfondire la tematica, esaminando gli innumerevoli risvolti umani che vengono scatenati dall'interazione degli individui con uno spazio costruito *per* loro, *da* loro ma che non risponde secondo nessun canone alle loro caratteristiche e necessità naturali.

1.

La connotazione del cyber-spazio e gli attori principali

"*The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location* "[3]

Introduzione

Da circa la metà degli anni Novanta, gli accademici di tutto il mondo e gli esperti militari dibattono in maniera concitata sull'essenza del cyber-spazio e sulla sua ipotetica implicazione in dottrine belliche. Nonostante i numerosi tentativi, ancora oggi, uno dei problemi principali in riferimento alla discussione sulle implicazioni di questa nuova realtà è la comprensione condivisa di quale sia la reale materia di studio. Non vi è infatti la certezza che il cyber-spazio coincida con la globalità di Internet, se esistono realtà tangibili che fuoriescono dallo spazio virtuale, anch'esse coinvolte nei processi cibernetici. Molti scritti delle più rilevanti menti operanti nel settore iniziano ancora[4] con interi capitoli dedicati alla definizione di cyber-spazio e delle normali caratteristiche di interazione tra soggetti, applicate ad esso: potere, sicurezza, attacco. Per questa ragione in questo primo capitolo ho deciso di analizzare innanzitutto le origini dello spazio cibernetico e la sua definizione. Per offrire un'interpretazione che reputo la più coerente e concreta, in modo da sviluppare gli argomenti d'interesse di questo elaborato all'interno di una struttura ben precisa.

Come ricorda Tabansky L. (2011) "*cyberspace is much less concrete than natural spaces, and therefore this conceptual discussion*

[3]Leiner et al. (2012) *Brief History of the Internet*, Internet Society Publication. Consultabile: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Origins ultimo accesso 28.02.2014

[4] Ad esempio negli incipit delle rispettive Strategie Nazionali che verranno trattate nel capitol 3, nei Documenti delle principali Organizzazioni Internazionali (i.e. ITU) e nei report di iportanti Think Tnks mondiali (e.g. SDA)

is essential".[5] È infatti questa lo scopo ultimo della mia ricerca: contribuire alla studio di un universo ancora poco compreso e sistematizzato, per allargare la base delle conoscenze sulla materia e aumentare la sensibilizzazione sia a livello dei *policymakers,* sia a livello di ricerca accademica. È infatti necessario aggiungere che il dibattito sulla materia fino a pochi anni fa sembrava esclusivo del mondo militare. Questo ha provocato una scarsa evoluzione concettuale anche in relazione alle dinamiche militari. Saranno gli avvenimenti del 2007 in Estonia e del 2008 in Georgia a richiamare l'attenzione internazionale sulle implicazioni delle nuove tecnologie informatiche nello scenario internazionale, e non solo come capacità integrativa applicata ai campi di battaglia.

In molti hanno sottolineato negli ultimi anni l'occasione persa in quasi vent'anni di dare una chiara risposta a molte delle domande che ancora oggi ci si pone sul cyber-spazio. Goldstein G.P. (2012) ad esempio, considera comprensibile la difficoltà di sviluppo di coerenti dottrine militari relative al neonato dominio virtuale, ma si stupisce del fatto che non sia avvenuto del tutto il processo analitico che invece avvenne con gli armamenti nucleari[6]. Questo, secondo l'autore, sorge da due ragioni specifiche: l'elevato livello di segretezza che circonda la il ciberspazio e la mancanza di definizioni precise del *man-made domain*.

Data l'impossibilità di intervenire sulla prima variabile, ho deciso di concentrarmi sulla parte di definizione (e di evoluzione) in modo da poter agevolmente svolgere il compito che questo elaborato si prepone, ossia analizzare l'approccio nazionale alla difesa cibernetica. Per arrivare a questa conclusione, sarà perciò necessario capire in maniera chiara *cosa* sia il cyber-spazio, quali sono le componenti che lo formano, quali gli attori che vi attuano e quali le dinamiche che si manifestano tra loro.

Per concludere, consapevole del ruolo di *leadership* che gli Stati Uniti esercitano ancora oggi nel cyber-spazio, sia in termini di

[5]Tabansky L. (2011), *Basic concepts in cyber warfare* in ""Military and Strategic Affairs", Vol.3, No.1, pp.77
[6]Goldstein GP. (2012), *Cyber Weapons and International Stability: New Destabilization Threats Require New Security Doctrines* in "Military and Strategic Affairs", Vol.5, No.2, pp.121-139

concettualizzazione (idee e termini sono di quasi totale ispirazione statunitense), sia in termini infrastrutturali (la rete globale dipende fisicamente dalle strutture statunitensi), ho deciso di non far trasparire nella mia analisi questa predominanza. La scelta di analizzare due piccoli paesi, seppur alleati prossimi degli USA (soprattutto in ambito cibernetico), è stata una scelta voluta precisamente per cogliere le caratteristiche più profonde del cyber-spazio, che mi ha portato ai risultati che sono descritti qui di seguito.

1.1. Cos'è il *cyber-spazio*? L'evoluzione delle tecnologie della comunicazione

"*The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location* "[7]

L'evoluzione del cyber-spazio viene considerato un processo relativamente giovane, ma il suo percorso ha le radici nel periodo delle invenzioni che rivoluzionarono il mondo della comunicazione, durante la prima metà del XIX secolo, e di cui l'invenzione del telegrafo è il più famoso esempio. In questo periodo si applicarono i riceventi ritrovati relativi allo spettro elettromagnetico per incrementare la capacità trasmissiva di informazioni, con lo scopo di migliorare in maniera rivoluzionaria il modo di comunicare. La velocità con cui venivano trasmesse le informazioni attraverso il telegrafo era per gli uomini dell'epoca una questione che comportava notevoli vantaggi in tutte le aree dell'esperienza umana, ma che poneva anche delle sfide, in termini di cambiamento di mentalità e di applicazioni pratiche.

[7]Leiner et al. (2012) *Brief History of the Internet,* Internet Society Publication. Consultabile: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Origins ultimo accesso 28.02.2014

Dal telegrafo, la ricerca avanzò incessantemente, tanto che dopo numerose invenzioni e scoperte, nel corso della Seconda Guerra Mondiale[8], gli Alleati cominciarono a sviluppare un sistema elettronico che permetteva di elaborare dati e che venne utilizzato per codificare i messaggi criptati dei paesi dell'Asse. Copeland J., in un recente libro, ha descritto minuziosamente la storia di Colossus, "*the first large-scale electronic computer, (that) was used against the German system of teleprinter encryption know at Bletchery Park as 'Tunny'*"[9]. Ebbe inizio così l'escalation dell'era digitale, che avrebbe provocato una crescita esponenziale in termini di capacità comunicative e di contenimento.

Da *Deep Blue*, il primo computer capace di vincere una partita a scacchi, agli *smarthphone* sono intercorsi pochi decenni, che hanno rivoluzionato non solo le interazioni personali, ma anche il paradigma di sicurezza degli Stati. È perciò necessario analizzare l'evoluzione della tecnologia a partire dalla fine degli anni Quaranta.

1.1.1 La genesi

Clark D., Leiner B.M. & al., in "*Brief History of the internet*" analizzano in maniera olistica l'evoluzione della rete, ripercorrendo i passaggi dalla creazione di ARPANET e di tutte le tecnologie associate all'odierna situazione. Il loro lavoro è descrittivo e analitico, poiché esamina non solo l'evoluzione tecnologica, ma anche le dimensioni operazionale e di gestione, le dinamiche sociali e quelle di commercializzazione. Per quanto di elevatissima rilevanza nello studio dei processi analitici dell'attuale società liquida[10]*,* le ultime due dimensioni analitiche trascendono il compito che questo elaborato si è preposto, perciò verranno tralasciate. Ci si concentrerà prevalentemente sulla caratterizzazione tecnologica, operazionale e gestionale della questione.

In un periodo in cui lo scontro tecnologico tra le due superpotenze aveva probabilmente raggiunto l'apice della propria

[8]Per una timeline dettagliata:http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/ ultimo accesso 28.02.2014
[9]Sulla storia di Colossus: http://www.colossus-computer.com/colossus1.html ultimo accesso 28.02.2014
[10]Bauman Z. (2000) *Liquid modernity,* Blackwell Pub., Oxford

rilevanza geostrategica, nel 1957 l'Unione Sovietica lanciò in orbita lo *Sputnik*, il primo satellite emittente onde radio inviato nello spazio nella storia dell'umanità. Considerando accuratamente le implicazioni tecnologiche di tale gesto, nell'ottica di una guerra nucleare, gli Stati Uniti si munirono dello strumento attraverso il quale intendevano diventare la forza trainante nelle scienze e nelle nuove tecnologie: l'ARPA[11], Advanced Research Project Agency. Fu questa la sede dove vennero sviluppati la maggior parte degli esperimenti dell'epoca sulle macchine computanti, anche se gran parte del merito, come si vedrà deve essere riconosciuto agli esperti appartenenti alle varie università statunitensi.

Considerata questa cornice, si può forse sostenere che la genesi del dibattito sulle possibilità di comunicazione interattiva attraverso network computerizzati sia partita dalle riflessioni di J.C.R. Licklider del Massachussetes Institute of Technology, che nel suo "Galactic Network" prevedeva la possibilità per i sistemi interconnessi di comunicare, di inter-scambiare serie di informazioni e di accedere a basi di dati da qualsiasi postazione. Divenendo il primo *head of research* del dipartimento relativo a *computing research,* Licklider fu fondamentale nel trasmettere ai sui successori l'impronta "networkizzata" dell'universo della macchine da computo.

Un altro eccellente ricercatore essenziale per lo sviluppo dell'interattività fu Leonard Kleinrock[12], anch'egli del MIT, il quale puntò fortemente sulla teoria del *packet switching* (preferibili per gli scambi, all'uso dei circuiti). Fu poi Paul Baran a convogliare questa idea nell'influente RAND Corporation e a renderla operativa. Nell'atto di studiare un efficace sistema per controllare gli operativi dell'Air Forces in caso di un eventuale attacco atomico, Baran mise in atto un sistema decentralizzato che adoperava il sistema del *packet switching.*

[11]A seconda dei periodi l'acronimo sarà ARPA o DARPA

[12]Kleinrock L.(1961) "Information Flow in Large Communication Nets", RLE Quarterly Progress Report. Consultabile all'indirizzo
http://www.lk.cs.ucla.edu/data/files/Kleinrock/Information%20Flow%20in%20Large%20Communication%20Nets1.pdf
ultimo accesso 28.02.2014

Nel 1965, Lawrence Roberts e Thomas Merril crearono poi la prima reale connessione tra macchine della storia: " (*they)connected the TX-2 computer in Mass. to the Q-32 in California with a low speed dial-up telephone line creating the first (however small) wide-area computer network ever built*". Le conseguenze furono di immensa importanza per l'evoluzione dei sistemi comunicativi, perché dimostrarono che due *time-shared* computer potevano lavorare costruttivamente insieme ma che il sistema di interazione attraverso lo *switched telephone system* non era sufficiente. La teoria di Kleinrock venne dunque resa operativa e Roberts poté cominciare a lavorare all'ARPA al progetto ARPANET, mentre la stessa ARPA affidò la missione di costruire il primo switch alla BBN (Bolt Beranek and Newman)[13].

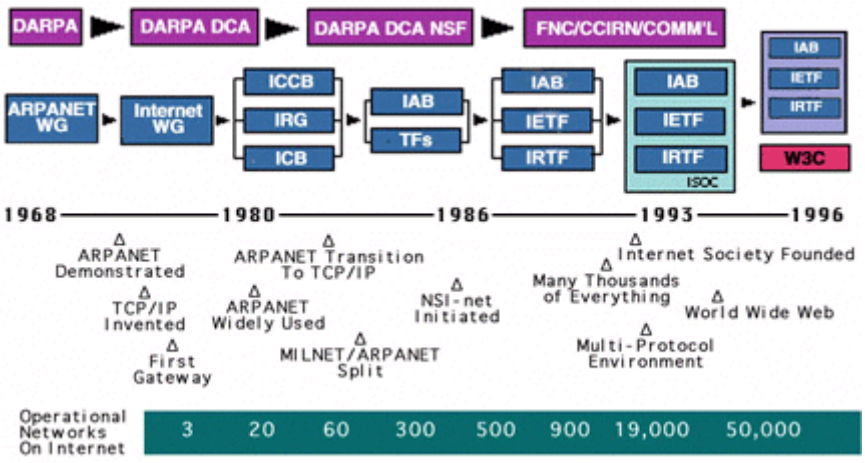


Figura 1: Evoluzione da ARPANET ad Internet

1.1.2 Da ARPANET a Internet

ARPANET (acronimo per Advanced Research Projects Agency Network) era un sistema che sfruttava le connettività con diversi *nodes* (i computer collegati) per permettergli di comunicare contemporaneamente tra loro. Ciò che rese possibile la reale

[13]Per un ottima ricostruzione della timeline si veda: http://www.investintech.com/content/historyinternet/ ultimo accesso 28.02.2014

trasmissione del messaggio fu la creazione dell'*Interface Message Processor* (IMP) l'anno precedente, da parte di un team di scienziati del BBN, capeggiati da Frank Heart, capace di interconnettere i *nodes* partecipanti ad ARPANET, attraverso interfacce particolari e irrobustite.

Nel 1969 "*The first message on the ARPANET was sent by UCLA student programmer Charles S Kline at 10:30 pm on October 29, from the campus' Boelter Hall to the Stanford Research Institute's SDS 940 host computer*"[14]. Il messaggio citava "LO", ma l'idea originale era trasmettere la parola LOGIN. Così, nonostante il fallimento dell'azione globale, il primo testo "reale" veniva trasmesso virtualmente attraverso le tecniche teorizzate nel modello del *packet switching.* All'epoca vi erano unicamente quattro computer connessi ad ARPANET:

- Uno all'Università della California a Los Angeles, scelta perché "patria" di Kleinrock (Il computer connesso era un SDS Sigma 7);
- Uno all'Università della California a Santa Barbara (dove il computer era IBM 360/75 con un processore OS/MVT);
- Uno allo Stanford Research Institute's Augmentation Research Center, per il lavoro svolto da (con un SDS 9409);
- Uno all'università dello Utah, per il lavoro svolto sull'operatività 3D dele informazioni in rete (DEC PDP-10 operativizzato da TENEX).

Si passò repentinamente da quattro computer nel 1969 a 15 nel 1971 e ben 37 nel 1973[15]. Nel 1975, dopo i primi tentennamenti, il sistema venne dichiarato operativo (vedi figura 2). Le possibilità che offriva erano potenzialmente infinite: dall'avvento delle *e-mail* (messaggi elettronicamente trasmessi) al protocollo di trasferimento dati (FTP), al controllo remoto (*telnet).* A quel punto, la vera necessità divenne trovare un sistema che supportasse la trasmissione delle informazioni. Il sistema IMF, infatti, non era efficiente quando si presentavano evidenti incompatibilità e quando aumentavano l'interconnessione e il numero di

[14]Per una precisa ricostruzione del primo collegamento ARPANET si veda http://www.edn.com/electronics-blogs/edn-moments/4399541/ARPANET-establishes-1st-computer-to-computer-link--October-29--1969 ultimo accesso 28.02.2014
[15]Denning P. (1989) *The ARPANET after Twenty Years,* American Scientists, No. 77, pp. 530-535. Consultabile http://denninginstitute.com/pjd/PUBS/AmSci-1989-6-arpanet.pdf ultimo accesso 28.02.2014

nodi. Non solo, persino il programma di controllo della rete, il Network Control Program, era insicuro e insufficiente per sostenere la comunicazione all'interno di ARPANET. Per questa ragione, il DARPA demandò all'Università di Stanford, all' UCL e alla BNN la progettazione di un meccanismo protocollare sicuro e in grado di gestire *large time sharing system* a più livelli.

Fu così che vennero largamente sperimentati e implementati sulla rete ARPANET i sistemi protocollari TCP (Transport Control Protocol) e IP (Internet Protocol[16]). E il primo gennaio 1983 venne ufficialmente lanciato rivoluzionando completamente le funzionalità della rete (che ormai comprendeva centinaia di connessioni). È questo, secondo esperti ed osservatori, la genesi di quello che oggi conosciamo come Internet.

"*IP would be responsible for routing packets across multiple networks and TCP for converting messages into streams of packets and reassembling them into messages with few errors despite loss of packets the underlying network. These two protocols provided highly reliable end-to-end communication in a network of networks, eventually exercising a significant influence on the protocols now approved for worldwide use by the International Standards Organization*."[17]

[16]Da cui deriva la terminologia "Internetworking" e di conseguenza Internet, per identificare tutte le reti che usavano i protocolli TCP/IP, coniata per la prima volta da Bob Kahn and L. Cerf

[17]Denning D. (1989) op. citata p. 531

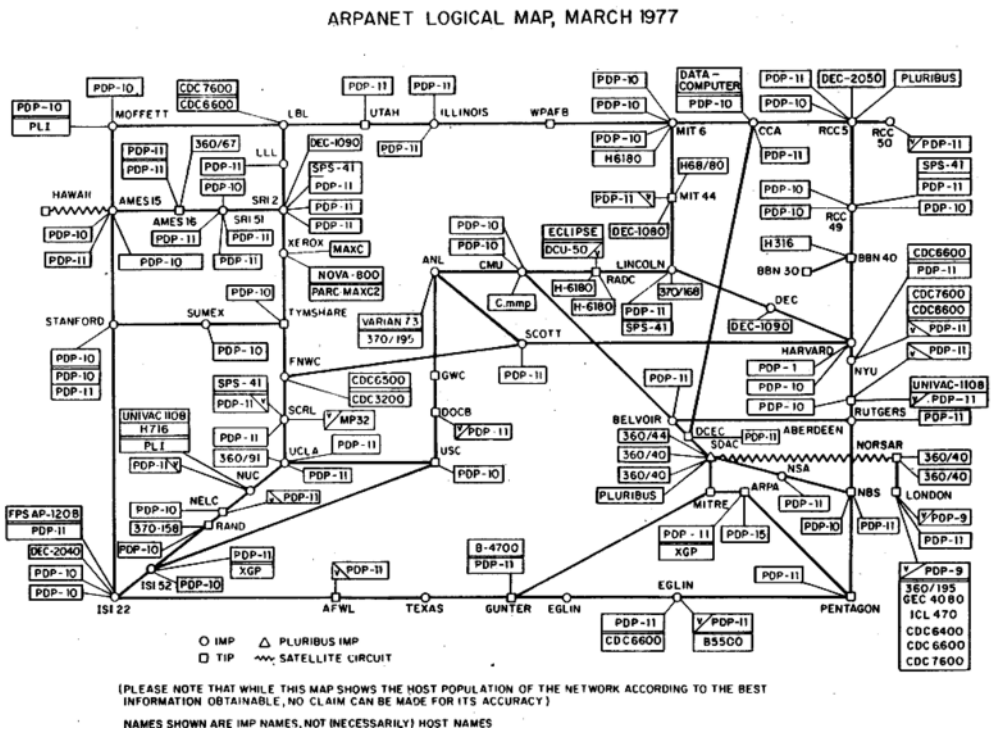


Figura : Mappatura logica di ARPANET nel 1977

Nello stesso periodo iniziarono a comparire miriadi di reti parallele locali: BITNET, CSNET, ecc[18]. Nacquero anche reti interne in alcune importanti compagnie (ad esempio IBM) e in Europa (X.25 e CYCLADES) vennero intrapresi dei progetti che puntavano allo sviluppo di sistemi simili ad ARPANET[19]. Nel 1976 venne inaugurato il SATNET, l'Atlantic Package Satellite Network, che collegava Europa e Stati Uniti tramite una connessione satellitare.

A questo punto fu necessario per il governo statunitense prendere due decisioni fondamentali: effettuare la separazione e implementare la regolamentazione dei network. Per quanto riguarda la prima, proprio nel 1983, il Dipartimento della Difesa americano fece una scelta che si rivelerà fondamentale per lo sviluppo, non tanto della dimensione o delle dinamiche, ma della gestione, del management del cyber-spazio. ARPANET venne scisso e una parte divenne MILNET

[18]Ibid

[19]Per approfondimenti: R. Kahn, ed. 1978. Special Issue on Packet Networks. IEEE Proceedings 66, 11 (November). .Re J. Quarterman and J. Hoskins. 1986. Notable computer networks. Communications of ACM 29, 10 (October). 932-971;

(Military Network), incaricato di gestire le comunicazioni etichettate come *unclassified* del Dipartimento della Difesa. Nonostante il mantenimento di alcuni *gateways* di comunicazione la distinzione tra i due fu netta e il network militare si incaricò della trasmissione di dati sensibili. La crescente mole di dati e di connessioni fece sì che entrambi i sistemi si espansero in maniera parallela e MILNET si evolse (con esponenziali livelli difensivi), trasformandosi prima in *Defense Data Network* e in tempi più recenti in NIPRNET[20], al quale successivamente si affiancherà anche SIPRNET (per informazioni classificate)[21].

Allo stesso modo, date le considerevoli dimensioni raggiunte dalla rete, si intrapresero misure legali vincolanti la gestione dei network e delle infrastrutture: responsabilità, spese e controllo vennero messe nero su bianco. Con una serie di regolamenti si mise in piedi il sistema di controllo che caratterizza il network internazionale ancora oggi in uso. Negli Stati Uniti venne istituito il Federal Network Council che cominciò presto a collaborare con le istituzioni governative per garantire loro il pieno funzionamento delle strutture di comunicazione. Venne inoltre fondato l'Internet Engineering Task Force (IETF), che aveva il compito di vigilare la rete e apportare dei miglioramenti qualora necessari.

L'ultimo passaggio fondamentale fu quello di trasformare Internet da sistema principalmente basato nelle università e a livello governativo a fattore includente privati, imprese e la comunità concepita nel senso più ampio. Il passaggio fu quasi fortuito, a dimostrare le potenzialità del network. Fu l'Organizzazione Europea per la Ricerca Nucleare (CERN) di Ginevra che lanciò il World Wide Web nel 1992[22], il quale prese subito piede e si diffuse a macchia d'olio in tutto il mondo. Il crescente numero di utenti dispersi in tutto il mondo diede vita a tutta una serie di organismi atti a diverse funzioni di sostegno per le utenze, tra cui la più rilevante l'Internet Society fondata nel 1993.

[20]http://www.defensenews.com/article/20100118/DEFFEAT01/1180306/Mapping-Pentagon-s-Networks

[21]Sul NIPRNET: http://www.strategypage.com/htmw/htiw/articles/20100123.aspx ultimo acceso 28.02.2014

[22]Sarà solo l'anno successivo che vedrà la comparsa dell'interfaccia MOSAIC, creata per semplificare le funzionalità della rete. Progettata e customizzata da Marc Andreesen (futuro inventore di Netscape) della NCSA (National Centre for Supercomputing Association)

Due eventi, in particolar modo, permisero la realizzabilità di questo sviluppo. In primo luogo, la creazione del NSFNET (National Science Foundation Network), il successore di ARPANET: una *backbone* da 56 kbits/s supportata dal supercomputer della National Science Foundation. E in secondo luogo, l'opera di Tim Berners-Lee[23], un giovane ingegnere informatico del CERN, che con l'intento di rendere possibile l'origine e l'allocazione di un (tendente all') infinito numero di documenti provenienti da diverse fonti (o utenti), inventò dei protocolli che sarebbero stati alla base del World Wide Web.

Ebbe inizio così lo sviluppo delle funzioni di Internet, aumentarono gli accessi (nel 1992 arrivarono alla prima soglia critica di 1 milione di *hosts*) e tutta una serie di centri di gestione cominciarono ad essere abilitati anche in altre parti del mondo: il CERN divenne il centro dello sviluppo in Europa, le università in Australia e il settore privato in Asia favorirono l'arrivo delle reti TCP/IP alla fine degli anni Ottanta. Cominciò inoltre il fenomeno della commercializzazione delle tecnologie legate al TCP/IP, che spianò la strada all'arrivo del Personal Computer.

Nello stesso periodo istituzioni investite della responsabilità di controllo vennero formate sia negli Stati Uniti che nel resto del mondo, e una delle premure principali fu di definire la materia di cui si stava trattando. Così, nel 1995, il Federal Networking Council approvò una risoluzione in cui proponeva una definizione di quello a cui ci si riferiva con il termine 'Internet':

"Internet" refers to the global information system that -- (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein".

[23]Pesce M. (2010) *A brief Story of Cyberspace*, ZDNET, consultabile https://www.cs.duke.edu/courses/spring01/cps049s/class/html/mp.history.html ultimo accesso 28.02.2014

1.1.3 Il Cyber-space del Nuovo Millennio

A partire dalla seconda metà degli anni Novanta comincia il periodo che riguarda preminentemente la trattazione di cui ci si vuole occupare. È questo il periodo in cui la rete diviene uno strumento di uso "globalizzato", numerosi servizi vengono offerti on-line (dall'home banking a *Pizza Hut*[24]), la frammentazione delle reti non garantisce una perfetta centralizzazione, ma molti sforzi vengono fatti in questa direzione, inoltre la quantità di dati cresce esponenzialmente, così anche come la possibilità di usufruirne per fini equivoci.

Il periodo a cavallo tra i due millenni costituisce un momento critico per la rete sotto tutti i punti di vista. Segna il cambiamento nella sua natura intrinseca e, di conseguenza, modifica l'approccio di istituzioni e paesi nei confronti del cyber-spazio e del concetto di sicurezza legato ad esso. È questo appunto il momento del cosiddetto Web 2.0, durante il quale le caratteristiche del WWW non cambiano di natura, ma di apparenza estetica. È un momento cruciale perché in questi anni milioni di persone vengono catapultate all'interno dell'universo cibernetico, che da quel momento si trasforma in un sostegno necessario per moltissime attività lavorative e lucrative. È questa la premessa per capire la cosiddetta *Internet bubble*[25]*,* che colpisce i mercati finanziari a cavallo tra i due millenni. Centinaia di migliaia di imprese, compreso il valore potenziale della rete, decidono di investire in progetti che forniscono servizi virtuali, finchè il mercato esplode mostrando l'infondatezza delle basi economiche di questo sviluppo. Diventa però chiaro quanto fossero dipendenti le società economicamente più progredite dalle tecnologie informatiche. Un'altra questione che aiuta a rendere chiaro questo aspetto è la problematica del Virus Y2K, infelicemente noto come *Millenium Bug*. Nonostante gli effetti ottenuti, quasi del tutto irrilevanti permette di riscontrare quanto a

[24]http://www.youtube.com/watch?v=2d7sPPlefok

[25] Sulla teoria delle *bubbles* si veda Miller R.T. (2009), "Morals in Market Bubble", University of Dayton Law Review, Vol. 35 pp 113-138; e Shi, S. and Song, Y. (2012), " Identifying Speculative Bubbles with an Infinite Hidden Markov Model"

livello globale la dipendenza da sistemi informatizzati sia percepita come reale e tangibile.

1.1.4 Riflessioni

L'aver riportato integralmente l'evoluzione della rete di cui usufruiamo oggi, non è un mero esercizio di precisione storica, ma un'azione funzionale al progetto esplicativo che si prepone questo elaborato. Nella sua nascita e nel suo sviluppo, la rete e la sua gestione portano in sé i germi delle problematiche che devono essere affrontate oggi nell'elaborazione e nell'implementazione della *cyber security*. Per questo, dopo questo succinto excursus storico è necessario concentrarsi sulle riflessioni che emergono da questo.

In primo luogo, la descrizione dello sviluppo di ARPANET (e in seguito di Internet) permette di trarre una conclusione molto importante sulla sua più intima essenza. Per via del suo carattere, il numero degli individui che hanno composto la comunità di utenti agganciati alla rete è sempre cresciuto, con differenziali differenti (ma senza mai arrestarsi), fino ad arrivare alle stime attuali- circa 2.4 miliardi di utenti[26] connessi alla Rete. Infatti, una delle caratteristiche principali della struttura che sarebbe col tempo diventata la rete *World Wide* resta nel fatto che questa sia un "*open architecture networking*"[27]. Nonostante le divisioni sopra descritte, e le infinità di reti parallele, è questa una delle principali ragioni per cui il cyber-space è oggi così vulnerabile ed è impossibile in termini pratici preservare interamente gli accessi e controllare la molteplicità di minacce.

In secondo luogo, si può notare come le dimensioni della progettazione e dell'operativizzazione siano frammentate e cosparse di ostacoli, quali la distanza tra l'idea e la messa in pratica della stessa. Come si è visto, l'idea di Kleinrock non era molto distante da ciò che sarebbe poi diventato l'odierno internet. Tanto che Denning J., in un

[26] Al riguardo si vedano statistiche: http://www.internetworldstats.com/stats.htm e per statistiche più dettagliate http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf entrambi consultati il 28.02.2014

[27] Leiner op. citata

testo del 1989[28], propone un'ipotetica similitudine: se Kleinrock e Henry Ford fossero tornati in vita dopo tutti questi anni di rispettivo sviluppo dell'automobile e dei sistemi di comunicazione, non sarebbero stati probabilmente troppo sorpresi dai risultati raggiunti. Infatti, l'idea di entrambi è rimasta, per molti versi, intatta fino ad oggi, sono state apportate numerose modifiche, ma non strutturali. Per quanto riguarda il sistema di interconnessione, il problema che ci preme sottolineare è che il passaggio dall'idea di Kleinrock (e ancor prima di Licklider) alla sua implementazione ha tardato diverse decadi. Sarà questo un concetto che verrà ripreso in seguito quando si parlerà di implementazione delle dottrine di sicurezza cibernetica.

Cambiando soggetto, e passando alla questione legata al *Millenium Bug*, si può notare come, anche per ragioni quasi fortuite, la mancanza di prospettiva di lungo periodo e la volontà di risparmiare fondi e risorse, abbiano condotto ad una complessa problematica che è stata risolta solo attraverso grandi sforzi di personale e finanziamenti. Lo stesso succede oggi nel mondo della *cyber security:* nella protezione delle banche dati, dei servizi e delle infrastrutture, si tengono troppo spesso in considerazione fattori legati alla mancanza di risorse, o al disinteresse del futuro a medio-lungo termine.

La storia dell'attuazione iniziale di ARPANET, invece, può anche essere esaustiva per descrivere un'ulteriore componente che verrà ripresa più tardi quando si parlerà di g*overnance*: quella collaborativa. Negli anni precedenti al messaggio di Charles Kline, ben tre entità differenti (ARPA, RAND Corporation e NPL) lavoravano allo stesso progetto, senza però esserne rispettivamente a conoscenza, e senza soprattutto scambiarsi informazioni che avrebbero potuto da una parte abbreviare il procedimento, dall'altra renderlo più efficiente e solido. Non si tratta di certo di una novità storia nella delle invenzioni, né in quella della gestione delle risorse. Si vedrà, ancora una volta, nel proseguimento dell'elaborato come questo rappresenti un grave problema odierno che affligge le diverse entità governative. Lo è sia per

[28]Denning D. op. citata

gli Stati Uniti che per i due casi analizzati, quello estone e quello israeliano.

In conclusione, è necessario parlare del risultato del lavoro di Denning D., più volte citato. Dopo aver spiegato la simbologia di Ford, nota come la rilevanza di ARPANET e dei suoi derivati giaccia non tanto nella tecnologia di *networking,* qunato nel cambiamento del pratiche umane che ne è risultato[29]. Come detto, in generale, Internet oggi funziona in maniera molto simile all'idea originale di Licklider, Kleinrock e Baran, ciò che è cambiato è: la conoscenza diffusa del suo utilizzo e delle sue funzioni; la permeabilità che ha avuto nella vita di un grossa porzione della popolazione mondiale; l'alta capacità funzionale di un numero sempre maggior di utenti. In poche parole, l'abitudine alle nuove funzionalità che hanno sviluppato coloro che sono stati toccati dalla nuova vita nel cyber-spazio.

1.2 CYBER-SPACE: una definizione operativa

Per iniziare ad analizzare una questione in maniera seria ed approfondita sono d'obbligo una serie di premesse. Il soffermarsi sulle definizioni non è un puro esercizio stilistico ma una precisa necessità. Quando si parla di *cyber-space* infatti si fa riferimento non solo allo spazio nel quale viaggiano milioni di dati al secondo, ma si considerano anche le attrezzature che rendono possibili questi collegamenti, le applicazioni che elaborano i dati e decodificano le informazioni e persino gli utenti che usufruiscono di tutti e tre i livelli citati precedentemente. Compiere la complessa operazione di ricostruire un significato univoco del ciberspazio è anche fondamentale per comprendere le potenziali vulnerabilità e identificare le azioni di protezione, "fisica" e legale, che debbono essere intraprese.

"*Cyberspace is a fact of daily life"*. Così Nazli Choucri inizia il suo ultimo libro sulle cyber-politiche nelle relazioni internazionali.

[29]Ibid p. 532

Affermazione tanto ovvia quanto veritiera[30]. Meno ovvia è invece la consapevolezza che non si tratta di uno strumento quotidiano solo per individui e semplici *users*, ma anche e soprattutto per istituzioni governative, organizzazioni internazionali, gestori di infrastrutture definite critiche (o vitali)[31]. Per questa ragione è tanto più importante capire esattamente quali sono gli spazi (e i tempi) precisi che devono essere considerati nell'analisi del cyber-spazio.

È fondamentale innanzitutto partire da un assunto che è sostenuto dalla maggior parte degli studiosi e delle fonti: "*Unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers*"[32]. Come ricorda Tabansky L.(2011)[33], essendo il cyber-spazio l'unico dominio sinora creato dall'uomo, è molto meno concreto degli altri, per questa ragione è così complesso definirlo, ma è tanto più utile sforzarsi di farlo. Il costruire una definizione il più precisa e puntuale possibile, in modo da rendere operative le conclusioni che si trarranno sul soggetto studiato, è il punto di partenza per poter elegantemente approfondire l'argomento.

1.2.1 L'origine del termine

Se ci si concentra sul termine in sé è necessario ricostruirne una genesi. La sua provenienza moderna è attribuita ad un'invenzione letteraria di William Gibson, che in Neuromancer descriveva così il futuristico *cyber-space*

"*The matrix has its roots in primitive arcade games. … Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. … A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable*

[30]Choucri N. (2012) *Cyberpolitcs in International Relations*, *MIT Press,* Chicago

[31]Al riguardo, Mr. Priit Laaniste del Siseministerium estone ha fornito un'interessante distinzione tra 'vital' e 'critical'. Per le direttive estoni le infrastrutture critiche sono considerate *servizi vitali* così da sottolineare la necessità delle stesse per la società civile

[32] Sulla questione delle definizioni si veda http://www.techterms.com/definition/cyberspace ultimo accesso 28.02.2014

[33] Tabansky, L. (2011) "Basic Concepts in Cyber Warfare", *Military and Strategic Affairs,* Vol 3, No.1, pp.75-92.

complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data."[34]

Il termine nasce quindi da un concetto più idealistico concretamente legato alle tecnologie che l'hanno reso possibile. Così, la percezione di una mente artistica, ha dato vita al sostrato teorico su cui si fonda la ricerca tecnologica, politica e legale che si deve basare su un concetto spesso troppo generico e vaporoso per dare vita a risultati completamente soddisfacenti.

In realtà, l'origine etimologica del termine è decisamente più antica e richiama la tradizione filosofica dell'Atene classica. Infatti, *kibernetes* deriva dal greco e significa 'colui che governa' o 'colui che si governa', il che sembrerebbe riportare direttamente al mito della caverna incluso ne *La Repubblica* di Platone[35]. Riprendendo nuovamente Tabansky, invece, si è costretti a riflettere sul fatto che l'accostamento delle due terminologie e dei due significati (cyber e spazio) ha poco senso se fatta fine a sé stessa, soprattutto perché l'idea di spazio varia immensamente a seconda dei contesti considerati: fisica, filosofia, geografia, psicologia e così via. Per questo è necessario analizzare in maniera più approfondita a cosa ci si riferisce quando si parla di spazio cibernetico, e di conseguenza di tempo cibernetico. Dopo questo breve excursus sull'essenza di due concetti così complessi, si ritornerà ad analisi più consone alla materia in esame, riportando una chiara descrizione di quello che si intende effettivamente per *cyber-space*, e le definizioni ufficiali che istituzioni e studiosi hanno elaborato sinora.

1.2.2 Una descrizione complessa

La confusione creata dalla rapida evoluzione del ciberspazio e dai fenomeni sopra descritti, ha prodotto una vasta gamma di interpretazioni differenti su cosa sia concettualmente il cyber-space, sia nel panorama della dottrina che in quello istituzionale.

[34] Gibson W. (1984) *Neuromancer,* Ace Pub., New York
[35] Choucri N. op. citata. p. 7

Ad esempio, per Kuehl D.T. il cyber-space è "*an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infra-structures"*[36]*.*

Mentre per Windfield T.C. "*is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, IT systems, and telecommunication infrastructures commonly referred to as the World Wide Web"*[37]*.*

Per Libicki[38] risulta invece fondamentale la sua capacità di essere "*constantly replicated"* e la cameleontica funzione degli *"IT systems and networks,* (that) *if damaged, can be quickly repaired and reconstituted".*[39] Vi è poi chi, come Thomas Rid[40] non riconosce l'unicità del ciberspazio soprattutto se viene osservato da un'ottica che verta all'analisi dello stesso in ottica militare.

Tutte queste definizioni non sono né errate, né immotivate, ma sono spesso incomplete e parziali, vanno per questo perfezionate per essere rese operative. Anche da parte governativa e istituzionale lo spettro delle definizioni è molto ampio (anche se non tanto vario).

Per il Dipartimento della Difesa americano ad esempio *"cyberspace is a domain characterized by the use of computers and other electronic devices to store, modify and exchange data via networked systems and associated physical infrastructures"*[41]*.* In maniera similare per il Governmental Accountability Office della Casa Bianca il "*Cyberspace is the globally interconnected digital information and communications infrastructure. The Internet is a decentralized*

[36] KUEHL, D.T. (2009), *From Cyberspace to Cyberpower: Defining the Problem,* in Franklin D. Kramer, Stuart Starr & Larry K. Wentz, eds., *Cyberpower and National Security*, Washington D.C., *National Defense University Press, Potomac Books*

[37] Wingfield, T.C. (2000) *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp.,

[38] Libicki M.C., "*Conquest in Cyberspace: National Security and Information Warfare",* New York: Cambridge University Press, 2007

[39] Cordani, G. (2013) *Cyber Weapons: il controllo tra Stati Uniti, Russia e NATO*, tesi magistrale dell'Università di Bologna

[40] Rid T. (2011) *"*Cyber War Will Not Take Place*", The Journal of Strategic Studies*, Vol.35, No.1, 5-32

[41] Joint Chiefs of Staff, *Joint Publication 1-02,* Washington D.C., US Department of Defense, 12 April 2001

network of computer networks with no single authority responsible for governing or securing it"[42].

Tutte queste discrepanze, seppur minime rendono necessaria una definizione che abbia la duplice capacità di comprendere sotto si sé tutte le definizioni minori di cui si è appena parlato e, inoltre, di essere facilemnte utilizzabile in termini operativi sia da esperti che da tecnici.

1.2.3 IL MODELLO OPERATIVO DI CLARK

Il modello a cui ci rifaremo in questa trattazione è quello proposto da Clark D.D.[43] E' accettato come operativamente valido da molti studiosi[44] e in esso si analizzano le differenti stratificazioni che compongono contemporaneamente il ciberspazio. La descrizione deriva la sua struttura dalla comprensione del funzionamento dei meccanismi interni del sistema-cyber. Il modello è composto da quattro diversi livelli, o *layers:*

1. **L'entità fisica** che supporta gli elementi logici, formata da tutte le entità tangibili aventi massa e volume: "*PCs and servers, supercomputers and grids, sensors and transducers, and the Internet and other sorts of networks and communications channels*". È la componente più facile da identificare, data la sua tangibilità, ma spesso risulta essere quello più sottovalutato. È il livello degli hardware e dei cavi sottomarini in fibra ottica, due delle principali vulnerabilità del cyber-spazio;
2. **The *logical layer*:** software, bits e componenti disseminate per tutto il ciberspazio che svolgono funzioni e danno ordini per azioni e reazioni. È il livello intermedio, che trasforma gli input inviati dagli operatori attraverso l'hardware e li trasforma in informazioni pronte per essere trasmesse o azioni da essere

[42]Comprehensive National Cybersecurity Initiative, Bush Administration, Gennaio 2008

[43] Clark, D. (2010) *Characterizing Cyberspace: past, present and future*, MIT Review, Chicago. Consultabile a http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf ultimo acceso 28.02.2014

[44] Per confronti si veda CHOUCRI, N. (2012) *Cyberpolitcs in International Relations*, MIT Press, Chicago; Tabansky, L. (2011) "Basic Concepts in Cyber Warfare", *Military and Strategic Affairs,* Vol 3, No.1, pp.75-92; Even, S. e Siman-Tov, D. (2012), *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 INSS Publ., Tel Aviv

compiute. Anche i malware appartengono a questo livello. Potrebbe essere definita come la dimensione più peculiare del ciberspazio: **"***the nature of cyberspace—its strengths and its limitations, derive more from the decisions made at the logical level than the physical level***".**

3. **Le informazioni**[45]**:** il massiccio e costante flusso di dati, trasmessi sotto miriadi di forme e per molteplici ragioni è la ragione stessa per cui è stato inventato internet. Da ARPANET in poi le difficoltà riscontrate sono state affrontate e superate per riuscire a trasferire quel semplice "LO" che aveva in sè le potenzialità per diventare il gigantesco traffico di dati che è il network odierno. Con le parole di Clark **"***Information in cyberspace takes many forms—it is the music and videos we share, the stored records of businesses, and all of the pages in the world wide web. It is online books and photographs. It is information about information (meta-data). It is information created and retrieved as we search for other information (as is returned by Google)".*

4. **Gli utilizzatori / utenti:** Clark intende questo layer come il più importante, in quanto rifiuta l'impostazione per cui gli utenti siano entità passive all'interno dell'universo cibernetico. Clark sostiene che siano gli individui stessi a determinare la struttura interagendo con essa. Tralasciando le dinamiche sistemiche di causa ed effetto che premono a Clark nella sua ricerca, per lo scopo prefissatomi ritengo importante evidenziare il ruolo degli individui (singoli o collettivi[46]). E' infatti fondamentale includerli nella descrizione del ciberspazio in quanto essi stessi sono causa ultima delle azioni (politiche, criminali o di qualsiasi altra matrice) offensive e difensive che prendono vita all'interno di questa dimensione.

[45] Numerosi studiosi includono questo layer in quello precedente, anche la definizione dell'International Telecommunication Union (ITU) riporta solo tre livelli e accorpa logica e informazioni. Ho ritenuto che Clark sia stato più accurato nella sua descrizione, soprattutto perché si denota che il punto di vista partiva dall'analisi delle minacce. In effetti con il suo modello è più semplice e lineare prendere in considerazione tutte le possibili fonti di minaccia per il sistema.

[46] Tordjman N (2012) "Facing Virtual Reality – European Union's response to Threats from the Cyber World", *Heinrich Heine Univertat,* Düsseldorf.

La definizione di Clark rappresenta sotto molti aspetti un passo in avanti rispetto alle descrizioni statiche riportate sopra. A conferma che il suo modello operativo è una perfetta sintesi tra eleganza teorica e pragmatismo operazionale, l'International Telecommunication Union (ITU)[47], ovvero il più importante organismo internazionale che lavora per la preservazione di uno spazio cibernetico pulito e non conflittuale, ha optato per l'adozione di una definizione molto simile alla sua in tutti gli elaborati in cui compare la necessità di definire il *cyber-space*, con la sola differenza che i *layers* delle informazioni e dei software vengono considerati contemporaneamente.

1.2.4 La mappatura del ciberspazio e conclusioni

Per concludere, può essere interessante (e sicuramente utile) analizzare il lavoro di Dottorato in filosofia allo University College di Londra di Martin Dodge[48]. Dodge con un lavoro sistematico[49] e preciso ricostruisce una mappatura cartografica del ciberspazio, separando tre modalità precise: mappatura nel, mappatura del e mappatura per il ciberspazio.[50] Il primo modello corrisponde alla traslitterazione della cartografia nel ciberspazio e non interessa alla nostra trattazione. Il secondo modello corrisponde ad una mappatura utile per potersi muovere nel ciberspazio, è di enorme utilità per gli utenti, ma di relativa importanza per lo scopo della ricerca qui preposto. È così la terza modalità, la mappatura del cyber-spazio, quella che più ci interessa. Secondo la descrizione di Dodge, questo strumento topologico è focalizzato sula mappatura che descrive le strutture di network e documenti le operazioni dello stesso cyber-

[47] http://www.itu.int/en/about/Pages/default.aspx

[48] Dodge, M. (2008) *Understanding Cyberspace Cartographies: a Critical Analysis of Internet Structure Mapping,* Doctoral Thesis at UCL. Consultabile http://personalpages.manchester.ac.uk/staff/m.dodge/thesis/thesis1.pdf ultimo accesso 28.02.2014

[49] Dodge ha anche elaborato un blog *Atlas of Cyberspace*per il periodo per cui è intercorsa la sua ricerca. Sono ancora disponibili i risultati grafici all'indirizzo http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/

[50] Ibid p. 72

spazio, così come si possono vedere dall'esterno[51], quindi non è di nessuna utilità di chi (l'utente) si trova in una posizione interna. Inoltre, così come nella definizione operativa di Clark, anche Dodge prende in considerazione la mappatura sotto tutti I punti di vista: le infrastrutture, le operazioni e i modelli di attività degli utenti contribuiscono a definire una mappatura precisa del ciberspazio.

Questa operazione, a mio avviso eccessivamente difficoltosa e poco utile per quanto riguarda la totalità del cyber-spazio, ha sicuramente un'incredibile rilevanza pratica se mirata a determinati obiettivi, soprattutto nell'ottica militare, in cui la continua creazione e modificazione di cyber-spazio, dovuta a necessità operative, rende necessario l'immediato riconoscimento della dimensione considerata. È perciò comprensibile che nel mondo militare si siano sviluppati dei software in grado di percepire la struttura dello spazio cibernetico utilizzato nella operazioni belliche in tempi rapidissimi. Questo permette a chi struttura la tattica delle operazioni di tenere sotto osservazione le modifiche "geografiche" che vengono generate da cambiamenti nella struttura del cyber-spazio.

1.3 Gli attori del cyber spazio

Avendo chiaro l'ambiente di interazione, è ora necessario analizzare gli attori principali e le modalità di influenza reciproca che si verificano al suo interno. Si inizierà con gli attori, riprendendo le distinzioni di alcuni influenti studiosi e le linee guida delle più rilevanti correnti dello studio delle relazioni internazionali.

La categorizzazione delle entità presenti nel cyber-spazio è condivisa a grandi linee dalla maggior parte di coloro che si sono soffermati sulla questione, anche se compaiono in diversi lavori alcune sottili differenza, a seconda delle necessità esplicative degli autori. Ad

[51] ibid

esempio Cohen D. e Rotbart A.[52] dividono gli attori operanti in cinque categorie relative alle tipologie di attacchi che possono essere compiuti:

- **Gli stati.** Cohen e Rotbart analizzano come la dimensione degli attacchi veda una grande partecipazione delle entità statali. Non solo, secondo gli autori, con l'avvento dell'era dell'informazione, l'intervento statale è aumentato anche nella gestione interna: infrastrutture civili, comunicazioni e difesa nazionale. Ne consegue che gli attori statali investano ingenti quantità per far fronte alle azioni intraprese nel cyber-spazio;
- **Le organizzazioni criminali.** Il loro obiettivo è quello di colpire individui e imprese commerciali sfruttando hacker o specialisti, per ricavare un beneficio economico dalle azioni criminali. Le azioni di questi gruppi sono estremamente remunerative, e di conseguenza dannose per l'economia e la sicurezza del settore privato e pubblico. Una ricerca del 2012 effettuata dall'INTERPOL[53] ha dimostrato che l'azione delle organizzazioni criminali producono una perdita annua per il governo americano di circa un miliardo di dollari;
- **Le imprese commerciali. P**er gli autori hanno valore di entità in quanto principali promotori dei settori sociali ed economici dell'universo cibernetico;
- **I gruppi terroristici**. Nonostante in un lavoro del 2000, ma ancora attualissimo, Denning[54] noti come in realtà non vi sia un condiviso accordo su cosa sia un'azione terroristica nel ciberspazio, questi attori sono molto influenti all'interno di questo universo attraverso azioni sociali, volte alla propaganda, alla raccolta fondi, al sabotaggio[55] e al reclutamento;

[52]Cohen, D. e Rotbart A. (2013) *The Proliferation of Weapons in Cyberspace*, Military and Strategic Affairs, No. 1, pp. 59-80
[53] Ibid p. 74, nota 21
[54] Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime and Militancy* (pp. 239–288). Santa Monica, CA: RAND Corporation
[55] Vedi differenza tra azioni militari, sabotaggio, sovversione nel prossimo capitolo e nell'opera di Thomas Rid

- Gli **hacker.** Hanno intenzioni sovversive che puntano al sabotaggio dell'ordine costituito o di determinate istituzioni.

Allo stesso modo Cornish, Hughes e Livingstone[56], sempre considerando le potenziali minacce provenienti dal cyber-spazio, riducono le categorie a quattro. Gli autori non considerano, infatti, le imprese commerciali; inoltre, trasformano il livello degli hacker in criminali individuali, senza scindere chi agisce per scopo di lucro o per compiere azioni di sabotaggio; infine, includono una generica categoria di coloro che agiscono per motivazioni ideologiche o politiche. Vi è poi chi considera le nuove entità di mercenari[57] come una categoria di attori essenziali, capace di ridistribuire le potenzialità relative all'interno del cyber-spazio.

In realtà, nessuna di queste categorizzazioni è sbagliata, ma rischia di essere troppo generica per considera come attore tutti coloro che in qualche modo entrano in contato con la dimensione cibernetica. Per quanto sia vero che l'accesso al cyber-spazio faciliti alcune dimensioni della partecipazione politica[58], non credo che l'influenza della maggior parte degli attori sopra elencati abbia una rilevanza in termini geopolitici che possa essere considerata più che circostanziale. Lo scopo di questa analisi è considerare gli attori che si contraddistinguono per capacità di controllo e competizione in un ipotetico conflitto. Nonostante sia stata avanzata addirittura una teoria *sull'homo cybericus[59],* l'interpretazione che qui si vuole offrire mantiene lo Stato al centro degli scenari di interazione cibernetica. È infatti lo stato che mantiene, con le limitazioni che si vedranno, la sovranità all'interno di determinati ambiti e "luoghi".

I numerosi studiosi che considerano il ruolo dello stato come secondario (o declinato) lo fanno sostanzialmente per due ordini di motivi: l'incapacità di esercitare a pieno la sovranità nazionale; e

[56]Cornish, P. e Hughes, R., e Livingstone, D (2009) *Cyberspace and the National Security of the United Kingdom: Threats and Responses*, Chantam House Report, London

[57] Per approfondire: http://www.darkreading.com/attacks-breaches/a-mercenary-approach-to-botnets/240164329 ultimo accesso 28.02.2014

[58] Choucri, N. (2012) *Cyberpolitcs in International Relation*s, MIT Press, Chicago

[59] Ibid p. 25

considerando la natura asimmetrica del cyber-spazio. Per quanto riguarda la sovranità, si parlerà ampiamente in seguito della questione, qui basti dire che nonostante indiscusse limitazioni nell'esercizio, lo Stato è tuttavia l'unico attore che dispone di tale strumento. Anche il discorso dell'asimmetria verrà ripreso in seguito, ma alcune precisazioni occorre farle ora, perché relative ai ruoli di alcuni degli attori sopra elencati. A livello internazionale, che si tratti di studiosi, di uomini politici o di commentatori, lo spazio virtuale risulta essere uno spazio dove ognuno può portare a termine *cyber-operations*, oppure "*the kingdom of hackers and indipendent attackers*" [60]. Queste parole corrispondo a verità, ma solo parzialmente. Molte delle proprietà del cyber-spazio, infatti, fanno sì che emerga preminentemente la dimensione qualitativa su quella quantitativa, nel senso che, se dotati delle conoscenze e delle capacità necessarie, pochi individui possono causare un grande numero di danni o penetrare un elevato numero di reti. Sintetizzando, le caratteristiche che rendono possibile questa tendenza asimmetrica sono: lo sbilanciamento dell'azione offensiva su quella difensiva; il basso costo necessario per ottenere tecnologie e capacità necessarie per sferrare un attacco; e la perdita di rilevanza delle caratteristiche di concentrazione di forze nello spazio e nel tempo. Tutte caratteristiche che sembrano favorire entità snelle e minute, contro i mastodontici apparati statali, lenti e incapaci di tenere tutto sotto controllo. La mia tesi è che ciò sia vero solo in parte e che, se si analizzano più in profondità le dinamiche di interazione (conflittuale o cooperativa), il cyber-spazio risulta dominato, così per gli altri domini reali, dalle entità statali.

All'interno del cyber-spazio si è venuto a creare un grado di competitività multilivello, che riproduce quasi *in toto* quella presente nella dimensione reale. Possono avvenire, infatti, furti compiuti da singoli ai danni di singoli o di entità di maggior aggregazione, come le banche. Così come possono avvenire azioni politiche, individuali o di gruppo, contro entità statali o altri gruppi, le quali possono assumere un carattere di contestazione o di vera e propria offesa[61]. Tutti i soggetti

[60] ibid p 30

[61] Nel capitolo successivo si parlerà brevemente della possibilità o meno di considerare il terrorismo nel cyber spazio.

considerati possono poi agire a loro volta nei confronti degli Stati, il che sembra essere la grande peculiarità del cyber-spazio: il quindicenne occhialuto che dalla sua scrivania disordinata mette in pericolo l'esistenza stessa dello stato nazionale è da almeno due decenni l'immagine stereotipica delle minacce provenienti dal cyber-spazio. In realtà, ritengo che questa affermazione, oltre ad essere iperbolica, sia solo parzialmente vera poiché non considera la variabile qualitativa degli attacchi e non corrisponda perciò assolutamente al fulcro principale del conflitto che si verifica nel cyber-spazio.

Seppur ancora oggi, una maggior incisività sia legata al fenomeno del cyber-crimine, se analizziamo la questione sotto il punto di vista delle relazioni internazionali e dell'analisi strategica, il punto focale rimangono gli attori statali, uniche entità capaci di interagire con le varie categorie di attori e destinatari ultimi delle offese politiche di individui e gruppi. Lo Stato è l'unico attore dell'arena internazionale capace di gestire non solo le tecniche offensive ma anche quelle difensive. È infatti più complesso, più costoso, più lungo in termini temporali, assicurarsi delle capacità difensive. Secondo l'opinione di chi scrive, così come lo Stato rappresenta ad oggi l'unica entità aggregativa capace di assicurare sicurezza e degni livelli di vita[62] nel dominio "reale", lo stesso vale per il cyber-spazio: le entità statali sono le uniche in grado di gestire l'enorme afflusso di utenti e dati. Anche in ambito militare è lo Stato l'unico attore capace di gestire in maniera efficiente situazioni e attacchi cibernetici. Questo per una serie di fattori. Innanzitutto, per quanto vero che gli attacchi cibernetici sono più facili da muovere che da respingere è necessario precisare che questo vale per attacchi limitati, nel tempo e nell'efficacia. Come dimostra il caso di Stuxnet[63], per coordinare un attacco di notevole ampiezza e durata è essenziale un immenso lavoro preparatorio e di supporto logistico: intelligence, analisti, operatori. Allo stesso modo per difendersi efficacemente e in maniera globale è necessario, non solo creare

[62] È questa chiaramente un'affermazione estremamente generica che non ha intenzione di essere inclusiva di tutte le realtà conosciute a livello globale

[63] Vedi prossimo capitolo

barriere difensive e ipotizzare teorie strategiche, ma creare un ecosistema difensivo che abbracci tutti i livelli della società e che sappia preparare non solo gli esperti ma anche il più alto numero possibile di coloro che hanno accesso alla rete. Si vedrà come Israele ed Estonia sono due esempi, pur nelle loro differenze, di questo *ecosistema.*

1.4 Il ruolo dello Stato nel cyber-spazio e i suoi limiti d'azione

"States have a right to exercise their territorial jurisdiction over cyber activities within their territories. However, the characteristics of cyberspace and the necessity to preserve the functionality of the Internet call for consensual limitations of an exercise of territorial jurisdiction".

Wolff Heintschel von Heinegg[64]

È quanto mai complesso stabilire quali siano o quali debbano essere le caratteristiche dell'azione statale nel cyber-spazio e ancor più difficile derivarne le responsabilità e gli spazi di manovra. Per quanto il cyber-spazio sia altamente internazionalizzato per sua natura, una quantità considerevole di infrastrutture e componenti risiedono sul territorio nazionale gestito dallo Stato. Inoltre, le recenti pratiche statali forniscono prove sufficienti che il cyber-spazio, o almeno alcuni componenti di esso, non siano immuni dalla sovranità nazionale. Come ricorda Liaoropulos (2011)[65], "*Cyberspace is non-territorial, but in sharp contrast to the land, sea, air and space, cyberspace is not a part of nature, it is man-made and therefore can be unmade and regulated*". Il suo punto di vista è quasi del tutto condiviso tra gli esperti del settore, ma sulla questione della territorialità si è sviluppato un inteso dibattito.

[64]Czossek, C. e Ottis, R. e Ziolkowski K. (2012) *4th Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, p.7
[65]Liaropoulos, A.N. (2011b*) Power and Security in Cyberspace: Implications for the Westphalian state system*, in *Panorama of Global Security Environment*, Centre for European and North American Affairs, Bratislava

In un articolo pubblicato da Forrest Hare della School Of Public Policy della George Mason University[66], l'autore analizza dettagliatamente il caso in cui si possa dare o meno rilevanza ai confini terrestri quando si considerano gli episodi relativi al cyber-spazio. Le conclusioni a cui giunge sono relative fondamentalmente al contesto statunitense, ma, a mio avviso, possono essere applicate universalmente in quanto stabiliscono che:

"*whether the problem is addressed from the standpoint of criminal behavior like drug trafficking, or cyber attacks in an interdependent, global domain, borders can be a potentially useful construct to address cyber security issues and inform national policy decisions, regardless of the physical location of relevant nodes. However, sovereign powers must be careful not to use the concepts of borders to curtail the progress our nations have made to connect and better the world via this evolving and expanding environment*."

Il concetto è di notevole importanza e, a mio parere, andrebbe analizzato in maniera più dettagliata nel contesto internazionale, seguendo magari le linee del mastodontico lavoro prodotto dal NATO Cooperative Cyber Defence Centre of Excellence di Tallinn[67] sotto la guida di Michael Schmitt. Il lavoro intitolato "*Tallinn Manual*" è un interessante studio riguardo l'adattabilità del diritto internazionale (soprattutto *ius ad bellum* e diritto umanitario) ai conflitti nel cyber-spazio. In particolare la prima sezione, intitolata "State and Cyberspace", analizza esaurientemente il rapporto tra la sovranità nazionale e il territorio. Il testo riconosce la piena possibilità degli Stati di esercitare sovranità sulle infrastrutture comprese nel territorio nazionale[68], sugli agenti che operano nel cyber-spazio sul proprio suolo nazionale e, nei casi previsti dal diritto internazionale, su infrastrutture che non appartengono al proprio territorio (i.e. ISP, Internet Service

[66] Hare, F. (2010) *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?*, in *Virtual Battlefield,* NATO CCDCOE Pub., Tallinn. consultabile http://www.ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf ultimo accesso 28.02.2014

[67] Schmitt, M.N. ed. (2013) *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge University Press, Cambridge.

[68] Il preambolo a questa regola è che ovviamente NESSUNO stato può avanzare rivendicazioni sul possesso del cyberspazio *per sé.*

Providers)[69]. Di conseguenza qualsiasi atto compiuto ai danni di una qualsiasi di queste infrastrutture (o persone) risulta una chiara violazione della sovranità nazionale. Nel caso di un attacco proveniente da un territorio nazionale, però, la questione diventa più complessa. Seppur vero che uno Stato deve far in modo che non vengano compiuti attacchi a partire dal proprio territorio (e certamente non deve favorirli), è anche vero che il mero atto di riscontrare un atto offensivo o danneggiante infrastrutture appartenenti ad altri Stati non comporta in immediato la responsabilità dello Stato dal quale è partito l'attacco. È questo il caso ad esempio degli attacchi DDoS (Distributed Denial of Service)[70] che sfruttano computer infetti che possono essere distribuiti in giro per il mondo per causare un flusso eccessivo di dati. Dimostrazione pratica è il caso dell'attacco in Estonia nel 2007, la maggioranza degli attacchi subiti proveniva da Egitto e Stati Uniti, ma ovviamente nessuno ha ritenuto colpevoli i due paesi di un attacco all'Estonia.

1.4.1 Offesa/difesa e controllo/libera circolazione

Gli Stati hanno costantemente rivendicato il loro diritto di esercitare il controllo sulle cyber-infrastrutture ubicate nei rispettivi territori, oltre che quello di esercitare la propria giurisdizione sulle *cyber-activities* che si svolgono sul loro territorio e di proteggere le infrastrutture informatizzate presenti sul suolo nazionale contro qualsiasi interferenza transfrontaliera da parte di altri Stati. Questa volontà è stata perseguita con modalità e intenti diversi, che si possono identificare attraverso due categorie differenti di azioni. Da una parte il continuum che va da Stati con modalità difensive a quelli con modalità offensive; dall'altra il continuum degli stati che esercitano un forte controllo autoritario contro quelli che lasciano libera circolazione di informazioni e intraprendono politiche più liberali nel controllo del cyber-spazio.

[69] Legato a questo concetto si apre un infinito dibattito sulla territorialità *di smartphone* e *portable devices*, che per lo scopo della trattazione risulta fuorviante. Rimando alla lettura del manuale per ulteriori informazioni o alla consultazione di https://cs.uwaterloo.ca/~cdimarco/pdf/cogsci600/Scott2013.pdf

[70] Vedi prossimo capitolo

Per quanto riguarda la categoria dell'approccio difensivo/offensivo non è sempre semplice posizionare un paese verso un estremo. Questo perché spesso è più complesso giudicare la discrepanza tra dichiarazioni di intenti e azioni effettive. Non tutti i paesi hanno necessità di operare in maniera eclatante, molti preferiscono agire di nascosto, sfruttando a loro beneficio la possibilità di far perdere le proprie tracce dopo aver effettuato un attacco (problema dell'attribuzione). Un paese che non risponde a queste categorie è Israele. Gli uomini politici e i militari israeliani hanno affermato più volte che secondo la loro interpretazione strategica il dominio cibernetico rappresenta un nuovo scenario di guerra e per questo bisogna attrezzarsi sia in termini difensivi che offensivi". Sono due gli eventi specifici che ci permettono di misurare le implicazioni teoriche nelle azioni militari israeliane: l'attacco del 2007 alle basi siriane e il *master pièce* degli attacchi informatici, Stuxnet[71]. All'estremo opposto del continuum vi sono la maggior parte degli Stati che invece hanno intrapreso un approccio puramente difensivo[72], sia attraverso la pubblicazione di strategie[73] nazionali, sia con la più semplice sistematizzazione delle forze. In mezzo a queste due categorie vi sono poi una schiera di paesi le cui attività sono più o meno offensive di quanto dichiarato.

Tra coloro che si dichiarano maggiormente difensivi di quanto in realtà siano: Stati Uniti, Cina e Russia. Tutte e tre, sono state accusate di aver utilizzato le proprie capacità offensive per scopi militari e si sono giustificate spesso affermando che la varietà delle minacce richiedono che vi sia un impianto militare pronto a farvi fronte. Vi sono poi anche Stati che si comportano nella maniera opposta, ovvero dichiarano di aver sviluppato potenzialità offensive e di essere in grado di adoperarle, nonostante le azioni da loro intraprese nel passato (e in alcuni casi anche la storia stessa del paese) non giustifichino tali dichiarazioni. È

[71] Per spiegazione dettagliata di entrambi gli eventi si veda il prossimo capitolo

[72] Per correttezza, è necessario dire che le tecnologie necessarie per sviluppare un efficiente Sistema di difesa sono quasi universalmente *dual-use* e ipoteticamente impiegabili anche per sviluppare capacità offensive.

[73] Tutte le strategie possono essere riviste al https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_national-cyber-security-strategies-in-the-world

questo il caso dei Paesi Bassi[74] che nella loro *National Cyber Strategies* hanno lasciato ampio spazio alle potenzialità offensive, ma, considerando situazione geopolitica e ipotetici scenari conflittuali, sembra che la ragione principale di tali intenti sia provocare una sorta di deterrenza in attori malintenzionati o persino, che il vero target degli ipotetici attacchi cibernetici nazionali siano entità non-statali responsabili di frodi o furti.

Passando alla diversità di approccio interno, è interessante notare come negli ultimi anni abbia preso piede il dibattito[75] sul libero utilizzo o la chiusura del cyber-spazio. Da una parte ci sono coloro che considerano il dominio virtuale come una *res commonis,* dall'altra troviamo coloro che si sentono minacciati dalle sue potenzialità e vorrebbero limitarlo. La dimensione virtuale spesso travalica quella nazionale, soprattutto in termini di idee trasmesse, per questa ragione determinati Stati scelgono di approcciarsi a questo flusso di informazioni in maniera più o meno restrittiva. Tre dimostrazioni possono aiutare a spiegare la questione. Il più chiaro e famoso esempio di censura della rete è senza dubbio il *Great Firewall cinese*: in Cina una quantità mastodontica di siti internet è infatti considerata illegale e ufficialmente inaccessibile[76]. Il secondo esempio riguarda gli eventi degli ultimi tre anni in Medio Oriente: in Egitto[77] così come in Siria, il totale blocco delle funzionalità della rete è stata una pratica usata in più occasioni durante i più conclamati momenti di ribellione. Nel caso siriano[78] ancor più che in quello egiziano le forze governative (così come anche i ribelli) hanno saputo sfruttare le possibilità di limitare il traffico di dati, trasformandola in un'arma a loro favore molto potente.

All'estremo opposto si trovano paesi e organizzazioni internazionali che credono profondamente nella necessità e nelle

[74] Consultabile https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf ultimo accesso 28.02.2014

[75] Si vedano ad esempio http://www.technollama.co.uk/open-web-vs-closed-internet o http://gigaom.com/2012/03/23/open-vs-closed-what-kind-of-internet-do-we-want/

[76] Per una lista completa aggiornata in tempo reale: http://www.greatfirewallofchina.org/

[77] Si sono occupati in molti della questione, tra cui anche numerose organizzazioni internazionali: http://www.freedomhouse.org/report/freedom-net/2012/egypt#.UwNeIfl5O4I

[78] Lo stesso per la Siria, che è stata oggetto di studio daparte i moltissime entità anche dal punto di vista del controllo di internet: http://surveillance.rsf.org/en/syria/

potenzialità di un cyber-space libero e aperto che possa promulgare i valori dell'inclusione sociale e politica a livello globale[79]. È questa in particolare la posizione dell'Unione Europea che sta cercando di portare avanti una campagna di liberalizzazione internazionale dei contenuti e delle possibilità di accesso. Queste abissali differenze di gestione del cyber-spazio risiedono nell'interpretazione divergente che i governi danno di questa dimensione. Se da una parte per gli Stati che più spingono per la liberalizzazione di internet questo rappresenta un network dal valore neutro, per i governi autoritari il canale di diffusione di informazioni può essere una potente fonte di *soft-power*[80] capace di diffondere pericolosi messaggi sovversivi. Per questa ragione internet deve essere rigidamente controllato e i messaggi trasmessi da parte delle autorità all'esterno posso (e devono) essere manipolate per veicolare l'ideale di giustizia promosso dal regime.

Come corollario a queste categorizzazioni è necessario osservare la situazione degli Stati Uniti, che, in relazione al cyber-spazio, occupano sicuramente una posizione internazionalmente privilegiata. Il fatto che la rete sia nata negli Stati Uniti non è solo di rilevanza storica ma anche strutturale. Essendo la fonte principale delle infrastrutture della rete mondiale, gli USA hanno anche in una certa misura ampio controllo del funzionamento stesso della rete. È infatti dai server di ultimo livello che parte la distribuzione globale di internet. Questa caratteristica si è resa particolarmente decisiva anche in recenti situazioni belliche, basti pensare al fatto che nel 2003 quando gli Stati Uniti invasero l'Iraq, la rete irachena venne completamente oscurata dagli stati Uniti, provocando notevoli svantaggi sia militari che di gestione sociale per il paese mediorientale. Nonostante gli Stati Uniti da sempre denuncino le vulnerabilità legate alla dipendenza mondiali dalle infrastrutture statunitensi, è innegabile che, quello che inizialmente poteva essere definito tramite le parole di Gramsci, come egemonia

[79] La strategia Europea è disponibile a http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[80] Thouy, E. e Maldre, P. (2013) *Dynamic Challenges, enduring Institutions: Cyber Security and the Future of the Tansatlantic Alliance*, ICDS Publ., Tallinn p.5

culturale[81], è diventata oggi un decisivo vantaggio sia commerciale che bellico, come dimostra la vicenda irachena.

In conclusione, riprendendo un concetto espresso in precedenza, il cyber-spazio viene erroneamente caratterizzato come un dominio che trascende lo spazio fisico e quindi considerato immune alla sovranità statale e resistente alla regolamentazione internazionale.[82] Condividendo il pensiero del professor Andrew Liaropoulos e di molti altri esperti, ritengo che il cyber-spazio, in comune con gli altri quattro domini (terra, aria, mari, spazio) sia, nonostante le sue caratteristiche uniche, una semplice rappresentazione dell'ordine mondiale odierno e che sia influenzato dale regole che da questo provengono. Per questo stabilire cosa significa sovranità nazionale is critico perr ogni discussione in riguardo alle future regole nel e del cyber-spazio[83].

Credo sia necessario rivolgere lo sguardo agli stati, alle loro interazioni ed obiettivi nel cyber-spazio, se si vuole cogliere la dinamica di potere che si sta generando nell'innovativo dominio cibernetico. Senza togliere importanza al fenomeno del declino dello stato[84] e alla crescente rilevanza che stanno assumendo, in modo particolare nel mondo virtuale, le entità non statali e le imprese multinazionali, credo che ad oggi, siano le entità statali a dover giocare il ruolo di oggetti e soggetti nelle competizioni e nei conflitti internazionali, persino nel c*yber-space*.

1.5Il Cyber-Power

Dopo esserci soffermati largamente sulla definizione di cyber-spazio e sui suoi protagonisti, è ora necessario analizzare le

[81] A. Gramsci, Quaderni del carcere, a cura di F. Platone, Torino, 1948-1951

[82] Liaropoulus, A.N. (2013) *Exercising State Sovereignti in Cyberspace: an International Cyber-order under construction?*, paper presentato all 8th *Conference on Information Warfare and Security,* Denver. Consultabile a https://www.academia.edu/3322607/Exercising_State_Sovereignty_in_Cyberspace_an_international_cyber-order_under_construction_in_8th_International_Conference_on_Information_Warfare_and_Security_Denver_Colorado_25-26_March_2013 ultimo accesso 28.02.2014

[83]Ibid p. 137

[84]Van Creveld, M. (1999) *The Rise and Decline of the State*, Cambridge University Press, Cambridge

caratteristiche dell'interazione di questi attori all'interno dell'universo cibernetico e quali siano i loro obiettivi e necessità.

È quindi il momento di parlare delle categorie di potere e sicurezza declinate al dominio cibernetico: la ricerca da parte degli stati di *cyber-power* e *cyber-security*. Come sostiene Nye (2010) "*power depends upon context, and the rapid growth of cyber space is an important new context in world politics*", perciò è comprensibile che gli Stati, in quanto principali entità agenti nel sistema internazionale, cerchino di massimizzare Il proprio *potenziale* di potere in modo da aumentare la loro competitività internazionale. La questione è essenziale ma complessa. Il concetto di potere ha da sempre diviso più che unito i teorici delle scienze politiche. Schematizzando e semplificando estremamente il pensiero di alcuni luminari delle relazioni internazionali si può dire che per Morgenthau [85] il potere rappresentasse il fulcro dell'interesse nazionale; per Wolfers [86] fosse uno strumento coercitivo, violento e costoso; Waltz[87] lo considerava, invece, un mezzo per ottenere la sicurezza, fine ultimo dello stato; Mearsheimer[88], al contrario, credeva che fosse centrale per intendere le politiche degli Stati, interessati alla sua massimizzazione per imporsi sugli antagonisti; infine per Rose e i realisti neoclassici[89] il potere assume una caratterizzazione materialistica fondamentale per influenzare gli altri attori.

Trasposta al cyber-spazio la questione non si ridimensiona né perde di complessità, al contrario acquista nuove dimensioni di controversia. Vi è chi ne dà una definizione sulla stessa lunghezza di quelle classiche sopra riportate, come ad esempio Kuehl che parla di *cyber-power* come "*the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power"*[90]*. Oppure v*i è chi, come Nye, sposta l'attenzione

[85]Morgenthau, H. (1948) *th politics Among Nations: The Struggle for Power and Peace*, Alfred Knopf, New York
86 Wolfers, A. (1962) Discord and Collaboration: Essays on International Politics (Baltimore: The Johns Hopkins Press, 1962, Chapter Five, "The Goals of Foreign Policy," pp. 67- 80
[87]Waltz, K. N. (1979) T*he Theory of International Politics*, Mc Graw-Hill, New York
[88]Mearsheimer, J. (2001) *The Tragedy of Great Power Politics*, W.W. Norton & Co., New York
[89]Rose, G. (1996) op. citata
[90] Ibid p. 546

sul cambiamento avvenuto all'interno del cyber-spazio, e crede che sia il perfetto esempio di quel fenomeno di globalizzazione della politica che sta erodendo in maniera lenta ma inesorabile il predominio dello Stato nell'arena delle relazioni internazionali. Infine vi è chi, come Liaropoulos, nota come in realtà siano proprio gli Stati a giocare il ruolo principale, nel tentativo non solo di assicurare il "proprio" cyber-spazio, ma di renderlo militarmente operativo (i.e. Stati Uniti).

Un'interessante analisi del concetto teorico di *cyber-power* è quella avanzata da Starr (2009)[91], che lo considera in relazione a categorie di misurazione del potere utilizzate in precedenza da teorici precursori nello studio dei domini bellici. Starr considera quindi le seguenti caratteristiche: il vantaggio tecnologico; la velocità e lo scopo delle operazioni, il controllo delle caratteristiche principali e la mobilitazione nazionale. Queste categorie sono utili più per definire il potere in sé all'interno del cyber-spazio, piuttosto che per chiarire la relazione di potere tra diversi Stati. Consideriamo il vantaggio tecnologico. Secondo l'autore il livello di vulnerabilità creato dalle nuove tecnologie ed il relativamente basso costo richiesto per la loro acquisizione hanno reso il cyber-spazio un dominio strategicamente attaccabile. Così anche l'aumento della velocità e la riduzione dell'orizzonte spaziale e temporale hanno posto in essere grandi limiti per il processo decisionale (i.e. OODA Loop[92]). Starr ritiene che il fattore chiave del cyber-spazio (una sorta di *centro gravitazionale* clausewitziano) siano i centri di concentrazione di informazione e tecnologia, che avrebbero un effetto opposto rispetto a quelli provocati dalle prime due caratteristiche, poichè la volubilità delle strutture renderebbe più complesso colpire *mortalmente* un avversario. Per quanto riguarda l'ultima categoria, la mobilitazione nazionale, risiede nella capacità di investire sulle capacità della propria popolazione. In

[91]Starr, S. H. (2009) *Toward a Preliminary Theory of Cyber Power*, in Kramer, F.D., et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington D.C.

[92] Per un'idea chiara su cosa sia l'OODA Loop si veda Brehmer, B. (2006) *The Dynamic OODA LOOP: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control*, Department of War Studies
Swedish National Defence College

questo caso l'esposizione quotidiana ai fenomeni cibernetici potrebbe essere un vantaggio per la concentrazione di potere.

Queste quattro caratteristiche incrociate con le categorie 'strategico', 'operative' e 'tattico', danno vita a uno scenario di rischi e opportunità illustrato nella tabella riportata qui sotto.

	Opportunità	**Rischi**
Strategico	- *Net-centric warfare* - Nuove possibilità di *centro di gravità* (e.g deterrenza)	- Perdita di vantaggio tecnologico - Cambiamento rapido dell'ambiente operativo - Dipendenza militare dai sistemi chiave (i.e. global information grid)
Operazionale	- *Phasing of operation* - Miglioramento del mix della struttura delle forze (più economiche e precise)	- Perdita di vantaggio nella capacità operazionale
Tattico	- Scoprire e tracciare avversari nel cyber-spazio	- Nuova schiera di avversari contro cui confrontarsi

Dallo schema di Starr si possono dedurre una serie di rilevanti riflessioni. Innanzitutto l'aumento degli attori nel cyber-spazio influenza la dimensione del potere solo da un punto di vista tattico, il che è ammissibile secondo la nostra teoria, perché la dimensione tattica non modifica l'equilibrio internazionale o il pensiero strategico. In secondo luogo, è interessante vedere come a livello operazionale vi siano immense opportunità per lo sviluppo di tecnologie integrate al C*ommand-and-Control* e la gestione del campo di battaglia. Infine, per quanto riguarda il livello strategico, quello che più ci interessa, è necessario notare due fattori chiave. Da un lato l'opportunità difensiva

che offre la mancanza di punti gravitazionali fissi e dall'altro il rischio insito nella dipendenza dai sistemi ICT.

Ciò che ora serve alla teoria è avere la caratteristica dell'operatività e la possibilità di essere applicata in termini relativi, così da poter spiegare l'impegno di diverse entità statali (e di organizzazioni internazionali, i.e. NATO) per acquisire determinate caratteristiche per garantirsi la superiorità. Ciò che occorre fare è ricollegare tra loro la definizione di Kuehl vista in precedenza, la triplice dimensione analizzata da Starr e le caratteristiche tecniche descritte. Il risultato è una complessa categorizzazione di abilità personali, metodi di organizzazione e capacità tecnologiche. Così considerato, il potere cibernetico si compone di tre dimensioni. La prima è quella tecnologica: la capacità dello Stato di seguire il ritmo del cambiamento ultra rapido delle tecnologie di *hardware* e *software* per sfruttarle a proprio beneficio, tentando dove possibile di essere innovatore. La seconda è di tipo organizzativo: uno Stato può prediligere una dimensione militare o economica o politica anche nelle sue attività nel cyber-spazio[93], così da influenzare la tipologia di potere che intende perseguire. Infine la terza componente riguarda le informazioni: che siano fini a sé stesse o istruzioni per lo svolgimento di qualche azione, la protezione e la capacità di trasmetter informazioni è sicuramente uno dei principali fattori che caratterizzano il potere cibernetico[94].

Non bisogna inoltre tralasciare un'ultima, importantissima caratteristica: il *cyber-power* è evolutivo. È evolutivo perché è evolutiva la natura del dominio in cui esso si esercita. Lo è anche perché la mente umana che modella il sistema spaziale è adattativa: a nuove minacce risponderà creando nuove difese e, viceversa, a nuove difese coincideranno nuove possibilità per aggirarle. Infine, è evolutivo, perché le tecnologie a cui si fa riferimento per essere all'avanguardia nel mantenimento e nello sfruttamento del *cyber-space* diventando

[93] Ne sono un chiaro esempio la differenza negli investimenti nel settore della *cyber security* di paesi con diversi interessi geopolitici come ad esempio il Lussemburgo, che investe quasi unicamente nella protezione delle sue infrastrutture bancarie, e l'Estonia che invece investe quasi interamente nella protezione delle infrastrutture critiche

[94] Ne sono una dimostrazione i massicci investimenti cinesi e statunitensi che (per scopi diversi) hanno costruito massicci sistemi di spionaggio e raccolta dati (i.e. PRISM e unità APT1)

rapidamente obsolete ed è necessario un determinato impianto sociale per rendere possibile il perpetuo rinnovamento. Per questo soltanto un sistema-paese impostato sull'elasticità della propria forma organizzativa e sulla rapida risposta alle innovazioni può e potrà permettersi di creare per sé stesso un *cyber-power* continuativo e credibile.

Per concludere, il *cyber-power* è diventato una componente essenziale per tutte le dottrine militari e le strategie di difesa nazionale negli ultimi due o tre decenni. Oggi, a prescindere dall'attratività espressa dal cyber-spazio, non esiste forza militare che trascenda dalle implicazioni militari nel dominio virtuale, così come non vi è militare che non ne esalti le caratteristiche, i pericoli e le potenzialità.

1.5.1.Quali sono gli attori maggiormente interessati ad acquisire cyber-power?

Il principale attore sulla scena cibernetica sono senza dubbio gli **Stati Uniti**. Inventori delle tecnologie necessarie per il funzionamento di Internet sono stati anche i primi a sostenerne lo sviluppo. Inoltre, molte istituzioni che dominano il mondo della *cyber-security* sono statunitensi, basti pensare alla californiana ICANN[95], che pur avendo funzioni di estrema rilevanza internazionale, ha sede legale a Marina del Rey, California. Questo vantaggio è aumentato dalla tendenza statunitense a ricercare militarmente la superiorità tecnologica e l'applicazione di scoperte all'avanguardia per incrementare le proprie capacità sia strategiche che tattiche. È così che sin dagli anni Novanta sono stati il primo paese che ha visto nell' *information dominance*[96] un'importante arma capace di cambiare le regole del gioco. L'eredità della guerra elettronica studiata ed implementata dall'Aeronautica Militare ha portato gli Stati Uniti verso una dimensione di integrazione delle capacità

[95] ICANN è The Internet Corporation For Assignments Of Names And Numbers, il suo ruolo principale è quello di distribuire e controllare indirizzi IP, mantenedo l'unicità di ogni indirizzo, permettendo un ordinato funzionamento del DNS (Distributed Name System). Per maggiori informazioni su http://www.icann.org/en/about/welcome

[96] Tirmaa-Klaar H. e Klimburg A. (2011) *Cybersecurity And Cyberpower: Concepts, Conditions And Capabilities For Cooperation For Action Within The Eu*

belliche cibernetiche[97] negli altri domini militari, piuttosto che la possibilità di colpire direttamente[98] con attacchi cibernetici strategici. Sono inoltre il paese che più spende al mondo (secondo stime ufficiali, spesso difficili da verificare in paesi meno trasparenti nella gestione delle spese militari) in *cyber-security* e nello sviluppo di nuove tecnologie difensive poiché per il modello militare occidentale è diventata fondamentale la *Network Centric Warfare*[99]*.* Nell'ambito della Difesa gli Stati Uniti sono senza dubbio tra i paesi più avanzati al mondo in termini di capillarità e di preparazione: la promulgazione del *National Cyber Incident Response Plan* e la coordinazione tra la difesa civile (affidata *al Department of Homeland Security*[100]) e quella militare (affidata allo *USCYBERCOM*[101]) hanno permesso un importante avanzamento nelle capacità militari del paese nel cyber-spazio (e gli sono valse numerose critiche dalla comunità internazionale).

Anche la **Federazione Russa** ha da sempre attribuito notevole importanza allo sviluppo delle *cyber-capabilities* dal punto di vista militare. La differenza con gli Stati Uniti è facilmente riscontrabile. Se, infatti, per gli USA le possibilità cibernetiche hanno prodotto una nuova forma di integrazione nell'arte bellica a tutti i livelli (i.e. tattico, strategico, operazionale), per il concetto strategico russo *l'Information warfare*[102] e il *cyber-power* sono divenute componenti fondamentali per poter sfruttare al massimo le potenzialità della *Psychological warfare*[103],

[97] *The Evolution of US Cyber Power* (2012) consultabile: http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf ultimo accesso 28.02.2014

[98] Da notare come l'attacco di Stuxnet sia estraneo a questa logica, per questo si pensa la teorizzazione tattica sia stata frutto delle menti israeliane

[99] Per NCW si intende una dottrina militare, di cui gli Stati Uniti sono stati i precursori, secondo la quale lo scopo ultimo è quello di cercare di tradurre un vantaggio informativo (reso possibile in parte dal vantaggio nel possesso di tecnologia atta all'informazione) in un vantaggio competitivo attraverso la robusta rete di comunicazione tra forze disperse geograficamente, ma costantemente informate.

[100] Confronta http://www.dhs.gov/topic/cybersecurity

[101] http://www.arcyber.army.mil/

[102] Giles, K. 82012) *Russia's Public Stance on Cyberspace Issues*, in CZOSSEK, C. e OTTIS, R. e ZIOLKOWSKI K. (2012) *4th Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn. E CCDCOE (2011) *Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space* consultabile http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf a ultimo accesso 28.02.2014

[103] Per maggiori informazioni http://www.fas.org/irp/doddir/army/fm3-05-30.pdf e http://www.psywar.org/

modalità considerata come un paradigma *conflict-winning*[104]*.* Nel 2011 la Russia ha pubblicato la "Convention on International Information Security"[105] nella quale vengono enunciate minacce e relative contromisure da adottare nell'i*nformation space*[106]. Inoltre, la Russia ha da sempre ostacolato la preminenza americana nel cyber-spazio e il suo dominio nel controllo, tanto da aver portato avanti numerose mozioni in seno alle Nazioni Unite per favorire l'internazionalizzazione del controllo (prevalentemente attraverso la proposta di un Board internazionale che gestisca l'ITU). Una caratteristica fondamentale della scena russa è la proliferazione del *cyber-crime* a tutti i livelli, dai singoli truffatori cibernetici alle grandi organizzazioni criminali che, data la storia di collusione tra governo e questo tipo di associazioni, potrebbero oggi giocare un importante ruolo nel muovere cyber-attacchi[107]. Per concludere, uno dei fenomeni più rilevanti è sicuramente la presenza di numerosissimi *cyber-patriots* che risultano essere fortemente collegati al governo centrale, tanto da aver preso attivamente parte ai due celebri attacchi del 2007 e del 2008 in Estonia e in Georgia. Come si vedrà, se nel caso della Georgia le evidenze sono più lampanti[108], nel caso dell'Estonia il contesto è più opaco e le responsabilità non sono del tutto chiare.

Secondo Siboni G. e Y.R. (2012) "*chinese activity in the field of cyberspace warfare is intensive and aggressive*"[109] . Allo stesso risultato, se non più dettagliato, è giunto il famigerato Rapporto Mandiant (2013) sull'attività svolta dalla cellula APT1 (o Unit 61398), apparentemente facente capo all'Esercito di Liberazione del Popolo cinese[110]. Per la **Cina** l'attenzione alla questione cyber è divenuta

[104] È questa una delle ragioni per cui la Russia applica un controllo così severo del cyber-spazio offerto ai propri cittadini, per il timore degli *information-psychological* attacchi. Per questo motivo, ogni Internet Provider in Russia è tenuto a dare il permesso all'intelligence russa di monitorare tutto il traffico che passa attraverso la rete.

[105] Consultabile http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument ultimo accesso 28.02.2014

[106] Vedi differenza in definizione vedi prossimo capitolo

[107] Bikkenin R. (2003) *Information Conflict in the Military Sphere: Basic Elements and Concepts,* Morskoj Sbornik, no. 10

[108] http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

[109] Siboni G., Y.R (2012) "What Lies Behind Chinese Cyber Warfare", *Military and Strategic Affairs*, No. 2, pp. 49-64

[110] Mandiant (2013) *APT1 Exposing One of China's Cyber Espionage Units.* Consultabile

fondamentale sin dall'indomani della Guerra del Golfo. L'idea degli strateghi cinesi è stata quella di acquisire delle capacità asimmetriche in modo tale da contrastare l'immenso predominio mostrato dagli statunitensi nella guerra convenzionale.[111] In Cina è l'esercito che gestisce le capacità cibernetiche, mentre nella sfera dei privati non si vede quella floridità che contraddistingue il mercato USA. Secondo un report prodotto da Tirmaa-Klaar e Klimburg A. (2011):

"*The Chinese military capabilities are probably two-fold: at the strategic level, the PLA cyber-capabilities are purported to be concentrated within the (very large) General Staff Departments, and cover both strategic defensive and offensive roles. At an operational level, the PLA has set up a large number of battalions that are integrated into military district and field-army structures. Some of these units probably directly support the operational capabilities of field units (as Western C4SIR units do), while others are perhaps officially intended as semi-autonomous militia units capable of waging 'strategic strikes' – i.e. attacking the enemies' critical infrastructure"*.[112]

Inoltre, l'esercito cinese sembra mantenere alle sue dipendenze schiere di hacker professionisti (si parla di decine di migliaia) solitamente legati ad imprese o università e spesso accusati dagli Stati europei e nordamericani di essere la fonte di attacchi cibernetici anche tecnologicamente avanzati (APT, Advanced Persistent Threat)[113]. Infine, il regime guidato dal Partito Comunista Cinese interpreta il cyber-spazio come una duplice minaccia: una proveniente dall'esterno con gli Stati Uniti come principale fonte di attacchi, ed un'altra dall'interno dove la crescita rapidissima dell'utilizzo di internet ha creato una schiera di *netizens* pronti a usare la rete come mezzo per criticare e condannare la gestione del partito.

Russia e Cina, hanno proiettato le loro volontà di massimizzazione di *cyber-power* anche all'interno del gruppo dei BRICS

---

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf ultimo accesso 28.02.2014

[111] ibid

[112] Ibid p 22

[113] Per approfondire le casistiche di attacco cinese si veda http://cryptome.cn.com/2014/uscc-chinas-cyber-activities.pdf; e Siboni e Y.R. sopra citato

(che comprende anche India, Brasile e Sudafrica) unito dalla volontà di mettere in discussione l'egemonia statunitense nel cyber-spazio[114]. Nonostante gli altri paesi del gruppo abbiano siglato con gli Stati Uniti degli accordi di collaborazione per quanto riguarda il cyber-spazio, sono tutti e cinque interessati a sviluppare un percorso di sfida nei confronti degli USA per il controllo e la gestione di internet, considerato come eccessivamente importante per i rispettivi interessi geopolitici.

Il tentativo di potenziamento nel cyber-spazio ha anche coinvolto le organizzazioni internazionali. A livello europeo l'attenzione al cyber-spazio è decisamente meno declinata al *cyber-power* e più rivolta alla mediazione di interessi e alla volontà di mantenere il libero accesso ad Internet. Lo dimostrano le tante iniziative supportate ed emanate dalla Commissione Europea a partire dalla recente *cyber strategy* pubblicata nel 2013 e intitolata "*an open, safe and secure cyberspace*"[115]. Il titolo e i contenuti fanno capire come il punto focale dell'Unione Europea sia interno e non abbia velleità di potenza (il che rientra nelle possibilità dell'Unione e nella sua prassi politica). A livello di Stati Membri, invece, molti hanno perseguito negli ultimi anni politiche di rinvigorimento delle proprie capacità militari nel cyber-spazio. Tra i più attivi vi sono sicuramente gli stati nordici, tra cui oltre all'Estonia spiccano Finlandia e Svezia, mentre nell'Europa continentale Francia e Germania hanno manifestato un discreto interesse nello sviluppo di competenze adeguate, con risultati migliori per la Germania che per la Francia.

Per quanto riguarda la NATO il discorso è notevolmente differente. Gli investimenti, l'interesse e la specializzazione militare nel cyber-spazio, hanno portato l'Organizzazione del Trattato Nord-Atlantico a sviluppare negli ultimi dieci anni un solido sistema difensivo e una discreto influenza nell'arena internazionale. La necessità di difendere il cyber-spazio condiviso è in agenda sin dal 2002, ma solo con gli incidenti in Georgia e Estonia, l'Organizzazione ha deciso di cambiare in

[114] http://jia.sipa.columbia.edu/cyberspace-and-rise-brics
[115] Vedi nota 79

maniera decisa la velocità e l'entità di investimenti e sviluppo. Nel 2011 veniva promossa una *cyber-Strategy* operativa e nel 2012 veniva istituito un NCIRC (NATO Computer Incident Response Capability) che è divenuto operativo un anno dopo[116]. Inevitabilmente il focus della NATO in termini organizzativi è l'i*nformation sharing,* operazione estremamente complessa, considerata la diversità dei membri che la compongono. Per questa ragione sono state programmate una serie di esercitazioni, di cui la prima si è svolta l'anno scorso in Estonia. Come è facile notare, la preponderanza dell'approccio strategico è di tipo difensivo (anche perché coincide con l'obiettivo principale dell'Organizzazione), ma bisogna tenere in conto due fattori estremamente rilevanti. In primo luogo, la duplice natura delle tecnologie informatiche, che consentono di trasformare facilmente una forza difensiva in offensiva. In secondo luogo la composizione interna è non solo variegata ma, in termini di capacità assolute, estremamente evoluta. Dando uno sguardo alle strutture militari dei singoli paesi membri[117] è facilmente intuibile che le potenzialità sono immense, non solo per la presenza di Stati Uniti, Canada e Germania, ma anche per le capacità manifestate dalla Turchia, dall'Olanda e dalla Danimarca.

Come si è visto le principali potenze del mondo e le più rilevanti organizzazioni internazionali si stanno dotando di competenze e capacità spendibili in termini di *cyber-power.* In realtà però lo spettro dei soggetti che stanno seguendo lo stesso percorso va notevolmente ampliato. Infatti, qualsiasi entità statale (e non solo) che abbia interessi regionali, situazioni conflittuali o un'ampia dipendenza dalle tecnologie informatiche, potrebbe cercare di esercitare sulla rete il maggior controllo possibile e in determinate occasioni sfruttare la possibilità di sferrare attacchi nell'anonimato, per indebolire i suoi rivali. È questa la storia di numerosi paesi: da Israele alla Repubblica Popolare di Corea,

[116] Per una descrizione precisa su struttura e attività della NATO in termini di cyber-sicurezza si veda l'articolo di Stefano Mele al seguente link: http://www.stefanomele.it/news/dettaglio.asp?id=396

[117] Gramaglia, M. E Pernik, P. e Thuoy, E. (2014) *Military Cyber Defense Structures of NATO Members: An Overview*, ICDS Pub, Tallinn consultabile a http://icds.ee/fileadmin/failid/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf ultimo accesso 28.02.2014

dall'Iran all'Uganda, sino ad arrivare alla Svizzera e a Panama[118]. La partecipazione attiva nel cyber-spazio è per altro più semplice che nell'arena internazionale *tradizionale,* ma, seppur le caratteristiche intrinseche favoriscano l'ingresso a basso costo, la possibilità di raggiungere livelli di potere consistenti non sembrano discostarsi di molto dalle dinamiche sperimentate nei secoli nelle relazioni internazionali.

1.6 Conflitto o cooperazione nel cyber-spazio?

Osservando lo scenario sopra descritto alcune domande sorgono spontanee: è dunque il conflitto (latente o esplicito) l'unico possibile risultato dell'interazione tra Stati che cercano di appropriarsi di porzioni di potere? Il cyber-spazio è un ulteriore dominio di competizione conflittiva, anche se ipoteticamente non violenta e coercitiva? O è possibile ipotizzare un ordine internazionale basato sulla cooperazione e sulla condivisione? Inutile dire che l'esperienza storica e le più rilevanti correnti delle relazioni internazionali sembrerebbero liquidare facilmente questi quesiti. Però, la prassi internazionale e le iniziative di diversi gruppi e organizzazioni lasciano intravedere possibilità differenti.

In questo senso la questione principale è ancora una volta il rapporto che intercorre tra ricerca del potere e della sicurezza. Le tendenze appena descritte mostrano come gli Stati stiano cercando di massimizzare il potere relativo in modo da imporsi sugli altri o, comunque, non essere messi in scacco da altri attori. Questa impostazione sembra riproporre in concreto le linee teoriche proposte da Mearsheimer, il quale interpreta le interazioni internazionali unicamente alla luce della ricerca di potere, inteso in termini relativi. Non è questa l'unica possibilità. Numerose sono state le voci che si sono schierate affinché non vi fosse una precoce militarizzazione del cyber-spazio e si trovassero modalità interattive differenti dalla mera

[118] Vedi nota 73(http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world)

conflittualità. Se, infatti, secondo molti[119] questo massiccio processo di militarizzazione del cyber-spazio è già stato avviato, causa di una versione cibernetica del dilemma della sicurezza[120], in molti si stanno prodigando per cercare di favorire la cooperazione nel cyber-spazio, sia a livello di normative, sia a livello di misure di *confidence-building* che dovrebbero servire a promuovere un ipotetico trattato internazionale per il controllo degli armamenti nel cyber-spazio. Il primo passo è stato effettuato lo scorso Dicembre, quando i rappresentanti di numerosi Stati aderenti al *Wasenaar Arrangement*[121]*,* hanno deciso di includere le armi cibernetiche nella lista di quelle per cui è vietata l'esportazione.

La comunità internazionale ha cercato di applicare pratiche risultate efficaci in precedenza e in ambiti compatibili alla situazione creatasi nel cyber-spazio. Anche l'Agenzia per il Disarmo delle Nazioni Unite[122], si è impegnata molto nella promozione di misure di *confidence-building* nel cyber-spazio. In una recente conferenza tenutasi al Palais des Nations di Ginevra, intitolata "*Cyber Stability: Preventing cyber conflict*", un gran numero di esperti e attivisti nel campo della cooperazione cibernetica si sono riuniti per tirare le somme della questione. La discussione e gli interventi dei numerosi speaker sono stati estremamente interessanti e la parola chiave 'collaborazione'. Il problema sostanziale è che ognuno intende la cooperazione in maniera diversa, poiché interpreta i concetti relativi al cyber-spazio in maniera distinta. Così i concetti di *cyber-security* e *cyber-governance* sembravano confondersi in un'unica categoria nei discorsi dei rappresentanti statunitensi, mentre la bandiera della sovranità nazionale veniva issata ogni qual volta che esponenti russi o cinesi prendevano la parola.

Tuttavia la linea del dialogo sterile è preferibile a quella del silenzio. È questo lo stesso atteggiamento che condiziona l'azione del gruppo Pugwash, il quale da sessant'anni si occupa di mediare a livello

[119] Cfr Siroli(2012) , *Cyberspazio e Cyberwar",* in *"L'ABC del Terrore. Le armi di distruzione di massa del terzo millennio",* a cura di Giampiero Giacomello e Alessandro Pascolini, V&P, Bologna
[120] Herz, J. (1950) *International Idealism and Security Dilemma*, World Politics, Vol. 2, No. 2 pp.157-180
[121] http://www.wassenaar.org/
[122] http://www.unidir.org/

tecnologico-scientifico tra le potenze nucleari per evitare una corsa agli armamenti, e negli ultimi anni si è mosso anche per tentare di evitare l'escalation di tensione nel cyber-spazio. A livello internazionale molte altre organizzazioni si sono mosse nella stessa direzione, consapevoli dell'importanza del cyber-spazio e del rischio che la corsa alla sua militarizzazione comporta. Ad esempio, l'ECOSOC ha pubblicato un report dal titolo "*A global issue demanding a global solution*" (2012)[123] che analizza il cyber-spazio dal punto di vista delle transazioni "transfrontaliere" e richiama alla necessità di porre alcune regole e limitazioni agli Stati. Oppure il World Economic Forum [124] che ha pubblicato un articolo su come gestire il fenomeno della sicurezza, attraverso la collaborazione interna ed internazionale. Infine, il più rilevante sviluppo sinora raggiunto risulta essere l'accordo siglato dai membri dell'OSCE (Organization for Security and Co-operation in Europe) nel dicembre 2013[125] che assicura il rispetto di alcune fondamentali misure di *confidence building*. Il fulcro della decisione risiede nello scambio di informazioni e nel proporre l'OSCE come sede per la gestione comune di determinate questioni legate al cyber-spazio. La Decisione stimola inoltre gli Stati a prender serie misure interne per omologarsi ai livelli internazionali di *cyber-security* sia in termini legali che tecnici.

Nonostante questi esempi, l'orizzonte della cooperazione, se non globalmente condiviso, rischia però di intensificare il conflitto. Data la difficoltà di concordare su concetti basilari da parte di attori in conflitto (i.e. Stati Uniti, Russia e Cina), le proposte avanzate da coloro che vogliono modificare lo status quo legato al cyber-spazio aumentano la diffidenza quanto la mancanza di apertura da parte della potenza egemone. Chiara manifestazione di questa è il *Code of Conduct* (2011) proposto da Russia, Cina, Tajikistan e Uzbekistan. Nel Code si propone che i firmatari si impegnino a:

[123]Il testo è reperibile a: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html ultimo accesso 28.02.2014

[124] Il testo è reperibile a : http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf ultimo accesso 28.02.2014

[125] Il testo può essere scaricato da http://www.osce.org/pc/109168 ultimo accesso 28.02.2014

"*not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression*" e "*to promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet*" [126].

Due questioni correlate che sembrano rappresentare un moneta di scambio troppo pesante per gli Stati Uniti, che dovrebbero volontariamente rinunciare alla propria egemonia strutturale nel controllo del cyber-spazio. Inoltre, un altro problema del Code è che ci sono espliciti riferimenti alla possibilità degli Stati di chiudere il cyber-spazio in nome della sovranità nazionale.

Alla luce di questo scenario, in cui sembra ormai propendere per la corsa agli armamenti nel cyber-spazio, se si vogliono ottenere reali successi è necessario approcciare un'ipotetica cooperazione nel cyber-spazio da un punto di partenza differente rispetto al passato, non si può tentare di riprodurre le modalità di riduzioni degli armamenti seguiti per le altre tipologie di armi (i.e. armi atomiche). È questo il concetto centrale di un articolo pubblicato da Ziolkowski K (2012), il quale insiste sul fatto che non sia possibile limitare le armi cibernetiche, perciò ogni tentativo in quella direzione è destinato a fallire, perché nel caso delle *cyber weapons* la parte centrale non è la componente fisica, ma le competenze di base degli esperti. Inoltre non avrebbe senso richiamare l'ipotesi di finanziare unicamente strumenti difensivi perché come si è visto (e come si vedrà più in dettaglio in seguito) lo sviluppo di armamenti difensivi presuppone la conoscenza e la capacità di replicare quelli offensivi. Il modello canonico di proposte di misure di *confidence-building* utili per raggiungere un miglior livello di collaborazione e diminuire le possibilità di conflitto prevede modi per incrementare lo scambio di informazioni e di esperti, la convocazione di esercitazioni congiunte e l'avviso reciproco in caso di test di penetrazione. Inutile dire che sono tutte manovre destinate a fallire perché manca la volontà politica di svelare i livelli di sofisticazione raggiunti dai vari eserciti

[126] Il Codice di Condotta può essere ritrovato alla pagina: http://www.citizenlab.org/cybernorms/letter.pdf

cibernetici. La proposta della Ziolkowski è più consistente e meno pretenziosa. L'autrice consiglia l'intercambio di informazioni relative alle strategie e a i *white papers,* che mettono in luce le intenzioni ma non le potenzialità, gli scambi di esperti a basso livello, così da diminuire il sospetto e aumentare l'informalità e, infine, il punto di contatto fondamentale dovrebbe riguardare non tanto le possibilità offensive quanto il settore della protezione delle infrastrutture critiche (mantenendosi sempre a debita distanza dalle informazioni confidenziali). È questo modello, improntato sulle più classiche tecniche negoziali che, a mio avviso, dovrebbe essere perseguito, se non unicamente, in parallelo alle pompose e internazionali conferenze nelle sedi ONU.

Per concludere, nonostante gli innumerevoli sforzi per limitare il conflitto nel cyber-spazio, per il momento, a livello internazionale, sembra prevalere la più classica delle interpretazioni realiste, ovvero lo scenario descritto dal dilemma della sicurezza e dalla corsa agli armamenti. Molti paesi, tra cui alcuni insospettabili (i.e. Paesi Bassi) stanno ricorrendo a misure offensive per incrementare la propria sicurezza nel cyber-spazio, scatenando così i timori deli attori e una corsa alla parità di risorse tecnologiche a livello globale.

È dunque la competizione, che spesso scade nella dinamica del conflitto (non necessariamente bellico), l'interazione predominante nel cyber-spazio? La descrizione della dimensione bellica che fornirà il prossimo capitolo sarà il punto di partenza per poter rispondere a questa domanda.

2.

Lo scenario conflittuale nel cyber-spazio*: is cyber-warfare real?*[127]

"Ora le circostanze sono diverse, ci occorrono
sistemi adatti alla realtà di oggi, bisognerà
aggiornare la tecnica della guerra moderna che può
coinvolgerci."

Guerra e Pace, film sovietico 1967

Introduzione

Era il 1993 quando, all'indomani della Prima Guerra del Golfo[128], Arquilla J. e Ronfeldt D., due esperti della *RAND Corporation*, pubblicavano un articolo in cui dichiaravano al mondo qualcosa di completamente nuovo: *Cyberwar is coming!*[129] L'impianto teorico del brano si concentrava sulla possibilità di acquisire una spropositata quantità di informazioni non solo sul campo di battaglia, ma anche sul sistema organizzativo dell'avversario, sulle sue infrastrutture e su qualsiasi cosa potesse interessare la controparte. Secondo una metafora divenuta ormai famosa, anche perchè ripresa da Nye J. (2010)[130], "*is rather like a chess game where you see the entire board, but your opponent sees only its own pieces*". Vent'anni dopo, Rid T. (2011)[131] pubblica un articolo che diventa subito un *must* per tutti gli esperti di studi strategici e storia militare: *Cyber War Will not Take Place.* Nella sua analisi Rid sostiene che tutto il clamore che circonda la presunta possibilità di una guerra cibernetica sia ingiustificato, sia da un punto di vista concettuale che da un punto di vista pratico.

[127]Limnéll J. e Rid T. (2014), *Is Cyber Warfare Real? Gauging the threats*, Foreign Affairs, consultabile a http://www.foreignaffairs.com/articles/140762/jarno-limnell-thomas-rid/is-cyberwar-real ultimo accesso 28.02.2014
[128]Quella del 1991 contro l'Iraq di Saddam Hussein è considerata in realtà la seconda, poiché viene generalmente considerata quella quasi decennale tra Iraq ed Iran come Prima Guerra del Golfo
[129]Arquilla J. e Ronfeldt D. (1997) *In Athena's Camp*, RAND Corporation, Washington
[130]Nye J.S. (2010) *Cyber Power*, Belfer Center, Harvard Kennedy School, Cambridge, p. 7
[131]Rid T. (2011) *"*Cyber War Will Not Take Place*"*, *The Journal of Strategic Studies*, Vol.35, No.1, 5-32

Analizzare a fondo la questione, considerando sia i numerosi spunti di riflessione proposti in questi anni che gli autori di riferimento nello studio delle scienze militari è perciò d'obbligo.

2.1 Dibattito sull'esistenza della cyber-warfare. Confronto con la dottrina militare classica.

"Cyber War will take Place!"[132], "The Myth of Cyberwar"[133],"Cyber War is inevitable!"[134]: questi sono solo alcuni dei titoli che sono apparsi recentemente su riviste specializzate in studi strategici. La divisione tra scettici e ferventi sostenitori è in qualche modo la misura della rilevanza che la questione *cyber* sta avendo nel mondo militare e tra i leader politici. Negli ultimi vent'anni, infatti, uomini politici, militari ed esperti di studi strategici (e di informatica) hanno invocato la necessità di aprire gli occhi sulle potenziali minacce provenienti dal cyber-spazio. "T*he next Pearl Harbor could very well be a cyber attack*"[135], avvertiva l'ex Direttore della CIA Leon Panetta. Mentre ancora più drammaticamente Gross M. (2011)[136] sosteneva che "*Stuxnet is the Hiroshima of cyber-war*!".

Per i "cyber-scettici", invece, tutto questo sgolarsi non rappresenta nient'altro che un clamoroso errore di considerazione. Il precetto di base è che effettivamente il mondo potrebbe essere all'alba di una nuova dimensione conflittuale come accadde negli anni Trenta, ma se così fosse, non sarebbe di certo a causa del pericolo di una guerra cibernetica. Quanto contestano Rid e Gartzke, i due principali esponenti di questo scetticismo, non è l'esistenza di minacce che possano essere diffuse tramite la rete globale, ma la natura bellica del cyber-spazio e del confronto "in rete" fra Stati. Come sostiene Gartzke

[132]Stone (2012) op. citata

[133]Gartzke E. (2013) *The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth* in "International Security*,"* Vol. 38, No. 2, pp. 41–73

[134]McGraw G. (2013), *Cyber War is Inevitable (Unless We Build Security In)* in "The Journal of Strategic Studies", Vol. 36, No. 1, pp. 109–119

[135]I prossimi due esempi sono citati nell'articolo di RID sopra citato

[136]Gross M. J., 'A declaration of Cyber-War*", Vanity Fair,* aprile 2011

"*is far from clear that conflict over the internet can actually function as war*"[137]. Ancora più categorico è invece Rid: "*cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future*". Senza sostenere nessuno dei due estremi (ossia il *cyber-skepticism* e il *cyber-hype*) è però necessario studiare le motivazioni che risiedono dietro queste affermazioni per smentirle oppure per mantenere alcune delle intuizioni. Infatti, gran parte della ragione di queste profonde differenze di interpretazione risiede nel fatto che non è ancora perfettamente chiaro a nessuno cosa sia di preciso la cyber-war. Partendo, quindi, dagli autori critici si cercherà di destrutturare i tratti ideologici di entrambe le fazioni per restare con dei concreti punti utili per costruire una teoria.

Thomas Rid nella sua critica parte dalla teoria clausewitziana e dal suo concetto di guerra. Secondo le definizioni del celeberrimo generale tedesco autore di *Vom Kriege*[138] per essere considerato tale, un atto di guerra deve rispettare tre criteri: essere violento, strumentale e avere una motivazione politica di fondo. Per queste ragioni risulta chiaro che un atto di guerra non può essere un fatto isolato. Rid trasporta queste categorie alla cyber-war e le incrocia con il concetto di 'atto di forza', in quanto ritiene necessario precisare che in un contesto cibernetico un atto di forza risulta avere una natura meno chiara rispetto alle sue precedenti forme. In riferimento alle categorie di Clausewitz, Rid sostiene che nessuna delle tre sia applicabile ai cyber-attacchi visti sino ad ora. Per questo sarebbe impossibile e ingiustificato, secondo Rid parlare di scenario di *guerra* nel cyber-spazio.

Innanzitutto, nessun attacco cibernetico, nessun virus, nessun *worm* e nessun *DDoS* ha mai avuto natura violenta, ha mai ucciso nessuno, né seriamente danneggiato nessun edificio. L'autore richiama alla memoria gli episodi sinora conosciuti di attacchi cibernetici, soffermandosi sulle vicende estoni e georgiane, analizzando le

[137]Gartzke E. (2012) op. citata p. 42
[138]Von Clausewitz C. (1832) *Vom Kriege*, trad. Howard M.

conseguenze dei *Denial of Service* che furono usati in entrambi i casi e sostenendo che, al di là dell'effettivo impatto sociale ed economico, non c'è stata nessuna forma di violenza, nemmeno potenziale.

Questi due attacchi fallivano anche nel rappresentare gli altri due criteri sopra enunciati. Per quanto riguarda la natura strumentale, vengono considerati fallimentari in quanto mere espressioni di protesta o episodi di tensione precedenti alla guerra vera e propria, senza nessuna motivazione concreta dietro le azioni degli hacker. Inoltre, le attività perpetrate, per Rid, erano più di tipo criminale che politico, poiché le identità degli agenti erano celate dall'anonimato reso possibile dalla cronica entropia della rete, mentre in un atto politico solitamente gli autori manifestano la loro identità apertamente.

Per queste ragioni, le azioni condotte nel cyber-spazio non dovrebbero essere considerate degli atti di guerra in quanto tali, ma semplici manifestazioni di sovversione, sabotaggio o spionaggio, in cui lo scopo ultimo e le violenze (qualora presenti) sono rivolti alle macchine (nel caso del sabotaggio) e alle menti (nel caso della sovversione) e mai costituiscono veri e propri atti di forza nei confronti di persone fisiche.

Tra i molti contestatori di questo apparato logico, Timothy Junio[139] si distingue in particolare poiché offre una visione razionale e improntata sullo studio delle cause della guerra. Innanzitutto contesta Rid e la criticità che conferisce alla letalità degli attacchi cibernetici, ritenendolo incapace di considerare le reali implicazioni di un attacco che pur non causando vittime iniziali è possibile fautore di una reazione violenta esponenziale. Sostenuto dall'interpretazione giuridica proposta dal *Tallinn Manual*[140] nella quale si evidenzia la possibilità legale di considerare un'interruzione del funzionamento dei sistemi di comunicazione (e simili) come un atto d'aggressione, Junio ha ragione

[139]Junio T. (2012) *How Probable is Cyber War?: Bringing IR Theory Back In to the Cyber Conflict Debate*, The Journal of Strategic Studies 36/1 consultabile http://dx.doi.org/10.1080/01402390.2012.7395614 ultimo accesso 28.02.2014

[140]Schmitt, M.N. ed. (2013) *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge University Press
Cambridge, p 45. Consultabile a :http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

nel sostenere che sia insensata la prima categorizzazione proposta da Rid.

Senza entrare nel pericoloso campo delle variabili interne agli Stati (su cui si sofferma Junio) per spiegare i processi decisionali legati alle cause delle guerre, può essere utile richiamare un concetto largamente condiviso, ossia che oggi, a causa di contingenze storiche e tecnologiche, la possibilità che si verifichi una guerra ad alta intensità è estremamente poco probabile, che sia convenzionale o cibernetica. A partire da questa affermazione si possono estrapolare due conseguenze. La prima è che la mancata attribuzione della colpevolezza potrebbe essere un'ottima via di fuga per governi intenzionati a compiere azioni belliche limitate senza incorrere con certezza in una risposta diretta da parte dell'oppositore. La seconda conseguenza è che il rischio implicito in questo tipo di ragionamento sia sottovalutare i potenziali risvolti che potrebbero scaturire. Infatti, se applicato alla possibilità che la corsa agli armamenti e il livello di conflittualità evolvano a stadi successivi, la prospettiva dell'impunità potrebbe fluire in scenari bellici globali, originatisi da incidenti cibernetici.

Spostandosi, ad un altro critico di Rid, anche Jarno Limnéll[141] contesta in maniera vibrante i tre assunti clausewitziani applicati alla guerra cibernetica, insistendo sul fatto che siano "*a simplified representation of the complex realities of war and security today*" e che la dimensione fisica della violenza non sia necessariamente l'unica da prendere in considerazione, poichè la storia delle teorie militari ha da sempre preso in esame anche le dimensioni morali e psicologiche del conflitto. Perciò, qualora fosse chiaramente dimostrato che la cyber-war non è capace di apportare danni fisici (assunto contestabile), secondo Limnéll, questo non sarebbe sufficiente ad inficiare l'importanza che va attribuita allo scenario bellico cibernetico, inteso come puro, in forma di *cyber-weapons*, o integrato, in termini di componenti IT di sistemi d'arma.

[141] Limnéll J. e Rid T. (2014), *Is Cyber Warfare Real? Gauging the threats*, Foreign Affairs, consultabile a http://www.foreignaffairs.com/articles/140762/jarno-limnell-thomas-rid/is-cyberwar-real ultimo accesso 28.02.2014

Un altro scettico della *cyber-war* è Erik Gartzke, il quale propone una critica più coerente al sensazionalismo di coloro che prevedono per il cyber-spazio un avvenire unico e spaventoso allo stesso tempo. Il suo punto di partenza resta sempre la teoria di Clausewitz. Gartzke nota come, se è vero che le azioni belliche sono influenzate da motivazioni politiche, difficilmente il cyber-spazio è e sarà "*the final arbiter of competition in an anarchical world*"[142], poiché incapace di essere l'ago della bilancia nello scontro bellico. Per questa ragione non si può considerare il cyber in maniera isolata dalle forme tradizionali di violenza politica. Questo perché, secondo l'autore, i mezzi cibernetici sono meno effettivi in termini di capacità coercitive e di persistenza dell'offesa, dato che, come si è detto in precedenza, mantenere attivo un attacco informatico nel lungo periodo è estremamente complesso. L'autore continua la sua analisi, e prende in considerazione le logiche della guerra, le modalità di imposizione della propria volontà (qualora effettivamente esercitabili) e, arriva alla conclusione che gli scenari che si propongono alla cyber-guerra sono incerti e dipendono in gran parte da ciò che strateghi e militari sceglieranno di farne.

Il ragionamento di Gartzke permette di far luce su una questione delicata, spesso invocata dai fomentatori del *cyber hype:* la *cyber warfare* può essere intesa come rivoluzione militare? La proposizione va direttamente ad inserirsi nel filone della teoria che analizza il rapporto tra la tecnologia e arte bellica. Nell'ambito degli esperti di *cyber-warfare* esistono tre scuole di pensiero: rivoluzionari, evoluzionari e reazionari. Ossia, coloro che pensano che, attraverso le innovazioni tattico-operazionali[143] (ma in parte anche strategiche) lo scenario bellico e di confronto cambierà radicalmente con il tempo, e i primi che riusciranno a imporre il proprio modello militare nel cyber-spazio, potranno prevalere anche nel mondo reale. È questa una corrente che si è sviluppata sin dalle azioni militari del principio degli anni Novanta in cui gli Stati Uniti hanno mostrato una netta superiorità nel combattimento, dovuta principalmente all'elevato livello tecnologico delle loro forze

[142] Gartzke op. citata p.45
[143] Vedi prossimo paragrafo

armate. Il cyber, inserito in questa evoluzione, rappresenta un ulteriore fattore di supremazia militare e, grazie alle sue caratteristiche operative, potrebbe essere un elemento di acquisizione di potere differente, che potrebbe rimettere in discussione gli equilibri mondiali[144]. In opposizione a questa categoria, vi sono gli scettici, di cui abbiamo parlato al principio del capitolo, secondo i quali la possibilità di utilizzare componenti o armi cibernetiche non comporterebbe la grande novità che viene tanto acclamata dai *policy maker* e dagli uomini d'arma. Infine c'è la categoria di quelli che, come Gartzke, pensano che le innovazioni apportate dal cyber-spazio in realtà non siano rivoluzionarie né per il loro utilizzo né tantomeno per gli attori che possono usufruirne, in quanto punirebbero ulteriormente coloro che sono già vulnerabili nelle modalità standard di confronto.

È plausibile che le tre prospettive siano tutte e tre esatte, poiché osservano la questione da angolazioni differenti. Un'idea che può aiutare a comprendere in maniere più completa l'apporto della componente cibernetica al mondo bellico può forse essere ritrovata in uno scritto di Douhet, citato da Van Creveld[145], nel quale il Generale spiegava come spesso l'approccio alle nuove tecnologie percorra diverse fasi. Da un iniziale distacco da parte dei corpi militari e degli strateghi nei confronti delle possibilità offerte da un nuovo tipo di tecnologia, si passa attraverso la sensibilizzazione di una più ampia fascia di addetti, militari e uomini politici. Vi è poi un momento, particolare, in cui ogni nuova tecnologia diventa il Santo Graal e il *silver bullet* delle arti belliche. Segue poi un intenso sviluppo, da parte di tutta la comunità internazionale. Una volta che la nuova tecnologia si è diffusa tra diversi membri dello scenario internazionale e sta vivendo un momento di rapida espansione, inizia un processo di analisi dei rischi dovuti alle pericolosità offensive degli altri attori coinvolti nella competizione, alla quale seguono tentativi di regolamentazione internazionale. Questo processo di approccio alle nuove tecnologie si

[144]Dombroski P. e Toss A. L. (2008) *the Revolution in Military Affairs, Transformation and the Defense Industry*, Security challenges, Vol. 4 No 4, pp.13-38. Consultabile a:
http://www.securitychallenges.org.au/ArticlePDFs/vol4no4DombrowskiandRoss.pdf
[145]L'opera citata da Van Creveld durante la nostra intervista è Douhet. G. (1931) *Le Profezie di Cassandra*

conclude non appena la nuova arma entra negli arsenali e viene considerata unicamente come un'altra arma a disposizione.

E' necessario ampliare questa visione, considerando non solo la tecnologia in sé ma anche le modalità di utilizzo e di interazione con il contesto sociale[146]. Secondo Weber, sono appunto queste due le caratteristiche che contraddistinguono la possibilità che si realizzi una "*transformation of warfare*". Trasponendo questo discorso alla materia trattata, il cyber-spazio non ha sicuramente ancora espresso le proprie caratteristiche rivoluzionarie, ma certamente presenta delle peculiarità per quanto riguarda le interazioni con il contesto sociale, in quanto la diffusione delle nuove tecnologie informatiche, pur essendo molto più evoluta nel caso del contesto militare, gode di un canale di promulgazione molto elevato tra le componenti civili. È perciò necessario attendere l'avvallo del tempo per capire se la sua introduzione negli scenari bellici sarà significata una rivoluzione o semplicemente una innovazione.

2.1.1 Sun-Tzu e la cyber-warfare

Dopo aver ampiamente messo alla prova alcune delle caratteristiche proposte da Clausewitz, in molti si sono sentiti in dovere di confrontare le novità del conflitto cibernetico con un altro colosso della strategia militare, Sun Tzu. Uno dei principali studiosi di strategie cibernetiche è Geers, il quale, nel suo celebre "*Sun Tzu and Cyber War"* (2011)[147] parte dal presupposto che la natura intangibile del cyber-spazio possa rendere complesso calcolare i danni provocati dalla battaglia e l'esito dei conflitti. L'autore crede che la difficoltosa interpretazione possa essere agevolata dalla reinterpretazione dell'*Arte della Guerra*, un'immortale opera prodotta ormai venticinque secoli fa dal maestro cinese delle strategie, Sun-Tzu.

Vi sono, infatti, molte caratteristiche nel cyber-spazio le cui implicazioni, secondo l'autore, sarebbero state profondamente

[146]Andreatta F. (2013) *Technology and War. An Historical Perspective*. Presentazione a Isodarco Winter School, Andalo http://www.isodarco.it/courses/andalo13/paper/Iso13-Andreatta.pdf ultimo accesso 28.02.2014
[147]Geers K. (2011) *Sun Tzu and Cyber War*, NATO CCDCOE Publication, Tallinn

apprezzate da Sun Tzu. In primis, il limitato livello della violenza prodotto dalla guerra cibernetica. Infatti lo stratega cinese "*argued that the best leaders can attain victory before combat is even necessary"*[148]*.* In realtà Geers è cosciente del fatto che l'utilizzo di armi cibernetiche non sia una garanzia di limitazione delle perdite umane ed è consapevole del rischio implicito nel danneggiamento delle infrastrutture critiche, ma ciò che ha in mente quando fa questa considerazione è la modalità del "trasporto" dell'attacco e di ricezione da parte degli eserciti. Un attacco cibernetico come si è detto, risulta meno violento (per usare la categorizzazione proposta da Rid e Clausewitz) e per questo preferibile, secondo le strategie di Sun Tzu, come prima scelta per portare alla vittoria. Un chiaro esempio di questa interpretazione tattica è sicuramente il caso di Stuxnet (spiegato in fondo al capitolo), il cui attacco *non violento* ha ottenuto uno scopo del tutto uguale a quanto avrebbe provocato un'incursione aerea, limitando però lo spreco di forze e il rischio per i propri uomini. Visto in questi termini, gli attacchi cibernetici sembrano essere una plausibile soluzione al problema che affligge le forze armate occidentali negli ultimi decenni, quello che Zambernardi[149] chiama il *security trilemma*: ovvero la necessità di colpire il nemico; difendere le proprie forze; e ottenere risultati concreti nei confronti del nemico. Secondo la linea del suo teorizzatore infatti uno dei problemi principali delle azioni di *counter-insurgency*, ma che in generale può essere applicato alle azioni belliche, risiede nel fatto che una delle tre dimensioni deve essere lasciata da parte. Ora, traslando debitamente le categorie, il caso di Stuxnet mostra come si possa (in determinate circostanze) tenere in conto tutte e tre le dimensioni del *trilemma* senza sacrificarne nessuna.

Un'altra delle caratteristiche principali che si possono considerare è la necessità del comando di non sentirsi mai al sicuro, ma essere sempre preparato ad un eventuale attacco. Questo è oltremodo utile nel cyber-spazio, dove la quantità di attacchi (che si tratti di spionaggio, crimine o aggressioni) sono esponenzialmente in crescita e,

[148]Ibid p.6

[149] Zambernardi, L. (2010) *The Counterinsurgency's impossible Trilemma*, Washington Quarterly, 33:3 pp. 21-34

in casi come quello israeliano addirittura nell'ordine delle decine di migliaia al giorno. È questo un aspetto approfondito dal Maggiore Lunas F.R., dell'Esercito statunitense, secondo il quale il pensiero di Sun Tzu è ad oggi estremamente rilevante per l'analisi di alcune dinamiche strategiche che avvengono nel cyber-spazio[150]. Il suo pensiero è tendenzialmente indirizzato agli strateghi del suo paese, ma è ugualmente applicabile all'universo cibernetico in generale. Nonostante gran parte dell'articolo del Maggiore sia un inno alla militarizzazione del ciberspazio, indicazione che come si vedrà in seguito non mi sento di condividere, il concetto di *preparedness* merita di essere analizzato. Sarà infatti ampiamente ripreso quando si parlerà della costruzione di solide basi per la costruzione del sistema difensivo nazionale.

Anche il concetto di *stealthiness*[151] è fondante per i suggerimenti militari di Sun Tzu. Egli sosteneva che il generale esperto in difesa fosse colui che mostrava le sue capacità anche nei luoghi più insospettabili. Certamente questo pensiero può essere trasposto alla realtà virtuale in cui, non solo il difensore, ma anche chi sta portando a segno un attacco può permettersi di nascondere la propria identità dietro una cortina di nebbia di codici. Questa dimensione di segretezza risulterà nell'incapacità (anche se non totale come si vedrà) di attribuire responsabilità per gli attacchi ricevuti. Questa caratteristica, influenzata dalla natura stessa del cyber-spazio, potrebbe essere considerata dai sostenitori della natura rivoluzionaria del cyber-spazio, come un'assoluta verità, capace di trasformare per sempre la dimensione della guerra. Si vedrà in seguito come in realtà questa segretezza non solo non sia assoluta, ma in termini politici, sia meno rilevante di quanto si possa credere. E questo perché, seppure una cyber-war possa in termini pratici esistere, non può essere fine a sé stessa, ma deve essere parte integrante di un più ampio attacco militare, che coinvolga gli altri domini classici dell'azione militare. Inoltre, come si è visto in

[150]Lunas F. W. (2011), *The Modern Application on Sun Tzu'z Art of War*, position paper per il Centre for Cyberspace Research, consultabile al http://www.afit.edu/en/ccr/docs/cyber_innovations/Lunas_The_Modern_Application_of_Sun_Tzu_Art_of_War.pdf ultimo accesso 28.02.2014

[151]Usato in questo contesto con il significato di "invisibilità", "segretezza".

moltissimi casi la segretezza spesso viene meno a causa di "inconvenienti" umani (rivelazioni, errori di scrittura), per cui per quanto rilevante, la *stealthiness* cibernetica sembra essere una caratteristica piuttosto temporale e indicata per i conflitti tra attori non-statali e gli Stati.

Ovviamente, data l'impostazione strategica di Sun Tzu è facile come la sua predilezione sarebbe ricaduta sulle infinite possibilità operative in termini di spionaggio che offre il *cyber-space*. Se infatti si nota come nella sua opera, Sun Tzu dedichi un intero capitolo sull'analisi e i metodi per percepire informazioni di nascosto, è facile notare come per lui, questa modalità di azione sia rappresentativa del più alto livello che l'uomo possa raggiungere nell'atto di vincere una guerra con il minore sforzo possibile.

In conclusione, Sun Tzu, secondo chi ha usato la sua opera per analizzare la natura del cyber-spazio, potrebbe essere un valido aiuto quando si prendono in considerazione conflitti cibernetici. In realtà però, l'analisi di questi autori si focalizza su quei conflitti definibili asimmetrici, i quali sono plausibili nel cyber-spazio, e secondo modalità più tattico-operative che strategiche. Secondo chi scrive, però, queste non possono essere considerate preminenti quando si considera la *cyber-warfare.* Occorre dunque distinguere quali siano le principali caratteristiche del cyber-spazio da considerare qualora si voglia parlare di strategie e ipotesi di conflitto all'interno di questo nuovo dominio.

Per concludere poi, il più ampio discorso iniziato con la categorizzazione clausewitziana proposta da Rid, è necessario affermare che l'analisi strategica sulla questione, tutt'altro che prossima a una risoluzione, deve continuare. È infatti questa l'unica idea in comune a tutte le scuole di pensiero strategico nel cyber-spazio. A prescindere, dunque, dalla sua rilevanza all'interno dello scenario delle interpretazioni strategiche, credo sia indiscussa la necessità di considerare la *cyber-warfare* come uno scenario ipoteticamente bellico, così da valutare eventuali minacce e plausibili scenari di confronto. È questa infatti l'unica possibilità per ridurre la crescente conflittualità (verbale, se non si vuole sostenere la tesi della conflittualità cibernetica)

che si sta sviluppando all'interno dello scacchiere internazionale. Detto questo, perché si possa studiare la cosiddetta *cyber-warfare* e considerarla in termini concreti, non è perciò necessario rapportarla con le teorie proposte da pensatori classici. Infatti costoro, pur delineando scenari bellici considerati dai più affezionati come immortali, sono stati pur sempre ideatori di un sistema strategico vittima dell'influenza del tempo in cui sono stati scritti.

La componente *cyber,* in un certo modo, modifica profondamente la maniera di intendere la *guerra* (e ancor di più la difesa). Le difficoltà di definizione e di precisa circoscrizione di ciò che rientra in termini assoluti nel concetto di *cyber-warfare* non dovrebbero ostacolare il processo di studio del fenomeno, anche e soprattutto per il fatto che numerosi Stati stanno procedendo alla militarizzazione di questo nuovo dominio dando vita a quello che sembra un chiaro scenario di corsa agli armamenti. Per questo motivo è necessario approfondire lo studio sulla questione e riscontrare in primis gli elementi da conservare presenti nei precedenti approcci militari e in seguito le novità delle azioni e delle dinamiche belliche nel cyber-spazio.

Prima di iniziare ad analizzare le caratteristiche della *cyber-warfare* è il caso di fare due brevi precisazioni: è necessario rimarcare brevemente ma in maniera chiara cosa si intenda per *information warfare*, un concetto spesso confuso con quello di *cyber-warfare*; e cosa si intenda per *cyber terrorismo*¸ categoria che racchiude un certo tipo di interazioni, distinte da quelle che contraddistinguono i rapporti nella *cyber-war*. Infatti come argomenta Walt (2013)[152] *"a critical preliminary task is to separate out different dangers grouped under the common rubric of cyber-warfare".*

2.1.2 Distinzione da Information warfare

Prima di procedere è necessario contemplare brevemente quest'importante differenziazione. Per molti paesi infatti, esiste una netta differenza tra *cyber* e *infowarfare*. Ciò che contraddistingue le due

[152]Walt, S. M. (2013), Is the cyber threat overblown?, Foreign Policy. Consultabile http://www.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown 28.02.2014

è che la seconda rimanda alla tecnica di controllo delle informazioni che è antica come la guerra stessa. Come sostiene Luttwak, la battaglia delle informazioni è necessaria per lo svolgersi del conflitto e se si perde "*la situazione osservata a livello operativo rimane troppo confusa per sferrare in tempo attacchi e contrattacchi*"[153]. L'*information warfare* non è nient'altro che la continuazione di questa idea strategica. Rona T. [154] la definisce molto bene considerandola come "*the strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives".*

Secondo questa distinzione l'*infowar* è decisamente più ampia e variegata di quanto possa essere la cyber-war. La sua conduzione, secondo i precetti delle principali forze armate mondiali consiste in cinque pilastri fondamentali: (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations, and (5) Electronic Warfare[155].

Ciò non toglie che, all'interno della *cyber-war* vi sia anche la necessità di mobilitarsi per effettuare una guerra di informazioni col nemico, fondamentali per la riuscita di piani successivi. Anzi, probabilmente la raccolta di intelligence e la sua analisi sono la componente principale per la riuscita delle operazioni cibernetiche, come dimostrano i numerosi esempi riportati alla fine del capitolo.

2.1.3 Distinzione da cyber-terrorism

Inoltre la *cyber-warfare* può essere differenziata dal cyber-terrorismo secondo tre principi fondanti: intento, metodologie e attori coinvolti. Secondo il Maggiore Scott S.D. (2010) dell'Esercito degli Stati Uniti distinguere tra le due forme di conflitto cibernetico è un'operazione importante e relativamente semplice. Il Federal Bureau of Investigation

[153]Luttwak E. N. (2001) *Strategy: the Logic of War and Peace,* the Belknap Harvard University Press, Cambridge P 157
[154]Citato in Cordani G. (2013) *Cyber Weapons: il controllo tra Stati Uniti, Russia e NATO*, tesi magistrale dell'Università di Bologna
[155]Per una spiegazione dettagliata delle caratteristiche rimando a Shreier (2010) *On Cyber Warfare,* DCAF Publication, Geneva, p. 20

(FBI) definisce cyber-terrorismo come "*un atto **criminale** perpetrato con l'uso di computer e capacità di telecomunicazione, con conseguente violenza, distruzione e / o interruzione dei servizi per creare paura provocando confusione e incertezza all'interno di una data popolazione, con l'obiettivo di influenzare un governo o di una popolazione di conformarsi ad una particolare agenda politica, sociale o ideologica*". Questo scenario si distingue notevolmente dalla cyber-war. Quest'ultima è infatti basata sulle azioni di Stati nazionali e sui loro obiettivi. Anche le modalità possono differire perché, in linea teorica (sono pochi gli esempi a disposizione)[156], negli scenari terroristici si cerca di fare pressione affinché certe istanze politiche vengano rivendicate, perciò si tende ad approcciare modalità *diversamente* distruttive rispetto agli scenari bellici in cui uno Stato vuole resistere o sconfiggere l'altro.

2.2 Quali sono le caratteristiche del quinto dominio militare

A differenza degli altri domini bellici l'ambiente cibernetico deve la sua essenza all'ingegno umano e alla comprensione di determinate leggi fisiche. Questa importantissima premessa permette di trarre immediatamente due conseguenze fondamentali riguardanti le sue implicazioni strategiche. La prima è che per quanto si possa considerare virtuale ed etereo il cyber-spazio si basa su fondamenta fisiche e per funzionare non può far altro che obbedire alle leggi elettromagnetiche e degli impulsi luminosi, il che provoca in qualche modo una limitazione[157]. L'altra componente è l'ingegno umano, che potenzialmente non ha limiti, perciò il cyber-spazio ha, in potenza, caratteristiche infinitamente mutabili[158], come hanno dimostrato le evoluzioni tecnologiche degli ultimi anni. Tutto ciò presenta inevitabilmente dei riscontri strategici, e il compito che ci si propone in

[156]Lachow I. (2009) *Cyber Terrorism: Menace or Mith?*, in Kramer, F.D., et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington D.C., p. 251

[157]Rattray G. J. (2009) *An Environmental Approach to Understanding Cyberpower* in Kramer, F.D., et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington D.C.p 256

[158]Siroli G. P. (2012) *Cyberspazio e Cyberwar*, in *"L'ABC del Terrore. Le armi di distruzione di massa del terzo millennio",* a cura di Giacomello G. e Pascolini A., V&P, Bologna

questo capitolo è proprio quello di descrivere le caratteristiche più evidenti ed importanti che lo spazio virtuale sembra avere in relazione allo studio della *cyber-war.*

Il cyber-spazio presenta una **topologia *mutabile***, unicità di questo dominio bellico, e questo riconduce direttamente alle nostre due premesse. La geografia può essere modificata un numero *n* di volte, con un numero *n* di modalità ma sempre e solo qualora si rimanga nei limiti delle leggi fisiche sopra indicate. Questa caratteristica ha notevoli implicazioni strategiche. Innanzitutto, non è inimmaginabile una "battaglia campale" cibernetica. Vanno qui considerate due situazioni distinte: un'operazione integrata e un cyber-attacco *puro.* La prima situazione è sicuramente di maggior interesse perché permette di analizzare tutti i livelli operativi. La battaglia informatica infatti, si svolge su due piani: uno riguarda la guerra fatta *sui* sistemi informatici (attacco/difesa di reti e sistemi operativi) e l'altro l'operatività nel campo di battaglia, ovvero il sostegno di tecnologie informatiche per operazioni militari che trascendono il cyber-spazio. Nel primo caso l'aggressore cercherà di infliggere danni via cyber-spazio, nel secondo caso userà le funzionalità di questo per incrementare le proprie capacità di attacco all'interno degli altri domini bellici. Partendo da questo scenario si possono analizzare molte altre caratteristiche, sia a livello tattico che strategico, fondamentali per la nostra analisi.

A livello tattico, possiamo considerare innanzitutto la **mobilità delle armi** e l'elevata capacità di fuoco offerta dalla natura in costante mutamento del cyber-spazio. In entrambi i casi è necessario specificare cosa si intende. Nel primo caso, non avendo limitazioni geografiche, l'attacco può essere direzionato da qualsiasi posizione utile: non servono basi che necessitano di protezione, sottomarini da nascondere, carri armati che devono avvicinarsi all'obiettivo. L'unica cosa che serve è l'accesso alla rete che si vuole penetrare e essere in grado di inserirvi il *payload* (vedi più avanti). Tutto ciò consente un'infinità di scenari tattici plausibili e una minore vulnerabilità delle armi d'attacco: è per questo che Lanceford B. (2008) sostiene che "*cyberwar is*

decentralized"[159]. Può infatti essere condotta da piccoli gruppi geograficamente dispersi, ma virtualmente connessi grazie a sistemi comunicativi dipendenti da diverse tecnologie. Questo permette di poter muovere attacchi da diverse parti del mondo, potenzialmente senza alcun preavviso[160]. Per quanto riguarda la **capacità di fuoco**, invece, va detto che, ancor prima di considerarla elevata, si dovrebbero analizzare i numerosi effetti di un'arma cibernetica: "*Cyberspace offers the potential for nearly imperceptible system effects all the way through massive electronic means of mass disruption"*[161]*. Q*uesta caratteristica è valevole sia a livello tattico che strategico, anche se nel caso della strategia c'è l'aggravante del *single-use*: dopo essere stata utilizzata, una cyber-arma, risulta disponibile all'entità attaccata che, tramite il *reverse engineering* può riuscire a impossessarsi dei codici che hanno reso l'attacco possibile. Quest'ultimo punto ci permette di analizzarne un altro che ha un'ambivalenza tattico-strategica: la **precisione** dell'attacco. Secondo Shreier "*The precision inherent in cyber attacks goes beyond the ability to address specific targets. The cyber realm is capable of imposing effects upon certain characteristics or parts of targets*"[162]. Un'arma cibernetica ha infatti una infinita varietà di possibili utilizzi e in particolare non ha solo modalità distruttive, caratteristica tipica delle armi in genere, ma è in grado di ricreare le componenti informatizzate dei sistemi d'arma o delle infrastrutture, in modo da alterare l'essenza stessa dei sistemi di difesa avversari.

Prima di passare all'analisi prettamente strategica, è necessario evidenziare l'impatto che ha, a livello di comando e controllo, la riduzione esponenziale dei tempi di reazione, resa possibile dai trasferimenti di dati e comandi alla velocità della luce. La conseguenza diretta è che i tempi di reazione umani non sono neanche prossimi all'essere adatti alla gestione di informazioni e comandi. Questo

[159]Lunceford B. (2009) *Cyberwar: the future of war?*, in *War and the Media: Essays on News Reporting, Propaganda and Popular Culture*, di Paul M. Haridakis, Barbara S. Hugenberg, and Stanley T. Wearden, 238-251. Jefferson, NC: McFarland

[160]"With no boundaries, attacks can come from anywhere. Ubiquitous access makes establishing a defense especially difficult because defenders must successfully parry every blow and must be always right, while the attacker must be right only once, and rarely has to face the consequences of his actions"

[161]Shreier F. (2010) *On Cyber Warfare,* DCAF Publication, Geneva p 94

[162]Ibid p. 102

comporta che il **livello di automazione** necessario sia elevatissimo, e destinato a crescere. Inutile dire, quale elevato valore possa avere, sia in termini militari che di difesa nazionale, quest'ultima caratteristica.

A livello strategico, la principale questione è determinare se il cyber-spazio sia o meno un dominio bellico intrinsecamente **asimmetrico**. Le giustificazioni a questa affermazione riguardano principalmente tre ordini di fattori: la presunta supremazia dell'offesa sulla difesa, la presunta incapacità di deterrenza e la presunta impossibilità di attribuzione della direzione degli attacchi. Ovviamente per studiare queste tre caratteristiche si considererà la *cyber-war* in senso stretto, non la possibile integrazione in conflitti che si svolgono in diversi ambienti bellici.

Iniziamo con il problema dell'**attribuzione.** Come già accennato, nascondere la propria identità o crearne una distinta da quella autentica è un'operazione limitatamente semplice. Questo comporta che le vittime di un attacco possano non essere in grado di identificare la sorgente. Nonostante questa rappresenti una realtà dal punto di vista tecnico, nel caso delle più complesse operazioni sinora condotte nel cyber-spazio si ha quasi sempre un'idea chiara dell'identità dell'aggressore per due ordini di motivi. Innanzitutto per la motivazione politica di cui si è ampiamente parlato in precedenza. Prendiamo l'esempio di Stuxnet: malgrado le dichiarazioni di esponenti israeliani e statunitensi era chiaro a molti che il promotore di quel tipo di attacco era uno Stato capace di mettere insieme molte risorse e competenze e che aveva intenzione di limitare il programma nucleare iraniano con mezzi meno invasivi dell'attacco diretto. L'altro ordine di ragioni è legato al linguaggio di scrittura: come un'artista (o un falsificatore) ogni programmatore (e ogni hacker) ha il suo stile di scrittura e tende a lasciare la propria firma o tracce del proprio background. È questo il caso di numerose operazioni cinesi (vedi la fine del capitolo) in cui, nascosti tra i codici vi erano indicazioni in un inglese fallace che chiaramente proveniva da traduzioni erronee dal cinese[163].

[163]Al riguardo si veda Siboni G., Y.R (2012) "What Lies Behind Chinese Cyber Warfare", *Military and Strategic Affairs*, No. 2, pp. 49-64. Va però ricordato che la situazione è più complessa, perchè si possono chiaramente simulare errori che

La questione dell'attribuzione è direttamente collegata a quella della **deterrenza**. Molti osservatori hanno notato come, data la numerosa varietà di attori potenzialmente pericolosi per lo Stato all'interno del cyber-spazio e l'incapacità di tracciare chi siano i reali colpevoli degli attacchi, sia impossibile per lo stesso seguire strategie volte alla deterrenza. In realtà questa affermazione è vera solo in parte, come può ben dimostrare l'esperienza israeliana. Difficilmente esiste al mondo un'entità statale bersagliata da così tanti e disparati *cyber*-aggressori come Israele, che eppure ha incentrato molti dei propri sforzi nei tentativi di deterrenza nei confronti di gruppi come l'esercito Elettronico Siriano e il Cyber-esercito iraniano[164]. Ciò che è impossibile, secondo le impostazioni strategiche israeliane, è affidare la propria protezione interamente alla capacità difensiva dei *firewalls*. Per questo si è aperta la discussione su come si possa gestire una deterrenza a questi attacchi. Innanzitutto, è necessario considerare gli assalitori costanti e le principali capacità offensive dei principali avversari. Per questo è necessaria una elevata capacità di intelligence e di previsione del rischio[165]. A questo punto interviene la possibilità di estrapolare il contesto dell'attacco cibernetico e considerare una reazione plausibile. Secondo alcuni Stati (i.e. Stati Uniti, Israele) una minaccia cibernetica merita talmente tanto l'attenzione della Difesa nazionale che ad un attacco di questo tipo può essere possibile, se non necessario, rispondere con un'azione *cinetica*, così da trasformare la dimensione del conflitto. Secondo i principi di diritto internazionale però, questo comportamento violerebbe una delle più importanti norme, la *proporzionalità* dell'attacco. Ad ogni modo, pur senza considerare la parte della reazione, con la sola capacità localizzativa si possono limitare i vantaggi di quegli attori statali che agiscono favoriti dalla segretezza delle loro azioni. La questione della deterrenza nel ciberspazio è decisamente più complessa di quanto non fosse con gli armamenti nucleari, ma non per questo va considerata impossibile.

potrebbero incrimanare attori che in realtà non hanno nessuna responsabilità nell'accaduto.

[164]Ma anche i gruppi che mandano attacchi da Gaza e quelli provenienti da Hizbu Allah.

[165] Questo processo verrà notato più in dettaglio nel prossimo capitolo

Infatti, come si può notare nel caso israeliano, nonostante numerosi attacchi siano andati a buon fine, il risultato finale dell'azione di deterrenza è decisamente positivo, come si vedrà nel capitolo ad esso dedicato[166].

La terza giustificazione all'asimmetria è la **predominanza dell'offesa** nel confronto cibernetico. Questo elemento è senz'altro favorito da tutte le vulnerabilità presenti nel cyber-spazio, che si descriveranno a breve, ma ha anche dei contraltari e delle limitazioni. Innanzitutto bisogna discutere delle entità delle operazioni offensive. Come si è detto infatti, lo scenario delle possibilità offensive nel cyber-spazio è estremamente variegato. Da questo si può dedurre che, per gli attacchi di bassa intensità, le potenzialità offensive hanno probabilità decisamente elevate di successo, mentre nel caso di attacchi cibernetici di maggiore rilevanza la possibilità di successo dipende da molti più fattori, tra cui la capacità di rendere i suddetti attacchi operativi. Infatti, un'altra lezione che si può carpire dalla vicenda di Stuxnet è che per la preparazione di un *malware* mirato e molto sofisticato, ad alta capacità distruttiva, sono necessarie risorse, tempo e uomini che difficilmente un gruppo esiguo può mettere a disposizione.

In secondo luogo, le potenzialità offensive sono limitate dall'unicità dell'attacco che le armi cibernetiche mettono a disposizione dell'aggressore. Infatti, una volta che il virus viene lanciato ed entra in azione, presto o tardi verrà trovato, isolato e analizzato dalla parte attaccata[167]. Il virus perderà così la sua forza esplosiva dopo il primo utilizzo. Per fare un esempio pratico è come se per sparare proiettili, bisognasse crearli adeguati a ciascuna pistola. Funziona perfettamente se si vuole sparare una volta isolatamente, ma diventa un problema non appena si presenta la necessità di sparare in maniera costante.

Infine, in termini di comportamento degli Stati, bisogna specificare che la predominanza dell'offesa non significa automaticamente che la scelta di

[166]Ciluffo F.J, Cardash S. L., Salmiraghi G. C. (2012) *A Blueprint for Cyber Deterrence: Building Stability through Strenght*, Military and Strategic Affairs, Vol. 4, No. 3 pp.3-23

[167]Nonostante vi sino evidenze che mostrano che il livello di criptaggio stia raggiungendo livelli talmente elevati da rendere possibile un *malware* non rintracciabile: http://securityaffairs.co/wordpress/17875/hacking/undetectable-hardware-trojan-reality.html ultimo accesso 28.02.2014

una modalità offensiva abbia un rapporto costo/benefici soddisfacente. Infatti l'inasprimento della tensione internazionale e l'allocazione di risorse, potrebbero essere alcuni dei fattori che possono far propendere gli Stati per un assetto predominantemente difensivo.

Un'altra considerazione che va a incidere sulla concezione asimmetrica del cyber-spazio è l'analisi del cyber-terrorismo. Secondo Denning D.E.(2007)[168] e Lachow I. (2009)[169] quella del cyber-terrorismo sarebbe più un mito che una reale minaccia, in quanto non sembra aver causato sinora reali pericoli (equiparate al terrorismo nel mondo fisico). Anche Tordjman del *Institute for Counter-Terrorism* di Herziliya in Israele ha condiviso questa opinione. La questione è quale utilizzo ne fanno le organizzazioni terroristiche del cyber-spazio. Tutti e tre gli esperti concordano sul fatto che i principali utilizzi sono: diffusione della propaganda, raccolta di nuovi membri e di fondi. È questa interpretabile come una dimostrazione indiretta del fatto che le potenzialità offensive o non sono alla portata di tutti o non sono così facili da sfruttare per entità che non hanno a disposizione le giuste risorse.

Per concludere, vorrei chiarire che il mio intento non è quello di cestinare l'intera bibliografia che si è occupata di *cyber-war* negli ultimi vent'anni. Tanto meno quello di sottovalutare le critiche sull'efficacia dello Stato-nazione come entità politica nell'arena internazionale, bensì mi preme chiarire il punto di vista degli Stati nell'arena della *cyber-war*. Se si parlasse di crimini, il mio punto di vista sulla rilevanza degli stati nello scenario cibernetico sarebbe certamente differente, ma trattandosi di un contesto bellico non mi è possibile cedere alla tentazione di presentare uno scenario rivoluzionario in cui la più piccola e sviluppatissima nazione può metterne in ginocchio un'altra più grande e sommamente più potente solo grazie alle armi cibernetiche. Questo non solo non è possibile perché prima della fine del confronto le truppe reali scenderebbero in campo, ma anche perché la natura stessa del cyber-

[168]Denning (2001) *Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign* Policy, in Arquilla J. e Ronfeldt D. (2001) *Networks and netwars: the Future of Terror, Crime and Militancy*, RAND Publications, Santa Monica. Consultabile http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf ultimo accesso 28.02.2014

[169]Lachow I. (2009) *Cyber Terrorism: Menace or Mith?*, in Kramer, F.D., et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington D.C.

spazio è solo parzialmente asimmetrica. È vero che una nazione più tecnologicamente avanzata corre rischi più grandi di una arretrata. E' vero anche che un attacco semplice è relativamente facile da mettere in atto. Così come è anche vero che in questo dominio metà della potenza di fuoco è data dalle menti dei programmatori che disegnano le armi cibernetiche. Ma anche vero che non esiste ad oggi entità politica in grado di generare potenzialità cibernetiche e mettere a disposizione di menti geniali le più evolute risorse, quanto lo Stato e le sue forze armate.

2.2.1 Confronto con gli altri domini bellici

Il tentativo di confrontare le proprietà del cyber-spazio con quelle degli altri domini bellici (terrestre, aerea, navale, aerospaziale) viene compiuto da diversi autori. In questa sede verranno considerate in particolare le proposte di Rattray (2009) e Shreier (2011) dalle quali verranno tratte considerazioni personali.

Inizialmente Rattray[170] evidenzia i tratti delle principali teorie di strategia militari nei diversi domini bellici, così come enunciati dai loro ideatori, mostrando come possano essere riadattate al cyber-spazio. In particolare, per quanto riguarda le strategie militari terrestri, Rattray spera che chi si occupa di elaborare gli equivalenti per il cyber-spazio, sappia riconoscere il fondamentale valore dei punti chiave in maniera altrettanto chiara così come negli altri domini bellici: così come secondo Spykman[171] chi fosse stato in grado di controllare l'Eurasia avrebbe controllato il mondo, bisogna trovare qual è l'Eurasia del cyber-spazio e se è possibile porla sotto controllo di un'unica entità. La teoria della guerra aerea di Douhet[172] viene invece utilizzata per due caratteristiche: la comprensione che la rapida evoluzione tecnologica può facilitare immensamente lo scopo di colpire con meno perdite il centro nevralgico del nemico; e il fatto che la componente morale ha un effetto di venti

[170] Rattray (2009) op. citata
[171] Spykman N. (1944) *Geography of the Peace*, Harcourt and Brace, New York
[172] Douhet G. (1942) *Il dominio dell'aria*, consultabile
http://www.liberliber.it/mediateca/libri/d/douhet/il_dominio_dell_aria/pdf/il_dom_p.pdf ultimo accesso 28.02.2014

volte superiore a quello materiale. Per quanto riguarda l'influenza del *Sea Power* studiata da Mahan[173] può invece essere utile per cogliere i profondi legami che esistono tra prosperità economica nazionale e sicurezza dell'ambiente considerato; inoltre spiega anche l'importanza del controllo dei *chokepoints,* che, nel caso del cyber-spazio, possono essere identificati con i cavi in fibre ottiche o i routers. Infine per quanto riguarda la rilevanza *space power*, potrebbe essere applicata al cyber-spazio in quanto costituisce un mezzo per incrementare altre forme di potere nazionale e in quanto è il dominio bellico in cui la digitalizzazione è più avanzata.

Subito dopo aver portato a termine questi parallelismi, Rattray presenta una categorizzazione che critica chi considera la sola dimensione tecnologica nell'analisi delle strategie nei diversi domini, e propone un'analisi di quattro ambiti: (1) avanzamenti tecnologici; (2) velocità e scopo delle operazioni; (3) controllo delle posizioni chiavi; e (4) mobilitazione nazionale. Nelle prime due dimensioni spiega in maniera approfondita le caratteristiche illustrate nel paragrafo precedente, e si concentra particolarmente sulle dimensioni e capacità degli attacchi, sulla necessità di automatizzazione del processi di comando e controllo (in quanto i tempi di azione e reazione non sono più appartenenti allo spettro di percezione e analisi umana) e sulle implicazioni della difficile capacità di attribuzione. La terza area sottolinea come le possibilità di nuovi scenari comporti anche delle vulnerabilità, soprattutto in termini di controllo delle infrastrutture fondamentali per il sostegno fisico del cyber-spazio (*chokepoints)*. Infine nella quarta categoria l'autore si concentra sul valore del capitale umano nello scontro cibernetico e su quale sia il miglior modello di *governance:* quello accentrato *à la* cinese o il *laissez faire approach* all'americana. Le conclusioni dello studio di Rattray sono mostrati nella tabella sottostante.

[173]Mahan A. T. (1890) *The Influence of sea Power upon History, 1660-1783*, Little Brown, Boston

	Dominio terrestre	D. marittimo	D. aereo	D. spaziale	Dominio cyber
AVANZAMENTO TECNOLOGICO	Treno e comunicazioni richiedono un focus sulla *heartland*	Con tecnologie si rese possibile proiezione del potere a livello mondiale	Possibilità di distruggere direttamente i centri di gravità nemici	Crea un nuovo *high ground*	Nuove vulnerabilità strategiche
VELOCITÀ E SCOPO DELL'OPERAZIONE	Decide le linee preferenziali di comunicazione	Possibili colpi globali contro la costa	Velocità nel mettere fine ai conflitti	Operazioni globali continue	Operazioni globali estremamente veloci; automazione di comando e controllo
CONTROLLO DELLE KEY FEATURES	La velocità di mobilitazione è cruciale per i vantaggi terrestri	Necessità di avere delle basi disposte globalmente; *chokepoints*	Colpeire per primi le basi dell'aviazione nemica è cruciale	Controllo dei punti chiave nell'orbita	Ambiente è creato dall'uomo; cambia continuamente
MOBILITAZIONE NAZIONALE	È cruciale il posizionamento del risorse chiave	Bisogna proteggere il commercio come chiave per il potere nazionale	È necessario avere molti professionisti; link con il mondo dei privati	Necessità di molti professionisti; link con il settore privato	Necessità di molti professionisti; link con il settore privato

Shreier[174] invece tocca livelli di astrazione più elevati. La sua analisi inizia con la tripartizione di *fini, mezzi e modi* per analizzare strategicamente un'azione militare. Secondo l'autore, quanto riguarda la c*yber-wa*r, è però quasi impossibile distinguere i *fini* a cui si tende, questo a causa della difficoltà nell'attribuire un'identità all'aggressore. Data la possibilità di nascondersi dietro l'anonimato non si ha mai la certezza se un atto compiuto possiede finalità politiche o belliche. I *modi* risultano essere ancora più confusi in quanto dipendono dalla percezione che ogni singola entità attribuisce alle potenzialità delle cyber-operazioni nel continuum che va da *force-multiplier* a *war on its own*. Infine per quanto riguarda i *mezzi* vi sono tre complicazioni: (a) è più facile produrre un attacco; (b) si è meno certi del risultato; e (c) la loro portata è infinitamente superiore rispetto a qualsiasi altro mezzo bellico. E' quest'ultima caratteristica, secondo Shreier, a fare delle *cyber-weapons* una sorta di via di mezzo tra le armi di distruzione di massa e quelle spaziali, con portata globale e senza precisa localizzazione geografica. Shreier si sofferma inoltre sul valore puramente strategico delle armi cibernetiche: una volta utilizzate non sono più uniche e possono essere adoperate dalla vittima dell'attacco (grazie al processo di *reverse engineering*) [175].

Inoltre, l'ambiente cibernetico risulta essere immensamente meno stabile rispetto i domini standard a causa della necessità di predilezione per un approccio offensivo. Questa preferenza sarebbe, secondo l'autore, la conseguenza dei vantaggi militari che portano questo genere di armi: meno costose dei sistemi d'arma complessi e macchinosi e la mancanza di uomini a rischio sul teatro d'azione.

In realtà la proposta di Shreier, pur essendo molto valida, pecca nel mostrare una visione parziale della questione. Infatti se quelli evidenziati sono tutti elementi che portano alla propensione per la

[174] Shreier, F. (2010) *On Cyber Warfare,* DCAF Publication, Geneva

[175]Anche se il caso di Stuxnet mostra che sia possibile utilizzare tecniche che ne complichino la fattibilità: sembra che alcune funzionalità e proprietà del malware non siano ancora state decriptate

modalità offensiva, esistono molte caratteristiche che limitano questa dimensione. Inoltre, la portata dei tre elementi (fini, mezzi, modi) è incerta nella misura in cui non viene fatta una distinzione tra attori nazionali e sub-nazionali. Nel momento in cui si considera uno scenario conflittivo inter-statale le categorie (eccetto quella dei mezzi) non risultano più complesse che negli altri scenari bellici. Al contrario trovo invece molto precisa e proficua l'analisi fatta da Rattray. Sicuramente in parte superficiale e con notevoli possibilità di miglioramento, però capace di equiparare molte delle caratteristiche che si considerano uniche del cyber-spazio con le questioni avanzate dalla strategia militare degli altri domini.

Per concludere questa breve analisi comparativa, è necessario richiamare al fatto che pur essendo un dominio distinto dagli altri, il *cyber-space* è proliferato in tutti i restanti domini militari, le cui forze operative si affidano in maniera sempre maggiore alle funzionalità informatiche, come si vedrà nel prossimo paragrafo.

2.3 Vulnerabilità cibernetiche

Dopo aver dibattuto sull'entità del conflitto nel dominio cibernetico, è ora necessario passare in rassegna le vulnerabilità che questa nuova dimensione presenta e quali sono le armi più usate per creare danni, recuperare o modificare informazioni, alterare i servizi o, in generale, per colpire un avversario attraverso il cyber-spazio. Alla fine del paragrafo si darà brevemente spazio alla definizione del concetto di *cyber-operations*, prevalentemente improntato sul modello americano.

2.3.1 I livelli di vulnerabilità

È fondamentale analizzare i livelli di vulnerabilità per tentare di definire precisamente un sistema di resilienza, scopo ultimo di questo

elaborato. Quando si parla di vulnerabilità è necessario tenere a mente un concetto prezioso, richiamato da Siroli G.P. (2012): la vulnerabilità *per sé* non è problematica, ma lo diventa se, affiancata alle categorie di probabilità dell'evento offensivo e costo relativo, ipotizza scenari di rischio. Non è mia intenzione considerare la probabilità degli eventi, ma mi soffermerò sulle caratteristiche che li potrebbero rendere possibili. Per questa ragione, non parlerò di rischio ma di vulnerabilità.

È innanzitutto doveroso fare due considerazioni. La prima è che quando si esaminano le vulnerabilità del cyber-spazio è necessario tornare alla definizione operativa di Clark per considerare tutte le sue componenti e verificare le potenziali debolezze di ognuno dei livelli che lo compongono. Tralasciando la componente umana, a livello di hardware, software e informazioni esistono determinate debolezze o incongruenze che possono essere sfruttate per creare *disruption.* In secondo luogo è necessario dividere le vulnerabilità civili da quelle militari. Non perché sia mia intenzione ipotizzare che, nell'atto di costruzione di un modello di resilienza, le due debbano essere tenute in differente considerazione bensì per mostrarne le differenti implicazioni. Infatti, in un ipotetico scenario di guerra cibernetica, le vulnerabilità di entrambi i gruppi (civili e militare) diventerebbero critiche o vitali per l'interesse nazionale. Si tratterà dunque inizialmente dei due ambiti in maniera distinta per poi vederli ricongiungersi quando si parlerà di difesa dai cyber-attacchi.

Si inizierà con il considerare le **vulnerabilità fisiche**, tangibili del cyber-spazio. Il primo appunto da fare, come ricorda Siroli G.P. (2012)[176], è che la prima problematica relativa al cyber-spazio è che si tratta di macchine e strutture fisiche che sono vittima di consumo e, in caso di eventi naturali distruttivi (terremoti, esplosioni, alluvioni), possono rimanere seriamente danneggiati. Ovviamente questo scenario non è influente nell'analisi della guerra cibernetica, ma lo diventa se si considera il più ampio contesto della dipendenza delle strutture civili e militari dalla tecnologia IT. Quanto maggiori sono le funzionalità gestite dai sistemi informativi tanto maggiori saranno i rischi collegati a un

[176]Siroli G.P. (2012) op. citata

disservizio accidentale. Lasciando da parte le casualità e considerando le vulnerabilità della dimensione fisica del cyber-spazio, sorprenderà scoprire come per numerosi esperti di *cyber-war*, sia proprio questa la principale vulnerabilità. Nir Tordjman mi ha confermato durante un'intervista che "*the bigger issue is still the physical damage: bombing the servers, cutting the wires*"[177]. In un interessantissimo articolo O'Neil W.D. (2009) considera nel dettaglio le possibili minacce per quella che abbiamo definito la dimensione fisica del cyber-spazio: "*cyber contents rest on a structure of physical elements that have physical properties and locations. (…) like other infrastructure networks, has a geography as well as a topology, and both effect its vulnerability and survivability"*[178]*.*

O'Neil vaglia innanzitutto i network cibernetici e nota che la topologia del World Wide Web è formata da un elevatissimo numero di nodi che consistono di computer (o super-computer) che forniscono globalmente la possibilità di collegarsi ad Internet, attraverso dei *link*[179]. A livello nazionale, si possono creare dei disservizi sia tentando di eliminare le vie di connessione con l'esterno, sia annichilendo i fornitori di servizi Internet (Internet Service Providers – ISP) nel territorio nazionale, che operano come centri di snodo (*hubs)* per la fornitura di network. In questo scenario può rientrare sia una tipologia fisica di attacco (bombardamento, black out indotti, ecc), sia una penetrazione informatica. Anche la proliferazione di connessioni di tipo *broadband* e senza fili (*wireless)* contribuiscono a incrementare le vulnerabilità fisiche legate ai network, in quanto il fornitore di rete è facile da disabilitare.

Le griglie elettriche che forniscono l'elettricità ai centri di snodo sono loro stesse probabili vittime di attacchi informatici[180], soprattutto attraverso la manipolazione dei sistemi SCADA (Supervisor Control And Data Acquisition o, in italiano, Sistemi di Controllo per Infrastrutture

[177]Intervista di gennaio 2014 con Nir Tordjman International Centre for Counter-Terrorism (ICT), Herzliya, Israele

[178]O'Neil, W. D. (2009) *CyberSpace and Infrastructure,* in KRAMER, F.D. et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington DC

[179]Nel mondo esistono 12 "server di ultima istanza" e sono dislocati 10 nel territorio degli Stati Uniti, uno in Europa e uno in Giappone (i siti sono segreti)

[180]Huma Khan in un articolo del 31.05.2011 per *ABC News* parla degli attacchi alle infrastrutture elettriche statunitensi. Consultabile: http://abcnews.go.com/blogs/politics/2011/05/cyber-attack-on-us-electric-grid-gravest-short-term-threat-to-national-security-lawmakers-say/ ultimo accesso: 28.02.2014

Industriali) grazie ai quali la maggior parte di esse funzionano. In particolare i sistemi di controllo di questo tipo "non furono originariamente progettati e costruiti per essere accessibili da reti esterne e quindi a volte contengono meccanismi di sicurezza informatica molto primitivi e che si stanno evolvendo lentamente nel tempo. Per ragioni gestionali negli ultimi anni queste infrastrutture SCADA sono state talvolta connesse ad Internet o a reti di comunicazione esterne, diventando quindi vulnerabili a intrusioni o attacchi informatici. L'aggiornamento stesso dei dispositivo e dei meccanismi di *cyber-security* risulta a volte problematico a causa della difficoltà ad interrompere il funzionamento di alcuni apparati anche per brevi periodi, oppure per la relativa obsolescenza di alcune componenti interne che possono non disporre delle necessarie risorse"[181]. Il problema dei sistemi SCADA, a sua volta, ci conduce a uno dei punti più importanti dell'analisi delle vulnerabilità delle infrastrutture collegate a Internet o che utilizzano sistemi informativi per alcune delle loro funzioni, che verrà trattato in seguito.

Infine una questione che coincide con le preoccupazioni di molti governi e istituzioni (come si vedrà nel caso particolare di Israele) riguarda la vulnerabilità dei cavi sottomarini in fibra ottica che collegano interi continenti alla rete. In un eccellente lavoro prodotto dal Belfer Center della Harvard Kennedy School, Sechrist M. (2012)[182] analizza approfonditamente la questione, prestando particolare attenzione alla congiunzione di vulnerabilità tra le componenti tecnologiche "vecchie" e quelle moderne, risultato dell'evoluzione IT. Secondo questa analisi, il crescente numero di operatori che utilizzano sistemi di gestione dei network in modalità di controllo remoto hanno introdotto rischi addizionali di attacchi su larga scala di attacchi cibernetici ai cavi sottomarini, i quali sono anche direttamente esposti alle possibilità di attacco diretto (fisico) così come sembra essere successo recentemente in Egitto, dove il presunto taglio di un cavo sottomarino ha

[181]Siroli G. P. (2013) op. citata

[182]Sechrist M. () *New Threats Old Technology: Vulnerabilities in Undersea Communication Cable Menagement Systems,* Belfer Center Harvard Kennedy School, Cambridge

causato seri problemi alla connessione di una buona porzione dell'Africa e della regione meridionale dell'Asia[183].

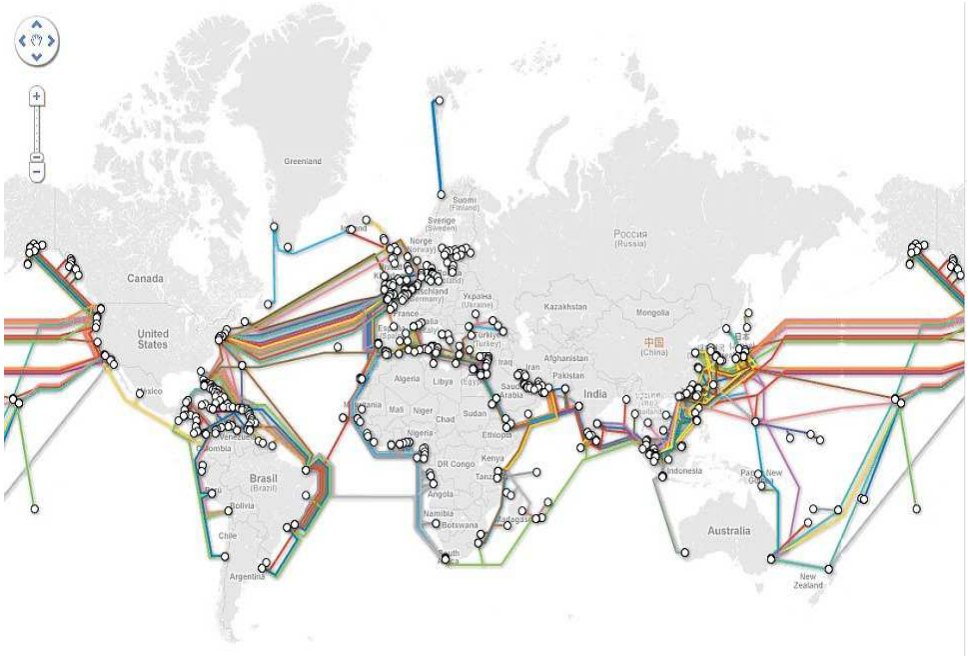


Figura 1: mappa del network dei cavi sottomarini in fibra ottica

Passando alle **componenti del software** e delle informazioni è necessario considerare una caratteristica essenziale: ogni progetto software, sistemi operativi applicativi, può presentare vulnerabilità intrinseche, configurazioni deboli e errori di programmazione, implementazioni imperfette e informazioni errate o imprecise. Perciò componente può essere deturpata o manipolata. In particolare gli hacker che tentano di rintracciare i punti deboli di questi software vanno a cercare le cosiddette *zero-day vulnerabilities*, ovvero delle falle nel programma che non sono ancora state "scoperte" e corrette dal produttore del software. Sono due le questioni rilevanti relazionate a queste vulnerabilità: da una parte, esiste un ampissimo mercato nero dove si possono acquistare informazioni riguardo alle *zero-day*

[183]Per ulteriori informazioni http://gigaom.com/2013/03/27/undersea-cable-cut-near-egypt-slows-down-internet-in-africa-middle-east-south-asia/ e http://www.wired.com/gadgetlab/2013/04/how-vulnerable-are-undersea-internet-cables/

scoperte[184]; dall'altra, è spesso impossibile modificare il problema perché interrompere il programma significherebbe sospendere delle funzionalità critiche[185]. Ovviamente le *zero-day* non sono le uniche debolezze dei software, esiste tutta una schiera di software aggiuntivi (*malware*) che, se inseriti (virtualmente o fisicamente) in un computer possono provocare la modificazione delle funzionalità del computer, ma di questo si parlerà a breve quando si analizzeranno gli attacchi nello specifico.

Prima di passare alla sicurezza dei dati, è importante ricordare che esiste una debolezza intrinseca ai sistemi informatici il cui posizionamento è intermedio ai due livelli sopra descritti, ovvero la possibilità che hardware e software siano alterati ancor prima del loro inserimento in un'unità operativa[186]. È questa una questione che, soprattutto negli Stati Uniti, desta moltissima preoccupazione. Considerando la catena produttiva dei computer nel mondo, si scopre che una buona parte dei microchip e dei semiconduttori alla base del funzionamento di qualsiasi hardware, vengono prodotti in Cina[187] e acquistati in Europa Occidentale e Nord America. Questo induce a temere che nell' hardware venduto come prodotto finale vi fossero delle *backdoor* dalle quali il governo cinese potesse facilmente ottenere tutte le informazioni processate dall'unità di cui lo stesso faceva parte. Le stesse accuse sono state mosse da Snowden verso gli Stati Uniti, i quali, secondo le rivelazioni, avrebbero apposto delle potenzialità nascoste all'interno dei sistemi progettati ed esportati. Senza rischiare di scivolare nel pericoloso terreno del complottismo, la possibilità che all'interno di microprocessori, di dischi di immagazzinamento e punti di accesso *wi-fi* vengano, inserite degli accessori utili al produttore dell'hardware è un rischio concreto in termini di possibilità tecnologiche. Rischio che aumenta se si considera che la probabilità di scoprire una

[184]Da alcune rivelazioni emerse il profilo dei compratori negli ultimi anni sembra essere mutato molto: in precedenza chi comprava le informazioni relative erano le compagnie stesse che cercavano di porre una soluzione al problema; oggi i principali acquirenti sembrano essere esponenti di gruppi (i.e. organizzazioni, stati) interessati a sfruttare

[185]Siroli op citata

[186]Per maggiori informazioni: http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/ ultimo accesso 28.02.2014

[187]Le statistiche dicono che la produzione cinese di semiconduttori ha superato quella americana negli ultimi due anni, rimanendo sempre molto arretrata rispetto a quella di Taiwan e Giappone

back-door è molto bassa, essendo estremamente difficili da individuare, e inoltre il processo di ispezione delle componenti di ogni singola unità risulterebbe monumentale e caotico.

La globalità dello scenario sopra descritto viene ampliato in un report dell'Ufficio del Primo Ministro francese intitolato *Menaces sur systèmes informatiques*[188], con la categorizzazione di quattro tipologie di vulnerabilità:

- Le vulnerabilità di concezione, le quali concernono tutti i tipi di entità e consistono nel fatto che un programma o una componente sia sta progettata in maniera fallace (i.e. un portatile è più volatile di un corpo fisso);
- Le vulnerabilità di realizzazione, che possono essere relative ai materiali, alle risorse e alla logica del software (i.e. *zero-day)*;
- Le vulnerabilità di messa in opera, che possono riguardare l'unità o l'ambiente in cui viene inserito (i.e. negligenza nella configurazione);
- Le vulnerabilità di utilizzo, che riguardano puramente il comportamento dell'utilizzatore finale (i.e. uso di reti non sicure).

Vi è infine la questione della certezza nella **protezione delle informazioni**. Quando si pensa alla protezione dei dati, il quadro sembra veramente essere quello di una scena da film, in cui il protagonista è un ladro professionista che deve entrare in un edificio molto ben sorvegliato, evitare le guardie che lo proteggono, identificare dove si trova il caveau e una volta lì trovare il modo di entrare. Nei film, se il ladro è il protagonista, riesce sempre a ottenere il tesoro che sta ricercando. Nella realtà digitale le probabilità di successo sono decisamente più elevate. Innanzitutto perché le vie per raggiunger "il caveau" sono molte di più e meno sorvegliate rispetto al caso di una banca e soprattutto perché il disincentivo dell'essere scoperto è esponenzialmente inferiore. Come si è visto nell'analisi delle caratteristiche della *cyber-war*, è infatti molto semplice celare o

[188]Secrétariat General de la défense nationale (2006), *Menaces sur les systèmes informatiques.*

falsificare la propria identità. Per questa ragione le informazioni vanno protette con modalità non unicamente passive (i.e. la password) e devono essere implementate modalità elastiche e in costante modifica.

2.3.2 Vulnerabilità nei domini militari e civili

E' doveroso analizzare il mondo civile e quello militare separatamente, almeno al principio, per capire precisamente quali sono le vulnerabilità peculiari di entrambi, e come si possono declinare le debolezze strutturali dei due domini. Per quanto riguarda il mondo militare "*Tactically and operationally, the increasing dependence of modern technologically advanced forces (especially U.S. forces) on networks and information systems create new kinds of exploitable vulnerabilities*"[189]. Queste vulnerabilità si riscontrano nei network utilizzati per la comunicazione e la conservazione di dati, nell'integrazione di tecnologie ICT (hardware e software) nei sistemi d'arma, e nei sensori, capace di creare porzioni di *cyber-space* sullo scenario di conflitto. Il problema fondamentale per quanto riguarda i network e le operazioni militari è appunto dovuto alla dipendenza dalle componenti informatizzate. Nel momento in cui si basa una rilevante parte della propria capacità operativa su un sistema che non è di per sé integralmente protetto e difendibile, il rischio di essere resi non-operativi e di non essere in grado di gestire le attività aumenta in maniera esponenziale. È questo quello che succede ai moderni eserciti, che stanno diventando ogni giorno più informatizzati e che per questo si espongono alla possibilità di essere vittima del mancato funzionamento (accidentale o programmato) dei propri sistemi di comando e comunicazione[190].

[189]Miller R.A. e Kuehn D.T. citati in Swan D. (2012) *Cyber security Vulnerabilities Facing IT Managers Today*, Tesi Magistrale. Consultabile: https://www.academia.edu/1416741/Cybersecurity_Vulnerabilities_Facing_IT_Managers_Today ultimo accesso 28.02.2014

[190] C4ISTAR systems – the Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, And Reconnaissance Systems Of The Armed Forces – sono particolarmente vulnerabili al cyber soprattutto perchè altamente interconnessi. Inoltre, i processori, le memorie e le altre parti dell'hardware sono u*biquitous*. La guerra cibernetica può avere effetti sui radar, sui missili, sulle comunicazioni, sui software. Può anche disabilitare i bersagli mobili come i missile. Infine anche il Sistema di localizzazione GPS può diventare un bersaglio.

Se si considerano i pericoli civili, invece, le vulnerabilità principali sono legate alla protezione delle infrastrutture critiche (o sensibili), anche detti servizi vitali. La definizione dipende molto dall'ampiezza di significato che gli attribuisce l'ente o l'istituzione che le considera. Ad esempio nel caso italiano, il recente Piano Nazionale per la Protezione della Sicurezza cibernetica[191] le definisce *infrastrutture critiche*, riprendendo la definizione classica di ispirazione anglofona dalla quale si derivano le pratiche del *Critical Infrustructure Protection* (CIP) *e Critical Information Infrastructure Protection* (CIIP) di cui si parlerà nel prossimo capitolo. Se si considerano i documenti ufficiali estoni, l'*Emergency Act*[192] definisce con chiarezza chi è responsabile del funzionamento dei *servizi* vitali. Pur essendo diversa la terminologia, ci si riferisce tendenzialmente alle stesse entità: infrastrutture che si occupano della fornitura di servizi essenziali per la vita pubblica di un paese. Fornitura di acqua, gas, elettricità, internet, telefonia, sistemi di trasporto, aeroporti, viabilità ferroviaria. La lista è molto lunga per ciascun paese (e.g. in Estonia sono 43 categorie distinte) ma, come detto, ognuna di queste unità ha in comune la criticità per la società a cui offre il proprio servizio. Come rientrano queste infrastrutture nelle vulnerabilità cibernetiche di un paese e soprattutto quali sono i caratteri fondamentali che le rendono così potenzialmente pericolose per gli stati, è l'obiettivo dei prossimi paragrafi.

L'intromissione delle tecnologie informatiche ha ormai permeato tutti i livelli della società, anche quelli produttivi e di diffusione di servizi e le potenzialità di un attacco cibernetico verso uno di questi settori potrebbe causare danni e perdite ingenti. L'immagine di una diga che si apre improvvisamente perché azionata da un operatore con accesso remoto alla struttura; di un aereo che segue una falsa rotta comunicata da un elemento esterno che si è inserito nel sistema di controllo del velivolo; o la compagnia che si occupa di distribuzione elettrica di un

[191]Consultabile al sito: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf ultimo accesso 28.02.2014

[192]In estone Hädaolukorra Seadus, pubblicato il 15 giugno 2009 consultabile http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=en&sk=et&dok=XXXXX26.htm&query=H%E4daolukorra+seadus&tyyp=X&ptyyp=RT&fr=no&pg=1 ultimo accesso 28.02.2014

paese costretta a interrompere il proprio flusso perché un virus ha bloccato la comunicazione o alterato le funzionalità del sistema di controllo sono solo alcune delle paure che "tengono svegli la notte"[193] i governanti delle nazioni più evolute dal punto informatico e non solo.

Secondo Tabanski L (2011)[194]

"*the development of cyberspace (…) create further vulnerability (for critical infrastructures). These are computerized relationships (for example, command and control by remote electronic means) and logical relationships (such as the international financial market as a factor influencing inputs and outputs of critical infrastructures), which are innovations that would not exist without information technologies. It is therefore worth distinguishing between infrastructures in the traditional sense and the modern use of this concept, which includes a cyber-dimension*".

In entrambi i casi, ormai, il livello di informatizzazione delle infrastrutture che producono servizi è in costante crescita. Rain Ottis, un esperto di sicurezza informatica all'Università Tecnologica di Tallinn, afferma che le infrastrutture estoni sono per il 90% dipendenti dalle tecnologie ICT: per il 40% in maniera critica e per il 10% senza possibilità di funzionamento alternativo[195].

La questione della criticità delle infrastrutture non è una novità dell'era cibernetica. Come spiega O'Neill "*infrastructure attack is as old as war*"[196], la componente informatica ha solo ampliato il contesto, perchè con le implicazioni attuali le possibilità di offesa non provengono più solo da un attacco (o un tentativo di sabotaggio) fisico necessariamente locale, compiuto da eserciti o gruppi operativi ma ad esso si aggiungono i possibili scenari causati dagli attacchi cibernetici remoti. Di conseguenza la questione si sposta sulla comprensione di quanto siano raggiungibili tramite la rete i sistemi di accesso che permettono di manipolare o attaccare le infrastrutture. Ovviamente, i

[193]Benjamin Netanyahu alla conferenza Cyber Tech 2014 a Tel-Aviv,
consultabile http://www.youtube.com/watch?v=FcJawnKzi3s ultimo accesso 28.02.2014
[194]Tabansky L. (2011) "Critical Infrastructure Protection against Cyber threats", *Military and Strategic Affairs,* Vol 3, No.2, pp.61-78
[195]Dichiarazione riferita a un'intervista concessami da Rain Ottis nel dicembre 2013
[196]Op. citata p 113

livelli di connettività sono immensamente distinti e quindi lo sono anche i gradi di vulnerabilità delle infrastrutture, ma la possibilità di penetrare in sistemi sconnessi non è del tutto remota, come dimostra il caso di Stuxnet. I sistemi cosiddetti *air-gapped* possono essere scardinati attraverso l'applicazione di hardware esterni (i.e. schede di memoria portatili) infetti che possono facilmente provocare danni al sistema. Infatti, solitamente, questi sistemi di controllo possiedono, volutamente, un livello inferiore di protezione poiché non connessi ad una rete.

È bene ricordare che i progettatori dei sistemi SCADA cercarono di non lasciare troppi livelli di autorità ad un singolo sistema di controllo, non soltanto per i rischi cibernetici, ma perché le possibilità di guasto accidentale o dovuto a fenomeno naturale sono alte. Nonostante questo, le vulnerabilità sopra descritte dei sistemi, fanno sì che una volta penetrati, gli aggressori possano causare danni ingenti anche se raramente di lungo periodo.

Un'aggravante del problema risiede nel fatto che spesso molte di queste infrastrutture sono gestite da privati, singoli o compagnie, che hanno la responsabilità delle proprie politiche di sicurezza aziendale, anche cibernetica. Consapevoli della pericolosità legate alla gestione di queste infrastrutture, la maggior parte dei paesi ha prodotto leggi, spesso confidenziali, che regolano l'interazione tra il settore privato e lo Stato in ambito di sicurezza nazionale. Per questa ragione i *provider* dei servizi erogati da queste infrastrutture dovrebbero mantenere dei livelli minimi di sicurezza, tra cui quello di restare isolati dalla rete pubblica. Come mostrano numerosi esempi, tra cui i rapporti CLUSIT[197] e CLUSIF[198] pubblicati da due Club privati (il primo italiano, il secondo francese) i livelli di sicurezza delle imprese considerate sensibili raramente sono commisurati agli standard minimi richiesti. Questo per due ragioni. Innanzitutto sviluppare un adeguato sistema di protezione può risultare molto costoso e, in secondo luogo, spesso si sottovaluta

[197]Associazione Italiana per la sicurezza Informatica (CLUSIT) pubblica annualmente un rapporto sulla situazione nazionale in termini di sicurezza informatica, richiedibile: http://clusit.it/rapportoclusit/

[198]Club de la Securité de l'Information Français produce un rapporto simile a quello del CLUSIT, ultimo consultato risale al 2007: https://www.clusif.asso.fr/index.asp ultimo accesso 28.02.2014

l'importanza di un'adeguata difesa, poiché la minaccia risulta poco tangibile.

2.4 Cyber-weapons , operations and attacks

Addentrarsi nel campo delle armi e degli attacchi cibernetici è molto più complesso di quanto si possa credere. In molti si sono cimentati nel cercare di categorizzare quest'ambito vastissimo che comprende strumenti così diversi, ma la sua consapevolezza è ancora legalmente limitata, tanto che le Nazioni Unite non hanno ancora adottato una definizione precisa. In questa sezione si procederà in primis con la definizione legale di attacco cibernetico, successivamente verranno presentate le principali proposte sulla categorizzazione delle armi cibernetiche e infine si cercherà di mostrare come viene condotta una *cyber-operation.*

2.4.1 Attacco cibernetico

Nell'atto di analizzare le possibili contingenze del diritto internazionale applicato al cyber-spazio, Schmitt M. N. (2012)[199] considera il contesto della legge dei conflitti armati per identificare una chiara applicazione della definizione di attacchi cibernetici. La motivazione di fondo è tutt'altro che accademica. L'autore, all'interno del gruppo di analisi sponsorizzato dal Centro di Eccellenza di Tallinn, cerca da anni di individuare le fondamenta legali che regolano i comportamenti aggressivi nel cyber-spazio, dichiarando illegali alcune operazioni oggi di uso comune. La conclusione a cui giunge Schmitt è che per essere considerato legittimo un attacco cibernetico deve rispondere alle categorie di necessità, proporzionalità e responsabilità,

[199]Schmitt M.N. (2012) "*Attack" as a Term of Art in International Law: The Cyber Operations Context ,* in C. Czosseck and K. Podins, Conference onCyber Conflict Proceedings, NATO *Cooperative Cyber Defence Centre of Excellence*, Tallinn

tipiche di qualsiasi attacco che comprenda l'uso della forza[200]. Un altro compito che si prepone questo lavoro è quello di dissolvere le nebbie tra le diverse interpretazioni presenti negli ambienti politici, tecnici e legali. Al principio del testo si legge: *"The U.S. Department of Defense's Dictionary of Military Terms defines "computer network attack" (CNA) as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." NATO adopts this definition in its Glossary of Terms, but adds the parenthetical that "[a] computer network attack is a type of cyber attack." Curiously, it does not define "cyber attack" and the reference contains the sole mention of "cyber" in the document. The term "computer network attack" is adequately descriptive for non-legal use. For instance, it usefully distinguishes such operations from computer network defence, computer network"*. Per questo Schmitt ipotizza un criterio (che la Ziolkowski definirà *Schmitt-criteria*) secondo il quale uno Stato può valutare l'entità di un'azione sul continuum tra coercizione e atto di forza. Lo schema di analisi contiene sette categorie:

- severità, impatto fisico dell'azione;
- immediatezza, dell'azione e delle conseguenze;
- *straightforwardness*, che misura la distanza temporale tra l'azione e la sua conseguenza;
- invasività, misura la prossimità dell'azione alla violazione della sovranità;
- capacità di misurazione (dell'evento);
- presunta legittimità (dell'atto);
- responsabilità.

[200]Per un approfondito studio sul concetto di 'uso della forza' vedi *Tallinn Manual* Capitolo II, p. 45-ss

Un'altra esperta di diritto internazionale che ha affrontato la questione è Ziolkowski K. (2012[201]), la quale condivide con Schmitt la critica per la facilità mediatica e politica di definire attacco anche ciò che legalmente non lo è, comportamento che se abusato, potrebbe minare l'equilibrio internazionale basato su pace e sicurezza. L'intenzione della Ziolkowski è quella di creare una categorizzazione coerente attraverso la modifica dei criteri proposti da Schmitt, pertanto applica delle migliorie ad ognuno di essi in modo da abbassare la soglia necessaria affinché un atto venga considerato una minaccia dell'uso della forza e/o un attacco. In particolare, l'autrice ritiene la prospettiva di Schmitt troppo materialista soprattutto nei confronti delle vulnerabilità presenti nel mondo civile (i.e. le infrastrutture critiche) e delle sue implicazioni indirette, tra cui quelle economiche.

Se analizzati alla luce delle dichiarazioni politiche di diversi leader mondiali[202] (che considerano un attacco cibernetico come sufficiente per scatenare una reazione cinetica) sembra auspicabile che la soglia consentita per dare il via ad un'azione militare in risposta ad atti cibernetici sia più elevata possibile, in modo da lasciare spazio di manovra alla diplomazia.

La complessità della questione e il fatto che non vi sia nessuna consuetudine internazionale accettata sia per quanto riguarda il temine "attacco" che per quello di "uso della forza", né per quanto riguarda il cyber-spazio, ma neanche come concetto generale. Nonostante questa diatriba legale, le armi cibernetiche esistono e sono state usate in diverse operazioni e attacchi che vale la pena di analizzare.

2.4.2 Cyber-weapons

Tralasciando le modalità e le ragioni del loro utilizzo, sono numerosi gli strumenti che possono essere impiegati per provocare danni. Si tratta di un numero talmente elevato che le definizioni a cui

[201] Ziolkowski K. (2012) *Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force*, in C. Czosseck and K. Podins, Conference onCyber Conflict Proceedings, NATO *Cooperative Cyber Defence Centre of Excellence*, Tallinn

[202] Il Presidente USA Obama si è espresso in questo senso sin dai primi mesi del suo mandato

fare riferimento per essere il più comprensive possibili devono restare estremamente generiche.

Se infatti è vero come ricorda Mele S. (2013)[203] che una definizione internazionale che spieghi quando un malware sia considerabile come una *cyber-weapon* è ancora mancante, è anche vero quello che ricordano Rid T. Mc Burney M. (2011)[204] ossia che neanche una semplice definizione di *weapon per sé* è facilmente rintracciabile[205]. Nonostante le difficoltà, però, in molti hanno cercato di spiegare cosa fosse una cyber-arma. Cohen D. e Rotbart A. (2013) tralasciando le difficoltà della definizione militare di arma, utilizzano una semplice *dictionary definition* da cui derivano che una cyber-weapon è *"(a mean) that strikes with the purpose of vanquishing another by attacking systems connected to cyber space"*.[206] La definizione risulta eccessivamente stringata, poiché non considera modalità e ragioni. Questa prima problematica viene risolta da Mele, il quale ritiene siano necessarie tre caratteristiche fondamentali per identificare una *cyber-weapon*: contesto, motivazione e lo strumento. Il contesto è quello della *cyber-war* in cui lo scopo è quello di "*achieving, keeping or defending a condition of strategic, operative and/or tactical advantage*". La motivazione deve essere essenzialmente quella di creare un danno (diretto o anche indiretto) all'avversario; mentre, lo strumento deve essere quello dei sistemi tecnologici d'informazione.

Rid e McBurney propongono una perfetta sintesi della questione quando definiscono le *cyber-weapons "*as *computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings".* Inoltre, aggiungono una caratterizzazione specifica per discernere tra le varie possibili *cyber-weapon*. Ipotizzano infatti uno *spectrum* al cui estremo con basso potenziale troviamo i *malware* capaci di causare danni dall'esterno ma incapaci di propagarsi autonomamente, mentre

[203] Mele S. (2013) *Cyber-Weapons: Legal and Strategic Aspects. Version 2.0,* Istituto Italiano di Studi Strategici Nicolò Machiavelli, Roma. Consultabile: http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf ultimo acceso 28.02.201

[204] Rid T., McBurney M (2011) *"*Cyber-Weapons", *The RUSI Journal*, 157:1, 6-13

[205] Ad esempio, nel dizionario del DoD statunitense non compare nessuna voce su *weapon.*

[206] Cohen D. Rotbart A. (2013) "The Proliferation of Weapons in Cyberspace", *Military and Strategic Affairs*, No. 1, pp. 59-80

all'estremo con alto potenziale si trovano i *malware* ad alta indipendenza e incidenza[207].

Infine, occorre discutere sulla categorizzazione proposta da Denning D (2000)[208], la quale divide le armi cibernetiche a seconda della loro capacità operativa, ossia le riparte in armi con scopo unicamente offensivo (i.e. malware), unicamente difensivo (i.e. antivirus) e di tipo *dual-use*. La Denning dichiara che l'intenzione (volontà di attacco preventivo, reazione, deterrenza) non conta nella categorizzazione delle armi cibernetiche, in quanto in esse stesse risiede la possibile azione che possono compiere. La conseguenza implicita di questo ragionamento è che si può giungere a un sistema di controllo degli armamenti, se si limitano la produzione dei sistemi puramente offensivi.

Notando ancora una volta quanto sia complesso trovare una definizione precisa per le armi cibernetiche è però necessario riflettere un secondo sulle tendenze e modalità di attacco ad oggi più adoperate. Non fornirò qui un elenco delle armi esistenti e del loro utilizzo che può essere ritrovato in annesso al termine dell'elaborato. La fonte principale d'informazione in questo caso sono i report periodici pubblicati dai produttori di sistemi di protezione (antivirus, firewall, ecc.), tra cui Symantec, Mc Afee, Kaspersky. Koch R. et al (2012) che propongono un'analisi interessante di queste tendenze e distinguono sette categorie di attacchi (e due di dual-use, come li definirebbe la Denning), nelle quali si possono ritrovare tutti le tipologie di *weapon* utilizzate contro tutti i *layer* descritti nella definizione proposta di spazio cibernetico:

- Attacchi all' *application layer*[209], ossia la struttura su cui si basa il modello TCP/IP. Meno frequente ma più pericoloso perché non protetto. Si possono utilizzare cdodici di traffico SSL criptati, *DDos*, ecc.;

[207]Come lo definiscono gli stessi autori una sorta di missile-intelligente che viene istruito prima di essere lanciato e poi non serve più interferire con la sua missione dall'esterno.
[208]Denning D., "*Reflections on Cyberweapons Controls",* Computer Security Journal, Vol.XVI, No.4, Fall 2000, pp.43-53
[209]Nel modello TCP/IP è il layer destinato ai protocolli di comunicazione. Cfr. http://technet.microsoft.com/en-us/library/cc958821.aspx

- Attacchi ai protocolli di comunicazione. È probabilmente il livello più attaccato per le numerose vulnerabilità. Si possono utilizzare *botnet, cookie poisoning, SQL injection;*
- *Zero-day exploits;*
- *Social engineering*, colpisce il livello più debole della catena: l'utente umnao. L'attacco consiste non nel tentare di penetrare nel sistema, ma nel convincere qualcuno a depositarne all'interno un codice infetto, senza che se ne accorga. Il caso classico è quello del *phishing*, ma esistono anche *scarreware, rogueware* e molti altri;
- Attacchi mirati, oggi sono molto più frequenti che i virus a larga diffusione. Di solito l'obiettivo è una persona e la modalità è simile al *phishing.* Un utilizzo crescente dei social network ha portato ad un incremento dell'uso del *cross-correlation;*
- *Dissemination routes* di malware, non solo attraverso Internet ma anche tramite inserimento di chiavette USB[210]. Il malware inserito nel computer è solitamente di tipo *Trojan* e va notato che il livello di automatizzazione di questa tipologia di armi è in continuo aumento (come dimostra il caso di Stuxnet);
- *Data leakage* e *insider attack,* il primo è probabilmente il più sopravvalutato dei problemi (soprattutto dopo lo scandalo legato alla NSA statunitense) mentre il secondo il più sottovalutato nonostante sia difficilmente prevenibile e facile da scoprire. A queste due modalità di attacco vanno anche aggiunte quelle dirette al *cloud computing.*

Per ognuna di queste categorie proposte esiste una vasta serie di tipologie di possibili attacchi che corrispondono ad altrettanti generi di armi. I più famosi sono certamente *virus*[211] e *worms*[212], ma moltissimi altre sono le possibilità a disposizione degli aggressori, a seconda di

[210]Ad esempio numerosi i casi di chiavette USB regalate a convegni in cui si sono scoperti malware.
[211]Questa la definizione di Shreier nell'opera sotto-citata: "*Viruses are harmful software programs secretly introduced into an IT system with the characteristic feature of being able to generate and distribute multiple copies of it, thereby spreading throughout the system*"
[212]Sempre secondo Shreier: "*Worms are programs in their own right, which hide within a computer and stealthily propagate themselves onto other machines. Viruses do not spread on the network, worms do, and a virus can be their payload*".

quali siano gli obiettivi perseguiti. Una caratteristica, però, accomuna ognuna di queste differenti categorie ed è la composizione tripartita delle armi stesse, come descritta sapientemente da Shreier F.(2012). Egli nota che similmente a un missile un'arma cibernetica "*is comprised of three basic elements: (1) a delivery vehicle, the rocket engine, (2) a navigations system which tells it how to get to the target, and (3) the payload – the components that cause harm*"[213]. Non importa quante modalità di recapito esistano (email, link infetti, intrusione in connessioni wireless, vulnerabilità di hardware e software) il concetto basilare è quello di depositare il *payload* sul bersaglio.

Quali sono dunque gli obiettivi di queste *cyber-weapons*? Secondo Cohen D. e Rotbart A. (2013) vi sono quattro modalità di impiego di queste tecniche offensive: attacco alle attrezzature fisiche, attacco nello spazio cibernetico, uso per spionaggio e guerra psicologica. Al di là delle definizioni vaghe del secondo e del terzo obiettivo plausibile per le armi cibernetiche, non si può che condividere la categorizzazione proposta perché ripropone la quadripartizione della definizione operativa di Clark, utilizzata come base teorica per tutto il corso dell'elaborato.

Per concludere, riprendendo il testo sopra citato di Rid e Mc Burney e considerando un'affermazione più recente dello stesso Rid (2013) è necessario osservare che, le *cyber-weapons* ad alto impatto distruttivo sono oggi molto poco comuni, sia perché sono molto complesse da progettare sia perché comportano delle conseguenze politiche più significative (in termini di reazione e di reverse engineering) Quindi, nonostante Stuxnet sia stato definito da tutti *un game-changer*, sinora è praticamente unico nel suo genere e la maggior parte delle c*yber-operations* che sono considerate offensive in realtà sono indirizzate a raccogliere informazioni, più che sabotare infrastrutture critiche[214]. Per ricollegarsi alla categorizzazione degli obiettivi di Cohen e Rotbart, sarebbe quindi predominante la concentrazione sulle possibilità offerte dalla manipolazione dei dati, tralasciando le più

[213]Shreier (2012) op. citata p. 66
[214]Ibid.

complesse operazioni indirizzate agli tre livelli. Questa tendenza è chiaramente dimostrata dalla serie di esempi analizzati in fondo al capitolo.

2.4.3 Operazioni cibernetiche

Le operazioni cibernetiche, così come le armi che utilizzano, possono essere di due tipi: offensive e difensive. Ciò che interessa analizzare ora è l'utilizzo bellico offensivo deli cyber-attacchi, intesi come *"cyberspace operations intended to project power by the application of force in or through cyberspace*"[215]. È importante notare come, le tecniche cibernetiche offensive descritte in precedenza, in ambito militare vengono prevalentemente usate secondo due indirizzi tattici: o in maniera isolata; o, prevalentemente, come integrazione a obiettivi "di terra". In entrambi i casi le operazioni cibernetiche sono condotte attraverso e nel cyber spazio (riferendosi a tutti i *layers)* per indebolire i governi, le forze di sicurezza e le popolazioni che si basano sulle infrastrutture a tecnologia informatizzata per sostenere determinate attività vitali per lo svolgimento della vita pubblica o per il mantenimento delle forze di sicurezza. Nel caso di operazioni integrate, gli attacchi cibernetici sono coordinate con le azioni delle forze armate tradizionali impegnate nelle operazioni belliche. Per esempio, le capacità cibernetiche possono essere indirizzate ai sistemi d'arma del nemico o ai sensori di sistemi d'arma, così come nel caso dell'attacco israeliano a Dair el-Zor, sotto descritto. Le forze cibernetiche in uno scenario di questo tipo sono di notevole importanza perché "*could create degrading effects on the platform while an information-related capability influences, disrupts, corrupts, or usurps the decisionmaking of the operator*"[216].

Da notare ancora una volta la rilevanza della dimensione psicologica, che non solo inficia le critiche di Rid che si son discusse precedentemente, ma che riporta a un'analisi di Harbulot C. (2013) il

[215]HeadQuarters department of Army (2014) *FM 3-38 Cyber Electromagnetic Activities,* consultabile http://www.fas.org/irp/doddir/army/fm3-38.pdf ultimo accesso 28.02.2014
[216]Ibid p. 31

quale nota come la moderna attività cibernetica, sia nientemeno che la risultante della strategia di *information war*, iniziata nella Seconda Guerra Mondiale e continuata nel periodo della Guerra Fredda, che in parte si basa su un duro scontro per sfruttare le informazioni con scopi di condizionamento psicologico.[217] È questo un approccio molto caro alla Federazione Russa.

2.5 Esempi storici di cyber-attacchi

Presenterò qui brevemente alcuni dei più salenti episodi identificabili con gli scenari delle guerre cibernetiche.[218] Alcuni sono notori e conosciuti anche da un più vasto pubblico, altri meno conosciuti, ma di notevole interesse. Alcuni casi sotto-descritti sono chiari esempi di spionaggio, ma le implicazioni belliche delle informazioni rubate sono riconducibili alle vulnerabilità sopra descritte.

Nei primi anni di attività di internet il numero di incidenti di cui si ha notizia è decisamente limitato. Le ragioni sono molteplici: la scarsa dipendenza delle infrastrutture dalle tecnologie informatiche, la scarsa quantità di informazioni trasmesse attraverso alla rete e la poca pubblicità degli eventi distruttivi perché l'opinione pubblica non era ancora interessata alla questione (e perché i sigilli militari erano ancora molto stretti). Però, due eventi degni di nota avvennero nel contesto degli ultimi anni della guerra fredda. Entrambi sono arrivati al grande pubblico avvolti da un velo di finzione, ma probabilmente dietro la versione ad effetti speciali vi sono due storie interessanti per lo sviluppo delle dinamiche cibernetiche. La prima è una storia di spionaggio raccontata nel libro *The Cuckoo's Egg*[219], nel quale si racconta la storia di una spia che penetra nel sistema più criptato dell'intelligence, ma

[217] Harbulot C. (2013) *La Piége technologique de la cyber*-guerre, Geopolitique, Vol.8 N.120 p. 64

[218] Per approfondire Haley J. (2013) *A fierce Domain: Conflict in Cyberspace 1986-2012,* recensito a: http://www.atlanticcouncil.org/publications/books/a-fierce-domain-conflict-in-cyberspace-1986-to-2012 ultimo accesso 28.02.2014

[219] Stoll C. (1989) *The Cuckoo's Egg*, Doubleday, New York. Consultabile http://paolodelbene.pbworks.com/w/file/fetch/70361504/cuckoo_s_egg.pdf ultimo accesso 28.02.2014

viene scoperto prima di portare a termine la sua missione. La seconda storia invece, è riportata anche da Rid e riguarda la manomissione delle griglie per il controllo di un gasdotto in Siberia. In molti mettono in dubbio che il vero motivo dell'esplosione che si sviluppò in quell'occasione fosse la manomissione da parte del governo statunitense nel sistema di gestione del gasdotto, ma se così è stato è sinora l'unico esempio concreto di attacco cibernetico distruttivo che ha causato morti.

Per ottenere esempi noti e degni di rilevanza è necessario avvicinarsi allo scadere del millennio.

1999.

Moonlight maze, nonostante sia ancora largamente sotto segreto militare, questa operazione era indirizzata prevalentemente allo spionaggio: vennero colpite prevalentemente i link del Dipartimento della Difesa, del Pentagono e della NASA.
Nello stesso anno in Kosovo si consumava una battaglia cibernetica parallela agli scontri sul territorio. Sia hacker, che entità governative disseminarono internet di propaganda e false informazioni. Allo stesso modo vennero intasati e deturpati i siti governativi dell'ex-Iugoslavia. Le interferenze delle comunicazioni portarono disagi alle zone di conflitto.

2006.

Il 2006 è forse il momento in cui si comincia ad avvertire che lo scenario della *cyber-war* sta in qualche modo cambiando. Innanzitutto il 2006 fu l'anno in cui cominciò (secondo le ricostruzioni della Mc Afee) il **Night Dragon and Shady RAT attack** che durò ininterrottamente sino al 2011. Questo programma di monitoraggio servì per penetrare i server di 21 organizzazioni governative, 13 tra compagnie elettriche e di sicurezza e 6 compagnie finanziarie, sparse in tutto il mondo. Di particolare rilievo l'attacco alla compagnia di olio e gas norvegese e il furto di circa 20 terabyte d'informazioni da NIPRNET, il network militare non classificato.

Nello stesso anno la **NASA,** avvertita del rischio di possibili attacchi informatici dovette bloccare tutte le email con allegati nei periodi precedenti ai lanci per paura che venissero sfruttati per eventuali attacchi. Informazioni circolarono dall'intelligence che intrusi si fossero appropriati dei dettagli dei lanci.

Dall'altra parte del globo nel frattempo la Repubblica Popolare cinese si trova nella circostanza di dover denunciare un'illecita sorveglianza cibernetica della **CASIC** (China Aerospace Science & Industry Cororation) la quale trovò degli spyware nel prooprio network interno e in particolare in dipartimenti posti sotto segreto militare.

2007

Il 2007 è sicuramente l'anno che rappresenta il primo giro di boa nella percezione della cyber-warfare a livello internazionale. Sono principalmente due gli eventi che accadono durante quest'anno, il primo si guadagnerà (inappropriatamente) il soprannome di Prima Cyber-War della storia, il secondo, molto più efficace da un punto di cista militare, permetterà all'aviazione del paese che l'ha impiegato un rapido successo. Si parla ovviamente del *DDoS* di cui è stata vittima l'Estonia in Primavera e ***l'Operazione Orchard*** portata a termine dalle Forze Armate israeliane alla fine dell'estate ai danni di una base siriana, adibita alla ricerca per lo sviluppo di un programma nucleare offensivo. In questo caso la componente cibernetica è stata complementare all'attacco fisico, come tiene a sottolineare Rid T. (2013)[220]. Presumibilmente, l'Unità 8200 o i C4I[221], hanno costruito un virus capace di infiltrarsi nei sistemi di controllo del sistema anti-aereo siriano (uno dei più avanzati al mondo all'epoca), oscurandolo ma senza che le forze di sicurezza siriane se ne accorgessero. Grazie a ciò l'aviazione israeliana ha potuto agire indisturbata, distruggendo la base di Dair el-Zor.

[220]Op. citata
[221]Vedi cap. 5.

2008.

In rapida successione la Federazione Russia si è trovata invischiata in un'altra situazione imbarazzante, alla quale ha saputo tenere fronte militarmente, utilizzando anche mezzi cibernetici. È il caso della guerra con ***la Georgia***. Come in Estonia, anche qui non vi sono prove evidenti di chi fosse all'origine dell'attacco, ma le contingenze politiche lasciano davvero poco spazio ai dubbi. In questo caso l'attacco si sviluppò in due momenti distinti, il 19 luglio e l'8 agosto. Nel primo caso, quasi fosse un avvertimento l'obiettivo del massiccio attacco fu il sito governativo del presidente Saakashvili, che fu colpito da un varietà di *data floods* su più protocolli[222]. L'attacco successivo seguì la stessa linea d'azione ma fu molto più violento e verso un numero più ampio di obiettivi (media, Banca Centrale, tutti i siti governativi). In particolare un problema grave fu che il Presidente faceva molto affidamento sul suo sito per distribuire notizie, rischiando così un blocco informativo. Ci fu anche un tentativo contemporaneo di diffondere *malware* per approfondire il livello dell'attacco[223]. A livello di violenza o effettività fu quasi insignificante, ma a livello di risonanza internazionale fu dirompente perché le azioni nel cyber- coincisero con quelle nella campagna militare.

Anche in **Lituania** vi fu un intervento russo[224], quando, in risposta a una legge "anti-russa"[225] passata dal parlamento lituano, per il tempo di un fine settimana vi fu una battaglia fatta di *phishing, spam e* interruzione di siti governativi. L'attacco fu attivato da computer *zombie* dislocati in Europa occidentale e Svezia, ma le force del CERT lituano determinarono che la sorgente dell'attacco risultava essere un sito russo *hack-wars.ru.*

Cambiando nettamente zona del mondo e contesto geopolitico, nello stesso anno il governo indiano denunciò la penetrazione, da parte (presunta) dell'esercito cinese, in sistemi di controllo relativi a siti

[222]Vedi Kaska K., Tikk E. e Vihul Liss(2010) *International Cyber Incidents: Legal considerations*, NATO CCDCOE Publication, Tallinn. Consultabile http://www.ccdcoe.org/publications/books/legalconsiderations.pdf p 69
[223]Rid T. (2013) op. citata
[224] Kaska K., Tikk E. e Vihul Liss(2010) op. citata, p 58
[225]Bandiva il simbolo sovietico

industriali governativi. Le stime ufficiali dicono che tra le centinaia di acquisizioni di dati e strutture, l'interesse cinese fosse indirizzato a carpire la mappa delle reti ufficiali indiane *"in order to plan how to disable or disrupt networks during a conflict".*

2009.

Nel 2009 si scoprirono due importanti operazioni portate a termine presumibilmente dall'Esercito cinese: ***Operation Nitro***[226] e ***Aurora***[227]. Entrambe dirette verso numerose compagnie e organizzazioni avevano lo scopo principale di disturbare le comunicazioni e appropriarsi di informazioni. Le due operazioni durano diversi mesi e interessarono pure gruppi internazionali tra cui Symantec, Google e Verizon.

Nel gennaio dello stesso anno Israele venne attaccato per tutto il tempo dell'offensiva nella Striscia di Gaza. L'attacco si concentrò sulle infrastrutture di rete legate al governo e venne portato a termine da alcune migliaia di computer. Israele accusò un gruppo di hacker russi assoldati da Hamas (o Hizbu 'Allah).

Nel 2009 si verificano altri due importantissimi avvenimenti: **GhostNet**, un'operazione condotta dalla Cina ancora sotto il velo del segreto di Stato statunitense e un esteso attacco simultaneo contro siti governativi e banche dati di Stati Uniti e Corea del Sud.

Un altro evento significativo riguarda la vicenda degli ***F-35*** statunitensi[228]. Ciò che il Pentagono ha cercato di negare finché è stato possibile, è stata l'intromissione di hacker stranieri nei programmi di scrittura dei codici di decine di sistemi d'arma di ultima generazione, tra cui appunto gli F-35. La questione, oltre che comportare un problema di immagine per la Casa Bianca ed economico per la necessità di rivedere i codici (operazione a detta di esperti impossibile per la quantità di linee di codice), ha anche costretto gli Stati Uniti a rivedere i piani per

[226]Per approfondimenti http://www.huffingtonpost.com/2011/10/31/nitro-attacks-china-hacker-chemical-firms-symantec_n_1067978.html

[227]Anche il gruppo Mc Afee ha pubblicato uno studio approfondito sulla questione, consultabile: http://www.mcafee.com/it/threat-center/operation-aurora.aspx ultimo accesso 28.02.2014

[228]Una lista completa di bersagli può essere ritrovata http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?hpid=z1 ultimo accesso 28.02.2014

l'esportazione di alcuni sistemi d'arma. Questa vicenda ha incrementato notevolmente le accuse e le critiche da parte USA per lo spionaggio agguerrito che fanno i cinesi a tuti i livelli dell'industria.

2010.

Il 2010 è sicuramente il secondo principale giro di boa per quanto riguarda la cyber-warfare. Infatti, fu l'anno in cui l'opinione pubblica (gli esperti, soprattutto militari, ne parlano invece da almeno dieci anni) si rese conto delle reali potenzialità del cyber-spazio e di quanto questo sia infinitamente più "esteso" dello stessa rete di internet. Il 2010 è l'anno di ***Stuxnet*** e della prima vera, universalmente riconosciuta *cyber-weapon*[229]*.* Come descrive ampiamente Gian Piero Siroli (2012)[230] in un recente articolo Stuxnet non è solo estremamente complicato ma dimostra di avere delle modalità di funzione uniche, tanto che "*è stata isolata ed analizzata in modo molto dettagliato da esperti informatici di organizzazioni non governative*". In dettaglio, il *worm*, autonomo e autoreplicante, è stato progettato per colpire e penetrare un particolare sistema di controllo industriale SCADA, che regolava la funzionalità delle centrifughe di arricchimento dell'impianto nucleare di Natanz. La complessità di cui si è appena parlato si riferisce non solo al fatto che il worm fosse così specifico, ma anche che per funzionare sfruttava quattro livelli successivi di *zero-day vulnerabilities*, una prima mondiale nel campo del malware. Per il livello di complessità e per la natura olistica della scrittura sembra che il worm sia stato accompagnato da un processo di *social engineering* e di *intelligence.* Stuxnet, nelle parole di Lewis (2011)[231] è il risultato di anni di ricerca su come sfruttare per usi militari i network digitali.

Un altro esempio, lievemente futuribile e cinematografico, che mostra la direzione che sta prendendo la competizione cibernetica e come questa si colleghi al mondo fisico tangibile, è rappresentato dalle dichiarazioni rilasciate dall'MI5 (i servizi segreti inglesi) riguardo ad alcune attività

[229]Per un approfondimento: http://blog.foreignpolicy.com/posts/2010/09/27/6_mysteries_about_stuxnet ultimo accesso 28.02.2014
[230]Op. citata p. 11
[231]Lewis J. A. (2012) *In Defense of Stuxnet*, Military and Strategic Affairs, Vol.4 No. 3 pp.65-76

sviluppate da settori dell'*intelligence* cinese. Secondo la denuncia, elementi in incognito dell'Esercito cinese e del Ministero della Sicurezza Pubblica avrebbero cercando di sfruttare i loro contatti con uomini d'affari inglesi offrendogli in dono dei dispositivi elettronici (i.e. macchine fotografiche e chiavi di memoria) che contenevano dei malware specifici che consentivano l'accesso remoto al computer così infettato.

2011

Il 2011 fu l'anno dei grandi attacchi andati a segno contro le principali compagnie multinazionali impegnate nel settore cibernetico[232]: Google, Lockheed Martin e Sony i nomi più prestigiosi.

Il 2011 però fu anche l'anno del cosiddetto **RSA attack**[233]**.** Un sistema molto complesso di bot-net concertato per colpire centinaia di diverse compagnie[234], cruciali per la sicurezza nazionale di diversi paesi. L'attacco era attivo dal 2010 ma venne scoperto soltanto con un intervento che ha reso possibile l'analisi dei processi che si verificano all'interno del server centrale del botnet. L'attacco era diviso in tre fasi precise. Nella prima si raccoglievano informazioni, nel seconda fase si produce un'analisi dei punti deboli e nella fase finale si lanciavano *phishing* email che sfruttavano vulnerabilità *zero-day* ed era specifica per le persone che le ricevevano. In questo modo veniva installata una *back door* nel computer in modo da poter controllare completamente il nodo da remoto. L'analisi dei codici usati e il fatto che sia stato necessario un grande impegno logistico e umano per sviluppare l'operazione ha fatto propendere per l'idea che all'origine dell'azione ci fossero gruppi controllati dall'Esercito della Liberazione del Popolo cinese.

Lo stesso anno accadde un altro evento che ha notevoli implicazioni soprattutto per quanto riguarda la concezione di operatività e integrazione delle tecnologie informative nelle dottrine militari odierne.

[232]Per una time-line degli attacchi del 2011 si veda: http://hackmageddon.com/2011/06/22/2011-cyberattacks-timeline/ ultimo accesso 28.02.2014
[233]Siboni G., Y.R (2012) op. citata p. 56
[234]Per una lista degli obiettivi del RSA: http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/ ultimo accesso 28.02.2014

Gli Stati Uniti perdono le tracce di un drone che sta sorvolando ***l'Iran***[235]***.*** La prima impressione è che l'UAV (Unmanned Aerial Vehicle) sia stato abbattuto, ma successive dichiarazioni e dimostrazioni di Teheran mostrano come il drone sia stato fatto atterrare dopo aver disabilitato il suo sistema di controllo con un attacco cibernetico.

2012

Un potente cyber-attacco in Iran[236] costringe il Ministro del Petrolio a bloccare le operazioni online per alcuni giorni. Il virus, trovato all'interno del maggiore sito di esportazione di petrolio (***Kharg Island***), ha poi costretto a bloccare del tutto le operazioi per alcuni giorni. L'attacco è andato a segno sui sistemi interni di gestione, dimostrando così una grande capacità di penetrazione. Le conseguenze economiche furono nulle perché la produzione è ancora legata a processi meccanici ma le funzionalità del sito internet sono state seriamente inficiate.

Il Kaspersky Lab scopre un *espionage toolkit* che rinomina "***Flame***"[237]. Il suo ritrovamento avviene nei sistemi del Ministro del Petrolio iraniano, ma anche in molti altri paesi mediorientali. Secondo il Kaspersky lab è il più grande e sofisticato sistema sinora scoperto per rubare informazioniIn grado anche di "muoversi" all'interno del sistema in cerca di informazioni specifiche. Si ritiene che costituisse il meccanismo di intelligence che ha permesso di ottenere scere le informazioni necessarie per la costruzione di Stuxnet.

Un Trojan chiamato ***Mahdi***[238] viene scoperto mentre si aggira tra i nodi di oltre 800 sistemi di controllo di infrastrutture critiche, siti governativi e di fondamentali istituzioni economiche e universitarie. Il codice contiene tracce di lingua farsi.

[235]Al riguardo si veda: http://www.globalresearch.ca/israeli-intelligence-report-us-drone-downed-by-iran-cyber-attack/28114 ultimo accesso 28.02.2014

[236]Come spiega Thomas Erdbring delNew York Times: http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html ultimo accesso 28.02.2014

[237]L'analisi dei Kasperky Lab è consultabile al: http://www.kaspersky.com/flame ultimo accesso 28.02.2014

[238]Per approfondire sulla origine del nome Mahdi si veda http://www.seculert.com/blog/2012/07/mahdi-cyberwar-savior.html

Il 2012 è anche l'anno del celebre attacco all'***ARAMCO***, una delle principali fornitrice di petrolio dell'Arabia saudita[239]. Un gruppo chiamato "*Cutting Sword of Justice*" direttamente collegato alle forze iraniane usa un virus chiamato '*shamoon'* per infettare i sistemi di controllo della compagnia. Il virus non riesce a sviluppare completamente le proprie capacità (che rimangono segrete) ma riesce nell'intento di cancellare decine di migliaia di file. Il virus era solo in parte modellato per i sistemi della ARAMCO perché altre imprese produttrici di petrolio vennero infettate, tra cui la RasGas qatariana.

2013

Dalle dichiarazioni di esperti e militari, *l'anno horribilis* per le minacce cibernetiche, il 2013 è sembrato essere l'anno della riproposizione della Guerra fredda. Infatti i principali eventi riguardano quelli che in passato erano gli attori principali della scena internazionale e che oggi si ripropongono come tali.

Innanzitutto all'inizio dell'anno un'operazione cinese riesce ad ottenere l'accesso ***all'Inventario Nazionale delle Dighe*** del Corpo degli Ingegneri militari USA[240].

Quasi come se fosse una risposta alla precedente scoperta, poche settimane dopo l'intrusione nell'archivio statunitense delle dighe, in Cina un gigantesco attacco **DDoS** causa per molte ore la paralisi di interfaccia di pagine web e interi domini .cn legati a istituzioni politiche, nazionali e locali.

A giugno vengono pubblicati dei documenti secondo I quali gli Stati Uniti avrebbero portato a termine 213 intrusioni nei confronti di Iran, Russia, Corea del Sud e ovviamente Cina, per scoprire informazioni rilevanti legate ai siti nucleari.

Durante I mesi burrascosi tra le due Coree, ***la Corea del Nord*** [241]approfitta della sua quasi totale invulnerabilità dal punto di vista

[239]La stampa internazionale si è occupata ampiamente della questione: http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all ultimo accesso 28.02.2014

[240]Si veda: http://freebeacon.com/the-cyber-dam-breaks/ ultimo accesso 28.02.2014

cibernetico per portare a termine una serie di attacchi a obiettivi sud coreani[242], tra cui il Ministero della Difesa, molte industrie collegate al settore della difesa e dei media. Anche il Sito presidenziale ha subito offuscamenti ed è stato corrotto.

[241]Data la scarsissima, se non assente, implementazione di tecnologie IT nella gestione dei servizi nordcoreano un attacco cibernetico a strutture civili risulterebbe molto poco efficace

[242]Al riguardo http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?_r=0

3.

LA NATIONAL CYBER-SECURITY E L'ECOSISTEMA DIFENSIVO

"The Art of War teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

Sun Tzu

Introduzione

Alcuni analisti sono persuasi che le minacce provenienti dal cyber-spazio siano sovrastimate, in realtà però I pianificatori della sicurezza nazionale non possono permettersi di sottostimare la potenziale pericolosità di queste minacce[243]. Secondo Geers, il dibattito che ha dato inizio al capitolo precedente può essere considerato totalmente ininfluente per chi si occupa di gestire la sicurezza nazionale. Secondo uno studio condotto in associazione dalla Mc Afee, nota compagnia produttrice di software per la sicurezza informatica, e la Security & Defense Agenda, una *think-tank* di Bruxelles che riunisce importanti personalità dei settori della Difesa appartenenti a NATO e Unione Europea, si può notare che la percezione dei *policy makers* coinvolti è decisamente incline a concepire la *cyber-security* come una problematica estremamente rilevante. Alla domanda se ritenessero la difesa cibernetica più, meno o di ugual importanza rispetto al sistema di difesa missilistico, il 38% degli intervistati ha risposto dando alle due modalità di difesa la stessa importanza, e ben il 36% ha considerato la difesa cibernetica *più* importante di quella missilistica[244].

Questo probabilmente perché, pur non essendo tecnici, i responsabili governativi della sicurezza nazionale sono perfettamente coscienti delle possibili minacce che imperversano all'interno del cyber-

[243]Geers, K. *(*2011) *Strategic Cyber Security,* CCD COE Publications, Tallinn p 5

[244]Security And Defense Agenda E Mc Afee (2012) *Cyber-security: The vexed question of global rules* consultabile a http://www.mcafee.com/au/resources/reports/rp-sda-cyber-security.pdf ultimo accesso 28.02.2014 p 47

spazio. Occorre specificare che molte delle vulnerabilità di questa dimensione sono possibili per via di una questione "evolutiva", per una sorta di default di progettazione. Come si è detto, infatti, il cyber-spazio è una derivazione di ARPANET e sin da allora i progettatori si sono concentrati su robustezza e possibilità di sopravvivere piuttosto che sulla sicurezza del sistema[245], anche perché le minacce erano poco plausibili sino a (relativamente) poco tempo fa. Inoltre, incrementare la protezione è contrario anche a molti principi "di mercato" e viene spesso sacrificata per la funzionalità. Infine la ricerca di una sempre maggiore complessità rende possibile una crescente esposizione a falle di concetto e di costruzione (oltre a provocare una maggiore possibilità di *zero-days)* che si annidano tra le migliaia di linee di codice.

Negli ultimi anni però, il paradigma della sicurezza è cambiato. Dalle numerose ricerche condotte risulta che il numero di attacchi informatici è in crescita esponenziale e produce insicurezza politica ed economica. Insicurezza che non si limita agli utenti, alle imprese e alle banche verso le quali si indirizza il filone principale del crimine informatico, ma che tormenta anche Stati e Organizzazioni internazionali.

Il concetto di sicurezza nazionale per il cyber-spazio si è originato negli Stati Uniti negli anni Settanta, si è costruito una rilevanza verso la fine degli Ottanta e si diffuso a livello internazionale alla fine del decennio successivo[246]. Ancora oggi, gran parte del lavoro deve essere fatto, non solo in termini tecnici, ma anche per quanto riguarda la teoria e la strategia difensiva individuale e collettiva. È perciò necessario fare studi approfonditi su quale siano gli approcci nazionali alla sicurezza cibernetica, quali siano le principali tendenze e più pressanti mancanze. L'importanza di analizzare in profondità l'idea di *cyber-security* è dovuta al fatto che, come dice Shreier: "*Cyber Security is Evolving from a Technical Discipline to a Strategic Concept"*[247]*.* Per

[245]Cavelty, M.D. (2012) *Cyber-security*, in Contemporary Security Studies, Oxford University Press, New York, pp. 363-377. Consultabile: https://www.academia.edu/2070669/Cyber-security ultimo accesso 28.02.2014
[246]ibid
[247]Shreier op. citata p.45

questo è necessario studiare precisamente le componenti della sicurezza, gli strumenti a disposizione degli attori statali e le possibilità di scelta a loro disposizione così da valutarne l'operato, comprenderne le scelte e selezionare le pratiche ripetibili in altri contesti. Questo capitolo servirà quindi a prendere in considerazione le modalità difensive proprie del cyber-spazio.

Nel tentativo di comprendere nella sua globalità le dimensioni della *cyber-warfare*, il capitolo antecedente ha rappresentato lo sforzo nell'analisi delle *pressioni* o minacce, mentre il capitolo corrente si concentrerà sulle *capacità* difensive.[248] Se nel capitolo precedente sono state elencate le possibili minacce, è ora il momento di considerare le modalità di difesa che offre il cyber-spazio, e vedere come e per quali motivi lo Stato nazionale rappresenti l'entità naturalmente predisposta al compito della difesa cibernetica. La modalità che verrà presentata alla fine del capitolo, come essenziale e indicata, è di tipo olistico. La scelta è caduta su questo approccio perché, come ricorda Cavelty M.D. "*Cyberspace connotes the fusion of all communication networks, databases, and sources of information into a vast, tangled, and diverse blanket of electronic interchange. A 'network ecosystem'*"[249]. Per questa ragione è necessario analizzare un modello ecosistemico, affinchè tutte le pericolosità insite nel cyber-spazio vengano tenute in considerazione.

3.1 Lo Stato e la difesa del cyberspazio: sicurezza o resilienza?

Dopo avere analizzato in dettaglio le vulnerabilità e i possibili attacchi che possono essere lanciati attraverso il cyber-spazio è ora necessario concentrarsi su come ci si può e deve proteggere. L'obiettivo di questa sezione è focalizzare l'analisi sulla difesa che deve adottare lo Stato, inteso come entità onnicomprensiva, capace di essere l'*hub*

[248] I due termini in grassetto si riferiscono alle categorie usate nell'analisi di Cavelty
[249] Ibid p. 363

coordinativo tra il settore pubblico e il privato; tra le strutture militari e quelle civili; e tra le varie istituzioni governative.

Come si è visto, il numeroso spettro di minacce che possono provenire dal cyber-spazio costringe gli Stati, (ma anche le imprese e i singoli individui) a dotarsi di contromisure efficaci per evitare di subire gravi danni ai propri sistemi di comunicazione, di comando e controllo. Questo obiettivo è tutt'altro che semplice da ottenere per una serie di motivazioni. Innanzitutto, la costante evoluzione tecnologica fa sì che siano necessarie sempre nuove modalità di difesa e sempre più contenuti e processi che necessitino protezione. Inoltre, l'elevata propagazione delle tecnologie informatiche ha provocato un aumento di criticità da proteggere sia in costante aumento e diffuso in pressoché tutti i settori della vita di una comunità. È anche per questo motivo che il concetto di sicurezza nazionale applicato al cyber-spazio assume delle connotazioni uniche.

Come ricorda Choucri N. (2012) il modo convenzionale di pensare alla difesa nazionale è in termini militari e di protezione del territorio (soprattutto da incursioni)[250]. La natura del cyber-spazio cambia drasticamente questo paradigma. La componente sociale, le minacce interne e l'annullamento del concetto spaziale sono solo alcune della caratteristiche che contraddistinguono questa dimensione e che devono essere tenute in considerazione quando si costruisce una coerente politica di sicurezza cibernetica. Avendo ben chiare queste linee guida Shreier (2013) afferma che *"Cyber security cannot be achieved at the level of the nation state alone. It requires fully integrated responses that include public private partnerships and international coordination and cooperation of an unprecedented nature."*[251]

Sarà mia premura analizzare tutte e tre le dimensione sopra evidenziate, tenendo sempre a mente che il punto focale resterà per tutta la trattazione la sicurezza nazionale e il sistema di difesa complessivo. La direzione sarà perciò quella dell'analisi globale della questione: lo studio delle tecniche difensive intraprese sino ad ora,

[250]Choucri op. citata p. 39
[251]Shreier op. citata p. 13

l'identificazione degli scenari plausibili per il futuro e la considerazione dei sistemi di difesa attuali attraverso l'utile strumento delle strategie nazionali, pubblicate da molti Stati.

Date le premesse, è necessario considerare la difesa cibernetica come un'entità isolata e indipendente rispetto alle altre componenti della Difesa, anche se in realtà è con esse interconnessa e spesso risponde alle medesime esigenze. Per lo scopo prefissatoci, è più semplice creare un modello artificiale in cui in prima approssimazione le altre dimensioni della difesa possono essere trascurate.

3.1.1 Resilienza

Per essere considerato efficace un sistema di sicurezza cibernetica deve essere in grado di poter fronteggiare una quantità elevatissima di minacce differenti, deve saper proteggere un numero sempre crescente di attori (appartenenti al settore civile, al mondo privato o a quello militare) e deve avere la capacità di difendere globalmente le infrastrutture informatizzate del paese da minacce interne ed esterne in contemporanea. Così come è praticamente impossibile considerare un territorio sicuro in ogni istante e in ogni luogo, lo stesso vale per il cyber-spazio: il concetto fondamentale da ricordare quando si considera la *cyber-security* è che la sicurezza assoluta *non* esiste. Nonostante dalla parte della difesa esistano anche numerosi vantaggi, sia tecnici che strategici, il livello di permeabilità dei sistemi informatici è notevolmente alto. Secondo Corben chi difende "*own what should be the most powerful asset in the battle – home-field advantage – and they must begin to use it more wisely"*[252]. Inoltre, persino le tecnologie informatiche hanno raggiunto ottimi livelli di efficienza: sistemi di rilevazione, di isolamento dei malware e di riconoscimento. Tutto questo non è però abbastanza per garantire una sicurezza soddisfacente. Per questa ragione si è puntato, nello sviluppo delle tecniche di difesa, sia a livello individuale che sistemico, nell'elaborazione di un modello difensivo basato su un'idea presa in

[252]GEERS, K. (2011) *Sun Tzu and Cyber War*, NATO CCDCOE Publication, Tallinn

prestito dalla meccanica: la *resilienza*, ovvero la capacità di subire degli stress, col ritorno, al termine della modificazione, allo stesso punto iniziale da cui si partiva prima dello stress. Secondo Sandro Bologna, ex Presidente dell'Associazione Italiana Infrastrutture Critiche[253], "*il concetto di resilienza (…) nasce da un modo di porsi che rende capaci di convivere con i fallimenti e le sconfitte, mentre spinge a trovare e valorizzare tutte le risorse e potenzialità: tecnologiche, organizzative, economiche e sociali. Il concetto del "non è mai successo" è sostituito dalla visione del "se dovesse succedere", che non significa necessariamente il sovradimensionamento delle soluzioni, ma la predisposizione e la preparazione all'accadimento dell'evento"*[254]*.*

Dall'affermazione di Bologna si possono riscontrare diverse caratteristiche fondamentali della resilienza: la consapevolezza di probabili sconfitte, l'elasticità, la *readiness*. Per quanto riguarda il primo elemento, come si è detto, è una necessaria forma mentis legata alla conoscenza delle pressoché infinite vulnerabilità; da questa coscienza si origina, secondo la logica del processo hegeliano di *Aufheben*, una necessità di reazione elastica alle minacce che dà vita a processi di incrementazione di capacità di risposta.

La *readiness*, viene definita come la capacità di gestire prontamente la sicurezza informatica. Robert Lentz ne elabora un modello a cinque *steps*[255]*,* nei quali identifica un passaggio verticale di competenze. I primi due livelli sono individuali: al primo vi sono le regole basiche di igiene (conoscere il proprio computer, tenerlo libero da minacce), mentre al secondo troviamo l'utilizzo di adeguati *Computer Network Defense Tools* come anti-virus e firewall che permettano di rilevare le minacce e le intrusioni. Il terzo *step* invece è sistemico e consiste nel creare un network efficiente di intercambio di informazioni utili e di comune utilizzo in modo da produrre un ecosistema difensivo. Al quarto step questo ecosistema deve essere reso snello, rapido e agile, capace di intercettare le minacce ancor prima che arrivino al

[253]http://www.infrastrutturecritiche.it/aiic/

[254]Juvara, R. (2013) Infrastrutture critiche, il centro dell'attenzione. A colloquio con Sandro Bologna, consultabile ultimo accesso http://www.securindex.com/downloads/59c2917e6a227d408c18714306fa4f44.pdf 28.02.2014

[255]Grauman B. (2012) op. citata

gateway. Infine, l'ultimo step implica maturità nel gestire i rischi, coinvolge anche gli utenti ordinari e si basa su *Chain Risk Management.* Da notare che Lentz non ha in mente un'impresa quando parla, ma si riferisce direttamente alla *readiness* statale, in quanto è proprio lo Stato l'unità che può propendere più facilmente a raggiungere l'obiettivo di creare un forte ecosistema. È esattamente questo il modello a cui ci si riferirà nel corso della trattazione e che si vedrà esplicitato nella descrizione dei sistemi israeliano ed estone.

3.1.2 Caratteristiche essenziali per incrementare la 'readiness'

Per incrementare la *readiness*, dalla prospettiva statale, è necessario considerare determinate caratteristiche, settori e capacità. Innanzitutto è doveroso incoraggiare l'utilizzo cosciente da parte dei cittadini e, soprattutto, delle istituzioni: bisogna promuovere l'idea che la sicurezza personale rappresenti non solo una necessità ma anche un beneficio. E' poi necessario creare un coordinamento centrale in grado di svolgere importanti mansioni, e mantenere il contatto con le realtà locali.

Il primo passo è quello di sviluppare un efficace metodo di riconoscimento e **monitoraggio dei rischi e delle minacce**. Questo lo si può fare con la creazione di una sorveglianza in tempo reale e costante, e un sistema di avviso rapido (*early warning*) e di condivisione delle informazioni relative agli eventi. È questa la funzione centrale che dovrebbe svolgere un CERT: agire da analista, mediatore e diffusore di allarmi. Il sistema di sorveglianza costante deve essere affiancato, inoltre da una serie di sensori passivi che misurano i flussi in entrata e isola quegli utenti che cercano di penetrare senza accesso o che compiono azioni pericolose. Questo è possibile unicamente attraverso un duplice sistema di protezione basato sull'imposizione di uno stretto e preciso sistema di autorizzazioni e di attribuzione delle credenziali; e sullo sviluppo di un sistema comparativo di analisi a lungo termine in grado di individuare la variazione dello spettro delle minacce.

Parallelamente a questo processo, è essenziale provvedere allo sviluppo di sistemi secondari che garantiscano il funzionamento del sistema quando sotto attacco massiccio. Questo però ha due agenti fortemente limitanti: i fondi necessari per erigerlo e la reale operatività di un sistema non basato sul network. I due problemi sono estremamente attuali e, come si vedrà nel caso estone, di difficile soluzione.

L'ultimo passo necessario alla creazione di un sistema di monitoraggio concreto è l'integrazione con i provider di Internet, soprattutto con quelli più esposti al traffico esterno. Senza questa manovra, si isolerebbe l'azione dei provider e si agevolerebbero le penetrazioni di *malware*s o altri agenti di disturbo nel network interno.

Il secondo passo è la gestione concreta delle misure per **contrastare le minacce e i rischi** rilevati. Esistono numerose componenti atte a rendere concrete le capacità di reazione. Bisogna innanzitutto puntare sulla riduzione dell'incapacità di attribuire la direzione delle minacce. Se poi si considera che, aumentando la collaborazione, diminuisce il carico di lavoro per la singole istituzione o nazione, la conseguenza logica è che, le prime cose da fare in termini gestionali, sono la condivisione del lavoro a livello interno e la collaborazione a livello internazionale (possibilmente sia in termini di conoscenze che di tecnologie). Questo è possibile solo se si sviluppano concrete politiche interne: le **Strategie nazionali**. Queste ultime dovrebbero indicare un piano ideale per contrastare ciascuna vulnerabilità attraverso le modalità e gli attori più indicati.

Oltre a considerare la dimensione collaborativa internazionale, fondamentale per un dominio interconnesso com'è il cyber-spazio, le Strategie nazionali non dovrebbero dimenticare la questione della protezione delle infrastrutture nazionali a elevata criticità. È infatti questo l'ulteriore punto nevralgico della formazione di un sistema sicuro e protetto, come si vedrà a breve. A questo va aggiunta la necessità di cooperare tra le diverse entità statali. I differenti settori che sarebbero naturalmente portati a interagire per garantire la sicurezza al cyber-spazio nazionale. In particolare si osserverà come, la cooperazione tra il settore pubblico e quello privato comportano le maggiori difficoltà.

Un ulteriore punto, sul quale ci si soffermerà solo brevemente, è la necessità di **legiferare**, tenendo in considerazione le minacce e lo scenario nazionale. Le direttrici principali dovrebbero indicare il cyber-crimine, ma anche la privacy e la gestione della *governance* di internet. Un ottimo esempio di sforzo legislativo in questo senso è il Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 contenente "Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale"[256]. È infatti questo un primo strumento per la distribuzione delle competenze nel settore della sicurezza informatica, nonostante all'epoca non fosse stata ancora prodotta un cyber strategia.

Per analizzare dunque le modalità necessarie per porre in essere una modalità efficiente di resilienza è doveroso studiare anche quali sono le risorse a disposizione di coloro che si occupano della sicurezza cibernetica; chi sono coloro che se ne occupano; quali sono gli obiettivi principali da preservare e qual è la migliore forma di farlo. Infine verrà mostrato come, per essere effettivo, un sistema di difesa gestito da un'entità statale deve contemplare, non solo le Forze Armate e quelle governative, ma anche la dimensione privata, delle imprese e dell'ambiente di ricerca. Così da sviluppare una sinergia capace di far fronte in maniera più globale sia alle minacce provenienti dal cyber-spazio, che ai più frequenti problemi di funzionamento ed efficienza.

3.2 Attori

3.2.1 Esecutivo

In sostanza, gli Stati hanno responsabilità giuridica, organizzativa, politica e gestionale per quanto riguarda la sicurezza informatica. Data la sua essenzialità (relativa prevalentemente ai network e alle infrastrutture critiche) e il benessere di una nazione, lo sforzo complessivo deve essere condotto dal più alto livello di governo. I

[256]Pubblicati sulal Gazzetta Ufficiale all'indirizzo http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg;jsessionid=QI0W7ckcZt5e7NUAX7Rj3Q__.ntc-as1-guri2a ultimo accesso 28.02.2014

suoi compiti principali devono essere la responsabilità ultima del funzionamento di infrastrutture e network; la supervisione di tutti gli sforzi necessari per garantire la protezione del paese nel cyber-spazio e l'adozione delle misure operative necessarie a livello nazionale. Nello svolgere questa mansione i governi devono essere capaci di ridurre i rischi, di sfruttare le opportunità migliorando conoscenze e capacità, e di cooperare con gli altri attori preposti a funzioni complementari, sia all'interno dello scenario nazionale sia a livello internazionale.

Tra le responsabilità politiche fondamentali dello Stato vi sono anche, come detto, l'istituzione di una strategia di sicurezza informatica che sia coerente con i principi generali di Strategia di Sicurezza Nazionale e l'adozione di un programma trasversale di governo che porti alla predisposizione di norme, criteri e orientamenti per la sicurezza dell'informazione e per la salvaguardia della resilienza delle infrastrutture critiche, attraverso la programmazione di adeguate capacità di monitoraggio e risposta.

Il governo è altresì responsabile del mantenimento e della protezione dei network utilizzati per lo svolgimento dei propri compiti. E' per questo necessario che applichi nel modo migliore possibile le funzionalità di resilienza *in primis* ai propri servizi così da poter svolgere, anche in caso di crisi, il ruolo coordinativo che gli compete. Infine è compito dei governi accertarsi che nella protezione delle infrastrutture critiche vengano inclusi piani per la creazione di strutture preposte alla preparazione di sistemi alternativi di fornitura di servizi essenziali ai cittadini.

3.2.2 Corpi legislativi

La rilevanza degli organi legislativi è duplice. Innanzitutto, servono per svolgere la funzione classica di controllo sull'operato dell'esecutivo, il Governo. In secondo luogo, sono necessari allo sviluppo di contesti legali benefici per la sicurezza del paese e che avvicinino il Paese a ad altri che condividano timori e prospettive. Per queste ragioni, numerosi Stati hanno provveduto a dotarsi di corpi

appositi capaci di valutare le politiche adottate in termini di sicurezza dei network e delle infrastrutture informatizzate. In alcuni paesi (i.e Gran Bretagna), questi comitati esercitano la sorveglianza nel settore della Difesa del territorio nazionale, in altri sono invece responsabili di tutte le reti informatiche e le risorse governative che in qualche misura dipendono dalle tecnologie ICT. Questa responsabilità è difficilmente assumibile unicamente da corpi legali, perché possiedono raramente le competenze tecniche per la comprensione dell'evoluzione progressiva delle minacce.

Spesso, anche dal solo punto di vista legale, è complesso comprendere il *discrimen* tra innovazione legale o no (i.e. *bitcoin*, una nuova forma di pagamento virtuale). Nonostante queste difficoltà, è necessario che i comitati preposti a questa funzione all'interno del Parlamento siano composti da esperti in tutte le aree che interessano il cyber-spazio: tecnologico, etico, legale, militare e della ricerca[257]. Il Parlamento dovrebbe, per sua natura, fare da collante tra le plurime dimensioni della sicurezza informatica: rappresentando gli interessi della popolazione; sostenendo il governo nella condivisione con il settore privato del peso della sicurezza; veicolando all'esterno le necessità di creare cooperazione e condivisione di impegno con altri paesi. Inoltre dovrebbe essere l'organo più indicato per promuovere le caratteristiche "supplementari" della difesa cibernetica che ne formano l'ecosistema: il benessere economico e la ricerca.

3.2.3 Forze Armate

Il ruolo delle forze armate in un settore così "civile" come la difesa cibernetica è probabilmente il compito più complesso per una trattazione generica come quella che si sta tentando di proporre. Prima di mostrare il ruolo che dovrebbero avere, è necessario fare due precisazioni. In primis, le forze armate hanno una diversa incisività e ruolo a seconda di quale sia il loro livello di permeazione della società in generale (al di là del fattore cyber) e del loro obiettivo strategico. Così

[257]Intervento di Erel Margalit, parlamentare isreliano, alla conferenza Cyber Tech 2014 a Tel Aviv

ad esempio, Israele e l'Estonia saranno due casi simili se si considera il servizio di leva obbligatorio e il livello con cui entrambi gli eserciti permeano (in maniera molto diversa) la società, però, dati gli obiettivi più offensivi delle Forze Armate israeliane la gestione del settore della Difesa è completamente differente rispetto a quello estone. Anche il settore del cyber risente di questa impostazione e si vedrà come il ruolo delle sfere militari in Israele è molto più intrusivo di quanto non lo sia in Estonia, ad esempio nella gestione del NISA israeliano[258].

In secondo luogo, va precisato che molto di ciò che concerne gli eserciti e le Forze Armate di solito è circondato dal silenzio o addirittura dal segreto di Stato, per preservare la sicurezza nazionale. Per questo motivo non si può sapere con esattezza quale sia il loro ruolo nello specifico. Tuttavia è possibile delineare un elenco di responsabilità che cadono sulle spalle dell'esercito.

Innanzitutto le Forze Armate sono le uniche a poter difendere le proprie strutture e reti comunicative informatizzate. È questo il principale obiettivo della difesa intrapresa dalle forze armate: mantenere costantemente operative le funzionalità di queste reti fondamentali per la sicurezza del paese. La questione è di vitale importanza come si è visto perché il rischio di perdere informazioni sostanziali per la sicurezza nazionale; la possibilità che il computer possa cadere sotto il controllo di un'entità esterna e l'ipotetica interruzione delle operazioni militari sostenute da tecnologia informatica (ormai pressoché la totalità delle azioni militari), sono scenari ipotetici ma altamente plausibili, come dimostrano gli episodi descritti nel precedente capitolo.

Secondo alcune dottrine, come si è visto, gli eserciti hanno la responsabilità di sviluppare sistemi deterrenti (i.e. offensivi) per contrastare attivamente le minacce provenienti dall'esterno. Il dibattito sulla militarizzazione del cyber-spazio e sull'effettiva possibilità di deterrenza attraverso di esso è estremamente attuale. Vede la presenza di autori e militari che si schierano con l'idea di una deterrenza classica basata sull'incremento graduale della forza, insieme a coloro che ritengono seriamente che la difficoltosa attribuzione possa essere alla

[258] Cfr. capitolo 5

base di problematiche valutazioni che potrebbero causare incidenti internazionali. Un ultimo appunto sarà fatto sulla necessità di cooperazione anche dei militari con il settore privato.

3.2.4 Settore privato

Se la risposta del governo alla sicurezza informatica può spesso essere definita ad hoc, la risposta del settore privato alla sicurezza informatica è meglio caratterizzata dalla mancanza di strutturazione. Secondo Geers et al.[259] per mantenere un profittevole rapporto con il settore privato è necessario applicare degli standard di sicurezza e persino delle sanzioni qualora questi non vengano compiuti. Eccetto casi limitati (i.e. Israele e Estonia) non sono presenti però concrete modalità di regolamentazione degli standard. Anche nel caso esistano normative al riguardo, studi di settore (ad esempio i già citati studi del CLUSIT e del CLUSIF) hanno dimostrato che sono scarsamente rispettate e che i governi hanno pochi mezzi per farli osservare. Una soluzione preferibile, come si vedrà, è l'affiancamento di incentivi che invoglino i privati non solo a rispettare gli standard prefissati, ma a cooperare con le istituzioni per promuovere l'innovazione e la diffusione delle tecniche difensive. Infatti secondo alcuni modelli di sviluppo[260] la promozione del settore privato in modo che faccia da traino a quello pubblico nell'adozione di nuove forme di tecnologie difensive, può costituire un vantaggio strutturale anche in termini di cyber-difesa.

Anche in questo ambito il dibattito è molto acceso soprattutto tra coloro che immaginano un governo meno assertivo e più incline agli incentivi e chi invece reclama a gran voce un intervento intrusivo del governo negli affari dello Stato. In generale, è la prima impostazione ad essere accettata, il cui chiaro esempio è la gestione estone, nonostante comporti numerose problematiche soprattutto in termini di effettiva messa in pratica delle misure standard di difesa. Anche in questo caso è

[259]Geers (2011) op citata p.26
[260]È palese il caso israeliano in questo senso

necessario che un alto livello di dialogo tra il governo e i privati che gestiscono infrastrutture critiche e che compongo il settore ICT.

Il settore IT è infatti una parte fondamentale di qualsiasi soluzione di cyber- sicurezza in quanto può e deve sostenere il settore nazionale della difesa. Per questo, nel breve termine, questa sezione deve essere incoraggiato a fornire soluzioni tecnologiche che permettano di trovarsi sempre un passo avanti rispetto alle minacce esterne. La parte pubblica e questo delicato settore produttivo devono lavorare insieme per accelerare lo sviluppo di prodotti di sicurezza *dual-use* e per semplificare l'integrazione della sicurezza dal livello degli utenti a quello della protezione delle risorse. Per quanto riguarda i tecnicismi, è necessario che il settore tenga in considerazione che la direzione degli attacchi non è più legata esclusivamente al sistema operativo ma che si concentra oggi soprattutto a livello di software, forse eccessivamente trascurato.

Un ultimo appunto riguarda la necessità (o meno) di considerare le compagnie responsabili in qualche modo per i danni causati da componenti IT insicure. Inutile dire che è una battaglia molto aspra e che sarà dibattuta ancora lungamente, ma che devierebbe eccessivamente il focus di questo lavoro.

3.2.5 L'accademia e il settore della ricerca

Fra questi settori l'accademia potrebbe, se adoperata e sfruttata adeguatamente, svolgere due compiti fondamentali, uno in termini di specializzazione della conoscenza, l'altro per ciò che concerne la diffusione della conoscenza e della consapevolezza. Per quanto riguarda la ricerca infatti, l'università potrebbe essere avvantaggiata da tutta una serie di fattori: la possibilità di ricerca svincolata dalle necessità di guadagno, la coordinazione con una serie di entità, dal settore privato, alle forze armate, la completa assenza di responsabilità, l'influenza di settori di ricerca prossimi ma non correlati[261]. Tutte queste peculiarità potrebbero offrire all'università una prospettiva unica, che

[261]Mi riferisco alla condivisione dei laboratori tecnologici nei campus universitari, con ricercatori di altre materie di ricerca

sarebbe sicuramente di grande aiuto alle attività nazionali. Ne è dimostrazione non solo i casi estone o israeliano, ma anche le attività svolte dal polo dell'Università la Sapienza gestito dal professor Roberto Balboni[262].

Per quanto riguarda il secondo compito, è chiaro invece che l'università, investendo su corsi direttamente focalizzati sulla sicurezza informatica, potrebbe formare schiere di esperti in questo ambito. Ciò che avviene oggi è la predilezione per la formazione ai principi dell'ingegneria informatica o alla programmazione, mentre nei settori della difesa non vi è nessun realtà diffusa. I corsi istituiti a Tallinn e nel Negev in Israele sono un esempio di come si potrebbe strutturare un corso universitario, considerando non solo questioni tecnologiche ma anche fondamentali principi legali e di teoria di conflitti. Usando le parole di Ben-Israel "*è necessario spostare questo sforzo di insegnamento verso ragazzi più giovani, istituendo dei corsi post scuola dell'obbligo o corsi universitari triennali*". Al di là del valore che questo processo di educazione potrebbe avere per la sicurezza nazionale, è anche corretto diffondere la conoscenza di questi processi per incrementare il sopra descritto fenomeno dell'igiene informatica.

3.3 I punti critici della difesa

Secondo il *National Cyber Security Framework Manual* pubblicato dal Centro di Eccellenza della NATO[263] il concetto di sicurezza cibernetica nazionale stimola cinque dicotomie, o dilemmi, alle quali è necessario fare riferimento se si analizza il concetto della difesa:

- Stimolare l'economia VS migliorare la sicurezza nazionale
- Modernizzare le infrastrutture VS proteggere le infrastrutture critiche

[262]Si veda ad esempio il Centro di Cyber Intelligence and Information Security dell'Università sapienza di Roma (http://www.cis.uniroma1.it/)
[263]Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012

- Il settore privato VS il settore pubblico
- Protezione dei dati VS *information sharing*
- Libertà di espressione VS stabilità politica

La soluzione di questi dilemmi ovviamente non risiede nella predilezione di un criterio rispetto all'altro, ma sull'equilibrio delle necessità di tutti i "contendenti" per ottenere un risultato benefico, dal punto di vista della sicurezza, ma anche dell'economia e della qualità della vita. Si è già discusso di tre di questi dilemmi nei precedenti due capitoli, è ora necessario soffermarci sulle restanti due dicotomie e analizzarle precisamente per ottenere un quadro più chiaro delle sfide che incontra chi si prepone di creare un ecosistema difensivo. Questi due scenari verranno arricchiti da un terzo in cui si considererà la cooperazione internazionale come punto di chiusura dell'osservazione.

3.3.1 La protezione delle infrastrutture critiche

Con l'evoluzione delle tecnologie informative e di comando, vi è stata una prepotente crescita del loro utilizzo nella gestione dei servizi critici (o vitali) per lo Stato: "*these infrastructures are being modernised, harnessing affordable access to broadband applications and services, and inexpensive ICT devices. As such, they increasingly comprise a heterogeneous composite of hardware and software products that, for the most part, combine unverified hardware and software that is manufactured by a heterogeneous global industry using global distribution channels"*[264]. Data la natura critica di queste infrastrutture, è facile comprendere perché sia una questione essenziale per la sicurezza nazionale risolvere la questione in maniera da bilanciare appunto le potenzialità economiche di breve periodo e quelle relative alla sicurezza nazionale di più lungo corso.

[264]Geers (2001b) op. citata p 36

Per gestire la questione è innanzitutto necessario selezionare e categorizzare le infrastrutture a seconda della loro criticità, questo per una questione precisa: le risorse sono limitate, quindi è consigliato concentrarsi su ciò che è più sensibile ad attacchi esterni. È questo ad esempio il caso dell'articolo Quarto dell'*Emergency Act* estone[265] in cui si indicano precisamente le categorie di infrastrutture critiche e le reciproche responsabilità.

La protezione del sistema di controllo di una diga non è ad esempio lo stesso che serve per preservare la sicurezza degli Internet Service Provider[266], è pertanto necessario adottare misure protettive specifiche e mirate a seconda del tipo di infrastruttura. Nonostante le differenze che separano il complesso mondo delle infrastrutture critiche tra loro, si possono riscontrare molteplici azioni considerate necessarie quando si deve assicurare la Protezione delle Infrastrutture Informatizzate Critiche (CIIP è la sigla in inglese). I passaggi sono in molti casi simili ai passaggi successivi descritti precedentemente: è essenziale raggruppare le informazioni e fare un analisi dei rischi potenziali[267]; definire precisamente i ruoli tra governo e gestori delle infrastrutture nelle responsabilità e mantenere costantemente il controllo sui network. Questioni che richiedono già di per sé notevoli sforzi, ma vanno accompagnate da altre pratiche necessarie se si vuole condurre un'effettiva CIIP.

Lo studio delle possibili minacce[268] deve essere accompagnato da altre due attività essenziali, la **previsione** e l'**educazione**. La previsione consiste in tecniche di analisi dei rischi incrociate con tendenze di attacchi passati, proporzionati al tempo[269]. Esistono molte tecniche di analisi dei rischi, non è importante essere specifici, l'importante è che nella modalità di analisi vi sia una componente futura-

[265]Estonian Information System's Authority – *Emergency Act*, 15 June 2009

[266]Sulla discussione riguardo la considerazione del cyber-spazio come infrastruttura vedi:

[267]Cfr. sulla CIIP italiana il "Italian Cyber Security Report" p 56 consultabile a http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html ultimo accesso 28.02.2014

[268]Va fatta un ulteriore digressione sulla gestione del rischio. Questa parte della gestione delle minacce avviene una volta che si è esaurita la parte di *assessment* del rischio e si compone di cinque momenti: (a) la prevenzione; (b) la *detection* ; (c) la risposta; (d) *recovery.*

[269]Un modello molto interessante di *Multy-Hypothesis Analysis & tracking* sperimentato, come si vedrà, dallo IAI israeliano

ipotetica sufficientemente elastica da soddisfare i criteri della resilienza senza cadere nel rischio di adoperare una modalità di difesa passiva, incentrata unicamente sulla difesa dall'attacco quando questo si presenta. Questo significa poter ridurre la frequenza degli attacchi e la loro intensità. Per educazione invece intendo la necessità di condividere le nozioni di base della protezione informatica con tutti coloro che, all'interno della struttura, entrano in contatto con il cyber-spazio relativo alla struttura stessa (tutti e quattro i *layer*).

In caso di crisi è inoltre necessario che ognuno sappia qual è il proprio ruolo, sia all'interno della struttura che gestisce la minaccia, sia in termini di collaborazione istituzionale con gli organi preposti alla difesa cibernetica nazionale (i.e. CERT). Devono perciò essere condotte delle lezioni per spiegare agli addetti e ai non propriamente tali le modalità d'azione in caso di minaccia, ma anche delle vere e proprie esercitazioni come quelle che si svolgono a livello internazionale tra CERT diversi (e tra ISPs), in modo che ognuno abbia ben chiaro in mente quale sia l'obiettivo da perseguire in momenti concitati come quelli di un attacco informatico.

Tabansky L (2011), in un articolo in cui considera la protezione delle infrastrutture come questione generica, ritiene necessario intraprendere un approccio olistico anche nella difesa delle infrastrutture critiche. In particolare, si riferisce al rischio di considerare unicamente la questione tecnologica dimenticando l'alto grado di dipendenza fisica delle strutture informatizzate. Idea condivisa da molti esperti di protezione di infrastrutture critiche (i.e. Toomas Vira, Magal Kats, Sandro Bologna).

In maniera similare, secondo Yakov Hain, il responsabile della sicurezza cibernetica all'Israel Electric Corporation, è necessario porre in essere un processo complesso dalle responsabilità condivise per ottenere risultati importanti, che egli definisce *Cyber Protection Concept*[270]. Pur ricordando la particolarità del caso israeliano, il modello per la difesa delle infrastrutture può essere preso come spunto, per la comprensione del fenomeno difensivo a tutto tondo. Innanzitutto è

[270]Presentazione di *Cyber Gym* alla Cyber tech di Tel Aviv gennaio 2014

necessario possedere una metodologia, non è pensabile gestire il *risk assessment* in maniera casuale, ma è essenziale direzionare la ricerca e setacciare ogni frammento di informazione per ottenere un risultato il più possibile accurato e meticoloso. Per avere arrivare a questo esito servono due componenti: il personale adeguato e i giusti strumenti informatici in grado di contrastare le minacce. Gli israeliani attribuiscono un valore molto elevato alla componente umana e alla possibilità di incrementare le sue potenzialità con le giuste modalità interattive. Nonostante si stia parlando di un modello difensivo che esiste ed agisce secondo modalità spazio temporali non umane, ad ogni livello della gestione della sicurezza il fattore umano è ancora quello più importante, per molti osservatori (tra cui Kristjan Prikk, come si vedrà nei prossimi capitoli). Ritornando al modello di Hain, tutto questo processo deve essere accompagnato da un'elevatissima dose di intelligence. All'interno di questo scenario il modello prevede anche la modalità di esercitazione congiunta tra operatori delle infrastrutture elettriche e membri dell'esercito.

Inevitabilmente, esiste tutta una dimensione tecnica fondamentale per percepire la possibilità di migliorare la protezione di queste infrastrutture. Non credo però che un'analisi delle principali tecnologie difensive costituisca uno strumento utile per la trattazione. Innanzitutto perché, come detto, il panorama delle tecnologie informatiche è in costante evoluzione e ciò che oggi rappresenta un'innovazione potrebbe risultare in breve tempo uno strumento obsoleto. E inoltre perché, in un'analisi comportamentale, la descrizione precisa dello strumento non modifica le modalità di interazione, almeno in questo caso. A prescindere dalla premessa, va però aggiunto che il livello di protezione dei protocolli di comunicazione e dei sistemi di comando è genericamente troppo basso, in parte, come si è visto nello scorso capitolo, perché la dimensione della sicurezza è da sempre considerata meno di quella della funzionalità (spesso addirittura non compresa, come nei sistemi SCADA), in parte perché mantenere aggiornato il sistema di protezione informatica ha dei costi decisamente elevati e chi gestisce le infrastrutture preferisce non sobbarcarselo. È da

questa affermazione che si può partire ad analizzare la seconda dimensione dicotomica, il rapporto tra settore pubblico e privato.

3.3.2 La partnership tra settore pubblico e privato.

Questa dimensione costituisce, nell'opinione di molti, uno dei punti deboli della gestione difensiva del cyber-spazio, mentre per altri potrebbe addirittura rappresentare un *force-multiplier*[271] nell'atto di impiantare una difesa solida. Certo è che, pur non essendo una prerogativa della *cyber-security*, in questo ambito la necessità delle istituzioni statali rappresenta un'innovazione per quanto riguarda i modelli difensivi standard.

Nel 1795, Edmund Burke notava che "*one of the finest problems in legislation [is to determine] what the state ought to take upon itself to direct by the public wisdom, and what it ought to leave, with as little interference as possible, to individual discretion*.'[272] La questione è più che mai valida per il cyber-spazio, in quanto nella gestione delle minacce provenienti dalla dimensione cibernetica lo Stato deve richiedere il coinvolgimento del settore privato perché gran parte delle infrastrutture sono di carattere, non militare o pubblico, bensì privato. Che si parli di gestione o di possesso, la casistica di possibili obiettivi di cyber-attacco che sono controllati da entità non governative è generalmente alta (le stime cambiano da paese a paese). I privati sono dappertutto nella gestione e nella protezione delle reti: progettano, vendono e installano software e hardware che sono utilizzai nei network governativi, i nuovi sistemi d'arma integrati sono per la grande maggioranza prodotti da imprese private e via di seguito. Secondo Buckland e Winkler (2010) questa innovazione renderà necessario un nuovo approccio di sicurezza, da un *whole of governement* ad un *whole of issues*[273], in cui la centralità del protezione non è assolutamnte centralizzata, ma *"leads to a fully integrated security sector approach*

[271]Stavridis J. E Farkas E.N. (2012), *The 21st Century Force Multiplier: Public–Private Collaboration* in "The Washington Quarterly", Vol.35, No.2, pp.7-20;
[272]Cit. in Buckland B.S., Winkler T.H. (2013), *Public Private Cooperation: Challenges and Opportunities in Security Governance,* DCAF horizon 2015 working paper No. 2, Geneva Centre for the Democratic Control of Armed Forces (DCAF);
[273]Stavridis e Farkas lo chiameranno *whole of society approach*

that reaches beyond established state structures to include select private companies"[274].

Secondo Thomas R. N. (2009) la necessità di sicurezza informatica, in particolare riferita alla protezione delle infrastrutture critiche, può essere la ragione principale di quel cambio di approccio, di cui si è parlato. Stavridis e Farkas (2011) definiscono addirittura la Partnership tra settore Pubblico e Privato (PPP in inglese), come l'elemento essenziale dei nuovi assetti militari nel XXI secolo, e la considerano un moltiplicatore di forze (*force multiplier)*. Inoltre credono che la cooperazione tra la l'efficienza e l'innovazione del settore privato e la possibilità di controllo centrale esercitata da parte del governo siano ingredienti fondamentali per la crescita potenziale della capacità difensiva nazionale. Gli autori però non sono ignari del fatto che sono molte le difficoltà nell'effettiva implementazione del partenariato a tutti i livelli. In particolare, la loro proposta è quella di trasformare la collaborazione in un canale prioritario nelle scelte dello Stato attraverso l'istituzionalizzazione del processo di collaborazione grazie anche ad un corredo di norme. Questo tipo di approccio è esattamente quello perseguito dall'Estonia, la cui strategia nazionale è appunto fortemente centrata sulla partnership con il settore privato attraverso la progressiva inclusione nei processi decisionali e l'istituzionalizzazione dei rapporti reciproci.

Questa nuova situazione presenta sia vantaggi che rischi. Se è vero infatti che lo sviluppo prodotto dal settore privato è in gran modo superiore rispetto a quello che produce il settore pubblico, è anche vero che un aumento della dipendenza dalle componenti del settore privato crea un aumento della diffusione delle vulnerabilità che crea un circolo vizioso di dipendenze e vulnerabilità. Perché le difficoltà e le vulnerabilità vengano superate è necessario un approccio concreto e cogente che generi sicurezza. Un obiettivo tutt'altro che semplice. Presenta infatti numerose problematiche. La prima e principale è legata alla **fiducia** reciproca. Da una parte lo Stato prova difficoltà nell'affidarsi a imprese private che sono tendenzialmente motivate da interesse

[274]Ibid p 10

economico più che nazionale. Inoltre spesso queste imprese possono essere di origine straniera, il che è sempre difficoltoso dal punto di vista di uno Stato che cerca di preservare la sicurezza nazionale e la propria sovranità (e.g. Maglan Group che opera in Italia). Da parte delle imprese la mancanza di fiducia concerne la possibilità di limitazione commerciale e la ripercussione internazionale alla nozione che quella determinata compagnia subisce condizionamenti statali. Un ulteriore problema è perciò capire quali siano le modalità attraverso le quali rendere possibile e persistente la cooperazione. La soluzione migliore in questo caso sono gli incentivi economici (i.e. Israele) o far leva sul sentimento patriottico-nazionalistico (i.e Estonia), poiché contare sul senso di responsabilità sociale è decisamente più rischioso. Inoltre è necessario istituire un insieme di sanzioni progressive per quelle realtà che non cooptano le necessità governative. Da parte privata, per cambiare l'atteggiamento mentale dei governi è necessario mostrare loro i vantaggi derivanti dal prendere atto di una situazione concreta che non è in potenza, ma è già in atto e per tanto va affrontata prontamente.

La questione ha stimolato anche l'interesse internazionale, infatti l'ITU, oltre ad aver auspicato e patrocinato un numero di cooperazioni, ha da sempre sottolineato l'importanza di concentrare gli sforzi della difesa cibernetica a livello di collaborazione tra privato e pubblico e di interazione regionale tra imprese simili, pur essendo consapevole delle difficoltà di raggiungere livelli accettabili.

3.3.3 La cooperazione internazionale

Infine, l'ultima dimensione che ci interessa analizzare è la collaborazione internazionale, in termini difensivi. Innanzitutto, riprendendo il discorso intrapreso nel primo capitolo, è importante ricordare come siano stati fatti numerosi sforzi internazionali per ottenere una dimensione cibernetica più pacifica e meno militarizzata. Sforzi che però non sono stati accompagnati da altrettanti successi. Infatti la successiva militarizzazione del cyber-spazio non ha certo contribuito ad avanzamenti nella diplomazia internazionale.

Una forma differente di approccio internazionale è costituita invece dagli accordi bilaterali, o regionali. Si tratta di cooperazione a fini difensivi di due o più entità unite che intraprendono percorsi di collaborazione più o meno intima. La collaborazione non deve essere necessariamente internazionale, può essere anche solo transfrontaliera, o come nel caso di Italia, Cipro e Israele, a capi opposti del Mediterraneo. L'esigenza di cooperare con i vicini, come nel caso di Estonia e Finlandia, nasce da tante ragioni, ma in particolare dalla condivisione di simili problematiche (clima, geografia), o componenti tecniche (ISPs, server di banche, rifornimento di gas).

Un settore particolarmente attivo nel creare collegamenti extra territoriali è quello delle infrastrutture critiche, che possono essere condivise da più paesi contemporaneamente. Così, partendo dalla co-gestione della sicurezza informatica su una determinata struttura si può arrivare a strutturare interi meccanismi di difesa in collaborazione.

La cooperazione può essere utile, oltre che alla gestione, anche all'analisi e alla risposta alle minacce. Così come avviene con le operazioni internazionali di polizia o militari la collaborazione, tramite condivisione di informazioni e supporto operativo, può essere una grande agevolazione, soprattutto nella lotta contro il terrorismo e nella protezione del flusso di dati in eccesso. Il cyber-spazio in questo caso risulta essere una facilitazione per la collaborazione, quindi un incentivo alla difesa.

3.4 I modelli adottati. Analisi comparata delle Strategie Nazionali

Uno dei modi principali in cui i Paesi hanno sinora intrapreso la schematica operazione di standardizzare le proprie modalità difensive è la pubblicazione (o l'adozione in forma segreta) di strategie in materia di difesa cibernetica. Ne esistono ad oggi una trentina ufficiali[275] e molte

[275]L'Italia è stato il 34° stato, pubblicando il "Quadro Nazionale per lo spazio della sicurezza informatica", leggibile al http://www.stefanomele.it/public/documenti/400DOC-521.pdf. Per un elenco completo

non pubbliche, come nel caso di Israele. Di solito le strategie vengono emanate dagli organi preposti al coordinamento interno della Difesa e includono quattro sezioni: una definitoria, una relativa alle minacce; una per le modalità adottate di difesa; e una per le raccomandazioni. È questa la ragione della struttura di questo elaborato di tesi, al posto delle raccomandazioni però verrà inserito un doppio studio specifico.

Considerando lo strumento della Strategia Nazionale, va detto che, nonostante ogni paese adotti la propria seguendo i preconcetti che ritiene maggiormente validi[276], nella maggior parte dei casi vi sono dei modelli che si ripetono. Così la strategia statunitense influenzerà una parte degli Stati, mentre altri particolarismi strategici fungeranno da riferimento, anche solo per ambiti particolari.

Nella maggior parte delle realtà inoltre vengono considerate come fondamentali determinate questioni: la protezione delle infrastrutture critiche; la necessità di aumentare e rendere più efficiente la condivisione di informazioni e l'implementazione di collaborazione internazionale. Al di là di questo ogni paese si specializza nei settori che reputa più sensibili. Quindi, per la Francia la variabile fondamentale sembra essere la protezione dei dati, la Difesa francese è fortemente strutturata sulle capacità di criptare codici, mentre per quanto riguarda il Lussemburgo[277], il forte sbilanciamento verso la protezione dal cyber-crimine ha fatto sì che il focus del paese sia indirizzato verso la scoperta delle frodi. L'approccio indiano[278] si concentra molto sugli aspetti tecnici delle tecnologie ICT, mentre quello olandese[279] sulla necessità di affiancare una prospettiva offensiva/deterrente alla classica difesa. Questo significa adattare i concetti di *best-practice* alle esigenze nazionali, attraverso gli strumenti a propria disposizione.

---

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[276]Czossek, C. e Ottis, R. e Ziolkowski K. (2012) *4th Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn p29

[277]La NCS del Lussemburgo è consultabile https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf ultimo accesso 28.02.2014

[278]La NCS indiana è consultabile al https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf ultimo accesso 28.02.2014

[279]Già citata: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf ultimo accesso 28.02.2014

Secondo il lavoro di Geers et al (2013)[280] in ogni strategia devono essere innanzitutto chiari obiettivi e priorità rilevanti. Si deve capire se l'impostazione nazionale predilige la difesa proattiva o una prospettiva più offensiva e si deve intendere il livello di coinvolgimento del mondo militare. Inoltre, la strategia deve conferire responsabilità ed autorità alle diverse agenzie dello Stato, investendole della competenze per poter supervisionare la politica nazionale di sicurezza cibernetica. Gli organi preposti devono essere indicati come principali esecutori e diffusori delle informazioni riguardanti il grande pubblico e la diffusione della consapevolezza sociale. Gli autori ritengono necessario istituire un organo *ad hoc che si occupi della gestione* e dell'implementazione della strategia. In realtà, nell'opinione di Geers, che condivido, non è necessario istituire un organo nuovo, come nel caso del *National Cyber Bureau* israeliano, ma basterebbe ridistribuire le competenze all'interno delle organizzazioni già esistenti, come nel caso statunitense. Questa decisione dovrebbe essere fortemente correlata alla natura precedente del sistema di sicurezza nazionale e alle necessità del paese.

Per di più, una strategia non può fallire nell'indicare le politiche di riferimento agli argomenti principali della sicurezza informatica: la protezione delle infrastrutture critiche e la cooperazione tra diversi settori del paese. A questo fine è necessario che la strategia contenga indicazioni per la produzione di leggi e regolamenti ulteriori capaci di agevolare il sistema di sicurezza nazionale. L'ultimo punto evidenziato da Geer è l'investimento nel settore della ricerca e dello sviluppo con l'intento di investigare sempre più approfonditamente le questioni tecnologiche e mettere a disposizione del paese un numero crescente di esperti.

Quello descritto sotto è invece il modello prospettato dalla International Telecommunication Union, che schematizza un'ipotesi del tutto simile a quello descritto da Geers.

[280]Op.citata p 43

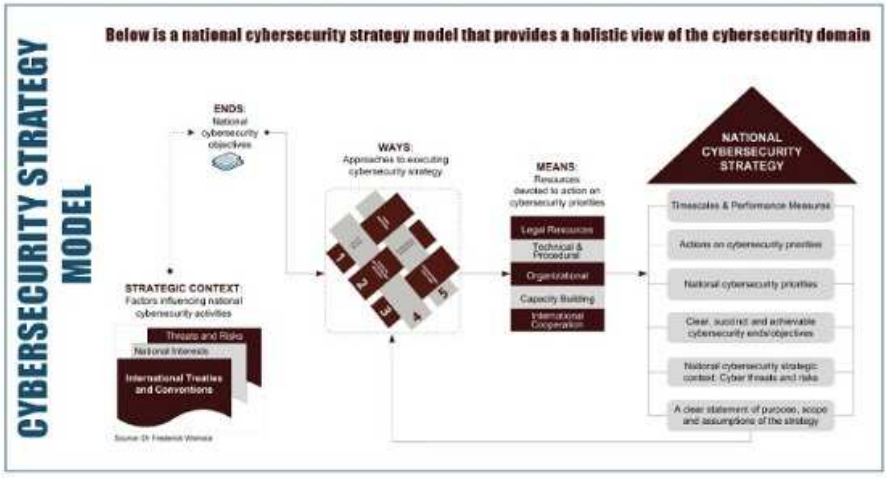


Figura 2: Cybersecurity Strategy Model - ITU

Mele S. (2013) e Hathaway M. (2013) hanno entrambi elaborato una preziosissima analisi comparativa dei vari modelli di strategia nazionale. Nel primo caso l'analisi è assolutamente qualitativa, in quanto Mele[281] ha creato una griglia composta da tredici variabili e ha categorizzato ciascuna strategia secondo il grado di osservanza delle suddette variabili. I pilastri strategici considerati dall'autore in particolare comprendono: l'identificazione delle infrastrutture critiche, la formulazione di leggi ad hoc, lo sviluppo di cooperazione internazionale, la creazione di organismi specifici, l'identificazione del cyber-spazio come un dominio bellico, la prospettiva di un aumento della resilienza dei sistemi informatici e l'istituzione di un processo formale per incrementare l'*infosharing* tra settore pubblico e privato[282]. Dall'analisi comparata sviluppata è possibile notare una serie di caratteristiche comuni e molte peculiarità. La tendenza degli approcci nazionali è decisamente improntata alla difesa, però non mancano le nazioni (tra cui Stati Uniti, Russia, Francia e Paesi Bassi) che considerano lo spazio cibernetico come un dominio in cui è possibile esercitare deterrenza e coercizione. Sono in maggior numero le entità statali che invece

[281] Mele, S. (2013) *I principi strategici delle politiche di cybersecurity* pubblicato su: http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/principi-strategici-delle-politiche-di-cyber-security.html ultimo accesso 28.02.2014

[282] Per un elenco completo si veda la tabella creata da Mele S. a http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2013/12/Mele-matrice-completa.pdf

considerano il cyber-spazio come un dominio di guerra, ma senza dichiarare necessario lo sviluppo di un programma offensivo. Inoltre si può identificare una chiara differenza posturale se si considerano l'Europa come contesto unificato e il resto del mondo. Per l'Europa infatti il focus principale è incentrato sulla protezione dai crimini informatici e gli attacchi isolati. La NATO, da questo punto di vista, crea una sorta di fusione tra le due impostazioni. L'Organizzazione, pur non identificando il cyber-spazio come dominio militare nel testo pubblicato nel 2009, opera attraverso la cooperazione militare con i Paesi Membri. Allo stesso tempo però, incita alla protezione dal crimine informatico e alla produzione di opere volte alla sensibilizzazione pubblica e dei governanti in questioni di comportamenti del cyber-spazio e normative internazionali (i.e. le pubblicazioni del Centro di Eccellenza di Tallinn). Tornando alla descrizione elaborata da Mele, è infine necessario notare tre importanti fattori: il ruolo degli Stati Uniti, la posizione Russa e la mancanza di Cina ed Israele[283].

Data la storia del cyber-spazio di cui si è parlato nel capitolo di apertura, è inevitabile che gli Stati Uniti abbiano svolto un ruolo fondamentale nello sviluppo delle pratiche cibernetiche. Nonostante i primi documenti (pubblici) risalgono al 2000, è con la strategia pubblicata nel 2009 che il modello difensivo statunitense prende finalmente atto, modellandosi in base alle necessità del paese. Non è da intendere come una tardiva rappresentazione della gestione del paese della difesa cibernetica, bensì come una tardiva realizzazione dell'arretratezza del settore della Difesa in materia di attacchi cibernetici. Ne sono una dimostrazione il grande impegno per mediare tra le istanze dei singoli Stati[284] e le capacità difensive della nazione nel suo complesso e tra la protezione del settore civile e quello militare[285]. A queste mancanze gli Stati Uniti hanno voluto far fronte attraverso l'emanazione di diverse leggi e la pubblicazione di differenti concetti

[283]Mele ha deciso di non includere la Raccomandazione 3611 nel novero delle strategie pubbliche. Per chiarimenti vedi capitolo su approccio nazionale di Israele.

[284]Secondo un'intervista concessami nel dicembre 2013 da Kristjan Prikk, un importante esempio di sviluppo nella protezione cibernetica è rappresentato dalle forze del Maryland

[285]È per queste problematiche che il rapporto pubblicato dalla *Security and Defense Agenda* in collaborazione con Mc Afee sulla *readiness* ha visto gli Stati Uniti posizionarsi peggio di quanto ci si aspettasse

dottrinali che hanno avuto anche dei notevoli effetti negativi in termini di implementazione e cooperazione tra le diverse agenzie coinvolte nella gestione della sicurezza informatica.

Per quanto riguarda la situazione russa, la pubblicazione di numerosi documenti e la persistente richiesta in sede ONU di una revisione delle normative internazionali per la gestione della rete, dimostra come sia pressante per la Federazione Russa la questione cibernetica. Nonostante, le accuse internazionali di antidemocraticità e di utilizzo di manovre repressive come il controllo di Internet, il Paese ha come detto pubblicato numerose strategie nelle quali si include anche la necessità di protezione dei diritti sulla privacy e misure contro il crimine cibernetico. Tutti i documenti russi considerati non vagliano la dimensione della protezione delle infrastrutture critiche. Questa è una scelta che dipende anche dal grado di segretezza con cui vengono trattate le componenti vitali per la sicurezza nazionale russa.

Infine per quanto riguarda Cina e Israele, non si può non approfondire la loro mancanza di strategie. Come si è detto sopra, la loro assenza non corrisponde all'inesistenza di un pensiero preciso riguardo alla sicurezza cibernetica. Nel caso di Israele, come si vedrà, la lacuna è più formale che pratica, in quanto è stato approvato nel 2011 un documento che fa le veci della strategia, e la struttura del paese è estremamente avanzata sia in termini di concetto che in pratiche di interazione interna. Per ciò che concerne la Cina invece il sistema nazionale è molto più nebuloso. Esistono chiare informazioni che mostrano come nel Paese la sicurezza informatica sia gestita principalmente dal mondo militare e che l'approccio al cyber-spazio sia decisamente offensivo[286].

Va ricordato però che le strategie di solito non sono altro che documenti pubblici che non includono un grosso livello di dettaglio né nelle procedure indicate per legge, né nella categorizzazione e nella descrizione dell'implementazione. Il lavoro della Hathaway[287] si riferisce

[286]Vedi capitolo 5

[287] Hathaway, M (2013) *Cyber Readiness Index 1.0,* Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge

proprio a questo problema, l'autrice, infatti, non analizza le strategie bensì i pareri degli esperti (nazionali ed internazionali) sulle funzioni reattive nazionali. Partendo dall'idea che "*no country is cyber ready*"[288] , crea un indice di *cyber readiness* che considera i livelli di preparazione di trentacinque diversi paesi, tenendo in considerazione cinque elementi cruciali:

- La pubblicazione di una Strategia Nazionale e il modo in cui è articolata;
- L'esistenza e l'efficienza del *Computer Emergency Response Team* (CERT) e del Computer Security Incident Response Team (CSIRT) nazionali;
- La lotta al cyber-crimine;
- I meccanismi di *information sharing* interni;
- Gli investimenti nel settore dello sviluppo della sicurezza informatica, intesa in senso ampio.

Dall'analisi di questi punti fondamentali la Hathaway ha scoperto numerose fragilità nei modelli incrementati dai singoli Stati, alcune delle quali saranno parte della proposta qui avanzata per creare un ecosistema coerente per la difesa cibernetica. Infatti, come si è visto per la Strategia Nazionale, non è sufficiente creare un organo perché questo diventi efficacemente operativo, bisogna che risponda a determinati criteri. Così per il CERT, perché abbia davvero delle funzioni utili alla carica che ricopre, quest'organo deve essere in grado di traslare le minacce imminenti in piani di analisi a lungo termine. Inoltre deve avere dei piani precisi di comportamento, con distribuzione dei ruoli e programmazione delle azioni in caso di scenario di emergenza. Deve inoltre essere costantemente tenuto in operatività e capace di ammodernarsi in maniera autonoma. Infine deve essere in grado di svolgere la funzione di coordinazione delle varie entità nazionali in caso di minaccia, ma anche in scenari pacifici e non rischiosi. Quest'ultimo

[288]Ibid p. 1

punto si ricollega perfettamente con la quarta caratteristica, che è la necessità di adottare dei meccanismi di condivisione delle informazioni, affinché tutti i settori siano equamente protetti e i problemi riscontrati in un settore siano di aiuto agli altri. Una minima parentesi qui va aggiunta sulla questione della classificazione di informazioni e la possibilità che settori civili possano essere resi partecipi di una frazione di quelle informazioni segrete che però interagiscono con la funzione svolta dal cittadino in quel momento (i.e. il responsabile di una infrastruttura considerata critica per il paese). È questo un punto cruciale che sarà analizzato in profondità quando si parlerà dei due casi specifici di Israele e dell'Estonia, per il momento basti sapere che è preferibile che esista un meccanismo che elevi progressivamente determinate personalità fondamentali per le funzioni di gestione e protezione delle infrastrutture, alla conoscenza di informazioni segretate. Infine, per quanto apparentemente veniale è necessario menzionare la questione finanziaria: le attività legate alla sicurezza cibernetica devono essere sostenute tramite il giusto ammontare di risorse, sia a livello nazionale sia a livello privato; il governo deve investire nelle università e direttamente nel settore tecnologico interno perché, come si vedrà, oltre a preservare la sicurezza nazionale, ha degli indiscussi ritorni economici.

Le conclusioni a cui arriva la Hathaway sono estremamente rilevanti per la nostra analisi, in quanto collega direttamente la questione della sicurezza informatica al benessere economico. Certo è che i Paesi più avanzati dal punto di vista della *cyber-security*, sono anche più ricchi e sviluppati, perché possono permettersi di investire di più in quel settore, che dal punto di vista di paesi meno prosperi, può essere considerato un vezzo più che una necessità, Invece la Hathaway, attraverso la comparazione di statistiche *dell'International Telecommunication Union* e del *World Economic Forum*, ha scoperto che, oltre una determinata soglia l'investimento nelle tecnologie informatiche, in particolare di sicurezza, potrebbe significare rendimenti di scala sia perché diminuiscono le perdite sistemiche dovute a frodi e danni, sia perché la specializzazione in un determinato campo favorisce

il commercio internazionale e la cooperazione, la quale a sua volta facilita il benessere economico e l'acquisizione di competenze per migliorare ulteriormente il sistema. Si vedrà, quando si studieranno i due casi proposti, che quando lo Stato favorisce questo tipo di interconnessione sia a livello interno (tra industria e Difesa), sia a livello internazionale (tra imprese di diversi paesi, i.e. la collaborazione tra *start-up* italiane e israeliane) il beneficio è duplice: in termini di efficienza della sicurezza e in termini di benefici economici. Inoltre, tralasciando il caso di Israele, lo studio dimostra comunque che i paesi con un impianto strategico più completo e onnicomprensivo sono quelli che rispondono in miglior maniera alle minacce del cyber-spazio. Lo studio presentato da Hathaway è estremamente efficace per la presente trattazione in quanto mostra come un approccio olistico nella concezione della sicurezza informatica sia essenziale e come questo debba considerare allo stesso livello tutte le componenti della sicurezza cibernetica: la coordinazione tra le agenzie interne, la cooperazione internazionale, gli incentivi economici per facilitare la sicurezza nel settore privato e la necessità di diffondere con forza il messaggio della sicurezza informatica alla cittadinanza.

Un altro studio estremamente interessante e molto utile per il nostro scopo è quello condotto nel 2012 da Mc Afee e dalla *Security & Defense Agenda*[289]. In questa elaborazione, le due istituzioni fondono le diverse aree di esperienza e analizzano i trenta paesi più avanzati al mondo e li comparano misurando le loro capacità offensive (reali o presunte), la loro abilità nel proteggere i sistemi infrastrutturali di controllo legati a SCADA, la sicurezza di tutta la catena di supporto di Internet, il ruolo delle entità governative e la capacità di adottare un approccio di tipo olistico alla questione della sicurezza cibernetica.

Nonostante siano molti i soggetti internazionali che si occupano di *cyber-security*, gli unici due che hanno adottato dei testi di tipo strategico in materia sono la NATO e Unione Europea, i quali hanno trasposto in ambito cibernetico aspettative, modalità e obiettivi delle due organizzazioni. È di particolare interesse la situazione dell'Unione

[289]Grauman B. (2012) *Cyber-security: The vexed question of global rules*

poiché la sua strategia è complessa e ben strutturata, nonostante il focus sia posto sulla salvaguardia degli interessi economici. Come spiega chiaramente Tordjman N. (2012) nel suo elaborato di tesi magistrale[290], è un ottimo modello di *governance*. Infatti, esistono numerosi centri che si occupano di minacce cibernetiche, da diversi angolazioni, ma ognuna di esse ha possiede una funzione specifica, disciplinata precisamente dai regolamenti europei: i*nfo sharing,* cooperazione e sviluppo sono sotto la supervisione della Commissione Europea. La commissione ha il compito di favorire attività volte a: (1) *preparedness* e prevenzione; (2) rilevamento e risposta; (3) recupero; (4) cooperazione internazionale; e (5) proporre criteri di CIIP per le infrastrutture europee. Dal 2004 la Commissione ha per altro costituito la European Network and Information Security Agency (ENISA), la quale è diventata il centro di riferimento per la sicurezza cibernetica in Europa.

3.5 Il modello (eco)sistemico di difesa

Dopo aver analizzato in profondità la caratteristiche, gli attori e le modalità della *national cyber security* è ora il caso di ampliare la visuale ponendo le basi di quell'ecosistema difensivo di cui si è accennato durante tutta la trattazione e che verrà riproposto quando si eseguirà la descrizione dei *cyber* approcci di Israele e Estonia.

Quando si parla di ecosistema[291] cibernetico è necessario considerarlo esattamente secondo il concetto derivato dalla biologia: un ambiente di cui fanno parte attori, le interazioni tra questi e le interazioni tra attori e l'ambiente. Nello specifico, per descrivere l'ecosistema è quindi necessario non solo analizzare gli attori che compongono l'ambiente cibernetico e le loro azioni, ma bisogna considerare come questi attori interagiscono tra loro, qual è il livello di competizione/cooperazione e come si presenta il più ampio scenario sociale in relazione alla questione cibernetica. È stato questo lo scopo

[290]Tordjman N (2012) "Facing Virtual Reality – European Union's Response to Threat from the Cyber World", H. Heine Institute of Dusseldorf

[291]Vocabolario Treccani: http://www.treccani.it/vocabolario/ecosistema/

dei capitoli precedenti: delineare lo scenario interattivo all'interno del dominio cibernetico. Ora, poiché lo scopo della trattazione è considerare la dimensione difensiva, è necessario sintetizzare le variabili viste in questo capitolo, così da fornire un quadro semplice e chiaro di riferimento.

Per fare questo, una prima importante operazione da compiere è l'analisi dell'espansione della dimensione sociale alla questione della difesa cibernetica. Se infatti come si è detto, vi è la necessità di formare un sistema difensivo che trasbordi la dimensione militare e intraprenda un costruttivo rapporto delle Forze Armate con il settore civile e, persino, con il settore dei privati (non limitato alle imprese produttrici di componenti per i sistemi d'arma), è necessario descrivere secondo quali modalità ciò avviene, se le interazioni sono istituzionalizzate o rispondono solo a criteri di consuetudine e infine se i meccanismi sopra descritti trovano una reale applicazione nel modello.

Declinare l'idea di ecosistema alla dimensione difensiva significa considerare le risultanti di un'organizzazione sociale sotto una determinato gruppo di caratteristiche, che possano aiutarci a individuare in primis le risposte alle domande: quali sono i fattori sociali che favoriscono questa risultante? Sono peculiarità nazionali o contingenze generiche? Quali sono le conseguenze di un suddetto contesto sociale o istituzionale? In secondo luogo da un punto di vista più ampio si può anche giungere alla risposta di ulteriori domande: Quali sono i suoi punti di forza e le sue debolezze? Quali lezioni si possono apprendere?

Il concetto di ecosistema cibernetico è stato inserito nell'arena della difesa cibernetica nazionale dagli Stati Uniti da pochissimi anni[292], con una connotazione fortemente tecnica: il concetto considerava futuri *cyber-devices* con *"innate capabilities that enable them to work together to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices,minimize the consequences of attacks, and recover to a trusted state"*. L'unico punto saldo che deriva da questa definizione resta proprio quello della definizione del termine, mentre la

[292]DHS, *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Actio*n." Washington, DC: Depart. of Homeland Security, Mar. 23, 2011

prospettiva è stata cambiata profondamente. Dai numerosi studi pubblicati dal Centro di Eccellenza della NATO di Tallinn è possibile derivare alcuni concetti fondamentali così anche dalle interpretazioni di tecnici e uomini politici da me incontrati durante la mia permanenza in Israele.

Innanzitutto un ecosistema per essere tale ed avere un buon funzionamento deve essere coscientemente gestito. Ognuno deve svolgere le proprie mansioni e deve esserci una comunicazione continua, non secondo modalità gerarchica, ma una vera e proprio rete magliata (*web*) di interconnessioni. Si è visto, come vi siano molti punti deboli nella possibilità di comunicare, ma le necessità di minaccia attuali rendono necessario un ecosistema difensivo con caratteristiche caleidoscopiche: **multisettoriale,** multidisciplinare e multidimensionale. È solo unendo le capacità, le conoscenze e le competenze di tutti gli attori che si possono fronteggiare i pericoli provenienti dalla rete. Per **multidisciplinare** invece si intende la capacità di condurre tutta una serie di operazioni sopra descritte[293], mantenendo il controllo della situazione attraverso un centro di raccolta con funzioni di supervisione. Inoltre, è solo con un approccio **multidimensionale** che si può ottenere un effetto di resilienza soddisfacente, in cui rischi e opportunità vengono bilanciati nel breve e nel lungo periodo.

Affinchè questo scenario sia plausibile è però necessario lavorare intensamente sulla mentalità, sulla percezione della minaccia e sull'intenzione di difesa. Non sarà certo il cyber-spazio a consolidare la responsabilità sociale, ma i governi possono puntare sulla massiccia dispersione di utilizzo delle reti e delle tecnologie informatiche per convogliare messaggi alla popolazione, insegnando pratiche basilari di utilizzo, igiene e sicurezza. In questo senso, il Tiger Leap estone è un perfetto esempio di come può essere condotto un fenomeno di questo tipo.

L'altra caratteristica su cui è necessario puntare, principalmente nella comunità che si occupa direttamente di sviluppo tecnologico e difesa, è la **flessibilità**. Flessibilità che significa resilienza, anche nel

[293]Tra cui: condivisione di informazioni, produzione legale, ricerca e sviluppo, commando, *command & control*, esercitazioni.

senso di saper cambiare approccio difensivo qualora ce ne fosse la necessità. Flessibilità che significa capacità di seguire un andamento non lineare nello sviluppo dei prodotti informatici. Ma anche flessibilità nella strategia difensiva, che non può essere statica e passiva, ma deve essere proattiva e basata sia sulla capacità di rilevare minacce ma anche di fare in modo che non arrivino a colpire parti importanti di sistema. Semplificando con un'immagine, è come se invece di avere un muro di cinta, il firewall si trasformasse in una struttura mobile e modificabile capace di cambiare costantemente la geografia dello spazio difeso. Come si notava prima, la difesa nel cyber-spazio ha il grande vantaggio del territorio e, attraverso le possibilità tecnologiche offerte dallo sviluppo continuo, si deve sapere mettere in atto una modalità difensiva il meno prevedibile possibile, così da (tentare di) ribaltare le capacità offensive. Secondo l'analisi di Geer, lo scopo della difesa dovrebbe essere quello di creare un ambiente unico che l'attaccante non ha mai visto prima. Questa operazione –costante- richiede immaginazione, creatività e la messa in opera di sotterfugi[294]. Questa caratteristica però non deve essere limitata al puro tecnicismo, ma dovrebbe diventare un'attitudine al problema: motivare la ricerca, essere la base delle esercitazioni e la modalità di *governance* da parte delle istituzioni. L'esempio estone ancora una volta dimostra come queste non siano solo parole, ma che grazie ad un adeguato e costante programma di insegnamento e sostegno, determinate forme di pensiero possano essere trasmesse a larghe fasce della popolazione. Per lo stesso scopo ci è utile l'esempio dell'industria hi-tech israeliana, che è diventata leader nel mondo grazie alla capacità di adattamento al problema e pensiero tecnologico *out-of-the-box*, vero pilastro di tutto il settore della Difesa israeliano, a partire dagli addestramenti dell'Unità 8200.

Infine, per fare un ultimo appunto, è necessario che la proposizione di un *ecosistema* non rimanga una dichiarazione scritta da compiere con condizionamenti interni o internazionali. Se, infatti, la fase dell'implementazione non risulta essere altrettanto seria che quella di

[294]Geers (2001b) p. 23

teorizzazione, l'idea stessa di ecosistema fallisce, così come accade per le strategie cibernetiche di alcuni paesi che sono state pubblicate ma il loro seguito in termini di implementazione è stato quanto mai vago e impreciso.

Per concludere, verranno ora presentati i due *ecosistemi* da me vissuti ed analizzati nei quali è possibile riscontrare tutte le caratteristiche, con le loro connotazioni positive o negative, elencate sino ad ora nell'analisi teorica. Israele ed Estonia sono due paesi che hanno fortemente investito sullo sviluppo e sulla sicurezza cibernetica, per questo sono stati da me scelti per un'analisi ravvicinata dei rispettivi modelli. Lo studio non sarà necessariamente comparativo nella sua globalità, ma la possibilità di osservare come due società differenti involucrate in realtà distinte siano state capaci di ricreare dei modelli altamente efficienti in termini di capacità difensive e *readiness*, può aiutare a chiarire alcuni caratteri fondanti della sicurezza cibernetica, come il rapporto con i settori non governativi e la necessità di investimento. Inoltre un breve excursus storico e sociale di entrambe le realtà mi ha aiutato a ripercorrere le linee logiche che hanno portato i due paesi a raggiungere il livello odierno. Questo non deve lasciar credere che la mia interpretazione sia meramente deterministica, anzi, questo lavoro vuol anche servire a sottolineare le infinite possibilità contemplabili nell' evoluzione del cyber-spazio.

4.

E-STONIA

"I would not consider it an exaggeration to say that "e" has put Estonia back on the world map. Living in a small country with limited resources, the pressure to make public administration as efficient as possible forced our Government to look for opportunities to take advantage of modern technology and turn Estonia into eEstonia."

— Meelis Atonen, precedente Ministro degli Affari Economici e delle Comunicazioni estone

Introduzione

L'Estonia è un piccolo paese baltico che confina con la Russia. La sua rilevanza geopolitica sino a pochi anni fa era limitata alla considerazione che Unione Europea e NATO davano al processo di allargamento verso est. Oggi, grazie a uno sviluppo nel settore della difesa informatica senza paragoni in Europa, può vantare di essere la sede del più specializzato centro di ricerca d'Europa in materia di *cyber*-security, di essere l'unico alleato degli Stati Uniti ad aver siglato con loro un'alleanza formale in materia di sicurezza cibernetica e di avere un ecosistema di difesa cibernetico invidiato dal mondo.

Questo capitolo si prepone l'obiettivo di descriverlo e di mostrare i suoi punti più rilevanti.

4.1 Come Estonia è diventata E-stonia

Quando si parla di Estonia, che si faccia riferimento a dinamiche sociali, economiche o politiche, non si può prescindere dal considerare l'ubicazione geografica e le effettive dimensioni del paese. La Repubblica di Estonia (in estone *Eesti Vabariik)*, è un piccolo paese

della regione del Baltico occidentale. I suoi territori si estendono per circa 45 mila km^2 e la sua popolazione è di appena un milione e trecento mila persone (l'equivalente di una piccola metropoli). Il paese si affaccia a nord sul mar Baltico così come Lituania, Svezia, Russia e Finlandia, mentre per terra confina a sud con la Lituania e, soprattutto, a est con la Federazione Russa.

Dopo cinquant'anni di inclusione nell'Unione Sovietica, la principale preoccupazione in politica estera della Repubblica dell'Estonia è mantenere l'indipendenza dall'odierna Federazione Russa[295], che pur non esercitando mire dirette sul minuscolo vicino baltico, resta la sua preoccupazione principale. Perciò, a partire dalla celebrata *singing revolution*[296] il maggiore cruccio estone è stato quella di mantenersi indipendente e capace di autodifendersi.

"Estonian leaders did not trust Russia. In the winter of 1991, the Soviet Union, unwilling to accept the Baltic states' pursuit of independence, used violence in the hope of "taming" the Baltic republics. Russian Special Forces killed civilians in outbreaks of violence in Vilnius and Riga. These events had occurred before Estonia regained independence, and before the ultimate collapse of the Soviet Union".[297]

Queste necessità, però, si sono scontrate con la cronica mancanza di risorse e personale specializzato. Per questa ragione è stato necessario ideare un programma che razionalizzasse al massimo le spese e l'impiego di uomini. Lo sviluppo delle tecnologie informatiche è legato proprio a questa necessità, e anche a una concezione in qualche modo patriottica e autoreferenziale, per la quale gli estoni non sono stati disposti a svendere il valore del proprio paese, ricercando gli investimenti stranieri e abbassando il costo del lavoro. Bill Waddel descrive così la scelta estone di sviluppo economico dopo l'indipendenza:

[295]Park, "Russia and Estonia security dilemma"

[296] Per maggiori informazioni sulla "singing revolution" consultare: http://www.singingrevolution.com/cgi-local/content.cgi?pg=3&p=19

[297] Kaldas, K.H.(nd) *The evolution of estonian security options during the 1990s,* tesi di Laurea Magistrale Università di Tartu. Consultabile*:* http://www.ut.ee/ABVKeskus/sisu/publikatsioonid/2006/pdf/ESTsecur.pdf ultimo accesso 28.02.2014

"Estonia came out from fifty years or so of Nazi, then communist oppression, but unlike most of their Eastern Block neighbours they did not set out to become a cheap labour source for Western Europe. They set out to become a high value source of stuff. With free markets, a flat tax scheme (that has steadily decreased), and commitments to supporting education and technology, they became an incubator for outfits"[298]*.*

Gli investimenti e lo sviluppo informatico hanno costituito scelte azzardate, ma in qualche modo necessarie per la crescita dell'economia. Secondo quanto si legge nella descrizione dell'Estonian Information System's Authority[299], inoltre, la volontà di ricerca di libertà personali ha favorito lo sviluppo delle tecnologie informatiche, viste ancora oggi come eccellenti mezzi per esprimere opinioni e ricercare conoscenza.

"We use information technology as an instrument for increasing administrative capacity and ensuring an innovative and convenient living environment for citizens. That is a lifestyle that values simplicity, speed, comfort and economic savings. Therefore the keywords behind the development of e-State in Estonia are sustainable development and high-quality environment"[300]*.*

Come spesso accade, i precursori dello sviluppo sono stati i privati, per ottimizzare il profitto. In particolare, si deve alle banche, veri pionieri degli *e-services* la prepotente intrusione del mondo informatico nelle vite degli estoni. La scelta operata dai principali istituti creditizi presenti sul territorio è stata, come detto, legata principalmente a necessità di guadagno, ma si è strutturata in modo da formare una solida base per la cooperazione nella difesa delle infrastrutture e nella creazione di *networks* votati all'*information sharing*. È Rain Ottis, oltre che la stessa RIA, ad analizzare questa dinamica. Secondo lui, la necessità per la banche di creare una rete informatica sicura, capace di

[298] Waddell, B. (2011*) That's What I'm Talkin' About*
http://www.evolvingexcellence.com/blog/2011/01/thats-what-im-talkin-about.html#ixzz2pKNLKSrG
[299] in estone *Riigi Infosüsteemi Amet*, d'ora in poi RIA (www.ria.ee)
[300] Estonian Information System's Authority; "Facts about e-Estonia" a
https://www.ria.ee/facts-about-e-estonia/

guadagnarsi la fiducia dei clienti, era persino maggiore della naturale tendenza alla competizione. Per questa ragione vi sono stati intensi contatti e una proattiva collaborazione tra i diversi istituti bancari[301], che secondo lo stesso Ottis sono stati alla base di molte delle dinamiche di protezione delle reti informatiche e di condivisione delle informazioni rilevanti per la sicurezza cibernetica.

Sono stati però impegno e fondi statali a creare il modello di *e-State* che ha reso l'Estonia un esempio unico al mondo[302]. Questa peculiarità ha rappresentato la sua fortuna perché, oltre a snellire la gestione amministrativa[303], ha riversato nelle casse del Paese un'ingente quantità di risorse, in parte per via di agevolazioni fiscali e facilità d'investimento garantite dal governo estone, in parte perché grandi e potenti nazioni hanno osservato lo sviluppo delle infrastrutture estoni come un banco di prova per la resilienza delle componenti informatiche. L'ex Primo ministro Mart Laar commenta così questo processo: "*The key message we can teach is that e-government is not only making governance more effective and transparent, but it gives the possibility to develop a real partnership between the government and people*".

Così, negli anni 90 il Paese fu immerso in un processo olistico volto a creare un paese capace di facilitare la gestione amministrativa e dei servizi, attraverso alle possibilità offerte dal nuovo dominio di interazione: il cyber-spazio. I progetti, iniziati alla fine del secolo, sono stati in gran parte operativizzati a partire dal nuovo millenio e comprendono "*e-voting, e-ID, e-taxation, e-health, e-signature, e-learning"*[304]*.*

Un progetto in particolare merita di essere spiegato in maniera più ampia: il cosiddetto *X-road*, la "*backbone of e-Estonia (…) the invisible yet crucial environment that allows the nation's various e-services databases, both in the public and private sector, to link up*

[301]Va detto che questa pratica era allora illegale,

[302] http://www.youtube.com/watch?v=egH4lGDvMCE

[303] Mihkel Tammet parla di uno studio, pubblicato solo in estone, nel quale si evidenzia come le funzionalità informatiche-e la loro efficienza- facciano risparmiare ad ogni cittadino estone due settimane di lavoro ogni anno.

[304]rimando al sito http://e-estonia.com/e-estonia/how-we-got-here per una spiegazione precisa e ampia del processo di informatizzazione della pubblica amministrazione.

and operate in harmony"[305], il sistema che permette l'interazione dei vari database legati alle diverse funzionalità cibernetiche[306]. E' straordinariamente ben strutturato perché non è rigido (si possono collegare tutte le agenzie che offrono servizi informatizzati, sia governative che private); è decentralizzato (non esiste un unico gestore del servizio e dei *databases);* il livello di sicurezza è decisamente alto grazie alle capacità di *encryption* e *decryption* (considerando l'elevato numero di sever interconnessi) e allo stesso tempo è capace di integrare tutti i sistemi informatizzati in maniera efficiente e funzionale.

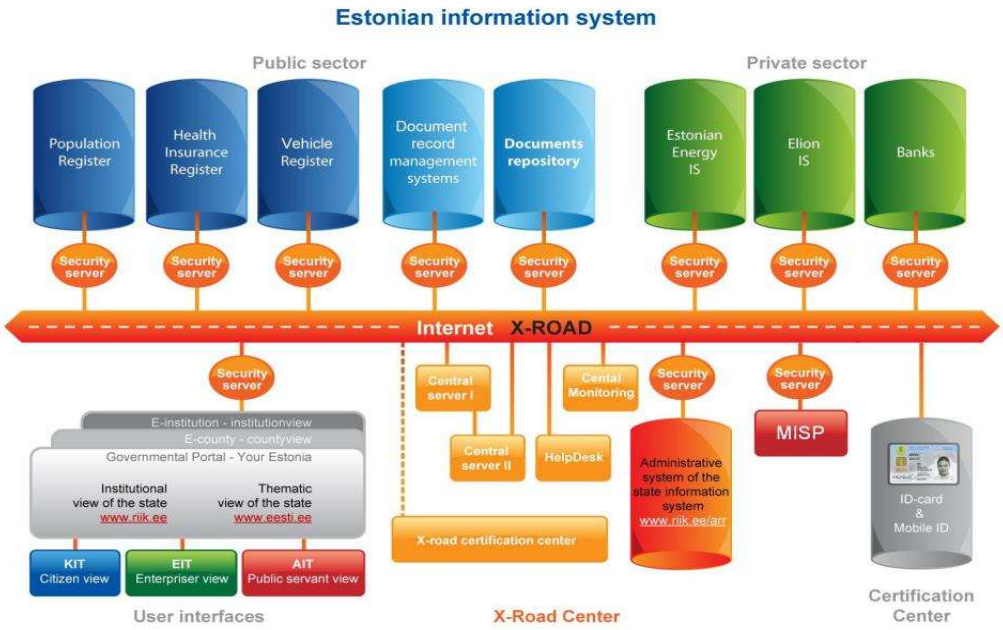


Figura 3: Struttura del sistema X-ROAD

Inoltre, va dato il merito ai policy maker estoni di aver portato avanti un processo parallelo di istruzione della comunità, chiamato *Tiger Leap*[307]*,* attraverso il quale gli enti governativi hanno messo in piedi un programma di sensibilizzazione e di educazione di tutte le parti della società civile, offrendo corsi gratuiti per migliorare le capacità individuali in ambito informatico. Le scuole sono state rinnovate e dotate non solo

[305]Per maggiori informazioni sul progetto X-road rimando al seguente sito: http://e-estonia.com/components/x-road
[306]Per affrofondimenti: http://estonianworld.com/technology/starting-scratch-case-e-government-estonia/ e http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf ultimo accesso 28.02.2014
[307]Per un approfondimento sui benefici del programma si veda http://lencd.com/data/docs/186-Bk3PartB_ESTONIA%20Tiger%20Leap.pdf ultimo accesso 28.02.2014

di macchine ma anche di accesso a internet, e coloro, che per età o per scelta propria erano allora lontani dal mondo dei computer e dell'informatica, hanno potuto appuntarsi a corsi gratuiti proposti dal governo. Particolare importanza è stata ovviamente data alla comprensione delle pratiche necessarie per garantire la protezione individuale, di dati e dei sistemi che si utilizzano: la cosiddetta, *pulizia informatica.* È infatti questa, apportata alla dimensione cibernetica, la prima e principale pratica di difesa nazionale considerata nel *Total Defense Concept:* "each man"[308] deve essere in grado di proteggere se stesso e in questo caso, il proprio computer (e smartphone!).

4.1.1 Dipendendenza e vulnerabilità

Ad una così alta dipendenza dalle componenti tecnologiche corrispondono due *outcome* opposti e paralleli. Da una parte i vantaggi crescenti, capaci di agevolare nuove economie di scala e potenzialmente infinite opportunità; dall'altra, un elevato livello di elasticità e di inter-comunicazione apre una serie infinita di vulnerabilità nei sistemi collegati in rete. Come sottolineano sia gli studiosi[309] che i protagonisti dell'epoca, come ad esempio Rain Ottis, la ragione per cui nel 2007 vi fu un tentativo di attacco informatico fu l'elevata rilevanza che avevano le infrastrutture informatiche sia per lo svolgimento della vita pubblica estone che per il mantenimento della sicurezza nazionale.

Come ricorda James Thomason[310], dipendenza, rischio e vulnerabilità sono tre dinamiche intrinsecamente collegate. Per il ricercatore di Studi Navali Americani la dipendenza è definita come la predisposizione alle perdite in utilità*,* il rischio come la probabilità che le perdite vengano inflitte, e la vulnerabilità come il valore atteso delle potenziali perdite delle suddette utilità*.* Perciò, intuitivamente la vulnerabilità è direttamente proporzionale alla dipendenza e la probabilità di rischio aumenta proporzionalmente alla crescita di

[308] Vedi dopo

[309] Eneken Tikk , Kadri Kaska, Liis Vihul (2010) "International cyber incidents. Legal considerations"; Cooperative Cyber Defence Centre of Excellence (CCD COE); http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[310] Thomason, J (1981); "Dependence, risk,and vulnerability"; Professional Paper 307 http://www.cna.org/sites/default/files/research/5500030700.pdf

dipendenza e vulnerabilità. Così accade anche per i sistemi, i *networks* e le infrastrutture gestite tramite reti informatiche.

La citazione dell'ex Ministro degli Affari Economici e delle Comunicazioni a inizio capitolo rappresenta solo una parte dei risultati ottenuti dal consistente sviluppo telematico e informatico. Come ricorda Soumitra Dutta[311], i problemi e le vulnerabilità sono ancora molti e devono essere risolti, sia per mantenere la competitività internazionale nella leadership della *e-government*, sia per limitare la possibilità di futuri attacchi come quelli accaduti nel 2007.

4.2 L'attacco del 2007. Le ragioni e le conseguenze

4.2.1 Rilevanza

Non c'è testo di analisi o articolo giornalistico che parli di cyber-*warfare, security o power* che non citi l'episodio estone come uno dei momenti più importanti nella storia del cyber-spazio. Così come non esiste scettico che non neghi la rilevanza dell'episodio. Persino Thomas Rid[312], accanito "negazionista" della possibilità di una *cyber-war* analizza nel dettaglio gli eventi della primavera 2007 in Estonia. È inevitabile parlarne, in quanto si è trattato di una situazione nuova nello scenario geopolitico mondiale. Non il concetto di infiltrazione in un sistema informatico o il tempestare di messaggi, informazioni e quant'altro i server per sovraccaricarli. Bensì, la combinazione di queste azioni insieme alla motivazione politica, che si è dimostrata superiore a quella di semplici *hacker* o *hacktivists.* L'ombra della volontà russa dietro gli attacchi è da subito stata un'idea fissa per gli uomini politici estoni, così come per gran parte degli osservatori internazionali. La combinazione di questo episodio, con le dinamiche della guerra in Georgia, hai poi forse fugato ogni plausibile dubbio.

[311] Dutta, S. (2007) *Estonia: A Sustainable Success in Networked Readiness*? consultabile http://www.weforum.org/pdf/gitr/2.1.pdf ultimo accesso 28.02.2014
[312] Rid (2011) op. citata

Se non i governanti o gli uomini d'armi, l'opinione pubblica si è trovata di fronte ad uno scenario nuovo, in cui tutte le più fantasiose idee delle correnti letterarie fantascientifiche (e della cinematografia *cyber-punk*) sembravano improvvisamente prendere piede. Sponsorizzate dalla volontà degli Stati nazione di combattersi l'un l'altro all'interno di un altro dominio militare, meno violento, più oscuro e più indicato a infierire ferite non mortali agli avversari geopolitici, così da risultare meno condannabili agli occhi della comunità internazionale. Sebbene, fossero pressoché vent'anni che Stati Uniti, Russia e i principali attori dell'arena internazionale stavano studiando le possibili implicazioni belliche dei network informatici, l'episodio estone, con la commistione di elementi rudimentali e nazionalistici che l'hanno contraddistinto, ha impersonato perfettamente il momento in cui tutto sembrò decollare.

In effetti, se riconsideriamo la descrizione fatta da Douhet[313] del rapporto tra tecnologie e mondo militare, è inevitabile non notare come l'attacco all'Estonia abbia prodotto a livello internazionale un passaggio chiaro dal secondo al terzo *step*: il profondo interesse per la materia. Il quale è cresciuto in seguito agli avvenimenti in Georgia e successivamente in Iran (i.e. Stuxnet a Natanz), ma è di certo nato a Tallinn, nel momento in cui un gran numero di hacker, più o meno indipendenti, ha deciso di punire l'Estonia e il suo governo per aver rimosso il *Bronze soldier* dalla storica e centrale collina di Toompea.

4.2.2 Il background politico

Gli avvenimenti della primavera del 2007 hanno un'origine politica che va ricercata nello scontro con il gigantesco vicino russo. Una volta ottenuta l'indipendenza, infatti, Estonia ha intrapreso un necessario processo di rilettura del passato e costruzione di un'identità nazionale, che in parte ha compreso (e comprende) sentimenti anti-russi. Nella dialettica di stato, la Russia, durante gli anni Novanta è passata dall'essere la liberatrice dal giogo nazista alla tirannica

[313]Vedi cap. 2

usurpatrice della libertà, che per più di mezzo secolo ha ostruito violentemente la volontà di auto governo del popolo estone. Gli eventi del 2007 si inseriscono in questa dinamica. Infatti, all'origine dell'attacco informatico vi è la rimozione da parte del governo estone di una celebre statua, icona degli sforzi dell'Unione Sovietica durante la Seconda guerra Mondiale. Il Milite Ignoto, chiamato anche *Bronze Soldier, che* durante il dominio sovietico rappresentava l'unanime sforzo compiuto per sconfiggere il nemico germanico, negli anni successivi all'indipendenza, aveva finito col diventare il simbolo dell'oppressivo governo sovietico[314].

Nel marzo 2007, la sopracitata statua è diventata il fulcro del dibattito elettorale nel parlamento estone e persino il presidente Toomas Hedrik Ilves espresse la sua volontà di lasciare alle spalle il passato sovietico, rimuovendo la statua dal centro storico e ricollocandola in un cimitero di guerra ai bordi della città. Da parte russa, la questione stava diventando fastidiosa, ma si optò per non interferire direttamente nella vicenda. Si arrivò così, il 26 aprile 2007, alla rimozione della statua, evento, che, lasciate da parte le molte dichiarazioni provenienti da Mosca, aveva avuto sino a quel punto i connotati di una riforma interna dell'identità nazionale. L'azione però, provocò reazioni sia da parte dell'ampia minoranza[315] russa presente nel paese sia del Cremlino. Le strade di Tallinn si riempirono di manifestanti, sbocciarono numerosi episodi di violenza e il giorno dopo, allo scoccare della mezzanotte (secondo il fuso orario di Mosca!)[316], cominciò un potente e continuativo attacco attraverso il cyber-spazio dei siti internet delle principali istituzioni e organizzazioni del paese. Cominciarono così la *Bronze Nights*, un episodio che ha cambiato totalmente la concezione internazionale delle minacce cibernetiche.

[314] Andreas Schmidt; "The Estonian Cyberattacks"; Chapter prepared for the edited book The fierce domain – conflicts cyberspace 1986-2012, edited by Jason Healey, Washington, D.C.: Atlantic Council, 2013 http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf

[315] L'Estonia ha una considerevole minoranza etnica russa: su una popolazione di 1,34 milioni di euro, 344 000 sono di etnia russa. (Statistiche: http//:pub.stat.ee/px-web.2001/Dialog/statfile1.asp). Una grande percentuale detiene la cittadinanza estone, parla la lingua estone, e considerare l'Estonia come loro patria. Alcuni sono cittadini della Federazione Russa. Alcuni, tuttavia, considerano il crollo dell'Unione Sovietica un errore storico e desiderano il ripristino del dominio russo sul territorio

[316] per Rain Ottis, oggi docente della Technology University of Tallinn, è stato il primo segnale che fece capire alle autorità la direzione reale da cui provenivano gli attacchi. Inoltre, sembrò un chiaro indicatore del fatto che gli attacchi non erano semplici e singole manifestazioni di protesta, ma erano l'espressione di un piano d'attacco orchestrato a più alto livello

Tabella 1. Attacchi nel periodo 27 Aprile- 3maggio

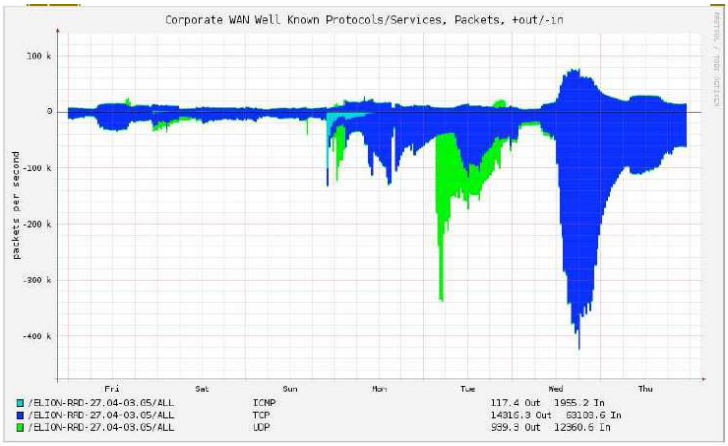


Tabella 2. Attacchi tra il 4 – 10 maggio

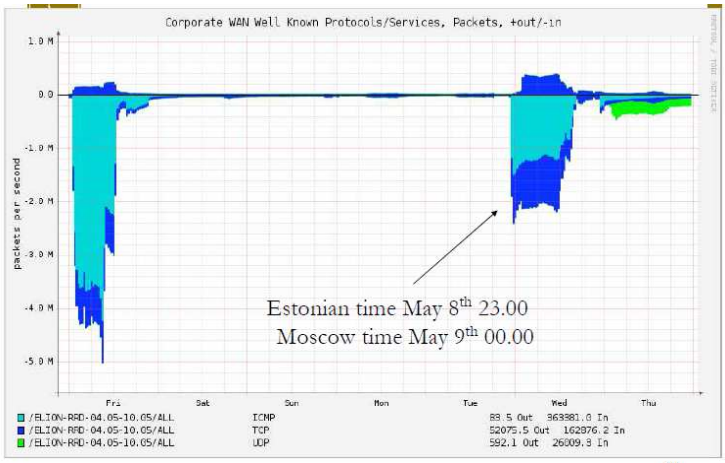
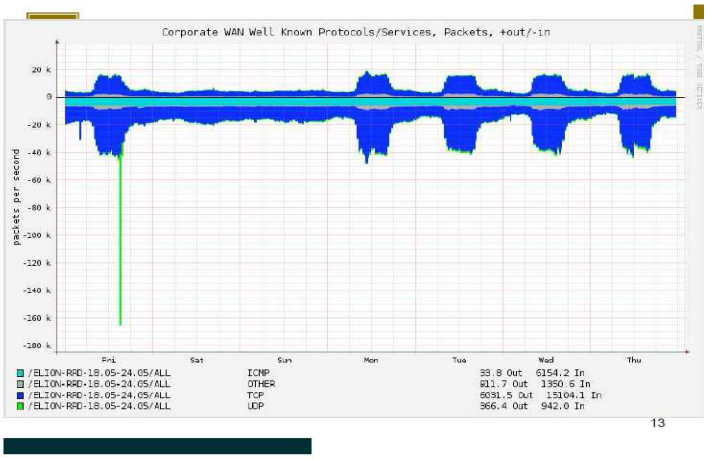


Tabella 3. Attacchi tra il 11-17 maggio



13

4.2.3 L'Attacco sui generis

> *"The attack came from an extermely large number of hijacked computers, up to 85,000; and the attacks went on for an unusually long time, for three weeks (…) The attacks reached a peack on May 9, whene Moscow celebrates Victory Day. Fifty-eight Estonian websites were down at once. The on-line service of Estonia's largest Bank (…) was unavailable for 90 minutes*"[317].

L'attacco, cominciato la notte del 27 Aprile[318], durerà in maniera alternata fino al 18 maggio. Le tipologie di attacco furono per lo più molto semplici, ma molto efficaci. Il concetto di base era quello di creare dei flussi di utilizzo[319] dei portali internet di molto superiori al normale utilizzo (si parla di 10 volte nella prima ondata e quasi 500 nel punto di massima frequenza dell'attacco[320]), in modo da creare disservizi nei siti internet attaccati. Si trattava quindi non di penetrare le banche dati dei siti assaltati ma di bloccare, temporaneamente, la distribuzione di un servizio, intasandolo di spam, di utenze a *cul de sac* e di messaggi provocatori.

Questo tipo di attacco, chiamato *DDoS* (Distributed Denial of Service)[321], è molto diffuso e utilizza dei *botnets,* ovvero una rete di computer infetti (*zombies*), che senza esserne a conoscenza, vengono colpiti da un virus *Trojan* che inserisce nello *zombie* una serie di servizi *Command-and-Control,* i quali forniscono all'artefice dell'attacco la possibilità di agire attraverso il computer infetto, senza che questo se ne renda conto. Questo tipo di Denial of Service si chiama *distributed* perché chi muove l'attacco è in grado di farlo attraverso un'ampia rete di computer distribuiti anche in diverse parti del globo (nel caso

[317] Rid, Thomas (2011) op. citata

[318] Per un approfondimento sulla diatriba riguardo l'inizio dell'attacco cfr. Arrelaid, Kaeo,Evron, paper http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf nota 14

[319] Come si può vedere dal grafico della frequenza, gli attacchi si concentrano prevalentemente nei giorni precedenti al weekend

[320] Nazario, J. (2007) *Estonian DDoS Attacks - A summary to date*. Arbor Networks. May 17th, 2007 Available at asert. arbornetworks.com/2007/05/estonian-ddos-attacks-asummary-to-date

[321] cerca fonte decente http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html

dell'attacco all'Estonia, ad esempio, i Paesi da cui proveniva la maggior parte degli *zombies* e quindi di *botnets* erano Egitto e Stati Uniti[322]).

La maggior parte delle disfunzioni vennero create da DDoS, ma vennero portati a termine anche altre modalità di attacco. Numerosi siti vennero deturpati[323], la quantità di spam inviata per mail e nei forum raggiunse livelli mai visti prima nel paese e, soprattutto, vennero attaccati direttamente i server DNS (Domain Name System)[324] degli Internet Service Provider (ISP), provocando reali disagi ai DNS del paese (anche se per breve tempo), come nel caso dei router di Elion[325].

Durante l'attacco del 2007 gli obiettivi furono specifici e ben ricercati. Il fine iniziale era quello di boicottare le istituzioni e bloccare la distribuzione di informazioni, per questo gli attacchi vennero indirizzati a siti governativi[326] quali: il sito del Governo, del Primo Ministro, del Presidente, del Riigikogu (Parlamento), i siti delle agenzie statali, di tutti i Ministeri e dei più importanti partiti politici.

Vennero inoltre colpiti i siti delle principali testate giornalistiche, Infrastruttre di ISPs, e servizi commerciali. In particolare, i servizi online delle due maggiori banche dell'epoca (Hansapank e SEB Eesti Ühispank che insieme detenevano circa l'80% di tutto il mercato bancario estone) e le interfacce dei siti di gestione delle principali infrastrutture critiche.[327]

Prima di considerare le modalità con cui si svolse la difesa *ad hoc* della rete estone, vanno fatte due precisazioni. Innanzitutto, riprendendo l'introduzione al capitolo, va ridimensionato l'effetto dell'attacco. E' senza dubbio erroneo pensare che il paese fosse completamente bloccato. Nell'arco delle tre settimane in cui si è svolto l'attacco si può parlare al massimo di disagi diffusi. Rain Ottis, ha sottolineato che in molti casi i disservizi sono stati incrementati dalle stesse entità colpite, in modo da eliminare selettivamente parte del

[322] Herzog, S., *(2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, Journal of Strategic Security, 4 (2): 49-60.

[323] Kadri Kaska racconta come numerosi furono i casi in cui comparvero foto del Primo Ministro Ansip con i baffi di Adolf Hitler

[324] Per maggiori informazioni si veda http://en.wikipedia.org/wiki/Domain_Name_System

[325] https://www.elion.ee/eraklient

[326] I dati successivi sono ricavati dal report del CCDCOE sopra citato

[327] Herzog, op. citata p. 71

flusso entrante: è il caso delle *white lists* compilate dalle banche, per evitare l'ondata di richieste provenienti da paesi potenzialmente rischiosi. Per questa ragione la maggior parte degli studiosi sono restii a considerare quello estone come un episodio di guerra cibernetica.

In secondo luogo, però, date le modalità, difficilmente può essere considerato un attacco terroristico o un atto criminale. Non può essere ritenuto un atto criminale in quanto lo scopo ultimo non era quello del guadagno o dell'estorsione. Più complesso è invece il discorso del terrorismo. Infatti se è vero che i singoli attaccanti vennero spinti da una simile ragione politica condivisa, la mancanza di organizzazione centrale, di violenza e l'inesistenza di un programma costruttivo sembrerebbero allontanare la possibilità di considerarlo un attacco terroristico.

L'impostazione diffusa da parte della comunità internazionale, e in particolare di coloro i quali erano a capo della difesa o del governo nel 2007 fu quella di considerare l'attacco come un vero e proprio attacco militare. Nel suo articolo, Thomas Rid, ricorda come Mihkel Tammet, all'epoca incaricato della sezione ICT al Ministero della Difesa sostenne che "*gathering of botnets (is) like gathering of armies*", mentre l'alllora Primo Ministro Andrus Ansip chiedeva quale fosse la differenza tra un blocco navale o aereo appartenenti a uno stato sovrano e invece un blocco delle istituzioni governative. In realtà, però, risulta difficile includere l'attacco estone in uno scenario bellico, dato che, pur ipotizzando un collegamento tra gli hacker coinvolti e il governo russo risulta molto difficile provarlo, e dato lo scarso impatto che ha avuto sulle funzionalità del paese.

4.2.4 La difesa

In base a molti studi e alle testimonianze di coloro che furono protagonisti durante la reazione difensiva nel 2007[328], l'attacco fu molto meno prolifico di quanto avrebbe potuto essere in quanto la difesa

[328] in particolar modo Rain Ottis e Mihkel Tammet

condotta dagli addetti estoni fu tempestiva e provvidenziale. Molti fattori concorsero per far sì che la difesa prevalesse sull'offesa.

Innanzitutto, è bene ricordare che la sofisticatezza degli attacchi soprattutto nella prima parte dell'azione fu abbastanza rudimentale, perciò gli esperti di sicurezza informatica ebbero gioco facile nel renderli inoperativi. Secondo quanto riporta un report prodotto dal Centro di Eccellenza NATO infatti:

"The first attack against government websites was reported to have hit in the late hours of 27 April 2007. (…) Initially, attacks were carried out by relatively simple means, therefore earning the label of "cyber riots". In various Russian-language Internet forums, calls and instructions were presented to launch ping commands (simple commands to check the availability of the targeted computers) with certain parameters on the MS Windows command line. Later on, executable .bat files were made available for users to copy onto their computers and then launch to carry out automated ping requests. This would amount to simple denial of service (DoS) attacks; however, being coordinated, they were effective in disturbing their targets. Attacks were also coordinated via Internet Relay Chat (IRC). Pinging was soon followed by malformed web queries, which were massively used mainly against the websites of the government and media outlets – this already implied the use of more specific means designed for attack. ***As a generalisation, though, the initial attacks on April 27 and 28 were simple, ineptly coordinated*** *and easily mitigated."*[329]

Inoltre, come detto in precedenza, una delle ragioni per cui si sviluppò questo genere di attacco proprio in Estonia fu perché il paese baltico era già all'epoca altamente dipendente dalle componenti IT per la gestione dei propri servizi e dei propri *vital services*[330]. Nonostante, come si è osservato, le funzionalità della rete siano nate e si siano sviluppate con un'attenzione alla sicurezza inferiore al necessario, in Estonia la parabola è stata lievemente differente.

[329]Kaska K., Tikk E. e Vihul L. (2010) *International Cyber Incidents: Legal considerations,* NATO CCDCOE Publication, Tallinn,p 30-31

[330]nomenclatura usata nell'Emergency Act per ampliare la categoria delle Infrastrutture Critiche

Questa differenza fu dovuta alla necessità di protezione, che richiedevano le implementazioni dei servizi informatizzati estoni. Infatti, osservando il percorso affrontato dal Paese nell'ambito dell'informatizzazione[331], è subito chiaro che molte delle funzioni siano *vitali* e la scelta d'informatizzarle non è stata la risultante di un processo di semplificazione bensì una scelta quasi obbligata, indotta dalla scarsità di risorse e dalla mancanza di personale da impiegare nei pubblici uffici. Questo significa concretamente, che non esisteva un vero e proprio *back-up plan* per molti dei servizi offerti (talvolta non esiste ancora oggi) e che la dipendenza critica del paese dalle sue funzioni cibernetiche ha fatto sì che le istituzioni e le imprese coinvolte fossero costrette a prestare molta attenzione alla sicurezza delle proprie reti, ritenute vitali per il funzionamento e la gestione dello Stato.

In particolare, come si è detto, nel 2005 si è inaugurato in Estonia l'e-*voting* (prima a livello locale, e dal 2007 a livello nazionale per le elezioni parlamentari). Questa procedura rese necessario ideare un capillare sistema di controllo sul corretto funzionamento del sistema e sull'effettiva protezione dei servizi dedicati alle funzioni virtuali (il focus del CERT non sarebbe stato solo relativo al voto, ma sicuramente fortemente focalizzato sulla protezione di quest'ultimo). A questo proposito fu creato ad hoc un centro responsabile del monitoraggio del livello di sicurezza e manutenzione dei servizi informatici sensibili e vitali per lo svolgimento del voto elettronico. Il CERT (*Computer Emergency Response Team),* allora composto unicamente da due persone, era sottoposto alla responsabilità di Hillar Aarelaid e dipendente dal governo. Le sue funzioni non erano consultive o di *problem solving* , ma di analisi e interpretazione dei dati. Ovviamente, data la recente nascita dell'organo e la rapidità dell'attacco, nel 2007 il CERT non fu in grado di svolgere a pieno le sue funzioni, ma fu capace di colmare alcuni dei gap d'informazioni e accorciare le distanze tra le diverse fonti dalle quale provenivano informazioni utili. In particolare, mobilitò esperti provenienti da tutti i settori.

[331]Per maggiori informazioni su "e-Estonia" consultare http://e-estonia.com/e-estonia/how-we-got-here

L'attività svolta dal CERT nei mesi precedenti, in vista delle elezioni parlamentari, si rivelò provvidenziale al momento dell'attacco di Aprile. Altri quattro fattori si rivelarono fondamentali per l'immediata reazione delle forze di sicurezza informatica. In primis, così come il dibattito sulla rimozione della statua non era nuovo nell'arena politica estone, allo stesso modo le minacce e le campagne di reclutamento di *low-entity cyber–warriors*[332] non sono nate nelle ventiquattrore successive la rimozione della statua. Le idee sovversive circolavano da molti mesi su numerosi forum in lingua russa. Questo ha facilitato il lavoro delle intelligence, che in molti casi avevano già ben chiaro il tipo di pericolo che avrebbero dovuto affrontare.

Inoltre, lo stesso anno dell'attacco venne stabilito dal Ministero degli Affari Economici e della Comunicazione l'Information Security Interoperability Framework[333] che obbliga imprese private e addetti del settore pubblico a mantenere determinati livelli (standard) in termini di sicurezza informatica[334] *e* ha reso possibile una più semplice comunicazione dei *fails* durante gli attacchi e il rapido scambio di informazioni tra coloro che già avevano iniziato ad adempiere al Framework (il quale sarebbe dovuto entrare in vigore solo l'anno successivo).

Terzo, le minute dimensioni dell'Estonia hanno facilitato la condivisione di informazioni tra individui e istituzioni, situate anche ai poli opposti del paese.[335] In una situazione di novità, la condivisione di informazioni e tecniche efficaci è un fattore fondamentale, e in questo caso la ridotta superficie del paese ha favorito il processo in maniera rapida e vantaggiosa. Sia Rain Ottis che Mihkel Tammet, nel rispondere alle mie domande, hanno fortemente voluto sottolineare come il fattore principale del successo difensivo sia stata una congiunta azione proattiva, legata all'alto livello di cooperazione raggiunto sin dai primi giorni.

[332]Intervista a Mihkel Tammet

[333]Information Security Interoperability Framework, MEAC, 31 gennaio 2007, http://www.riso.ee/et/files/InfoturbeRaamistik.pdf (solo in estone).

[334] Riigi Infosusteemi Amet; (2012) ; "Estonian Security System Overview" https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf

[335]Intervista a Rain Ottis

Quarto, la tendenza estone allo sviluppo di un *Total Defence Concept* ha fatto sì che i cittadini fossero in gran parte pronti ad una difesa di prima istanza. “Each man for himself” è il precetto basilare[336] della difesa nazionale e della preparazione militare individuale. Infatti, considerando l’evoluzione della protezione della sicurezza nazionale, le necessità del paese hanno imposto a tutti i cittadini di essere costantemente disponibili e in grado di far fronte alle più basiche emergenze. Negli ultimi anni, questa pratica è stata implementata includendo le principali pratiche di protezione informatica. L’intero sistema è stato benefico al momento dell’attacco di Aprile 2007, sia per la predisposizione mentale a gestire personalmente la crisi, sia per le competenze specifiche, percentualmente più diffuse rispetto alla maggior parte dei paesi del mondo.

Infine, l’evoluzione storica, statuale e delle alleanze tra i paesi circostanti ha fatto sì che i governanti estoni avessero a disposizione il sostegno di molte entità statali, dei paesi appartenenti all’Organizzazione del Nord Atlantico e dagli alleati classici, Svezia e Finlandia[337] (anche e soprattutto per ragioni commerciali, banche in primo luogo). In particolare con il paese scandinavo ubicato sulla riva più prossima del Mar Baltico le opportunità e le necessità di collaborazione sono molteplici e quotidiane, tanto che secondo Vahur Made, Estonia e Finlandia non sono competitori in materia di sicurezza, anzi l’incremento di sicurezza in un paese corrisponde ad un incremento anche nell’altro: “*This compatibility can be explained by history, geography, and culture. Estonia and Finland share the same (coastal) border, as well as the same ethnic origin*”[338]. Anche in occasione dell’attacco informatico del 2007 il vicino e alleato si comportò in maniera solidale -anche se in parte distaccata.

Per quanto riguarda la NATO, invece l’attenzione si fece subito viva e l’opinione condivisa era: "*Today Estonia, tomorrow, someplace*

[336] Estonia’s new National Defence Strategy (2011) consultabile al sito http://www.kaitseministeerium.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf p 8

[337] CCDCOE p 25 e Herzog ibid p 8

[338] Kai-Helin Kaldas op. citata p.40

else", come disse il portavoce Robert Pszcze[339]. L'attacco spinse la NATO a inviare degli esperti in Estonia, e nel lungo periodo a intensificare la presenza sul territorio estone dando particolare importanza alla questione cibernetica, e velocizzando l'inaugurazione del NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) di Tallinn.

Entrando brevemente in dettagli tecnici, va menzionato che la difesa venne gestita in due modi. In primis, si cercò di allargare la banda dei server del sistema informativo statale e di aumentare la capacità di filtraggio del traffico dei dati. In secondo luogo, la capacità difensiva venne aumentata da sistemi attivi di protezone (firewall, connessioni attraverso molteplici server, bloccaggio degli accessi, ecc), resi possibili dalla cooperazione con gli ISPs: la quantità di dati provenienti dall'esterno diminuì sensibilmente. Per concludere, come detto, la collaborazione internazionale fu di notevole aiuto nella gestione della lunga crisi virtuale.

Infine, molti degli intervistati hanno concluso i loro interventi affermando che gran parte della ragione del successo ottenuto dalla difesa estone fu dovuto ad una fortuita concatenazione di eventi che avrebbe potuto svolgersi in maniera completamente distinta, causando molti più danni al paese.

4.2.5 Conseguenze dell'attacco

L'attacco ebbe importanti effetti sia per il paese *in sé* che per la popolazione, l'economia, l'organizzazione e la percezione delle minacce cibernetiche della NATO. Innanzitutto i problemi economici che causò questa (relativamente) breve crisi furono avvertiti da tutti i settori della popolazione e da tutte le categorie commerciali, dalle più importanti banche alle più svariate imprese di piccole dimensioni. Secondo un'analisi de Centro di Eccellenza NATO a Tallinn, l'attacco cibernetico ebbe un effetto percettibile sul funzionamento dell'economia

[339]Helsingin Sanomat: *Cyber-attacks in Estonia: Finland observes from a distance NATO sent experts to Estonia immediately,* consultabile http://www.hs.fi/english/article/Cyber-attacks+in+Estonia+Finland+observes+from+a+distance/1135227745145

domestica[340], essendo l'economia estone fortemente legata alla componente IT. Non soltanto il carico di lavoro delle tre settimane di attacchi venne irrimediabilmente perso, ma anche la strategia di mercato e l'allocazione delle risorse vennero profondamente riviste all'ottica dell'effetto distruttivo dei cyber-attacchi.

Molto più profonde furono le conseguenze a livello sociale. Come detto, la componente IT nella vita dei cittadini estoni era notevolmente elevata, perciò l'attacco alla maggior parte dei fornitori di servizi offerti dallo Stato, preoccupò non poco la popolazione. La risultante principale fu l'aumento della sfiducia nella relazione telematica con le istituzioni governative, ma anche l'incapacità di svolgere determinate attività in maniera alternativa fu un fenomeno degno di nota. Senza ricadere in un'analisi catastrofista, va sottolineato come in Estonia l'impatto di questo attacco fu proporzionato alla dipendenza che, non solo le istituzioni governative e commerciali, ma anche i singoli individui, avevano rispetto alle componenti cibernetiche di servizi e processi.

Infine, estremamente rilevante per lo scopo della trattazione è stato l'impatto che gli attacchi hanno avuto nella gestione nazionale delle minacce cibernetiche. Senza anticipare i contenuti del prossimo paragrafo, è importante dire che con gli eventi del 2007 gli esperti e i policy makers hanno acquistato una consapevolezza prima inesistente che ha loro permesso di collaborare per migliorare l'approccio nazionale alla sicurezza informatica, soprattutto attraverso l'adozione di una strategia precisa che regolasse comportamenti e responsabilità individuali delle varie istituzioni coinvolte nella protezione di network e infrastrutture informatizzate.

Come è stato detto in precedenza l'attacco ebbe l'effetto di agevolare il processo negoziale tra l'Estonia, la NATO e altri Stati fondatori del Centro di Eccellenza. Sia Mihkel Tammet che Rain Ottis mi hanno confermato che il progetto del Centro era in piedi già da anni[341], ma considerato di basso rilievo. Gli eventi del 2007 mostrarono all'Alleanza come la minaccia di attacchi cibernetici non solo era uno

[340]Kaska et al. Opera citata p 29

[341]Confronta anche cronologia attività CCDCOE: http://www.ccdcoe.org/423.html

scenario futuro su cui investire in termini di difesa e sicurezza, ma che era il caso di agevolare rapidamente il sistema di sicurezza collettiva nel cyber-spazio. Fu così che l'anno successivo venne inaugurato il Centro di Eccellenza (CCDCOE) di Tallinn con il compito di analizzare e studiare approfonditamente[342]: l'ambito legale e la necessità di elaborare politiche efficaci; l'elaborazione di chiari concetti e strategie difensive; l'ambientazione tattica; e la protezione delle Infrastrutture Critiche di Informazione (CIIP).

Dal 2008 il CCDCOE non è solo il principale centro per lo studio delle questioni *cyber* all'interno della NATO ma anche un'importantissima voce in ambito internazionale. La più chiara dimostrazione di questa affermazione è la rilevanza avuta dal "*Tallinn Manual*"[343], pubblicato nel 2013 dal CCDCOE e prodotto da Gruppo Internazionale di Esperti di studiosi internazionali sotto la supervisione di Michael Schmidt, che ha cercato di analizzare come le norme internazionali si possano conformare a questo nuovo dominio di *warfare.*

Per concludere, dal 2010, la NATO ha siglato un accordo con il governo estone[344] per facilitare la collaborazione tra il Paese baltico e l'Organizzazione in caso di un nuovo attacco cibernetico. Questa considerazione verrà ampiamente analizzata successivamente.

4.3 **La Strategia Estone (ECSS): 2008-2013**

Secondo Helena Raud, l'analisi della strategia nazionale è la chiave per valutare la comprensione dello scopo delle minacce cibernetiche da parte dei governi e la loro capacità di mettere in evidenza compiti e priorità[345]. Sicuramente nel caso dell'Estonia, il

[342]Le aree di focus del CCDCOE: http://www.ccdcoe.org/37.html

[343] Schmitt, M.N. ed. (2013) *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge University Press, Cambridge.

[344] Strategy page; "Information Warfare: The NATO Cyber War Agreement" (May 2010) https://www.strategypage.com/htmw/htiw/20100501.aspx

[345]Raud, H. (2012) *Securitization and Governance of Cyberspace –Case study on cyber security policy and public administration capacity in Estonia,* Tesi Magistrale University of Tartu Pag 30

giudizio non può che essere positivo. La strategia è stata proposta da un Comitato diretto da Mihkel Tammet che raggruppava esperti provenienti da tutti i ministeri[346], facenti capo al Ministero della Difesa (MoD). Secondo quando raccontato da Tammet, il lavoro portato avanti dal comitato è stato lungo e difficoltoso, prima di arrivare al risultato finale, infatti, sono stati necessari alcuni passaggi importanti: la definizione di *cyber-warfare,* la categorizzazione delle modalità di identificazione dei responsabili e le misure da applicare e la descrizione dei comportamenti da adottare per assicurare una gestione efficace (quali leggi attuare, quali misure perseguire, quali collaborazioni perseguire). Nella sua intervista, Tammet ha voluto ricordare, come nell'elaborazione delle linee legali e di gestione politica, fosse sempre elevatissimo il riferimento al diritto internazionale umanitario e all'apporto che seppe dare Fyodor Martens nel considerare la popolazione civile come il primo e più importante obiettivo da difendere durante le crisi e le guerre[347]. Fu così che l'Estonia adottò un approccio *puro* al nuovo dominio bellico: venne deciso di intendere per attacco tutto ciò che provocava *harm* ai civili in tutte le sue forme, a prescindere dalla tecnologia utilizzata per compiere questo obiettivo.[348]

Analizzandola nello specifico, pur essendo non priva di possibili migliorie[349], la ECSS è una proposta di elevatissimo valore strutturale sia pratico che teorico. È un documento specifico che analizza in maniera esaustiva lo scenario della sicurezza cibernetica nel paese.

"Estonia's cyber security strategy seeks primarily to reduce the inherent vulnerabilities of cyberspace in the nation as a whole. This will be accomplished through the implementation of national action plans and through active international co-operation"[350]*.* Da queste prime parole si possono identificare una serie di elementi fondamentali per

[346] Parteciparono il Ministero della Educazione e della Ricerca, il Ministero della giustizia, Ministero degli Affari Economici e delle comunicazioni, il Ministero degli Affari Esteri e il Ministero degli Interni.

[347]Di Gangi, C. (nd) *Il diritto internazionale umanitario,* Pegaso, Università telematica; pag. 6 http://www.unipegaso.it/materiali/PostLaurea/DiGangi/ModI/Lezione_I.pdf

[348]A tal proposito vorrei includere una dichiarazione di Rain Ottis, il quale ha voluto sottolineare come l'Estonia non spinse mai la NATO a considerare l'attacco del 2007 come ricadente sotto le eventualità dell'articolo 5 della Carta Atlantica, richiedendo così un intervento di legittima difesa. Iniziò però in questo senso il *dialogo* sulla questione.

[349]Una nuova strategia è appena stata pubblicata per il quinquennio 2014-2019 ma una versione in inglese non è ancora disponibile

[350]ECSS p. 3

comprendere la complessità dello studio che ha portato a questo documento. La completezza dell'analisi denota una chiara consapevolezza della debolezza intrinseca della nazione nello spettro del cyber-spazio, acquisita inequivocabilmente in seguito all'esperienza delle tre settimane della primavera 2007. Infatti, le vulnerabilità *connaturate dell'intera nazione nel suo complesso* non derivavano nient'altro che dalla comprensione della dipendenza dalle componenti informatiche nella vita quotidiana di tutti i cittadini, di tutte le imprese e di tutte le istituzioni. Gli analisti estoni capirono, prima di molti altri esponenti nel mondo della sicurezza cibernetica che ogni componente del network di un paese può costituire l'anello debole e diventare il punto di accesso di un possibile attacco esterno. Per questo *l'implementazione di piani d'azione nazionali* devono avere come soggetto tutti i settori della società e della vita pubblica estone. Inoltre, la consapevolezza della duplice debolezza del piccolo paese baltico ha spinto gli autori a includere immediatamente un rimando alla necessità di collaborare oltre i confini nazionali per mantenere un livello più elevato di sicurezza. Infatti, l'Estonia non soffre come tutti gli altri paesi semplicemente delle vulnerabilità connesse con l'internazionalità del World Wide Web, ma, date le sue dimensioni e capacità è estremamente dipendente dai paesi vicini e alleati per molte componenti necessarie al funzionamento corretto delle infrastrutture e dei network (i.e. ISPs). Per questo, come ricorda Tammet, il livello di cooperazione con Stati Uniti e Unione Europea nel processo di costruzione della cyber-strategia, è sempre stato elevatissimo e lo scambio di informazioni e opinioni costante e assiduo.

Se si guarda ancor più in dettaglio alla strategia, i punti centrali sono:

1. Lo sviluppo e l'implementazione di larga scala di un Sistema di misure di sicurezza.
2. Una crescente competenza nella sicurezza informatica;
3. Miglioramento dello spettro legale in supporto della cyber-sicurezza;
4. Incremento della cooperazione internazionale;

5. Incremento della consapevolezza (*awareness)* della *cyber-security*.

All'interno di queste sezioni moltissime riflessioni meritano di essere considerate, prima ancora di analizzare la struttura istituzionale e l'impalcatura legale che questa strategia pongono in essere. Innanzitutto, la prima preoccupazione di coloro che hanno redatto il documento è stata quella di legare a doppio filo la sicurezza dei network con la sicurezza delle infrastrutture critiche*: "The key objective(s) in developing and implementing a system of security measures (is) to tighten the security goals of the information systems and services provided by the critical infrastructure"*[351]. È questo un approccio molto razionale (che, ancora una volta, risente dell'esposizione personale al rischio) che illustra perfettamente uno dei punti di forza dell'*implementazione* estone della ECSS: la cognizione della natura reale e virtuale della minaccia cibernetica. A partire da questa considerazione è stato formato un comitato investito del compito di elaborare le migliori strategie per quanto riguarda la CIIP, coordinato inizialmente da Mihkel Tammet e in seguito da Martin Hurt.

Nelle pagine iniziali, da cui ho tratto questo elenco, gli autori hanno voluto ribadire quando detto inizialmente: la dipendenza dalle componenti IT è, e sarà, una grave minaccia per la sicurezza nazionale se non viene considerata in maniera efficacie. E' importante rimarcare che per componenti IT non si intendono unicamente i dati e le reti che rendono possibili la loro trasmissione, ma un'attenzione particolare va anche posta sulle strutture fisiche che rendono possibile il funzionamento di tutto il processo informatico.

Un altro punto messo in chiaro da subito dagli autori è la necessità di cooperazione, a tutti i livelli, sia internazionalmente, che, soprattutto, in termini intra-nazionali. Due tipi di difficoltà in particolare vengono riscontrate: la collaborazione e la coordinazione tra diverse agenzie preposte a diversi compiti nel settore della difesa; e la partecipazione del settore pubblico nel settore della sicurezza

[351]Raud op. citata p. 25

cibernetica, che rende necessario un processo biunivoco di comunicazione tra settore pubblico e privato per la protezione dei network e, soprattutto, delle infrastrutture critiche. Il messaggio non è chiaramente rivoluzionario, come si è visto nei capitoli precedenti, l'approccio della difesa "partecipata" è sostanzialmente condiviso in tutte le strategie pubblicate, la differenza dell'Estonia è che, data la sua breve storia d'indipendenza e le ridotte dimensioni del paese, è possibile dare a questo approccio un tocco estremamente pragmatico, senza rischiare di lasciare inoperose le misure proposte dietro regolamentazioni inapplicabili.

Un ulteriore elemento fondamentale, che spesso risulta poco chiaro ancora oggi a molti governi e ai responsabili del settore cyber di molte organizzazioni internazionali (i.e. NATO)[352], è la necessità di investire risorse e sforzi per creare esperti. L'universo delle infrastrutture e dei network è talmente vasto che non esistono abbastanza specialisti, in nessun paese, in grado di affrontare le sfide poste dal cyber-spazio. Per l'Estonia, e per gli autori della strategia più nello specifico, questa è stata un'ulteriore necessità derivante dall'incombenza degli attacchi del 2007. Si vedrà in seguito come quest'esigenza sia stata presa seriamente e costruttivamente in considerazione nel corso degli anni.

Lasciando da parte per il momento la dimensione legale e della cooperazione internazionale, che verranno ampliamente analizzate successivamente, vorrei soffermarmi brevemente sulla capcità di diffondere consapevolezza a tutti i livelli della popolazione. Questo perché, nell'approccio estone, è da sempre presente la necessità di educare la popolazione alle modalità di sicurezza e utilizzo essenziali delle nuove tecnologie. Come si è visto in precedenza con il progetto portato avanti dalla Tiger Leap Foundation[353], le ragioni di questa scelta sono sia pragmatiche che legate alle necessità difensive.

[352]A proposito cfr. GRAMAGLIA, M. e PERNIK, P. e THUOY, E. (2014) *Military Cyber Defense Structures of NATO Members: An Overview*, ICDS Pub, Tallinn

[353] Cfr. nota 14 e Magi, E. (nd) *Tiger Leap Program As A Beginning Of 21-St Century Education.* Consultabile http://www.ut.ee/eLSEEConf/Kogumik/Magi.pdf ultimo accesso 28.02.2014

4.3.1 Analisi dell'effettività della ECSS

Prima di passare a un'analisi più dettagliata dell'implementazione e della gestione nazionale vanno fatti una serie di appunti, che riprendono i lavori di due ricercatrici, la sopracitata Helena Raud e Piret Pernik[354] (quest'ultima in collaborazione con Emme Thoyu, entrambi ricercatori *senior* all'International Centre for Defense Studies di Tallinn). Entrambi gli studi hanno analizzato l'effettività della ECSS e ne hanno tratto conclusioni interessanti, anche se bisogna ammettere che le loro interpretazioni godono dei benefici del tempo e analizzano le applicazioni dell'implementazione invece che concentrarsi sulla strategia in sé.

Partendo ancora una volta dai punti forti della strategia è necessario soffermarsi su tre cose. La prima è che l'approccio di cyber-security non è stato inserito nel contesto difensivo come una costante esogena difficilmente mitigabile con l'impianto generico ma è stata perseguita integrando la I piani d'azione della cyber-sicurezza all'interno dei processi abitudinari di pianificazione della sicurezza nazionale, con sforzi coordinativi di tuti gli attori coinvolti. Inoltre si è posto l'accento da subito sulle responsabilità condivise di tutti nel diffondere consapevolezza sulle potenziali problematiche legate al cyber-spazio: non solo gli attori politici e gli organi legislativi, ma anche da parte di tutti coloro che hanno una parte nel gestione delle informazioni e dei network.[355]

Inoltre, meritorio per le istituzioni estoni, il processo di incremento della sicurezza non ha provocato sbilanciamenti negativi dal punto di vista dello sviluppo di un *information system* indispensabile sia per i privati che per le imprese, libero nel suo utilizzo e punto centrale dello sviluppo economico e sociale del Paese. In breve, le necessità del funzionamento della società moderna non è stato cooptato dalle istituzioni estoni per un più stretto controllo dei dati, della privacy e delle libertà personali, ma al contrario, in uno sforzo bidirezionale (sia dall'alto

[354] Pernik. P. e Thuoy, E. (2013) *Cyber Space in Estonia: Greater Security, Greater Challenges*, ICDS Pub, Tallinn

[355] CZOSSEK, C. e OTTIS, R. e ZIOLKOWSKI K. (2012) *4th Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn p 30

verso il basso che viceversa), l'attenzione per le necessità individuali è stato il punto centrale dell'evoluzione del *National Cyber Approach* estone, sancito nei suoi termini più generici nella ECSS.

Per di più, per rimarcare ulteriormente il pragmatismo dei *policy-makers* estoni, è importante notare come la ECSS prevedeva sin dal primo momento dei piani di implementazione biennali, per discutere di azioni concrete e fondi necessari per portare a termine determinati obiettivi inclusi nella ECSS. I piani sono composti da proposte provenienti da diverse agenzie governative e sono gestiti dal MEAC il quale si incarica di fornire dei report periodici sull'andamento della situazione, i quali vengono presentati in seduta collegiale con tutte le istituzioni coinvolte.

Arrivando quindi alle zone d'ombra della ECSS, non si può non partire con la critica più concreta, avanzata sia da Pernik e Thouy che da Raud: l'allocazione di fondi. Secondo le parole di Helena Raud "*The second major element when evaluating policy, according to the Fisher criteria is allocation of resources (Fisher 2005, 19). In this instance the ECSS fails*."[356] Pernik e Thoy invece individuano due problematiche concernenti la situazione interna ed internazionale, che aiutano a favorire una difficoltosa gestione ed allocazione dei fondi. Da una parte l'imperversante crisi economica che ha diminuito la base effettiva disponibile al governo per gestire la sicurezza cibernetica. Dall'altra le difficoltà amministrative che hanno complicato un processo di distribuzione che avrebbe potuto essere molto più semplificato ed efficiente.

Il secondo problema, che entrambe le autrici evidenziano come fondamentale è la scarsa chiarezza nell'identificazione dei responsabili delle singole attività proposte nella ECSS. Questo argomento verrà ampiamente trattato nel prossimo paragrafo, per il momento è importante sottolineare come uno dei criteri principali identificati da Pernik sia la mancanza di una forte leadership che si prodighi per una chiara risoluzione delle controversie riguardanti la *governance*[357]*.* Raud

[356]Ibid. p 33
[357]Raud (2012) op. citata Pag 5

invece rimarca come l'identificazione del Ministero per gli Affari Economici e la Comunicazione (MEAC) come principale responsabile per l'implementazione delle misure di sicurezza per le infrastrutture critiche[358] non sia sufficiente a chiarire precisi compiti, neanche nel caso del suddetto ministero.

Per concludere, secondo Pernik solo due dei cinque obiettivi sanciti nella ECSS (ed elencati in precedenza) sono stati raggiunti pienamente[359]: l'applicazione di misure su larga scala necessarie ad incrementare un sistema di sicurezza; e la capacità di imporsi internazionalmente come campione nella cooperazione internazionale per l'aumento della sicurezza cibernetica. Per quanto riguarda gli altri tre obiettivi molti sono stati perseguiti coerentemente ma spesso i risultati sono stati lontani dalle attese, come si vedrà in seguito.

A mio avviso, è inevitabile sostenere la duplice critica che hanno mosso le due ricercatrici all'implementazione della ECSS. È certo che l'insufficienza di risorse e la mancanza di una chiara distribuzione di ruoli, abbiano creato un deficit di efficienza rispetto all'*optimum* che si immaginava la Commissione che approvò la ECSS. Non sono invece estremamente d'accordo con la critica di Pernik che vede nella mancanza di un sistema di valutazione dei rischi di lungo periodo un'altra pecca del sistema istituito con la ECSS del 2008. Credo, anzi, che come documento, e quindi entità legale statica per sua natura, la ECSS sia stata una base fertile per l'elaborazione di scenari ipotetici di lungo periodo e plausibili risposte capaci di prendere in considerazione le necessità di sicurezza richieste dallo spazio cibernetico.

Concordo nuovamente con Pernik quando sostiene che una delle principali mancanze della strategia sia quella di non avere una portata *comprensiva,* poiché non identifica chiaramente la distinzione tra crimine cibernetico e attacchi di natura politica, anche provenienti da attori statali, preferendo una suddivisione in base all'entità della minaccia.[360] Infatti, per elaborare una coerente strategia, ma anche un

[358]Ibid p 34
[359]Pernik e Thuoy op. citata Pag 4
[360]Ibid p 6, si rifà a ECSS p. 10

framework legale (sia nazionale che internazionale), è necessario tenere in considerazione le intenzioni di compie determinate azioni, in modo da reagire in maniera indicata.

Lasciando alla parte finale del capitolo ulteriori spunti di analisi, ci si concentrerà ora su alcune delle peculiarità dell'approccio estone: la distribuzione dei compiti tra diverse entità governative; la protezione delle infrastrutture critiche (CIIP); la relazione tra settore pubblico e privato (PPP); e le unicità del sistema estone.

4.4 La distribuzione di compiti tra le diverse istituzioni governative

All'interno dell'ECSS è presente un capitolo intitolato "*Development and implementation of a system of security measures",* e un sottocapitolo che recita "Strengthening of Organisational Co-operation**"**. Nelle tre pagine a cui faccio riferimento, vengono sviluppate ampiamente le diverse modalità di implementazione, ma non si fa nessun chiaro riferimento alla distribuzione dei ruoli. Il massimo che possiamo leggere, al di là dell'attribuzione al MEAC del ruolo principale nella protezione delle infrastrutture critiche è che le Agenzie Statali assicurino la sicurezza informatica attraverso i tre livelli ipotizzati dall'ISKE, per questo un sistema multilivello di cyber-sicurezza è stato pensato dalle autorità competenti estoni[361]. Per questo, in collaborazione con Piret Pernik, mio supervisore all'International Centre for Defense Studies, ho pensato di ricostruire, attraverso delle interviste a personaggi chiave, le relazioni e le collaborazioni tra le varie entità governative (e non solo) nell'ambito della sicurezza informatica.

Come detto in precedenza, il principale attore nella scena della *cyber-security* è senza dubbio il Ministero degli Affari Economici e delle Comunicazioni (MEAC). La sua rilevanza deriva dal ruolo sancito dalla

[361]ECSS p. 27

ECSS ma anche dal suo precedente impegno nella protezione delle comunicazioni e dei sistemi di informazione. In particolare, per gestire direttamente la *cyber-security* è stata fondata, nel 2009, l'Estonian Information System's Authority (EISA)[362], derivata dal gruppo di analisi che manteneva sotto controllo le funzionalità IT nel settore pubblico. Oggi l'EISA coordina lo sviluppo e la gestione del sistema informatico dello Stato, organizza attività legate alla sicurezza delle informazioni, e gestisce gli incidenti di sicurezza che si verificano nelle reti di computer estoni. Inoltre, consiglia i fornitori di servizi pubblici su come gestire i loro sistemi informatici secondo i requisiti e li controlla. In dettaglio tra i suoi compiti[363] vi sono:

- Esecuzione di supervisione sui sistemi informativi utilizzati per fornire servizi vitali e l'attuazione delle misure di sicurezza del patrimonio informativo ad essi connessi. Organizzazione delle attività relative al sistema d'informazione dello Stato e la sicurezza delle informazioni delle infrastrutture critiche di informazione estone;
- Gestione degli incidenti di sicurezza che si verificano nelle reti di computer estoni;
- Esecuzione di vigilanza sul rispetto dei requisiti derivanti dalla legislazione che regola la gestione del sistema informativo dello Stato;
- Mantenimento del sistema di gestione per il sistema di informazione dello Stato;
- Mantenere X-Road[364], il livello di scambio di dati del sistema informativo dello Stato (sviluppo e amministrazione);
- Coordinare il funzionamento delle infrastrutture a chiave pubblica.

Inoltre tra le sue principali attività si annoverano[365]:

[362]In estone Riigi Infosüsteemi Amet (RIA)
[363] Estonian Information System's Authority, vedi:
https://www.ria.ee/about-estonian-information-system-authority/ ultimo accesso 28.02.2014
[364]Vedi inizio del capitolo
[365]Cfr. https://www.ria.ee/activities-of-ria/

- Organizzare la protezione delle infrastrutture critiche di informazione, tra le altre cose da preparare analisi dei rischi e di sviluppare le misure di sicurezza necessarie per la protezione delle infrastrutture critiche informatizzate;
- Coordinare l'attuazione delle norme di sicurezza delle informazioni (include il sistema di sicurezza di base a tre livelli[366]) nelle istituzioni statali e amministrazioni locali e dei privati che svolgono funzioni pubbliche, e sviluppa le linee guida di sicurezza delle informazioni al fine di attuare tali norme;
- Gestire gli incidenti di sicurezza segnalati e che si verificano nelle reti di computer estoni, dà avvertimenti in modo che gli incidenti di sicurezza potrebbero essere evitate, solleva la consapevolezza in materia di sicurezza degli utenti, e prepara rapporti circa la diffusione di malware e gli incidenti che hanno avuto luogo in informatica estone reti;
- Sviluppare strategie e delle politiche connesse alla sicurezza informatica;
- Eseguire la vigilanza sui sistemi informativi utilizzati per fornire servizi vitali e la costante attuazione delle misure di sicurezza del patrimonio informativo ad essi connessi;
- Organizzare la progettazione, lo sviluppo e la gestione delle aree di informazione tecnologica generali necessarie per lo Stato;
- Può organizzare lo sviluppo e la gestione della realizzazione e server di database dei sistemi informativi appartenenti nel sistema informativo di Stato durante un periodo di incubazione;
- Può organizzare lo sviluppo e la gestione dei servizi IT pubblici erogati dallo Stato;
- Partecipare allo sviluppo di strategie, piani di sviluppo, programmi di ricerca specifici e dei bilanci relativi allo sviluppo del sistema informativo dello Stato;
- Partecipare alla sviluppo della legislazione concernente la sua area di attività e rende suggerimenti su come modificare e integrare loro;

[366]Per un approfondimento su questo punto si veda https://www.ria.ee/iske-en

- Rappresentare lo stato in comunicazione internazionale nel suo settore di attività ai sensi della procedura prevista dalla legge;
- Fornire consulenza alle altre istituzioni statali sulla risoluzione di problemi relativi ai componenti che garantiscono il funzionamento del sistema d'informazione dello Stato.

Ho voluto riportare un così lungo elenco per evidenziare come sia complesso e completo il ruolo della EISA. Va poi aggiunto, come spiegato in un'intervista da Toomas Viira, responsabile della Sezione incaricata della Protezione delle Infrastrutture Critiche alla EISA, che tutte le precedenti attività e compiti sono ripartite tra tre diversi gruppi di lavoro: uno responsabile della protezione delle infrastrutture critiche, uno responsabile della supervisione, e uno composto dal *Computer Emergency Response team* (CERT) che è attivo costantemente e senza interruzioni.

Il CERT è il centro gravitazionale del sistema di difesa e, dal 2006 (anno della sua fondazione[367]), è l'organizzazione responsabile della gestione degli incidenti di sicurezza nelle reti informatiche .*ee.* Il suo compito è quello di assistere gli utenti di Internet estoni nell'attuazione delle misure di prevenzione al fine di ridurre i possibili danni da incidenti di sicurezza e di aiutarli nel rispondere alle minacce alla sicurezza. CERT Estonia si occupa degli incidenti di sicurezza che si verificano nelle reti del paese (o che cominciano da lì). I suoi compiti si suddividono in quattro categorie precise[368]: gestisce gli incidenti; fornisce consigli, avvertimenti e sostegno; supporta le istituzioni e gli ISP; mette in piedi programmi preventivi, che favoriscono la consapevolezza del pubblico sulla *information security.*

Sembrerebbe quindi che EISA possa gestire tutto ciò che riguarda la *cyber-security*[369]. In effetti è decisamente vero che EISA è intitolata di gestire la supervisione, l'analisi e il supporto del sistema di difesa, però non è sola né onnipotente nell'adempimento di questo

[367]Come detto la ragione della sua fondazione era direttamente collegata all'istituzione delle votazioni on-line.
[368]https://www.ria.ee/28201
[369]È interessante notare come, per quanto riguarda la *cyber-security*, la EISA possa contare su circa 27 addetti (civili) che si occupano di mantenere effettiva la sicurezza del informatica del paese.

ruolo. Uno dei problemi della gestione è costituito dal fatto che le sue competenze non sono precisamente definite da atti o leggi (tranne che per la gestione delle infrastrutture *vitali*, come si vedrà in seguito).

Il Ministero della Difesa è stato il promotore della prima ECSS (attività che adesso è passata sotto la gestione del MEAC) e fondamentalmente oggi, si occupa solo del sostegno alla preservazione della reti militari, attraverso la collaborazione con le Forze Armate attraverso la Cyber Defense League. Inoltre il Ministero della Difesa entra in azione qualora la calamità dell'attacco diventasse di portata nazionale. La questione diventa più complessa se si considera il fattore Alleanza Atlantica. Infatti, come si è già accennato e come si spiegherà ampiamente successivamente, l'Estonia confida profondamente nella cooperazione con la NATO[370] (non solo per la *cyber defense* ovviamente), date le sue dimensioni e le sue relazioni con il vicino russo. Le strutture militari estoni sono direttamente collegate a quelle NATO, anche in ambito cibernetico. Perciò, nel caso di attacco proveniente da un altro paese ci si trova davanti a una problematica importante. EISA è incaricata di gestire la crisi, attraverso il coordinamento delle varie entità incaricate di occuparsi della Difesa e il mantenimento delle direttive del suo Ministero di riferimento, il MEAC. In particolare, nel caso di una richiesta di sostegno internazionale, EISA sarà indirizzata a richiedere la partecipazione degli alleati storici, Finlandia e Svezia, mentre in realtà il primo passo che muoverà il Ministero della Difesa, preoccupato per la sicurezza nazionale sarà far intervenire il NCSIRT della NATO. Questo crea due tipologie di problemi: il primo legato alla poca chiarezza e al caos operativo nel momento dell'intervento difensivo; la seconda legata al fatto che sia Finlandia che Svezia non fanno parte dell'Alleanza, quindi i responsabili della NATO si potrebbero trovare ad operare in livelli di *cleareance* non condivisibili con entità statali esterne all'Alleanza.[371]

[370]Si pensi anche solo al CCDCOE e all'accordo tra NATO ed Estonia per la difesa in caso di cyber-attacco.
[371]Tutta questa riflessione mi è stata suggerita da Siim Alatalu, responsabile della *cyber security* al Ministero della Difesa estone

Il Ministero degli Interni possiede un Dipartimento predisposto alle analisi e *management* dei rischi e delle crisi. Priit Laaniste, del Ministero degli Interni, mi ha spiegato che il *crisis management* in Estonia è di tipo decentrato, basato sulla coordinazione (quasi spontanea, data la mancanza di procedure specifiche) tra i diversi attori. Nonostante questo, l'allineamento tra l'EISA e il Ministero sembra essere ormai corroborata: l'EISA ha il compito di preparare i piani di analisi del rischio; mentre il Ministero dell'Interno li controlla e li inserisce in un più ampio scenario di rischio a livello nazionale.

Il Ministero degli Affari Esteri, invece svolge unicamente una funzione complementare rispetto agli altri organi. Il suo scopo principale è rafforzare il quarto punto della ECSS e va detto che lo fa in maniera a dir poco eccellente. In particolare, il Ministro degli Esteri Urmas Paet è riuscito a siglare un accordo (*partnership)*[372]con il governo degli Stati Uniti per una cooperazione particolarmente ravvicinata nel settore della *cyber-security.* L'importanza di questo accordo risiede nel fatto che normalmente gli Stati Uniti non siglano accordi con gli alleati. Anche nell'ottica delle organizzazioni internazionali il Ministero estone è stato particolarmente attivo, con particolare enfasi riguardo alla collaborazione con l'Unione Europea[373] e l'International Telecommunication Union (ITU).

Infine, per concludere, nell'ufficio del Primo Ministro è presente una commissione che si occupa di sicurezza nazionale, nella quale rientra il management della *cyber-security*. La commissione è presieduta dal Primo Ministro, ma include i rappresentanti degli altri ministeri: Difesa, Interni, Affari Esteri, Finanze, ma non il Ministero degli Affari Economici[374], che abbiamo visto essere il principale attore nella

[372]Cfr. http://www.state.gov/r/pa/prs/ps/2013/218234.htm ultimo accesso 28.02.2014

[373]Al riguardo va ricordato il costante impegno della deputata europea Heli Tiirma-klar, che dopo aver occupato posizioni rilevanti in Estonia, nel Ministero della Difesa si sta prodigando per lo sviluppo delle politiche di sicurezza informatica nell'Unione Europea

[374]Lo sarà presto, ma è stata una recente iniziativa.

gestione della *cyber-security*. Come affermato da Kristjan Prikk, responsabile della *Homeland Security Policy,* il ruolo di questa Commissione è quello di produrre documenti atti a migliorare la sicurezza nazionale e la *governance*, cercando di avere un effetto reale per quanto riguarda la riduzione della conflittualità tra le diverse agenzie governative impegnate nel difesa nazionale.

Inizialmente il compito della commissione doveva essere solo coordinativo, ma lentamente il suo ruolo sembra essersi spostato verso la gestione delle problematiche vere e proprie nella sicurezza nazionale, una maggiore attenzione alle problematiche legate ai crimini informatici e, soprattutto, il difficile legame tra protezione dei civili e il ruolo militare della Difesa. Detto questo, Prikk ha assicurato che il Governo non ha nessuna intenzione di interferire con il lavoro della EISA o del ministero degli Interni, anche perché non possiede nessuna autorità per farlo, per svolgere l'attività di collegamento in maniera sufficientemente efficiente però è condizione necessaria (ma non sufficiente) che MEAC venga incluso nella Commissione che si occupa della *homeland security*, altrimenti il compito che si prefigge la commissione è destinato a fallire.

4.4.1 Il mondo militare

Il focus principale della *cyber-security* estone è la protezione delle infrastrutture *vitali* civili (considerando i network informatici come uno di essi), perciò, come ricordano molti degli intervistati[375], la partecipazione militare non è prevista nell'attività diaria, né ad un più basso livello di emergenza. Le strutture militari adibite alla sicurezza informatica sono peraltro abbastanza ridotte. Esiste un CSIRT, composto da un numero esiguo di militari, [376]che si coordina direttamente con il Ministero della Difesa e con la EISA. Con questa ha degli accordi segreti relativi prevalentemente alla protezione dei network e dei dati sensibili.

[375]Intervista a Toomas Viira

[376]"Il numero non è dato conoscerlo, ma sembra che gli addetti siano solamente due", mi ha rivelato un militare che non ha voluto che il suo nome comparisse nella ricerca.

Particolarmente rilevante è il ruolo del Paese e delle sue Forze Armate nell'azione svolta dal Centro di Eccellenza della Nato di Tallinn[377], guidato dal Tenente Colonnello Ilmar Tamm. In questo centro, oltre a sviluppare analisi sugli aspetti legali e bellici del cyber-spazio, vengono organizzate attività preparatorie, volte a migliorare la competenza delle istituzioni preposte.

Incluso questo, in termini cyber-sicurezza il ruolo preminente dell'esercito è proteggere le proprie infrastrutture, interagire con il sistema di difesa civile attraverso l'opera della Cyber Defence League, e stringere legami con i paesi baltici, con gli alleati storici e con le forze NATO. In generale, il ruolo dell'esercito nella gestione pubblica della sicurezza informatica è estremamente limitato e si limita indicativamente alla gestione di situazioni che vengono definite come dannose per la Sicurezza Nazionale. Nella stragrande maggioranza delle situazioni la componente militare del CDL è sufficiente per fare fronte alle minacce provenienti dal cyber-spazio. In caso di crisi, invece, l'ENISA cessa di essere il riferimento

4.5 La protezione delle Infrastrutture Critiche (*Vital Services)*

Rain Ottis sostiene che "*in Estonia il 90% delle infrastrutture critiche sono dipendenti da componenti informatiche. Il 40% ne sono dipendente in maniera critica. Il 10% non ha nessun altra opzione di funzionamento se non tramite le componenti informatiche*"[378]. Non sorprende quindi che il fulcro della protezione informatica in Estonia ruoti attorno alle infrastrutture critiche, o meglio *servizi vitali,* come li definisce l'Emergency Act, pubblicato nel 2009[379] dal EISA, attraverso il Ministero degli Affari Economici e della Comunicazione. Questo documento è di notevole rilevanza per numerosi motivi. Innanzitutto,

[377] Al riguardo si consultino il sito delle Forze Armate e del Ministero degli Esteri agli indirizzi: http://www.vm.ee/?q=en/node/9250; e http://www.mil.ee/et/arhiiv/7961. Consultati il 28.02.2014 Eesti Kaitsevagi Estonian Defence forces; "Estonia to host NATO cyber defence exercise" (2013).
[378] Mia traduzione di una dichiarazione di Rain Ottis durante una intervista concessami
[379] Estonian Information System's Authority – *Emergency Act,* 15 June 2009

definisce quali sono i servizi vitali che il governo considera fondamentale proteggere. Sono oggi 42[380] e racchiudono effettivamente molte delle categorie di infrastrutture fondamentali per la vita e la sicurezza del paese: dalle telecomunicazioni, all'elettricità; dagli aeroporti, all'approvvigionamento di gas. Inoltre nel documento vengono distinte chiaramente le responsabilità nella continua operatività dei servizi vitali[381]. In particolare il Ministero degli Affari Economici e delle Comunicazioni è responsabile per diciannove, il Ministro degli Interni di sette, quello degli Affari Sociali di quattro e il Ministero dell'Ambiente, quello delle Finanze e quello dell'Agricoltura di un paio ciascuno.

Dopo aver stabilito quali sono gli obblighi per coloro che devono garantire un effettivo funzionamento di questi servizi, l'Emergency Act parla delle responsabilità del Ministero degli Interni nella coordinazione della provvigione del servizio di continua operatività.

La protezione di queste infrastrutture si collega con la questione della sicurezza informatica, come visto, per il fatto che la maggior parte di questi servizi utilizzano componenti informatiche per il loro funzionamento. Per questa ragione vanno assiduamente protette. È questo il compito della EISA, che si occupa di evitare che i"t*he failure of an information system (can) have a substantial impact on the functioning of commercial enterprises and/or state agencies, thus also affecting the way customers/citizens are able to use services"* [382]. Esiste un Dipartimento specifico[383], a capo del quale vi è Toomas Vira, il cui scopo è quello di proteggere le infrastrutture critiche informatizzate (CIIP) e di mantenere un funzionamento senza problemi dei sistemi di informazione e di comunicazione essenziali del paese in circostanze ordinarie e per assicurare la loro continuità ad un livello minimo durante le situazioni critiche. In particolare, il compito principale del dipartimento è quello di organizzare la protezione per i sistemi informatizzati critici (sia a livello pubblico che privato) a livello nazionale.

[380]Secondo indiscrezioni starebbe per cambiare a 43.
[381]Emergency Act, cap. 4 par. 34
[382]Estonian Information System's Authority: *Critical Information Infrastructure Protection* (https://www.ria.ee/CIIP/)
[383]Il Dipartimento per la Protezione delle Infrastrutture Critiche ICT

Il ruolo principale della EISA è quello di mantenere costante il controllo non solo sulle infrastrutture ma anche sulle entità politiche che sono identificate dall'Emergency Act come *provider* di servizi vitali. Le varie entità provinciali, locali, nazionali che sono incaricate di vigilare sui provider di servizi, in modo che siano sempre garantiti servizi continuativi. Si parla in questo caso non di intromissione del privato nel pubblico, ma di determinati standard che il settore privato deve dimostrare di poter mantenere sotto qualsiasi circostanza.

Come già si era visto nella ECSS, un concetto fondamentale è quello di aver deciso di includere legalmente il network di internet nella lista dei servizi vitali, tanto da considerare "*The security of the Internet (is) vital to ensuring cyber security, since most of cyberspace is Internet-based. The main priorities in this respect are: strengthening the infrastructure of the Internet, including domain name servers (DNS); improving the automated restriction of Internet service users according to the nature of their traffic, and increasing the widespread use of means of authentication*"[384] .

Un'aggravante per la gestione dei servizi vitali del Paese è legata alla fonte dei server e delle imprese che offrono i suddetti servizi. È una questione che ha assunto particolare rilevanza negli ultimi anni, come mi ha spiegato Mihkel Tammet, dopo che il settore bancario è stato completamente "colonizzato" da enti stranieri (finlandesi e svedesi soprattutto). Per evitare problemi legati alle funzionalità dei server e delle riserve bancarie nel loro paese di origine, è stata approvata una legge che obbliga i *service provider* a mantenere un livello minimo di efficienza in qualsiasi situazione (anche di crisi), così da evitare scenari potenzialmente pericolosi per la sicurezza del paese. Questa legge include anche le componenti informatizzate dei servizi e, in pratica, obbliga i gestori del servizio a creare dei *back-up plan* limitati che tengano in considerazione la possibilità di offrire servizi alternativi, in caso di blocco delle funzionalità informatizzate. Indirettamente questa legge ha anche provocato un aumento degli investimenti per la

[384]ECSS p 4

sicurezza, così da accrescere il livello medio della protezione delle infrastrutture *vitali.*

L'attenzione alla CIIP porta direttamente a un altro fattore fondamentale per la cyber-sicurezza estone: l'incredibile capacità di amministrare il rapporto tra settore privato e pubblico nella gestione della sicurezza nazionale. Come si legge nell'ECSS L'effettiva cooperazione tra settore pubblico e private dovrebbe essere incrementata per avvantaggiare la protezione delle infastrutture critiche. In particolare, un esempio di ottima collaborazione tra forze private e pubbliche è la formazione del Comitato per la Protezione delle Infrastrutture Critiche formato nel 2011[385], che include i rappresentanti del settore privato e del pubblico. È perciò necessario soffermarsi sulle caratteristiche che contraddistinguono l'approccio estone a questa questione.

4.6 La relazione tra settore Privato e Pubblico (PPP)

La relazione creatasi tra settore privato e pubblico è senza dubbio l'arma segreta che permette all'Estonia di essere all'avanguardia, non solo nel campo dei servizi informatizzati offerti, ma anche nel settore della sicurezza cibernetica**.** Le ragioni ancora una volta, vanno ricercate nella sua storia recente e nelle scelte fatte dagli uomini politici degli ultimi tre decenni. La necessità di ricreare uno Stato dal nulla, dopo la dissoluzione dell'Unione sovietica ha costretto l'Estonia a ingegnarsi rapidamente per raggiunger livelli di sostenibilità e sussistenza immediati, dopo che, con la loro dipartita, i sovietici si erano portati via persino i telefoni.

Heli Tiirma-Klar spiega perfettamente in poche righe cosa è successo al paese una volta raggiunta l'indipendenza:

"*As a small state with scarce resources, Estonia decided to focus on protecting critical infrastructure and creating/enhancing public-private*

[385]Pernik e Thouy (2013) op. citata p 6

partnerships. Today Estonia's example has become a model internationally on how to build resilience in public-private domain"[386]*.*

È proprio questa combinazione tra dimensioni del paese e necessità di creare un sistema-paese completo in breve termine ad essere stato il motore affinchè si instaurasse una cooperazione così solida tra privati cittadini e forze statali. Lo Stato non possedeva le risorse necessarie per gestire e provvedere a tutti i settori della vita pubblica, mentre i cittadini non potevano vivere senza una completa fornitura di servizi. Si è così sviluppata una pratica di interazione e di fiducia che persiste tutt'oggi e che è alla base del funzionamento del paese. Questa convergenza di interessi ha permesso di mettere in atto un sistema di resilienza cooperativo che ha portato il paese ad essere un modello di sicurezza cibernetica.

La scelta fatta dal governo estone negli anni successivi all'indipendenza è stata quella di non interferire pesantemente, come erano soliti fare i governanti sovietici, e di lasciare quanta più libertà individuale possibile anche a livello di mercato e di impresa. Per questo, si è scelto di sostenere la gestione della sicurezza delle infrastrutture attraverso due linee politiche: investendo moltissimo[387] sul settore dell'educazione e legiferando in maniera olistica sulle minacce presenti ed eventuali.

Gli investimenti sull'educazione sono stati indirizzati sia alle scuole primarie che a quelle superiori. Nelle scuole primarie, il Governo estone ha provveduto alla fornitura di computer e classi specializzate, con l'intento di formare intere generazioni di individui capaci non solo di usufruire della varietà dei servizi offerti dalla rete virtuale, ma anche capaci di autogestirsi e proteggersi dalle possibili minacce provenienti dalla rete. Per quanto riguarda l'educazione superiore, l'Estonia vanta uno dei più alti livelli di studenti che si indirizzano ai poli tecnologici e informatici, ma non solo: la Technology University of Tallinn ha istituito il

[386]Cit di Tirmaa-Klaar, in un'intervista concessa all'International Institute for Strategic Studies nel 2010, consultabile al http://www.iiss.org/en/events/gsr/sections/global-strategic-review-2010-946c/sixth-plenary-session-6e03/q-6d98 ultimo accesso 28.02.2014

[387] Dutta, S. (2007) *Estonia: A Sustainable Success in Networked Readiness*? Consultabile http://www.weforum.org/pdf/gitr/2.1.pdf ultimo accesso 28.02.2014

primo corso magistrale in *Cyber Security*[388], che offre corsi di elevata specializzazione sia in questioni tecniche che nell' analisi dei rischi e concetti di base degli studi strategici.

Questo circolo virtuoso di reciproca fiducia e cooperazione ha creato una realtà in cui il settore pubblico e quello privato riescono a interagire positivamente, anche perché, come sostiene Kristjan Prikk, la relazione diretta, favorita da questo tipo di gestione, agevola i meccanismi di funzionamento e i problemi sono facilmente risolvibili. Un esempio, quasi aneddotico, di quanto appena detto è senza dubbio la vicenda successa alla Swedbank nel 2009[389], dove un pool di investigatori della polizia estone sono stati aiutati dagli esperti informatici della banca nell'atto di bloccare un attacco criminale che si stava perpetrando ai danni della banca stessa.

4.7 Le peculiarità della difesa estone: CDL e la Total Defense Strategy

Anche nel campo della Difesa esiste una realtà che si ricollega direttamente alla *partnership* tra settore pubblico e settore privato: la Cyber Defense League. Kadri Kaska, esperta legale estone appartenente al CCDCOE, ne parla profusamente in un report recentemente pubblicato[390]. La Cyber Defense League (CDL) è un'agenzia formata da privati cittadini volontari, che rientra però ufficialmente nel sistema difensivo nazionale[391]. È una modalità che esisteva già per quanto riguarda altri settori della difesa, ma che è stata introdotta in Estonia per la prima volta nel settore cyber[392]. Nonostante l'idea di un approccio *bottom-up* nel settore della Difesa cibernetica fosse già stato avanzato nel 2007, la CDL è stata istituita nel 2009, ma solo con la National Defence Strategy del 2010, venne posta in essere

[388]http://www.ttu.ee/index.php?id=25424
[389]Raud (2012) op. citata pag 28
[390]Kaska, k. et al (2013) *Cyber Defense Unit of the Estonian Defense League*, NATO CCDCOE Pub, Tallinn
[391]Sancito ufficialmente nel *Estonian Defense League Act* del 2013
[392]Ad oggi è stato emulato da Lithuania e, con modalità differenti, da Regno Unito

sotto la Estonian Defense League[393], agevolata dalla cooperazione tra i Ministeri della Difesa e degli Affari Economici e della Comunicazione.

Per entrare a fare parte del gruppo è ovviamente necessario rispondere a determinate caratteristiche. Bisogna innanzitutto essere esperti acclamati nel proprio settore, che sia la difesa tecnica o la valutazione dei rischi*;* inoltre, è necessario che almeno due membri della CDL sostengano la candidatura; infine, data la natura patriottica del servizio di volontariato, il candidato deve dimostrare una indiscussa lealtà verso lo stato estone. Pur essendo a partecipazione volontaria (anche per quanto riguarda le singole attività) esiste una catena di comando che fa capo a un Comande militare e a un secondo in gerarchia civile, che mantiene indipendenza in tempo di pace, ma che in stato di guerra risponde agli ordini del Comandante delle Forze Armate estoni.

Le funzioni del CDL sono sufficientemente speculari a quelle della EISA: sviluppo di un network di cooperazione, incluso per le risposte in caso di crisi*, incremento* della sicurezza delle infrastrutture critiche e promozione della consapevolezza e dell'educazione. La differenza sostanziale risiede nel campo d'azione della CDL. Secondo le parole di Kadri Kaska, la CDL, essendo legalmente sotto la responsabilità del ministero degli Interni, ha l'obbligo di entrare in azione in caso di stato di emergenza nazionale e di rischio per l'ordine costituzionale estone. In situazioni di normalità però l'azione della CDL nella vita civile del paese deve subire l'intercessione della EISA, che, a seconda della situazione, richiede il sostegno delle strutture militari a cui il CDL fa riferimento. Lo stesso vale se un'entità civile che necessita aiuto chiede il sostegno della CDL: questo non può interagire direttamente con i singoli servizi vitali*.*

Questo modello è estremamente benefico perché rende possibile quel processo che si origina dalla fiducia reciproca, si materializza con la capacità di condividere informazioni e si conclude con la

[393]http://www.kaitseliit.ee/en/edl

cooperazione effettiva tra entità appartenenti a diversi settori, che rende possibile una migliore gestione della sicurezza informatica.

4.8 L'*international framework.* NATO, USA, UE

Come è stato notato in precedenza dall'analisi di Piret Pernik, uno dei campi in cui l'Estonia è stata maggiormente prolifica, è stata la cooperazione internazionale. La scelta di questa predilezione deriva da molte ragioni: l'essenza intrinseca del cyber-spazio, la natura internazionale di molte delle infrastrutture critiche, le necessità del mercato high-tech e soprattutto l'esigenza di sicurezza.

La verità è che per il sistema di difesa estone, il poter contare sugli alleati internazionali è inevitabilmente necessario. Per questa ragione a partire dal 1991, i governi di Tallinn hanno cercato di interagire in particolare con Stati Uniti, con L'Unione Europea (membro dal 2004) e con la NATO (membro dal 2004). Le capacità estoni in *cyber-security* hanno in parte aiutato il Paese ad acquisire uno status privilegiato rispetto a gli altri paesi baltici, come ricorda Meelis Atonen, ex Mininstro degli Affari Economici e della Comunicazione: *"I would not consider it an exaggeration to say that "e" has put Estonia back on the world map*".

Un importante evento organizzato l'anno scorso dalla NATO[394], chiamato Cyber Coalition 2013, che ha preso luogo nella città di Tartu, nel centro del paese. Toomas Viira racconta che sia questa esercitazione, sia quella condotta in collaborazione con l'Unione Europea (cyber-Europe 2014[395]) sono ancora scenari molto semplici e rudimentali, ma servono per instaurare un rapporto di fiducia e conoscenza tra i vari membri dell'Alleanza e tra i membri e l'Alleanza. Inutile dire che anche in questo caso la scelta del territorio estone non è una scelta casuale, sia dal punto di vista della rilevanza internazionale sia per l'importanza che rivolge la NATO nei confronti del paese.

[394]Per informazioni sulle esercitazioni *LockedShield* cfr https://www.ccdcoe.org/334.html ultimo accesso 28.02.2014
[395]Cfr. European Union Agency for Network and Information Security (ENISA): Cyber Europe http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe ultimo accesso 28.02.2014

Fondamentale infine ricordare nuovamente lo stretto legame tra Estonia e i due alleati storici: Finlandia e Svezia. Con questi due storici sostenitori si è visto che i legami sono molto stretti, soprattutto attraverso le istituzioni politiche. Anche le forze armate però sono connesse in maniera inscindibile con i due paesi scandinavi distanti poche decine di miglia nautiche. L'esperienza del 2007 ha mostrato come il sostegno svedese e finlandese sia necessario alla difesa estone. Oggi questo legame è ancor più rilevante, in quanto le infrastrutture bancarie del paese baltico sono interamente dipendenti da istituti svedesi o finlandesi. Per questa ragione l'Estonia ha rafforzato ancor di più la cooperazione sia con le imprese private di origine straniera sia con gli Stati che sono oggi una risorsa molto utile per la sicurezza estone, soprattutto se si considera l'elevatissimo livello di r*eadiness*[396] riscontrato dai due paesi.

Considerazioni conclusive

L'analisi dell'ecosistema estone ha permesso di metterne in evidenza luci e ombre. Sicuramente il principale problema è la poca chiarezza nella suddivisione dei ruoli a livello istituzionale e la scarsità di fondi a disposizione. I due problemi sembrano in qualche modo fisiologici, ma sono più che convinto, così come lo sono Pernik e Raud, che la questione possa essere risolta con la pratica e l'esercizio. Quest'anno sarà promossa la nuova ECSS e, da quanto è trapelato, prenderà in considerazione entrambe le questioni, nonché un ampliamento delle categorie dei servizi vitali, così da estendere il numero di quelli protetti direttamente dai rispettivi ministeri. Infine il Ministero della Difesa sta lavorando duramente per cercare di provvedere un framework più chiaro per la collaborazione con il settore privato e per la cooperazione a livello internazionale (soprattutto Stati Uniti, attraverso la NATO).

[396] Entrambi i paesi sono al primo posto nella classifica rilasciata da Hathaway, M (2013) *Cyber Readiness Index 1.0*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge

L’analisi del modello ha permesso di notare come uno stato piccolo e intrinsecamente debole possa puntare ad essere un leader nel settore della sicurezza informatica. Le scelte operate dal paese hanno permesso in poco più di quindici anni di poter raggiungere uno tra i più elevati livelli di *readiness* al mondo. Questo perché, oltre a credere fortemente nella necessità di innovazione, non solo di tecnologie ma anche di mentalità, il paese è stato in grado di ripresentare un modello sociale e un ecosistema difensivo altamente informatizzato, in cui ognuno espleta una funzione. Le Forze Armate in questo processo hanno avuto un piccolo ruolo, mentre il nerbo dello sviluppo e dell’evoluzione difensiva è rappresentato dal settore privato e da lungimiranti uomini politici. Inoltre, la peculiarità che rappresenta il CDL è una soluzione ottimale a risolvere il problema della cooperazione tra privati e Forze Armate nel settore della difesa, in particolar modo cibernetica.

5.

ISRAELE - NATIONAL CYBER ECOSYSTEM

"*As we all know there are three kinds of cyber-security. Intelligence. Deterrence. And the one nobody talks about it*."

Oren Bratt, Cyber director
Israeli Military Industry[397]

Introduzione

Quando si parla di Israele in termini cyber-warfare il primo pensiero va quasi sempre a Stuxnet, qualche volta all'Operazione Orchard. La componente offensiva, nel caso del cyber-approach israeliano, è senz'altro una delle caratteristiche principali, che differenziano Israele dal resto dei paesi del mondo. L'altra, caratteristica fondamentale, è la quantità di attacchi ricevuti: ogni giorno il Paese subisce decine di migliaia di attacchi, da migliaia di aggressori[398]. Per questa ragione il modello israeliano di difesa è unico e combina le capacità offensive con quelle difensive, dando vita a una modalità proattiva che è tra le più efficaci del mondo.

Quando si parla di Israele, inoltre, è necessario tenere in considerazione la fortissima rilevanza dell'Esercito nell'ordine sociale e nella gestione della Difesa. Questa particolarità ha profonde influenze sia sulla gestione del cyber-spazio che sulla possibilità di studiarlo approfonditamente. Infatti una delle caratterizzazioni delle Difesa israeliana è la strepitosa capacità di mantenere segreto una grande quantità di informazioni sensibili.

Un risvolto positivo, in termini di raccolta di informazioni, risiede nel fatto che solitamente i militari di carriera, una volta terminata la loro

[397] Intervento a Cyber Tech 2014, Tel Aviv
[398] Cfr: http://www.upi.com/Science_News/Technology/2012/10/27/Israel-shuts-down-police-computers/UPI-77211351363492/2012 ultimo accesso 28.02.2014

attività nell'Esercito, si spostano nel mondo civile per fare da tramite tra questo e le Forze Armate. Mi è stato quindi possibile, nonostante la difficoltà di reperire numerose nozioni in inglese, poter apprendere della situazione israeliana da esperti che provenivano dal mondo militare (e sapevano quindi interpretarne le esigenze), ma che facevano in quel momento della comunità scientifica o politica, comunque civile.

Questo mi ha dato la possibilità di capire come, per gli israeliani, la difesa non sia una questione che si può demandare a un organo preposto –l'esercito- ma deve essere foraggiata con idee e sostegno. Lo stesso vale per l'interpretazione della *cyber-security.* Riprendendo le parole del Direttore del Yuval Ne'eman Workshop Isaac Ben-Israel, "*cyber security is not about saving information or data, but about something deeper than that. It's about securing different life systems regulated by computers. In Israel we realised this 10 years ago*"[399].

È questo ciò che rende l'ecosistema israeliano un *unicum*: la visione olistica da parte delle istituzioni e delle forze armate e la volontà di partecipazione della popolazione. Ovviamente, queste sono anche le risultanti di una situazione di perenne conflitto con i vicini che rappresenta anch'essa un *unicum.* E, ovviamente, esistono notevoli aspetti che rendono il modello molto meno efficiente di quanto potrebbe esserlo.

Nonostante quello israeliano è un modello (eco)sistemico prossimo alla perfezione teorica.

5.1 Genesi e caratteristiche

L'interesse israeliano per il mondo dei network e dello sviluppo delle nuove tecnologie cibernetiche può essere datato intorno alla prima metà degli anni Ottanta. Nonostante le ragioni e le necessità di due universi, quello civile e militare, fossero molto differenti, per via di un

[399]Grauman, B. (2012) *Cyber-security: The vexed question of global rules. An independent report on cyber preparedness around the world*; e anche Security And Defense Agenda e Mc Afee. consultabile a http://www.mcafee.com/au/resources/reports/rp-sda-cyber-security.pdf ultimo accesso 28.02.2014

meccanismo di onnipresente interazione tra i due mondi, lo sviluppo tecnologico è stato parallelo e ha beneficiato di una sinergia unica, che ha reso possibile l'incredibile parabola di innovazione all'interno del settore della Difesa e dell'Economia israeliane.

Nella ricostruzione della genesi dello sviluppo delle tecnologie informatiche in Israele, ho avuto la possibilità di confrontarmi con due esperti del settore: il Professor Isaac Ben Israel[400], che da sempre è una testa di ponte tra il mondo militare, la ricerca e il governo; e il Professor Martin Van Creveld, storico e profondo conoscitore del mondo militare e del rapporto tra questo e le nuove tecnologie.

In particolare, sembrano essere tre gli ordini di ragioni che hanno spinto Israele ad intraprendere un cammino di intensivo sviluppo tecnologico. Il primo e più importante è senza dubbio la percezione dei probabili vantaggi bellici legati alle tecnologie informatiche.

Nella breve storia dello Stato d'Israele, la sicurezza è stata da sempre la più grande necessità di statisti e popolazione civile. Considerate le dimensioni e la elevata vulnerabilità del proprio territorio, per le forze Armate israeliane è sempre stato fondamentale basarsi su un tipo di sicurezza che non fosse preminentemente difensiva, ma che fosse allo stesso tempo di tipo proattivo. I pilastri di questo tipo di strategia sono da sempre la capacità di ottenere un elevatissimo ed accurato numero di informazioni sui nemici (intelligence) e l'ipotetica possibilità di prevedere gli attacchi e, nel più efficace degli scenari, prevenirli con azioni rapide e basate sulla sorpresa. Questo scenario è stato ulteriormente complicato alla fine degli anni Settanta e durante tutti gli anni Ottanta, quando i campi di battaglia attorno al piccolo Stato ebraico sono cambiati significativamente, limitando gli scontri contro grandi eserciti nazionali e vedendo l'emergere di gruppi armati ostili e bellicosi (i.e. Ḥizbu 'llāh) con capacità di offesa ridotte, ma più flessibili. Riprendendo il lavoro di Steinbeg G.M. (2011), "*while the details of the conflict have changed over time, Israel's existential threats, asymmetry,*

[400]Il Professor Ben-Israel served as head of the Defense Ministry's Administration for the Development of Weapons and the Technological Industry, and is currently the director of the Yuval Ne'eman Science, Technology & Security Workshop at Tel Aviv University. Mentre Martin Van Creveld è professore di Studi Strategici alla Tel Aviv University e autore di numerosi volumi sulla strategia militare.

and a high level of vulnerability remain"[401]. Fu proprio lo sviluppo di nuove minacce dai confini e questa predominanza per i conflitti cosiddetti a bassa intensità[402], a spingere gli strateghi israeliani a ricercare nuove possibilità deterrenti anche all'interno dello spettro dello sviluppo tecnologico. Così a partire dalla fine degli anni Ottanta l'insieme delle forze armate (e in particolare il settori dell'intelligence) è stato indirizzato verso le possibilità offerte da quella che inizialmente veniva definita *info warfare*, l'automatizzazione del campo di battaglia e, per finire, la *cyber-warfare*. Le ragioni sono semplici. Come sostiene Baram G. (2012)[403], va ricordato che la superiorità militare israeliana si è sempre dovuta basare sull'innovazione tecnologica e sul livello qualitativo di forze e sistemi d'arma, necessari per bilanciare il forte sovrannumero delle popolazioni ostili dei paesi vicini. Le innovazioni tecnologiche in generale, e nello specifico la sperimentazione di tecnologie ICT, hanno reso possibile una maggior incisività dei tre pilastri difensivi che si accennavano precedentemente: deterrenza, allerta (sulle azioni nemiche) e gestione del comando.

Il secondo motivo che ha favorito la crescita delle tecnologie e dell'interesse per il mondo cibernetico è di ordine economico. A metà degli anni Ottanta il sistema produttivo e il mercato israeliano erano in forte crisi, sia nel mondo militare che in quello civile. Lo stesso Van Creveld ricorda come la situazione economica si relazionò con l'industria e la strategia militare: "*a worsening economic situation has forced Israel's Weapon Development Authority (RAFAEL) to cut the period during which newly developed system cannot be exported*"[404]. Il paese si trovava in una situazione in cui il sistema produttivo stava rapidamente perdendo la sua efficacia, il modello basato sui *kibbutz* stava dimostrando la sua inefficacia nella competizione internazionale e, verso la metà del decennio, i tassi di inflazione iniziavano a raggiungere

[401] Steinberg, G. M. (2011) *Israel Studies An Anthology: The Evolution of Israeli Military Strategy: Asymmetry, Vulnerability, Pre-emption and Deterrence*; Israel Studies Anthology. Consultabile: http://www.jewishvirtuallibrary.org/jsource/isdf/text/steinberg.html ultimo accesso 28.02.2014

[402] Van Creveld, M. (1991) *The Transformation of War*, The Free Press, New York p.18

[403] Baram G. (2013) *The effect of cyberwar technologies on force buildup: the Israeli case* in "Military and Strategic Affairs", Vol.5, No.1, pp. 23-43

[404] Van Creveld, M. (1991) *The Transformation of War*, The Free Press, New York p.210

valori a tre cifre[405]. Questo scenario portò a delle precise conseguenze. Innanzitutto il Governo e il Parlamento si accordarono per attuare una serie di riforme, il cosiddetto "Programma di stabilizzazione"[406] (1985) che mirava a limitare la perdita di competizione a livello internazionale e frenare l'incremento vertiginoso del costo della vita all'interno. Inoltre, il Paese decise di basare la propria produzione su prodotti innovativi, a basso costo e facili da esportare. Non va infatti dimenticato che, usando le parole di Neno Malisevic, responsabile per le cyber-policies all'OSCE, Israele è un'isola politica e commerciale, a causa delle ostilità dei suoi vicini[407] e, per questo motivo, la necessità di puntare sullo sviluppo di beni facilmente esportabili è un'esigenza fortemente sentita dai *policy-maker* israeliani. In questo modo ebbe inizio quel percorso che porterà il Paese all'accrescimento della produzione di nuove tecnologie e della sua competitività internazionale, sviluppando un modello che risulterà essere unico al mondo. Modello che viene descritto in "Start- up Nation" (2009), un libro di Sanor e Singer (vedi paragrafo successivo)[408].

Infine, il terzo motivo è di ordine culturale. Come rimarca Van Creveld, storicamente il popolo ebraico ha avuto una forte predilezione per quelle attività che permettono di non sporcarsi le mani. Così l'importanza che il mondo culturale ha nella dottrina ebraica e la preferenza per i commerci hanno rivestito una grande importanza nell'evoluzione del carattere identitario legato all'ebraismo. Sotto questo punto di vista, l'evoluzione di processi digitali che permettono di diminuire le azioni concrete e tangibili che ognuno deve compiere nel corso della propria esistenza, può inserirsi perfettamente in questa caratterizzazione, così da aiutare a spiegare la florida azienda di tecnologie ICT che si sono sviluppate nel paese.

[405] Il *Central Bureau of Statistics* Israeliano stima fosse del 450% 1984 (http://www1.cbs.gov.il/reader/?MIval=cw_usr_view_SHTML&ID=423, ultimo accesso 28.02.2014)
[406] Zalman, F. S (May 1986); "Adjusting to High Inflation: The Israeli Experience"; FEDERAL RESERVE BANK OF ST. LOUIS (http://research.stlouisfed.org/publications/review/86/05/Adjusting_May1986.pdf , ultimo accesso 28.02.2014)
[407] Intervento a Cyber Tech 2014, Tel Aviv
[408] Per una critica vedi Yusuf Mansour : "*Financing the start-up nation*" presso http://urdunmubdi3.ning.com/profiles/blogs/financing-the-startup-nation?xg_source=activity

5.1.1 Il modello d'interazione tra Forze Armate e mondo civile

Come corollario a queste motivazioni va inserita una breve descrizione del sistema di reclutamento per i giovani israeliani, e come questa interagisca con il mondo delle imprese e dell'università. Questa interazione è fondamentale perché, a detta di molti esperti, costituisce la chiave di volta per comprendere lo scenario di competenze tecnologiche e di *cyber-security* del Paese.

Al termine delle scuole superiori, mediamente all'età di 18 anni, i giovani israeliani sono solitamente tenuti ad arruolarsi nell'esercito. Questo vale per tutti coloro che sono in buona salute e sono escluse solo due categorie di giovani: coloro che per svariate ragioni sono fisicamente o mentalmente impossibilitati a svolgere il servizio militare e coloro che scelgono di approfittare del progetto ATUDA[409]. Circa l'1% dei giovani, grazie alle capacità e potenzialità espresse durante il percorso accademico, viene selezionato per intraprendere i primi tre anni di università prima di essere arruolato nelle Forze Armate. Questo poiché nel mondo militare viene richiesto del personale specializzato in determinate aree (ingegneria, fisica, legge) da inserire nei programmi di sviluppo. Al di là di questa piccola percentuale, però, i giovani israeliani sanno che, una volta terminata la scuola superiore, li aspetta una lunga esperienza nelle Forze Armate del loro paese: sono infatti tre anni di servizio obbligatorio per gli uomini e poco più di due per le donne. In questo arco temporale imparano molte cose, e acquisiscono un importante background di conoscenze e capacità che porteranno con sé una volta terminato il servizio militare, quando si riaffacceranno al mondo universitario e della vita privata.

E' necessario sottolineare il fatto che nella tradizione del Paese si attribuisce grande importanza alla carriera militare, perciò non è difficile vedere come i più alti gradi nel mondo politico e in quello dell'Impresa e del business siano occupati da militari di carriera, che al termine della scalata all'interno delle forze armate, si spostano verso

[409]Per maggiori approfondimenti su ATUDA consultare http://atuda.org.il/

incarichi di gestione nel mondo civile.

Questa interconnessione è di notevole importanza per tutte le aree della vita sociale israeliana ma fondamentale per l'universo dello sviluppo tecnologico, sia dal punto di vista economico, sia da quello delle capacità difensive. Infatti, per quanto riguarda le capacità economiche, un esempio particolarmente esplicativo è il fenomeno del boom nel settore dell'high-tech delle Start-up. Innanzitutto ai vertici delle compagnie che producono nuove tecnologie vi sono spesso personalità proveninti dall'orbita militare (vedi il caso dell'Unità 8200). Anche la tendenza dei prodotti che vengono sviluppati denota come l'atteggiamento mentale sia quello imposto dalla vita militare e dalle richieste quotidiane della sicurezza nazionale: non è un caso che il settore di maggiore crescita economica nell'ambito delle nuove tecnologie in Israele sia oggi la sicurezza informatica e della protezione delle componenti ICT per le imprese.

Inoltre, se si considera il sistema paese e la gestione del settore della sicurezza legata alle nuove tecnologie (e in particolare della cyber-security, punto centrale della ricerca) è facile notare come molte delle posizioni sia all'interno delle pubbliche amministrazioni che del settore privato siano occupate da persone che provengono da una particolare area dell'esercito e grazie a questo hanno acquisito determinate capacità, competenze e sistema di pensiero. È questo un punto fondamentale che verrà sviluppato nel corso del capitolo e permetterà di cogliere meglio alcuni fattori essenziali per l'interpretazione del modello di sicurezza informatica di cui si è dotato sinora lo Stato d'Israele.

5.2 Il percorso della cyber-security israeliana

Per quanto riguarda invece lo sviluppo delle politiche di gestione del cyber-spazio, la storia ufficiale dello Stato Israeliano ha alle spalle vent'anni di esperienze. L'evoluzione della sicurezza informatica a livello nazionale segue la necessità da parte dell'esecutivo di rendere sicuri gli

obiettivi strategici all'interno del proprio paese, in particolare le infrastrutture considerate vitali per lo svolgimento di funzioni quotidiane. Nello specifico, fu a partire dagli inizi degli anni Novanta che il dibattito sulla necessità di proteggere le componenti informatizzate si presentò all'interno dell'arena politica israeliana. Fu solo con la decisione presa dal Gabinetto israeliano del 1996 (Cabinet decision1886 BK/9)[410] che il primo "*establishment of a steering committee on computerization in every government ministry*" vide la luce. In questo preciso periodo storico non molti Stati, al di là degli Stati Uniti, erano sensibili a queste questioni, ma, a partire da questa decisione, Israele diede avvio ad una pratica di analisi delle più rilevanti minacce e delle migliori modalità per contrastare i *cyber-attacks.*

Da precursore, il passaggio successivo dello Stato d'Israele fu quello di istituire un programma nazionale volto a proteggere le connessioni dei vari ministeri e la possibilità per gli stessi di navigare in maniera sicura. Il progetto venne attivato nel 1997 sotto il nome di TEHILA (acronimo in ebraico, che significa Infrastrutture Governative per l'Era di Internet) con la creazione di un Corpo centrale che fornisse al Governo e ai Ministeri il più elevato livello di servizzi informatici, compresa ovviamente la messa in sicurezza[411]. Le sue funzioni inizialmente consistevano nel proteggere gli utenti e nel fornire loro *pacchetti di servizio* per contrastare le possibili minacce. Inoltre TEHILA aveva la funzione di *host* delle piattaforme che offrivano servizi pubblici (sempre solo in ambito governativo), con il conseguente incremento dell'information *security* sia degli utenti governativi sia degli utenti privati che usufruivano dei servizi governativi. Come si vedrà successivamente, anche a livello informatico, lo Stato di Israele è ed era solito subire un numeroso spaventoso di attacchi ogni giorno e, già nel 2002, TEHILA poteva vantare al suo attivo 90 mila tentativi di penetrazione, di cui 14mila di elevata qualità : "e*ach day approximately 100 virus attacks and attacks of other harmful software are avoided*."

[410]Alla nota n° 25 dell'articolo di TABANSKY, L. (2011) *Critical Infrastructure Protection against Cyber threats*, Military and Strategic Affairs*,* Vol 3, No.2, pp.61-78 vi è una lista di decisioni governative prese successivamente al 1996
[411]Per una più ampia descrizione del progetto TEHILA: http://147.237.72.58/Tehila1/english_site

Un altro passaggio fondamentale nell'evoluzione della protezione informatica, fu l'adozione, l'anno successivo della Legge che regolava la sicurezza nelle organizzazioni pubbliche (1998), che offriva la prima – incompleta- lista di definizione di ciò che veniva considerato come esseniali sistemi computerizzati e analizzava la sicurezza relativa e le modalità di protezione. Questa legge costituì la necessaria premessa della legge B/84 emanata dal Comitato Ministeriale per la sicurezza Nazionale, il quale legislava in materia di protezione di sistemi computerizzati nello Stato d'Israele[412] (11 Decembre 2002). In essa si declinava interamente nelle mani di un organismo specifico la protezione delle componenti informatiche delle infrastrutture considerate critiche per il Paese. Iniziò così il periodo di monopolio della ISA (Israeli Security Agency[413]) in materia di protezione informatica per le infrastrutture civili, che in parte dura ancora oggi.

La pubblicazione di questa legge ebbe particolari risvolti. Innanzitutto, era la prima volta che si cercava di sistematizzare sia il ruolo dell'ISA che la gestione delle infrastrutture critiche in ambito civile. Sarà questa la base dell'evoluzione della capacità di rispondere a minacce cibernetiche rivolte alle infrastrutture computerizzate. Nel contesto venne inoltre creato un Comitato di Governo che stabilisse quali effettivamente fossero le entità essenziali per il funzionamento della vita pubblica israeliana, sia in materia di servizi pubblici che privati. La conseguenza di quest'azione, fu la collaborazione con il Consiglio di Sicurezza Nazionale, nella realizzazione di un ulteriore comitato governativo il cui obiettivo era quello di stilare ufficialmente una serie di misure per contrastare le minacce informatiche nel Paese. Il testo finale comprendeva i principi difensivi della dottrina della protezione, le minacce incombenti e le agenzie preposte alla difesa dei principali siti interessati.

Nello stesso anno, grazie anche all'interazione tra le istituzioni citate, venne creata la *National Information Security Authority* (NISA[414]),

[412]Legge 2002
[413]In ebraico שירות הביטחון הכלל' (http://www.shabak.gov.il/english/Pages/default.aspx)
[414]In ebraico RE'EM (http://www.shabak.gov.il/about/units/reem/pages/default.aspx)

con il compito di fornire le linee guida per le entità incaricate e emanare sanzioni contro le rispettive agenzie in caso di mancato rispetto delle direttive. Il problema principale, che verrà però analizzato più avanti, era il fatto che le iverse agenzie tenevano (e lo fanno ancora oggi) a prendere azioni indipendenti senza alcuna linea guida ufficiale dalla NISA[415].

La svolta nella storia della protezione informatica israeliana arrivò verso la fine del primo decennio del nuovo millennio, quando il Primo Ministro Benjamin Netanyahu decise di ottenere una fotografia veritiera del sistema di protezione relativo al cyber-spazio e, dato il rifiuto del *National Security Council, fu costretto ad* istituire un gruppo *ad hoc* formato da un' ottantina tra specialisti e ricercatori del settore del cyber-spazio e guidato dal professor Isaac Ben-Israeli, all'epoca a capo del Consiglio Nazionale per la Ricerca e lo Sviluppo al Ministero della Scienza. Nacque così la *National Cyber Initiative*[416]*,* che porterà all'inizio ad un semplice elenco di raccomandazioni che il Primo Ministro avrebbe dovuto seguire e, successivamente alla formazione del *National Cyber Bureau.* L'iniziativa portata avanti con la NCI rappresentava una sistematica rivisitazione di tutte le possibili sfide e minacce che lo Stato di Israele avrebbe dovuto affrontare in vista di un attacco cibernetico. Il motto dell' iniziativa era:

"*To preserve Israel's standing in the world as a center for information-technology development, to provide it with superpower capabilities in cyberspace, to ensure its financial and national resilience as a democratic, information-based, and open society*"[417].

Le ragioni che portarono il Primo Ministro all'adozione di questa iniziativa erano essenzialmente due: la volontà di sviluppare il settore delle cyber-tecnologie, con lo scopo di diventare nel 2015 uno dei cinque top leader mondiali e la consapevolezza degli obiettivi da proteggere e delle tecniche da implementare per combattere nella maniera più efficace possibile le nuove minacce provenienti dal cyber-

[415]Baram G. (2013) op. citata p. 31

[416]Tabansky L. (2013) op. citata p.4

[417]"The national cyber initiative" – a special report for the Prime Minister *In:* the state of Israel, m. o. s. a. t., the national council on research and development, the supreme council on science and technology (ed.). Tel-Aviv in Tabansky (2013)

spazio. Le conseguenze di questa scelta sono in parte ancora da valutare data la novità e il poco tempo intercorso, ma sembrano avere avuto un impatto decisamente positivo in entrambi i settori, se si considerano, da una parte, i forti investimenti internazionali per sostenere lo sviluppo informatico nel paese e, dall'altro, la reazione alle decine di migliaia di attacchi giornalieri che subiscono le infrastrutture israeliane.

Le raccomandazioni vennero raccolte in un testo proposto dal Primo Ministro (che verrà ampiamente analizzato più avanti). Il consiglio principale era quello di formare un *National Cyber Bureau*, che potesse servire come Corpo consultivo per il Governo e le cui attività fossero focalizzate alle politiche e alle iniziative nel cyber-spazio. Funzione da svolgere attraverso la considerazione del dominio cyber da un ampio punto di vista, e la collaborazione con i settori militari, della ricerca e delle imprese private. Molti punti della raccomandazione risultarono poco chiari o in contrasto con le funzioni di altri organi, ma sarà questo motivo di indagine in seguito[418].

5.3 Le minacce

Se si tralasciano i criminali semplici, ovvero coloro che utilizzano il cyber-spazio per compiere reati di natura economica, sono numerosi quelli che vengono considerati dalle Forze Armate israeliane come potenziali cyber-nemici, che agiscono quindi con scopi politici contro il Paese. Infatti, come è risaputo, Israele continua ad essere ancora oggi un'isola dal punto di vista politico ed economico. Lo status, unico al mondo, dello Stato ebraico in Medio Oriente è quello appunto dell'isolamento, essendo circondato da una serie di stati ed attori non statali a lui ostili. Questa situazione si amplia se si considerano i confini telematici. Tutti i nemici storici e "tangibili" di Israele, infatti, sono diventati dei potenziali aggressori nel cyber-spazio. *Ḥizbu 'llāh, Ḥamās o*

[418]La pagina ufficiale:
http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx

la Repubblica Islamica iraniana, sono solo alcune delle entità con le quali Israele deve competere nel cyber-spazio. A queste vanno aggiunte frotte di attivisti da tutto il mondo che cercano di portare avanti azioni cibernetiche: celeberrimi esempi sono il caso di Anonymous durante l'ultima stagione bellica contro la Striscia di Gaza nel 2012, o il caso dell'hacker saudita OxOmar che, nel Gennaio del 2012 rubò dati per quasi l'1% del totale delle carte di credito emesse nel paese.

Su questi episodi si ritornerà prima di procedere con l'analisi dell'*ecosistema* della cyber-sicurezza israeliana, prima però è rilevante fermarsi sulle principali direttrici delle minacce alla sicurezza di Israele, così come vengono percepite dalle Forze Armate: Iran, Siria, Libano e Palestina. Va aggiunto che negli ultimi anni anche la Turchia[419] e l'Arabia Saudita sono diventate pericolose fonti per i cyber-attacchi, ma le informazioni e le dichiarazioni israeliane non consentono di studiare i due fenomeni separatamente.

L'Iran, è sicuramente il principale nemico del paese sionista, anche perché senza dubbio è lo Stato più potente e con interessi più ampi nella regione (al di là della roboante politica antisemita portata avanti da parte del suo establishment). Il paese è stato straordinariamente attivo nel mondo cibernetico, tant'è che ha istituito non solo una forza di polizia e un commando difensivo, ma si è dotato di un vero *Cyber-Army*[420] e sfrutta le capacità di decine di gruppi paramilitari formati da hackers intenzionati ad aiutare la causa del proprio paese.

Numerosi sono gli episodi che riguardano il confronto tra i due paesi. Il più rilevante è sicuramente il famigerato Stuxnet, di cui si è ampiamente parlato in precedenza[421], che ha provocato un totale cambiamento delle percezioni sulle potenzialità delle *cyber-weapons*. Se ne possono però citare molti altri. Innanzitutto, per restare sulla falsa

[419] Ungerleider, N. (2011) *The middle east cyberwar: "new media fighters" battle attacks in Israel and Turkey*; Fast Company. Consultabile: http://www.fastcompany.com/1725909/middle-east-cyberwar-new-media-fighters-battle-attacks-israel-and-turkey ultimo accesso 28.02.2014

[420] Per approfondimenti sulla struttura delle Forze cyber in Iran vedi: http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf

[421] Vedi cap. 2

riga del legame tra mondo cibernetico e non, è necessario riportare i sospetti sulla natura e sullo scopo di Flame. Così come è inevitabile non parlare dell'assassinio di Mojtaba Ahmadi, il presunto responsabile delle forze del *Cyber-Army*, che sarebbe stato vittima di un attentato ordinato da Israele[422].

Anche l'Iran però non è passivo agli attacchi cibernetici. Se, infatti, sono sinora stati più fruttuosi quelli contro altri paesi mediorientali (i.e. Arabia Saudita e Qatar), anche nei confronti di Israele gli sforzi non sono stati del tutto vani: sembrerebbe esserci la mano iraniana, infatti, sia dietro l'attacco dell'anno scorso alla struttura di gestione delle acque di Haifa e dell'incidente riscontrato nel Carmel Tunnel, un condotto di viabilità che collega la città di Haifa con il centro del Paese.

Per finire, poco tempo fa, il leader supremo Khamenei, durante la commemorazione della Rivoluzione del 1979, ha avvertito gli studenti del suo paese a prepararsi alla *cyber-war*[423]: *"You are the cyber-war agents and such a war requires Amman-like insight and Malik Ashtar-like resistance. Get yourself ready for such war wholeheartedly,"*[424]*.* Questo è un episodio di notevole rilevanza perché ci fa capire quanto sia importante, anche per la Repubblica Islamica, investire sulle potenzialità cibernetiche. Del resto, non sorprende che quasi negli stessi giorni il Generale Maggiore Aviv Kochavi, Capo dell'Intelligence israeliana, dichiarasse che, presto, le componenti cyber si dimostreranno "la più grande rivoluzione negli affari militari, ancor più di polvere da sparo e aerei"*[425]*.

In conclusione, il dominio cibernetico è soltanto un'altra dimensione in cui si declina l'aspro conflitto tra la Repubblica Islamica iraniana e Israele. Entrambe le parti riconoscono le estreme potenzialità (e probabilmente ne esagerano le applicazioni presenti per ragioni di

[422]McElroy, D. e Vahdat, A. (2013) Iranian cyber warfare commander shot dead in suspected assassination, The Telegraph; 2 October 2013, Telegraph, London . Consultabile http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html

[423] RT NEWS; "Iran's supreme leader tells students to prepare for cyber war"; 13 Febbraio 2014 http://rt.com/news/iran-israel-cyber-war-899/

[424]Il Leader Supremo si riferisce a due compagni del profeta Mohamad, che lo sostennero agli albori della storia islamica

[425]La traduzione è mia e si riferisce a una dichiarazione del Generale Maggiore Kochavi, espressa alla 7° conferenza annuale dell'ISS, più volte citata, alla quale ho presenziato.

demagogia) ed si stanno impegnando, in termini di investimenti e di preparativi militari, per non lasciare all'avversario nessun vantaggio.

Siria. Sebbene al momento i problemi del paese levantino sembrino essere più focalizzati verso la situazione interna, la rivalità contro Israele si esprime fortemente nel cyber-spazio, poiché dal punto di vista dello scontro fisico il paese del dittatore alauita Assad non può permettersi uno scontro. La principale minaccia per lo stato d'Israele, al di là dell'imprevedibile Al-Qaeda, risulta essere il Syrian Electronic Army[426], un gruppo di hacker apparentemente indipendente, ma con una forte inclinazione per le forze governative siriane. Riportando le parole di Nir Todjman, un ricercatore dell'International Institute of counter-Terrorism (ICT) di Herzliya, pur non avendo affiliazione diretta con il governo siriano, è chiaro che il SEA agisce in difesa del governo di Assad. Le ragioni sono svariate, dalla scelta degli obiettivi alle modalità di attacco (phishing, DDos e tecnologie di basso costo)[427]. Il suo obiettivo è colpire coloro ritenuti sia internamente che internazionalmente come nemici dello stato legittimo siriano (i.e. il regime di Assad). Considerando la situazione nel nord del Paese (il difficile rapporto con il Libano oltre ai tempestosi confini con la guerra civile siriana) e la possibilità di sfruttare le potenzialità dell'assenza di distanza spaziale offerte dal ciberspazio, le Forze Armate e le personalità di governo israeliane sono molto preoccupate dai possibili pericoli in cui potrebbero incorrere a causa del SEA. In particolare perché, pur provenendo da un'entità apparentemente indipendente, questa sembra avere alle spalle le risorse e i fondi messi a disposizione dal governo di Assad.

In conclusione, in questo caso il confronto tra le parti risulta essere decisamente asimmetrico, ma ancora una volta, pur essendo un attore non-statale colui che offende (anche se si è visto come il SEA sia probabilmente legato al governo di Bashar al-Assad), l'obiettivo degli

[426]SEA in arabo الجيش السوري الإلكتروني

[427]Dichiarazione ottenuta durante un'intervista con il signor Tordjman e che trova riscontro in un report presentato dall'ICT http://www.ict.org.il/LinkClick.aspx?fileticket=QG0c9BKNLq0%3d&tabid=492 alla pag. 30

attacchi risulta essere sempre l'entità statale in quanto tale, attraverso i tentativi di offuscamento parziale di alcuni servizi o infezione di alcuni network.

Libano e Palestina. Per quanto riguarda il Libano certamente il principale esponente è *Ḥizbu* 'llāh, mentre per la Palestina Ḥamās. Entrambi i gruppi sono considerati da Israele come una minaccia perenne alla propria sicurezza nazionale. Dalle parole del Primo Ministro Netanyahu, scopriamo come le minacce tipiche di questi due gruppi terroristici siano considerate dall'establishment israeliano come parte del passato, ciò che veramente spaventa oggi sono gli attacchi indiretti e apparentemente non violenti. Tra questi il cyber rappresenta sicuramente una delle principali preoccupazioni.

Per questo motivo Israele mette in atto, nei confronti di entrambi gli attori, una politica di difesa preventiva che porta il paese ad essere accusato di violazioni di sovranità. Nel caso del Libano, Israele è accusata di aver violato il diritto alla privacy e alla sicurezza del Paese per essersi infiltrato nei network dell'esercito libanese e delle forze di Ḥizbu 'llāh[428]. Per quanto riguarda Ḥamās, invece, la conflittualità è decisamente più limitata perchè le forze palestinesi si concentrano su attività di tipo limitato.

Hacktivists. Come detto in principio, Israele subisce circa 150 mila attacchi cibernetici, di diversa entità, ogni giorno. Seppur vero che la maggior parte sono a scopo di lucro e riguardano i settori dell'economia e della finanza, una gran parte di questi hanno motivazioni politiche, legate alle politiche espletate dallo stato di Israele. In particolare sono tre i gruppi di attori che agiscono e tentano di creare disordine all'interno della rete israeliana. I primi due sono stati analizzati nei paragrafi precedenti, sono attori di matrice statale e para-statale. Il terzo gruppo di individui è costituito da attivisti che, per diverse ragioni,

[428]Winstanley, A. (2012) *Cyberwarfare: US, Israel's electronic attacks on Iran and Palestinians*; The electronic Intifada; 2 July 2012
http://electronicintifada.net/content/cyberwarfare-us-israels-electronic-attacks-iran-and-palestinians/11453 (ultimo accesso 28.02.2014)

bersagliano i siti, le mail e le infrastrutture israeliane per esprimere il proprio dissenso nei confronti dello stato e delle sue politiche nell'arena internazionale. Due esempi chiari di questi gruppi sono, chiaramente, Anonymous e l'Islamic Cyber Resistance Group (ICRG).

Anonymous è stato protagonista delle cronache internazionali per il suo impegno nella difesa dei diritti umani, attraverso campagne di attivismo cibernetico. In particolare, contro Israele sono state lanciate due imponenti campagne: la prima durante l'attacco da parte delle Forze Armate israeliane nella Striscia di Gaza nel novembre 2012[429], la seconda nella primavera del 2013. Secondo l'opinione del professor Ben-Israel, il gruppo sarebbe tuttavia poco preoccupante in comparazione con gli altri attori sopra descritti: "*Anonymous doesn't have the skills to damage the country's vital infrastructure. And if that was its intention, then it wouldn't have announced the attack ahead of time. It wants to create noise in the media about issues that are close to its heart".*

L'**Islamic Cyber Resistance Group** (ICRG). La sua attività più rilevante è stata quella all'interno del progetto soprannominato *opIsrael*[430]*:* il gruppo tentò di penetrare all'interno del network dell'Israel Aviation authority, ma l'attacco non ebbe apparentemente successo (le due parti hanno dichiarato risultati opposti e l'ICRG ha sostenuto che l'attacco sia andato a buon fine). Il gruppo possiede un alto grado di specializzazione e si batte all'interno dell'universo cibernetico per punire quelle che considera "le nefandezze di Israele". Un altro importante successo rivendicato dal gruppo è stata l'appropriazione di informazioni relative alla presunta collaborazione tra Israele e Arabia Saudita, impegnati in una collaborazione volta alla lotta contro lo sciismo politico (i.e. *Ḥizbu 'llāh* e l'Iran). Ufficiosamente l'affiliazione del gruppo allo Stato iraniano pare ovvia, ma, ufficialmente, ne mantiene le distanze.

[429]In risposta agli attacchi considerati sproporzionati da parte dell'esercito israeliano nei confronti dei combattenti palestinesi della striscia, Anonymous lancia un dichiarato attacco ai siti istituzionali e alle banche date dello Stato d'Israele. Per maggiori informazioni si veda, tra gli altri: http://www.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/ e http://www.bbc.co.uk/news/technology-20356757 (ultimo accesso 28.02.2014)

[430]*opIsrael* è stata una campagna di boicottaggio nei confronti di Israele portata a termine attraverso cyber attacchi (Ddos)

Per concludere, Israele è forse il paese al mondo che subisce il numero più elevato di attacchi cibernetici (in termini relativi alle sue dimensioni), per questa ragione deve impegnarsi costantemente per mantenere elevatissimi livelli di difesa. Si vedrà ora quale sono quindi gli obiettivi sensibili che il Paese cerca di difendere.

5.3.1 Obiettivi degli attacchi

La definizione operativa di cyber-spazio ci permette di analizzare concretamente non solo l'entità di questa dimensione ma anche le sue debolezze. È questo il caso anche per quanto riguarda le necessità difensive di Israele. Infatti, tralasciando la dimensione umana (che comunque rientra nella linea difensiva dell'IDF) il Paese deve occuparsi della difesa di tutti e tre i *layers* di cui si compone il cyber-spazio: quello fisico, i network e le informazioni contenute nelle banche dati. In questo capitolo ci si concentrerà prevalentemente sui primi due aspetti, in quanto la protezione dei dati è affidata prevalentemente alle entità predisposte alla crittografia e alla difesa delle banche dati, così come descritta nei capitoli precedenti. Per quanto riguarda le reti e le tangibilità del cyber-spazio vi sono un paio di questioni che è necessario approfondire.

Per quanto concerne i network le sfide sono numerose e persistenti. La necessità di mantenere un elevato livello di guardia ha fatto sì che in tutto il mondo, così come in Israele, i sistemi di monitoraggio delle reti siano uno dei più importanti elementi per mantenere alta la difesa, come si è visto in precedenza. A complicare lo scenario israeliano vi è però il fatto che non esiste un'entità unica predisposta alla sorveglianza generale né tanto meno a quella delle varie entità che si occupano di controllare le diverse porzioni del network del Paese. A questo proposito, le istituzioni israeliane si sono impegnate nello sviluppo di sistemi autonomi via via più competitivi. Vale la pena citare la proposta incrementata dalla Israel Aerospace Industries (IAI), partita da un contesto differente, quello dell'aviazione e dell'industria aerospaziale. Il progetto, come è stato spiegato da Esti

Pashin alla conferenza organizzata dalla stessa IAI nel Gennaio 2014, parte dal presupposto che si debba mantenere un persistente livello di allerta e sorveglianza, evitando però i rischi impliciti nei numerosi falsi allarmi. La soluzione a questo problema viene dalla gestione del sistema di analisi e tracciabilità a *multi-ipotesi,* nel quale la sorveglianza di un ipoteticamente infinito numero di eventi è affiancato ad uno studio in matrice di dati incrociati relativi al tempo degli attacchi e alla localizzazione. Questo perché, se si considera l'evoluzione delle tendenze di attacchi, costantemente in crescita, è necessario avere un chiaro framework di riferimento al momento della rilevazione, in modo da interpretare immediatamente il tipo e il carattere di minaccia indirizzata ad un qualsiasi network, ed eliminare la discrepanza temporale tra rilevamento dell'anomalia e la sua analisi.

Quando ci si occupa di protezione cibernetica, inoltre, è fondamentale non tralasciare le componenti fisiche. Infatti, come ricordato da Hagai Kats della Magal Security System Ltd, la sicurezza cyber non può mai essere isolata, ma deve essere integrata ed omnicomprensiva. In particolare, nel caso di Israele, al di là delle generiche problematiche legate alle componenti fisiche del cyber-spazio descritte nei precedenti capitoli, un problema particolarmente spinoso risulta essere quello dei cavi sottomarini in fibra ottica[431]. Sono questi infatti i principali elementi di debolezza del cyber-spazio gestito da Israele. Il Paese è infatti connesso alla rete unicamente attraverso tre cavi in fibre ottiche che la collegano alle sponde opposte del Mediterraneo. Il paese di riferimento, in questo senso, per Israele è l'Italia, due dei tre cavi sottomarini, infatti, sono diretti verso l'Italia: uno, il MedNautilus[432], collega Israele con la Sicilia, passando per Cipro, ed è posseduto da Telecom Italia; l'altro, gestito da Bezeq[433], collega invece Israele con un sito di Bari. Inutile dire che le Forze Armate e le cariche di governo israeliane sono estremamente sensibili alla questione, dato che, pur essendo in gran parte segretate, le informazioni di riferimento

[431]SECHRIST, M. (2012) *New Threats Old Technology: Vulnerabilities in Undersea Communication Cable Menagement Systems,* Belfer Center Harvard Kennedy School, Cambridge
[432]Per maggiori informazioni su MedNautilus: http://www.mednautilus.com/ ultimo accesso 28.02.2014
[433]Per maggiori informazioni su Bezeq: http://www.bezeq.co.il/

di questi casi sono di pubblico dominio e le vulnerabilità ad esse relative, come visto sono immense.

Infine, vorrei soffermarmi su quello che, come detto, costituisce il più rilevante campo di ricerca per l'incremento della sicurezza cibernetica: le infrastrutture civili considerate critiche (vitali) per le attività quotidiane. Sono queste un punto di contatto tra le due vulnerabilità sopra considerate, perché attraverso attacchi ai network è possibile creare delle conseguenze *tangibili* nel mondo fisico, come nel caso di Stuxnet o del Carmel Tunnel. Il punto focale della diatriba difensiva legata al cyber-spazio gravita sicuramente attorno a queste infrastrutture. Banche, ospedali, infrastrutture di trasporto, reti elettriche, sistemi di approvvigionamento dell'acqua, sono solo alcune delle possibili infrastrutture che vengono definite critiche o vitali per il Paese. In particolare, in Israele, data la forte predisposizione a legare il mondo dell'economia cibernetica a quello della sicurezza, i principali beneficiari degli sforzi nazionali di protezione sono quelle infrastrutture correlate all'universo economico, come la Bank of Israel. È questo un esempio perfetto per comprendere l'efficienza del modello israeliano. Le strutture della Bank of Israel sono in parte supervisionate dal Ministero delle Finanze, il quale ha pubblicato un ampio e dettagliato elenco di direttive sulla sicurezza informatica e sulla protezione degli *information systems* all'interno delle istituzioni finanziarie: *"Information technology is a central component in the proper operation and management of a banking corporation, as information, in all its aspects and implications, has a decisive effect on the stability of the banking corporation and its development".* Al contrario, il sistema ospedaliero e il sistema di approvvigionamento delle acque nel paese sono due casi che evidenziano il settorialismo della difesa delle infrastrutture israeliane. Il problema di fondo è la **mancanza di un approccio di tipo sistemico**, basato su uno statuto preciso, viene infatti seguito un procedimento legato all'interesse o alla percezione del pericolo, che tralascia spesso entità (anche private) estremamente rilevanti. Senza addentrarsi nello studio della *partnership* tra soggetti privati e pubblici, che verrà affrontata in uno dei paragrafi successivi, preme sottolineare come a

livello nazionale si presti poca attenzione alle istituzioni connesse al sistema- paese, che a uno sguardo disattento non sembrano rientrare nello scenario della sicurezza nazionale. Come detto, un esempio clamoroso è la gestione del sistema di rifornimento delle acque. Even e Sima-Tov (2011)[434] a proposito affermano : "*protection of water supply and water quality infrastructures in Israel does not only affect processes in Mekorot, Israel's national water company, but also dozens of other water suppliers, associations, water corporations, desalination and delivery facilities, sewage and wastewater treatment facilities, and so forth*". Lo stesso vale per le strutture ospedaliere. Ad una recente conferenza organizzata da numerose istituzioni nazionali, il cui acronimo è IPRED[435], si è discusso di sicurezza informatica nel mondo ospedaliero e dei network ad esso collegati. Inutile dire che le analisi finali hanno mostrato come il livello di sicurezza fosse incredibilmente basso[436] e la possibilità di dar vita a reali incidenti e situazioni pericolose fosse immensamente più elevata rispetto a infrastrutture legate al mondo dell'economia e della finanza.

Come accennato in precedenza, nonostante ciò comporti una rivalutazione delle potenziali minacce per la sicurezza nazionale è necessario includere la protezione delle infrastrutture considerate vitali per il Paese, in toto e non solo in maniera parziale, all'interno delle strategie e delle operazioni difensive dello Stato.

5.4 N*ational Cyber Defense:* attori e funzioni nel modello israeliano

In un articolo pubblicato recentemente[437] da Rami Efrati, il Capo della sezione Affari Civili del National Security Bureau, ci si domanda se la protezione del cyber-spazio sia da interpretare e considerare come la

[434]Even, S. e Siman-Tov, D. (2012), *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 INSS Publ., Tel Aviv

[435]IPRED III: http://video.new-app.com/customers/ipred/

[436]La dimostrazione di Ram Levi ha mostrato l'inefficienza del sistema di sicurezza di una importante infrastruttura ospedaliera

[437]Efrati, R. Yafe, L. (2013) *The challenges and opportunities of National Cyber* Defense, ISRALE DEFENSE, Tel Aviv. Consultabile http://www.israeldefense.com/?CategoryID=512&ArticleID=1557 ultimo accesso 28.02.2014

protezione di qualsiasi altro dominio spaziale considerato sino ad ora. Efrati si chiede "*chi è il protettore naturale (del cyber-spazio)? È l'esercito l'organo adatto a proteggere*" i confini? Questa domanda, come visto in precedenza è centrale per uno Stato come quello israeliano nel quale non esiste l'equivalente di una *National Security Agency* americana e nel quale la difesa viene interpretata da svariati organi preposti a funzioni limitate, ma che mancano di un controllo centrale.

È per questo importante, prima di iniziare un'analisi e suggerire delle raccomandazioni, avere una chiara idea di quali siano gli attori coinvolti nella *cyber-security* israeliana, di quale sia la loro relazione ed appartenenza e quali i loro compiti. È soprattutto necessario fare una differenziazione netta tra sicurezza nel mondo civile e in quello militare, per cercare di ritrovare poi delle possibili interazioni tra i due.

5.4.1 NISA

Il ruolo della NISA, è quello di proteggere le infrastrutture critiche. Come detto in precedenza, con la legge B/84 del 2002, si è istituita formalmente la responsabilità dell'*Authority* a controllare e consigliare le imprese private e pubbliche, per quanto riguarda la protezione delle componenti informatiche nei sistemi di gestione delle infrastrutture nazionali indirizzate a provvedere alle funzioni vitali per il regolare svolgimento dell'esistenza civile del Paese. Questo organo è gestito all'interno dell'ISA (Israel Security Agency), che pur essendo predisposto alla difesa del Paese, non fa capo né alle Forze Armate israeliane e né al Ministero della Difesa, bensì rientra sotto la copertura diretta del Primo Ministro.

Il punto nevralgico per il funzionamento della NISA (e, più globalmente, della ISA) sta nello sviluppo di tecniche di acquisizione di informazioni e nell'analisi delle minacce passate. La capacità operativa dell'Autorità si basa sulla possibilità di ottenere dati di intelligence capaci di prevedere attacchi futuri, nel monitoraggio in tempo reale delle infrastrutture e nella consapevolezza della miglior fonte tecnologica per

far fronte alle corrispettive minacce. Per questo, una delle unità più importanti è quella di Sviluppo delle Tecnologie IT, che svolge il fondamentale compito di armonizzare le necessità di sicurezza con le possibilità tecnologiche a disposizione.

Tra le entità supervisionate dalla NISA vi sono la Banca d'Israele, la Israel Electric Corporation, le Ferrovie Israeliane, compagnie di fornitura dell'acqua (i.e. Mekorot) e molti altri servizi. Per questo motivo è forse l'organo più sensibile, perché svolge una serie di funzioni che gli permettono di essere una punto centrale per l'interazione multi-livello nella gestione della sicurezza nazionale. È infatti la NISA che interpreta le necessità di sicurezza richieste nella gestione della Difesa e la comunicazione con entità private che non rientrano in questo schema, ma che inscindibilmente ne fanno parte. Come detto, è infatti inevitabile che le imprese private che gestiscono le infrastrutture considerate rilevanti (o critiche o vitali) del paese, siano punti deboli e vulnerabili, ma è altrettanto inevitabile che, per ragioni politico-culturali e per logiche di mercato queste entità decidano di restare indipendenti anche dal punto di vista della protezione e della sicurezza. Questione che, come visto e come si vedrà in seguito, è estremamente sensibile per l'*ecosistema* che si sta cercando di studiare.

5.4.2 National Cyber Bureau (NCB)

Il Cyber Bureau è oggi l'entità più importante a livello nazionale e internazionale nello spettro delle istituzioni che si occupano di cyber-sicurezza in Israele. La NCB è inserita all'interno dell'Ufficio del Primo Ministro ed è gestita da Aviatar Matania. La sua funzione al momento è puramente consultiva, ma in una recente conferenza sulla *cyber-security* sia il Primo Ministro *Bibi* Netanyahu sia Dr. Matania hanno dichiarato che verrà formato un CERT nazionale, sotto l'egida dell'NCV, che rientrerà all'interno dell'operazione di rivitalizzazione del sud del Paese. Secondo le parole del PM Netanyahu[438], l'intento è quello di creare un *cyber hub* e un *cyber spark* nella città di Be'er Sheva:

[438]Dichiarazione rilasciata durante un intervento a Cyber Tech 2014, Tel Aviv

attirando investimenti e multinazionali straniere nel settore della *cyber-security*[439] e allo stesso tempo sviluppando un centro nevralgico di coordinazione delle attività tra settore militare, imprese e accademia.

Al momento questa operazione è ancora *in potenza* e molti osservatori sono scettici sulla possibile efficienza dell'istituzione del CERT e della centralizzazione sotto il NCB. Il suo ruolo oggi è quello di portare avanti raccomandazioni di politica nazionale nel campo della difesa cibernetica e della promozione della sua implementazione, in accordo con la legge e le implementazioni di governo.[440] Gli obiettivi principali sono agevolare la *preparedness* del Paese e aumentare la sicurezza informatica delle infrastrutture critiche (collaborando difficoltosamente con la NISA).

Tutti i suoi compiti specifici sono racchiusi nella Raccomandazione n° 3611 dell'agosto 2011 e tra questi, oltre alla funzione consultiva sopra citata, vi sono i seguenti:

- Aumentare la coordinazione e la cooperazione tra i vari corpi governativi, la comunità di difesa e tutti gli altri organi rilevanti nel campo del *cyber;*
- Produrre sviluppi nel campo della legislazione e nella produzione di norme;
- Produrre un concetto nazionale che valga per le situazioni di emergenza;
- Essere l'intermediario con il pubblico, con l'intento di aumentare la consapevolezza a tutti i livelli della società riguardo ai possibili pericoli per lo stato derivanti dal cyber-spazio;
- Promuovere lo sviluppo e la ricerca nel settore e agevolare il settore accademico e quello industriale;
- Sostenere la cooperazione internazionale.

[439]Lockheed Martin, Google Microsoft le principali.
[440]Raccomandazione B/3611, si veda dopo

5.4.3 L'universo Militare

In Israele la rilevanza delle Forze Armate è pregnante in tutti i livelli della vita sociale, ancor di più lo è quando si entra nell'ambito della Difesa e della Sicurezza Nazionale. A differenza di molti altri paesi (soprattutto nel panorama degli stati considerati occidentali), la presenza del mondo militare all'interno dei processi di *decision-making* e di gestione è ancora molto spesso sproporzionata rispetto alla componente civile, anche perché spesso questa distinzione è solo formale. Infatti, frequentemente chi ricopre cariche rilevanti per la sicurezza proviene dal mondo militare e mantiene dei saldissimi legami e condivisione di interessi con questo.

Questo fenomeno genera una serie di conseguenze, in primo luogo una mancanza di trasparenza nella separazione netta delle responsabilità civili e militari nella gestione della Sicurezza Nazionale. Questo scenario è poi amplificato dall'assenza di strategie pubbliche e ufficiali di Difesa. Scelta che potrebbe essere anche stata intrapresa dalle Forze Armate e dai Ministri della Difesa per fornire meno riferimenti possibili a eventuali nemici nel caso avessero intenzione di portare a segno attacchi o attentati. La natura evolutiva delle minacce allo Stato stanno rendendo necessaria una modifica di questo paradigma. Secondo le parole del General Maggiore Gadi Eizenkot dell'IDF: "*The Yom Kippur War was the last war in the world where the (opposing) forces maneuvered against one another and employed massive fire and air power. Today's (military) essence is different*." Infatti, la predilezione degli attacchi terroristici in prima battuta e la nascita di modalità di attacco non convenzionali ma non letali (i.e. i cyber-attacchi), hanno reso necessario una maggiore esposizione delle Forze Armate e una crescente partecipazione nella gestione della Difesa.

È fondamentale ricordare che quando si parla di rapporto tra le Forze Armate e la Difesa in argomenti ed ambiti sensibili le informazioni sono per la maggior parte secretate e tenute confidenziali all'interno del mondo militare, e per lo più tra gli Alti Gradi di comando. Perciò, l'unica

cosa che si può fare per avanzare la ricerca è basarsi su dichiarazioni ufficiali di esponenti di spicco del mondo militare o su ciò che si evince dal rapporto politico con il mondo civile. Seguendo questo metodo d'indagine, spesso poco scientifico, sembra di che stia prendendo piede una nuova impostazione strategica per far fronte alle nuove minacce sopradescritte, in una prospettiva di lungo periodo.

I nuovi sviluppi della suddetta strategia militare sono legati prevalentemente al fatto che gli obiettivi degli attacchi (spesso provenienti da entità non statali o parastatali) sono in maniera crescente identificabili con obiettivi civili e allo stesso modo. La provenienza degli attacchi è sempre più incerta perché sapientemente celata all'interno dello scenario civile, sia che si parli di razzi sia che ci si riferisca ad attacchi informatici. La principale prospettiva per le Forze Armate israeliane è stata, sinora, quella di incrementare le fonti di *intelligence* e strutturare una difesa multi-livello in modo da ovviare alle pericolosità delle minacce asimmetriche. Sempre secondo il General Maggiore Eizenkot: *"What will be required in the future is an improved intelligence capability at the tactical, operational and strategic levels; an improved defensive layout; improved fire potential on a very large scale; an improved offensive potential, and defensive and offensive capabilities. (…) Another key issue that we have had on the agenda for some time – the change in the national scale of priorities, so that all elements of society share the burden.*"[441]

La natura asimmetrica delle minacce influenza la gestione strategica della Difesa in particolare in relazione alla possibilità di generare deterrenza. Gli *early warnings* e la crescita dell'allerta tattica sono oggi difficilmente percepibili, soprattutto nel mondo della *cyber-security,* per questo, secondo gli strateghi militari israeliani, sembra essere necessario un nuovo paradigma che non si basi unicamente sull'osservazione passiva ma sulla prevenzione di minacce attraverso la combinazione di intelligence e difesa (e offesa) multi-livello. Un concetto difensivo proattivo che verrà ampiamente studiato successivamente.

[441]Il Gen. Mag. Eizenkot ha parlato al Cyber Tech 2014, Tel Aviv

Se si osserva la composizione delle Forze Armate e si considera la rilevanza delle rispettive Unità nella gestione della Sicurezza cibernetica, sono principalmente due le entità incaricate di mantenere la sicurezza del Paese: la C4I e l'U8200.

5.4.4 C4I

L'unità chiamata C4I[442], che è l'acronimo in inglese di *Command, Control, Communications, Computers, and (military) Intelligence*, è senza dubbio il più rilevante corpo militare che si occupa di *cyber-warfare*. La sua missione principale è di mantenere operative e funzionanti le reti del paese. Il corpo è responsabile dei mezzi operativi di *teleprocessing*, il che significa, in generale, il coordinamento dei vari rami delle Forze Armate (dal livello del *General Staff* al livello più basso). Inoltre, costruisce e gestisce le infrastrutture telematiche all'interno dell'IDF ed è responsabile delle frequenze, pubblica le istruzioni operative e di manutenzione tecnica.

La missione del corpo è quella di plasmare le capacità dell'IDF e rendere operative azioni integrate in terra, aria e mare, migliorando al contempo l'efficacia operativa e l'utilizzo delle risorse cibernetiche. Sono inoltre incaricati di creare un metodo unificato per i processi di test, per ottemperare alle esigenze tecniche e nell'uso dei mezzi di comunicazione. Inoltre è incaricato di creare e gestire un sistema difensivo dei network informativi delle Forze di Difesa israeliane. In poche parole le funzioni di questo gruppo operative sono autoreferenziali: l'obiettivo della protezione sono le strutture e i network unicamente militari, ma con un forte interesse a portare sotto uno stesso ombrello protettivo tutte le forze, marine, terrestre e aeree.

La sua formazione (o la sua ufficializzazione) risale al 2003 ma recentemente sono state rivisitate la struttura e la composizione. Per quanto riguarda la composizione, il numero dei membri è stato recentemente aumentato (nonostante la tendenza generale delle forze armate israeliane a diminuire gli effettivi), ed è stato pianificato un

[442]Cfr. http://www.idfblog.com/about-the-idf/idf-units/c4i-computers-and-communications/

ulteriore aumento nei prossimi cinque anni, per incrementare la connettività tra le diverse forze militari: l'idea è quella di collegare tutti i posti di comando sul campo e lo schieramentp di posti di comando di supporto mobile anche per gradi di comando inferiori.

Per quanto riguarda invece la struttura il discorso è più ampio e rientra a pieno titolo nell'analisi dell'evoluzione delle strategie delle forze armate dovute a una mutevole natura delle minacce, di cui si è parlato in precedenza. Lo schema interno è stato rinnovato per cercare di aumentare l'efficienza del corpo e per cooptare alla trasformazione del sistema di Difesa israeliano in uno prevalentemente *network-centered* (altamente dipendente dalle possibilità offerte dalle tecnologie ICT)[443]. Per questo, in risposta alle numerose critiche emerse nel passato che accusavano C4I di essere inefficiente per via della mancanza di visione globale e di leadership, sono state create numerose unità specializzate, coordinate in ultima istanza a livello centrale. In particolare è importante menzionare l'unità Hoshen, responsabile delle comunicazioni; la Mamran, il Centro responsabile per le attività di gestione e protezione dei computer e degli *Information systems*; e il Centro per la crittografia di cui si parlerà a breve.

Per concludere, C4I ha due importantissime funzioni: è il centro delle attività di crittografia e sviluppa sistemi operativi di Comando-e-Controllo a livello del campo di battaglia. A proposito di quest'ultima funzione C4I sta lavorando a progetti prevalentemente focalizzati su sistemi mobili di coordinazione, altamente integrati[444]. Per quanto riguarda le sue funzioni crittografiche, la questione è molto rilevante. Data la natura delle operazioni, la maggior parte dei dettagli sono secretati ma si è a conoscenza di alcuni dettagli rilevanti. E' il Center for Encryption and Information Security (CEIS), un'unità militare segreta, ad occuparsi di criptare e decriptare messaggi rendendo possibile le comunicazioni tra piloti e le loro basi, nell'eventualità di funzione

[443]Cfr. capitolo 2

[444]Dichiarazione di Dorom Rotem, Direttore del C4I, a Cyber Tech 2014, Tel Aviv

dell'Iron Drome[445] e in moltissime altre situazioni. Il Centro è parte della IDF, ma è considerata come un'unità nazionale in quanto fornisce la soluzione e i mezzi per crittografare ogni bit di informazione che deve essere trasmessa attraverso la comunicazione radio e deve essere codificato in Israele. È importante riprendere il concetto, espresso in precedenza, della rilevanza della crittografia nella cyber-difesa, non solo perché uno degli obiettivi principali perseguiti è per l'appunto l'appropriazione di dati sensibili, ma perché grazie ad essa è possibile nascondere il contenuto di messaggi operativi che stanno alla base di azioni concrete relative al funzionamento dei network e delle infrastrutture critiche. Il Generale Brigadiere Danny Bren, Comandante dell'Unità Lotem, ha dichiarato a riguardo che sono numerosissime nel dominio tattico le implicazioni del lavoro del C4I in termini di crittografia[446], in particolare facendo riferimento a *"the importance of cryptography (has to do) with the technological changes the IDF underwent over the last few years. Like other military organizations around the world, the IDF has also become a technology-based military and as such, communication and data networks became a primary tool of the tactical echelon*". Per questa ragione è così importante essere maestri nell'arte di criptare e decriptare: per ovviare alle debolezze intrinseche che l'integrazione delle tecnologie di informazione e comunicazione hanno portato sul campo di battaglia, che è oggi interamente dipendente da queste e relativamente vulnerabile.

5.4.5 *U8200*

L'unità 8200 è un Corpo di Intelligence israeliano[447] responsabile della raccolta dei *signal intelligence* (SIGINT) e per la decriptazione dei codici. È un'unità speciale, che vanta numerosi *alumni* di rilievo nella vita pubblica e politica israeliana: per citarne due estremamente rilevanti, il Presidente della Verint System Inc. e il Presidente della

[445]Grandoni, D. (2012) Israel's '*Iron Drome' Anti-Missile System is Scary* Efficient, 12 marzo, the Wire. http://www.thewire.com/global/2012/03/israels-iron-dome-anti-missile-system-scary-efficient/49769/ ultimo accesso 28.02.2014

[446]Estratto da http://www.israeldefense.com/?CategoryID=512&ArticleID=2675 ultimo accesso 28.02.2014

[447]Israeli Militari Intelligence (AMAN)

CheckPoint Software Technologies Ltd[448]. Negli ultimi anni quest'unità è diventata rinomata internazionalmente perché considerata endemicamente interconnessa al boom economico del settore hi-tech (e in particolare del cyber). Ciò che è rilevante a questo punto della trattazione è identificare le responsabilità dirette dell'Unità nella gestione e nella protezione dello spazio cibernetico.

La maggior parte delle informazioni riguardanti le attività concrete di questa Unità sono ovviamente celate dal segreto di stato: Fino a poco più di dieci anni fa l'esistenza stessa dell'Unità era mantenuta sotto il segreto militare, ma il già citato boom tecnologico e la pubblicazione del (demagogico) "*Start-up Nation*" di Sanor e Singer[449], hanno contribuito a diffonderne il mito e a svelarne i segreti. Nonostante ciò, è noto che il compito principale dell''Unità 8200 è quello di intercettare, monitorare e analizzare le comunicazioni nemiche e del traffico dati: dal telefono cellulare alle e-mail, da traiettorie di volo e segnali elettronici. L'obiettivo del gruppo è to "*fish out from an ocean of data the piece of information that will help the Israeli security forces identify and thwart a potential attack*"[450]. Questo non deve trarre in inganno, infatti secondo Meir Elran l'Unità 8200 non è l'equivalente della National Security Agency Americana, infatti non ha un mandato subordinato per quanto riguarda gli affari interni, ma è in qualche modo orientata verso la raccolta dati provenienti da fonti esterne. L'Unità ha una base nel deserto del Negev (visibile persino su Google Maps), e diversi altri impianti in tutto il paese, ma la posizione precisa di queste strutture resta segreta, così come l'identità del comandante attuale, il bilancio del gruppo, e il numero esatto di soldati e ufficiali in servizio nell'Unità.

La rilevanza dell'Unità 8200 nello specifico della cyber-*warfare* risale probabilmente a molto prima, ma nel 2009 il Capo di stato Maggiore israeliano Generale Gabi Ashkenazi, definisce il cyber-spazio

[448] Per la Verint System Inc (http://www.verint.com/) Dan Bodner è Presidente e manager, così come Gil Schwed lo è per la CheckPoint Software Technologies Ltd (http://www.checkpoint.com/).

[449] Sanor e Singer, op. citata

[450] Buck, T. (2013) *Israel Army to Tech Start-up,* Financial Times, London http://www.ft.com/intl/cms/s/0/d45b0c5c-1a83-11e1-ae4e-00144feabdc0.html?siteedition=intl#axzz1wsFEuw3X

come uno "*strategic and operating space for Israel*"[451] e istituisce una Commissione e una sotto-Unità all'interno della Unità 8200, specificamente indirizzate a proteggere i network e le infrastrutture militari dalle minacce provenienti da attori esterni, attraverso l'incremento dell'Intelligence mirata.[452] Il compito dell'Unità non si riduce alla protezione, ma è fortemente decentrato verso un'interpretazione proattiva della difesa cibernetica: la prevenzione delle minacce da un lato e il supporto per le operazioni militari (e.g. scenari di confine) dall'altro.

L'Unità 8200 è anche stata molto utile nel sostegno di operazioni offensive, nella ricognizione di dati e nella penetrazione di sistemi di difesa avversari. In particolare ha giocato un ruolo determinante nell' Operazione Orchard del 2007 ai danni della Siria, dove sembra essere stata l'artefice dell'attaccoal sistema anti-aerei dell'Aviazione siriana.

5.4.6 Mossad (The Institute for Intelligence and Special Operations)

E' la vera "entità oscura" della cyber-sicurezza (e della *cyber-warfare)* israeliana. Impegnato prevalentemente nel combattere entità ostili appartenenti ai vicini stati di Iran, Siria e Libano, (e.g. the Syrian Electonic Army). Le informazioni che riguardano le attività del Mossad in campo cibernetico sono poche e spesso provenienti da fonti poco affidabili, ma vi è la certezza che vi sia una forte attenzione da parte dell'*intelligence* israeliana per la prevenzione di attacchi da parte di Stati e organizzazioni ostili. In particolare il Mossad è stato accusato dall'Iran di essere la *longa manu* dietro a due importanti eventi che hanno colpito lo stato sciita: l'offensiva del virus Stuxnet nella base di Natanz (vedi) e l'assassinio di Mojtaba Ahmadi, il presunto Comandante dell'Unità dedita al *cyber-warfare* in Iran.[453]

[451]Oren, A (2010) "The IDF's New Battlefield is Found in Computer Networks," *Haaretz*, Gerusalemme http://www.haaretz.co.il/misc/1.1182490
[452]Gil Baram, op. citata p 37
[453]Cfr. http://www.israeldefense.com/?CategoryID=483&ArticleID=2492

5.5La strategia israeliana

Pur non avendo un documento chiamato "Strategia", gli osservatori del sistema israeliano hanno considerato come tale la Risoluzione 3611 pubblicata nel 2011, dopo la *Cyber National Initiative.* Sia il rapporto di Mc Afee citato ripetutamente, che i lavori della Hathaway (2013)[454] adottano questa impostazione. Invece, gli scienziati politici che hanno osservato la situazione israeliana dall'interno del Paese[455], hanno preferito rimarcare il fatto che una vera e propria strategia non esista e il set di regole pubblicate nella Raccomandazione suddetta non siano sufficienti. Tralasciando la diatriba per un'analisi finale, e considerando le promesse sia di Nethanyau che di Metanya, sul fatto che nei prossimi sei mesi il National Cyber Bureau pubblicherà un documento ufficiale identificabile con la Strategia cibernetica israeliana (corredata da una sorta di *code conduct* per il cyber-spazio), costruirò la mia analisi partendo dalla Raccomandazione del 2011 e dalle dichiarazioni da me raccolte durante il mio periodo di studio in Israele.

Nella Raccomandazione, si possono ritrovare una serie di indicatori importanti per quanto riguarda la *governance* del paese in materia di cyber-difesa. Innanzitutto, con l'istituzione del National Cyber Bureau, vengono ad esso attribuiti alcuni ruoli, che in precedenza, come voluto dalla legge 84/D del 2002, appartenevano all'ISA o al Ministero degli Affari Esteri. Nonostante vi sia la premura nel testo di definire il Bureau come un organo meramente consultivo, la sua ideazione cela chiaramente intenzioni più lungimiranti. Secondo i suoi promotori, dovrebbe infatti diventare presto[456] il centro principale della sicurezza cibernetica israeliana, capace non solo di elaborare teorie, analizzare minacce, ma soprattutto di raccogliere informazioni da tutti gli organi nazionali preposti alla Difesa e gestirne prontamente i dati. Ciò che

[454]Hathaway, M (2013) *Cyber Readiness Index 1.0,* Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge

[455]Baram (2013) op. citata e Tabansky(2013) op. citata

[456]Questa funzione è endemicamente connessa con il progetto Be'er Sheva di cui si parlerà a breve.

manca per il momento è la presenza di fondi, personale, strutture e la legittimità da parte delle altre istituzioni nazionali (comprese quelle militari)[457].

In termini più generici, la *cyber (military) strategy* israeliana si basa su una serie di pilastri fondamentali: (i)la grande capacità di raccogliere intelligence; (ii) la necessità di costruire meccanismi di deterrenza; (iii) la cooperazione internazionale; (iv) la "cyber-risposta-flessibile", a seconda della possibilità o meno di attribuzione del colpevole; (v) una forte collaborazione con il settore privato e tra il mondo militare e quello civile (*multy-sector approach*); (vi) la ricerca di soluzioni multi-disciplinari alle problematiche cibernetiche (ovvero non solo cyber, ma sicurezza *in toto*)[458].

Se invece si considera l'approccio da un punto di vista più focalizzato alla strategia difensiva, è subito chiaro che l'impostazione è quella della più volte citata difesa proattiva, in cui le componenti di inteligence e difensa mobile giocano un ruolo essenziale.

5.6 L'*ecosistema* nazionale: uno scenario più ampio della semplice Difesa

Quando si parla di cyber-security è necessario pensare che, come tutti i sistemi di difesa, non sia un modello nel vuoto[459], bensì uno di protezione che si ricava da impostazioni sociali e istituzionali preordinate. Infatti, ad esempio, è la NISA l'organo incaricato della protezione delle infrastrutture, un organismo creato recentemente ma che si innesta sul più anziano ISA. Questo perché è più naturale

[457]Senza entrare in diatribe di politica interna, è importante ricordare che, essendo il Cyber Bureau sotto le dirette dipendenze del Primo Ministro, conferirebbe a questi un importante ruolo in ermini di leadership della Difesa, poco bilanciato dalle altre istituzioni

[458] Questo elenco deriva da due interventi alla conferenza Cyber Tech 2014 che avevano come argomento principale la *cyber defense strategy di Israele.* Il primo di Aaron Eilat, un Senior Director del C4I, e di Orem Bratt, Cyber Director dell'IMI (Israel Military Industries)

[459] Van Creveld p. riguardo all'evoluzione tecnologica delle armi come espressione della società che le inventa e produce. L'espressione è pregna di significato anche in questa accezione

modificare un organismo già esistente, piuttosto che crearne uno ad hoc.

Un discorso simile è possibile farlo per tutto ciò che riguarda il modello difensivo, ma che non rientra preminentemente all'interno del sistema-Difesa, quindi esterno a organismi governativi e militari.

Pur non essendo mia intenzione addentrarmi nella descrizione delle abitudini sociali e le tendenze personali riferite al mondo virtuale, è importante ricordare che, quando si parla di Israele, è necessario considerare l'ambiente altamente tecnologizzato in cui vive la popolazione. La presenza (e la dipendenza) del cyber-spazio nelle attività quotidiane è infatti molto elevato. La connessione è ormai una parte imprescindibile di ogni servizio offerto al pubblico. Per citarne alcuni: esiste una banca dati riguardante pazienti e malattie; i servizi bancari on-line sono all'avanguardia da circa due decenni; le percentuali di settore commerciale che per almeno una parte della loro attività passano attraverso internet si avvicina al 10%[460]. Infine, gli israeliani sono tra i più presenti sui social networks[461] sia in termini di percentuale di utilizzo che di ore per persona.

La pressante presenza del cyber-spazio nelle quotidianità degli israeliani non è sufficiente a spiegare di *per sé* nessuna delle caratteristiche del sistema difensivo del paese, è necessario pertanto osservare minuziosamente il mondo delle entità accademiche, delle imprese e dei privati che sono più o meno direttamente coinvolti nella gestione e nella protezione del cyber-spazio.

In primis, le università hanno il compito di preparare i singoli individui ad ottenere quelle competenze necessarie per prendere parte attivamente alla difesa del cyber-spazio a livello nazionale. Ciò che però è maggiormente influente nella descrizione dell'*ecosistema* cibernetico è il ruolo di alcuni atenei e organismi come consiglieri e teorici delle *best-practices* da seguire per migliorare i livelli di sicurezza cibernetica a livello nazionale. In secondo luogo, il settore dell'industria e del mondo

[460]Per cifre più precise http://ennovate.withgoogle.com/files/E-conomyEnglish.pdf

[461]Winkel, M. (2013) *The Global Social Network Landscape*, pag 30. Consultabile: http://www.optimediaintelligence.es/noticias_archivos/719_20130715123913.pdf; e le statistiche pubblicate da Statistic Brain: http://www.statisticbrain.com/social-networking-statistics/ ultimo accesso 28.02.2014

privato sono al centro dell'analisi per capire come questi contribuiscono al panorama della sicurezza cibernetica e come sono spesso lasciati indifesi, da parte degli enti governativi e militari, nella gestione dei propri sistemi. Questione critica, perché le funzioni di privati e imprese sono spesso rilevanti (o critiche) per le funzionalità essenziali del sistema-paese. Sarà questa la sede anche di un breve ragionamento sulla rilevanza della penetrazione statale- e militare- nella gestione delle entità private, considerando gli immanenti concetti di sicurezza e libertà sociali e personali.

Quella che segue è una descrizione delle maggiori entità extra governative ed extra militari che contribuiscono ad arricchire l'*ecosistema cibernetico* di cui si è parlato. Alla quale segue una breve descrizione delle interazioni tra i diversi settori sin ora analizzati: quello governativo, quello militare e quello meramente civile.

5.6.1 L'accademia

Il mondo accademico in Israele è eccezionalmente florido, particolarmente per quanto riguarda le materie scientifiche e le applicazioni di queste al mondo militare. Il legame tra mondo accademico, governativo e militare è particolarmente florido. In particolare vi sono quattro entità principali che vanno analizzate nello specifico.

Università del Negev - Ben Gurion. Il primo organismo da considerare è l'Università di Ben-Gurion, nel sud del Paese, nella regione del Negev. La sua rilevanza nel settore della sicurezza cibernetica è dovuta a tre componenti principali. Innanzitutto, a livello didattico l'Università ha portato avanti un progetto in cui ha fondato un istituto, l'*Homeland Security Institute,* il cui compito è quello di analizzare la sicurezza nazionale sotto tutti i punti di vista. Il grafico

sotto riportato[462] mostra la ripartizione delle aree d'interesse. Risulta chiara l'importanza che svolge per questo istituto la sicurezza relativa alla *cyber-security*[463]. Il responsabile degli studi in questo settore, la professoressa Bracha Shapira, dopo lunghi studi sulle pericolosità del cyber-spazio, sta sviluppando studi empirici sulle strategie da adottare nei confronti di attacchi cibernetici (in particolare malware diretti verso *wireless devices*). Nelle parole della stessa ricercatrice la sfida è *"(to) develop new technologies and new algorithms to defend and protect users (against cyber-attacks)*" L'analisi è diretta a tutti i livelli. Il livello basilare della ricerca è la protezione dei singoli *users (*con accento sulle entità che sono collegate alla rete attraverso tecnologie *wireless*). Per quanto riguarda la protezione delle imprese, l'accento è posto sulla protezione di informazioni rilevanti e sul rilevamento di possibili *leaks. I*nfine, a livello nazionale, il focus della ricerca è lo sviluppo degli algoritmi che agevolino il riconoscimento di anomalie a infrastrutture critiche e a network sensibili.

[462]Ho scelto di riportare il grafico del corso in Homeland Security perché riporta precisamente quelle che sono le principali minacce sulle quali sta lavorando l'IDF (Israel Defense Forces) in termini di incrementazione della Difesa. La stessa ripartizione, infatti, è stata proposta dal General Maggiore Aviv Kohavi, capo dell'Intelligence Militare nell'IDF, durante una presentazione dal titolo "*Strategic, Operational and Intelligence Challenges"* durante la 7° Conferenza annuale dell'INSS precedentemente citata

[463] Una presentazione può essere vista a: http://in.bgu.ac.il/en/hsi/Pages/Movie.aspx ultimo accesso 28.02.2014

La seconda componente da evidenziare è sicuramente la collaborazione diretta con le agenzie di Stato e con il mondo delle imprese. Due casi sono particolarmente rilevanti per l'indagine qui proposta: la cooperazione con il Ministero della Difesa e quella con i laboratori di ricerca della Telekom tedesca per lo sviluppo di tecnologie di *Information Technology*[464]*.*

Terzo punto, il Centro di Be'er Sheva dell'Università Ben-Gurion è il recipiente di investimenti milionari da parte del governo per la costruzione dell' *Advanced Technology Park (ATP)*[465]*,* cioè un luogo di cooperazione tra università, settore privato e Forze Armate[466] per lo sviluppo di tecnologie dedicate alla sicurezza nazionale. Questo progetto, che sino ad ora è stato indirizzato verso aree di ricerca quali le Telecomunicazioni, la medicina e la Biomedica, diventerà, secondo le previsioni di gran parte dell'establishment israeliana, il principale centro per lo sviluppo dell'economia e della difesa cibernetica. L'idea è quella di convogliare in un unico luogo migliaia di esperti, le sedi delle principali imprese nazionali ed internazionali nel campo della sicurezza informatica e la sede di rilevanti Unità delle Forze Armate (i.e. U8200 e C4I) così da dare vita ad un *cyber-spark, nel* quale sia possibile sfruttare al massimo il circolo virtuoso di investimenti e ricerca per la produzione di tecnologie e sistemi all'avanguardia per la difesa di utenti, network e infrastrutture; e un *cyber-hub,* dove convergano le principali entità della Difesa, che possano comunicare e lavorare a stretto contatto per lo sviluppo delle tecniche e strategie innovative nel campo sicurezza cibernetica . Secondo le più rosee previsioni questo centro dovrebbe essere anche propedeutico alla formazione di un sistema

[464] Sul sito dell'Università si legge: "*University has been collaborating with Telekom Innovation Laboratories in the field of network security since 2004. The close and fruitful cooperation between the two institutes led to the signing of an agreement for the founding of Telekom Innovation Laboratories at Ben-Gurion University. Here, leading scientists collaborate with Telekom Innovation experts to translate their visions for the future design of information technology and telecommunications into reality. In this way, Telekom Innovation Laboratories pools the know-how of Deutsche Telekom AG with the expertise of some of the world's top research scientists. Telekom Innovation Laboratories serves as a crystallization point, where cutting-edge knowledge is boldly transformed into revolutionary technologies of the future*"

[465] Il sito dell'Advanced Technology Park http://www.atp-israel.com/ ultimo accesso 28.02.2014

[466] Dalle fonti si ricava che "*The Israel Defense Forces are building a 2-million-square- foot high-tech telecommunications R&D center next to the park that will attract private contractors who will generate further opportunities for collaboration*"

centralizzato di difesa che fa capo al neo istituito CERT gestito dal *National Cyber Bureau.*

Yuval Ne'eman Workshop for Technology, Science and Security. Un altro centro nevralgico è il workshop formatosi all'interno dell'Università di Tel Aviv, con lo scopo di creare un dialogo tra pubblico, mondo accademico e istituzioni nei campi della sicurezza legati inscindibilmente alle capacità tecnologiche, quali le politiche spaziali israeliane e, ovviamente, quelle legate al cyber spazio. Il focus del Workshop è fortemente centrato su politiche nazionali e sull'elaborazione di relative strategie operative. Il direttore dello Yuval Ne'eman è proprio il Generale Maggiore Isaac Ben Israel, figura di spicco nel mondo della cyber-difesa israeliana. Infatti, tra i vari incarichi ricordati in precedenza, il Professor Ben Israel è stato il responsabile e il capo della Commissione che ha prodotto la Raccomandazione 3611 (vedi sopra) che ha portato alla formazione del *National Cyber Bureau,* organo fondamentale per l'amministrazione della cyber-sicurezza, e con il quale il Workshop ha ancora oggi uno strettissimo livello di collaborazione[467].

Come detto, scopo principale del Workshop è diffondere la consapevolezza e i livelli di *awareness* all'interno delle istituzioni governative. Le direttrici di questa opera che il Workshop sta portando avanti dal 2002, anno di fondazione, sono la protezione di internet e dei social networks; i dilemmi etici e psicologici che porta con sé il nuovo dominio cibernetico e la prospettiva di un'ampia collaborazione internazionale sancita attraverso la stesura di Trattato internazionale, volto a regolarizzare i comportamenti e le azioni .Il tutto veicolato allo studio delle possibilità di uso della forza e delle sue conseguenze, analizzate in rapporto allo sviluppo delle nuove tecnologie.

[467]Inoltre in veste di teorico e stratega militare, il professore Ben-Israel è da molte fonti considerato l'ideatore dell'attacco aereo israeliano alle presunte infrastrutture nucleari sirianedel 2007, reso possibile solo grazie all'annullamento, non scoperto, dei radar siriani. Per maggiori informazioni sulla cosiddetta Operazione Ochard si veda: http://www.phantomreport.com/israel-invests-millions-in-drive-for-elite-cyber-warriors-unit-8200 e http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

Inoltre lo Yuval Ne'eman Workshop è stato l'autore della prima reale esercitazione cibernetica[468] svoltasi in collaborazione con unità militari, enti governativi e altri istituti di ricerca. L'entità dell'esercitazione ha subito un aumento nel livello di pericolosità e rilevanza del conflitto[469]. Se infatti inizialmente la questione consisteva in un tentativo di Al Qaeda di penetrare nei network israeliani per provocare disordini e fastidi, durante la seconda parte dell'esercitazione gli attori erano tutti Stati nazionali (Israele, Siria, Stati Uniti, Iran, Russia) e la pericolosità dell'attacco comportava delle componenti che avrebbero potuto facilmente inasprirsi. Dall'esperimento i responsabili della simulazione hanno dedotto che la mancanza della capacità di attribuzione, soprattutto nel secondo scenario, comporta delle implicazioni pericolosissime se incrociate con la necessità di esprimere capacità di deterrenza. Sono stati analizzati in particolare due problemi, già ampiamente considerati: la necessità di creare un *framework* legale capace di considerare in anticipo gli scenari e dare la possibilità ai *decision-makers* di potere agire liberamente, all'interno dei vincoli legali e l'esigenza di includere tutte le strutture critiche (ospedali, fornitori di energia, et al.) nella rete di protezione cibernetica nazionale.[470]

Herzljia: cooperazione tra università e servizi segreti**.** Ad Herziliya è stato recentemente formato un *InterDisciplinary Center (IDC)* nel quale si affrontano moltissime materie e problematiche differenti, con la peculiartà degli studi incrociati tra soggetti complementari. In quest'ottica si affronta anche lo studio e la ricerca delle minacce cibernetiche per il paese**.** In particolare sono due i centri che se ne occupano: the *Institute for Policy and Strategy* (IPS)[471] e l'*International*

[468] First Israeli Simulation: http://www.israeldefense.com/?CategoryID=483&ArticleID=2594 ultimo accesso 28.02.32014
[469] Israel Hosts Major Cyber-War Simulation, Times: http://times.altervista.org/israel-hosts-major-cyber-war-simulation/ ultimo accesso 28.02.32014
[470]In proposito il commento del professor Ben- Israel è stato: "Without an appropriate defense, the response capability is very limited and the manoeuvrability space of the decision-makers is narrow. The defense must include all of the hospitals, and medical, electricity, transportation and civilian infrastructure. Anything that is linked somehow to computers is a target of a cyber attack, and physical damage can be inflicted through harming computers that control and regulate vital systems like the supply of water or electricity production"
[471]Si possono leggere molti dei commenti della Conferenza: http://www.herzliyaconference.org/eng/?CategoryID=425

Institute for Counter Terrorism (ICT)[472] entrambi facenti capo alla Lauder School of Goverment Diplomacy and Strategy. Vengono considerati rilevanti perché al loro interno, oltre a ricercatori accademici, partecipano alla produzione di report e di raccomandazioni, anche personalità del mondo militare e dell'intelligence israeliana.

I contatti con le Forze Armate però non sono l'unica forma di collaborazione che ha stipulato formalmente l'ICT. Infatti, recentemente, una collaborazione strategica[473] è stata sancita con la *Israel Electric Corporation (IEC)*[474]*.* La IEC è l'organizzazione che occupa della fornitura dell'energia elettrica nel maggior parte del Paese (persino nei territori Palestinesi e in parte della Striscia di Gaza), la quale recentemente ha instituito un centro di training per la cyber-sicurezza (vedi dopo).

INSS: all'interno dell'Istituto Nazionale per gli Studi sulla Sicurezza[475] è stato istituito da circa dieci anni un workshop concentrato sulla *cyber-warfare* gestito da Gabi Siboni, un ex Generale Maggiore delle Forze Armate (Intelligence). Il gruppo è composto da numerosi studiosi israeliani e internazionali, che svolgono un importante ruolo di collegamento tra informazione pubblica, suggerimenti all'esecutivo e nozioni militari. Il ruolo dell'Istituto, infatti, non è solo quello di diffondere notizie, ma anche di agevolare la comunicazione tra i diversi soggetti. In particolare date le entità che sono a capo dell'Istituto, di particolare rilevanza sembra essere il legame con il mondo dell'Intelligence militare.

Al di là di questo, l'INSS è il maggior produttore israeliano di report e articoli sulla questione cibernetica. Il suo focus è preminentemente strategico e concentra la sua attenzione sia sulla descrizione (l'ottimo lavoro di Gil Baram) e sulla concettualizzazione (il lavoro più volte citato di Cohen e Rotbart), che sulla proposizione di soluzioni a questioni estremamente rilevanti per il cyber-spazio.

[472]Sito ufficiale: http://www.ict.org.il/

[473]Sul rapport tra ICT e Israel Electric Company si veda http://portal.idc.ac.il/en/main/pages/newsDetails.aspx?idcid=142&idclang=English ultimo accesso 28.02.2014

[474]Sito ufficiale http://www.iec.co.il/EN/IR/Pages/default.aspx

[475] In inglese The Institute for National Security Studies, in ebraico המכון למחקרי ביטחון לאומי : http://heb.inss.org.il/index.aspx?id=4494 ultimo accesso 28.02.2014

5.6.2 Il rapporto con il mondo privato: la PPP come force-multiplier[476]

Se si considera la natura stessa del cyber-spazio è facile capire la seguente affermazione: "*Defense in cyberspace is a new kind of challenge (…), a small breach of one weak link – whether human or technological – is enoughto cause a defense already in place to fail*".[477]Le necessità difensive fanno sì che siano necessarie collaborazioni a tutti i livelli, sia intra-nazionali che sovra-nazionali. Per quanto riguarda la cooperazione interna, in particolare, due sono le bisettrici che vanno perseguite: la collaborazione tra il mondo militare e quello civile e quella tra settore privato e pubblico. In Israele, tutto questo si mischia, perché tutti sono obbligati a entrare a far parte del mondo militare per alcuni anni e perché il paese, a causa delle sue dimensioni, può concedersi di essere più unito di quanto non sia un gigante geografico.

Nel 2013 Mc Afee ha attribuito il massimo punteggio alla *readiness* di Israele, in uno dei suoi più celebri report[478], pubblicato in collaborazione con la Strategy & Defense Agenda (SDA) di Bruxelles. Una delle ragioni è senza dubbio la sua vocazione per la collaborazione tra mondo privato e dimensione pubblica, soprattutto nell'ottica della gestione della sicurezza delle infrastrutture critiche.

Esistono tutta una serie di fattori positivi nella collaborazione *à la israelien*, che in parte derivano dalla struttura sociale del paese e dal forte legame che si crea tra le diverse istituzioni, a causa della forza collante che esercita l'esperienza del servizio militare obbligatorio per tutti gli uomini e le donne israeliani. Usando le parole di Tabanski:

"Israeli case demonstrates an environment of dynamic information sharing and organizational flexibility –qualities that a government and particularly security organizations perceivably lack. Moreover, the defense leaders were interested and able to transit their

[476]Stavridis J. E. e Farkas E.N. (2012), *The 21st Century Force Multiplier: Public–Private Collaboration,* The Washington Quarterly, Vol.35, No.2, pp.7-20
[477]Even, S. e Siman-Tov, D. (2012), *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 INSS Publ., Tel Aviv
[478]Grauman B. (2012) *Cyber-security: the vexed question of global rules*, Security and Defense Agenda publications, Bruxelles

understandings of emerging cyber-risks to civilian sectors, despite the understandable reluctance of the latter to take on a whole new set of concerns. It appears that the State of Israel's characteristics – the small size of the country, the informal culture, military service and the common experience of insecurity, – have all contributed to the rather considerable cooperation between defense and civilian sectors"[479]

La condivisione delle informazioni, come visto è la chiave iniziale per instaurare una relazione proficua e vantaggiosa e, in Israele, se si trascende dall'elevatissima quantità di nozioni secretate, il restante carico di informazioni legate alla Difesa viene scambiato agevolmente tra i vari soggetti che giocano un ruolo più o meno attivo nell'assicurare la sicurezza del paese. Le quattro ragioni elencate da Tabansky sono probabilmente le più valide per spiegare la facilità di interazione tra le diverse entità.

Un caso particolarmente florido che va citato per spiegare inequivocabilmente questo legame, riguarda la relazione tra l'Unità8200 delle Forze Armate e lo sviluppo di tecnologia *cyber* in Israele. La correlazione tra le capacità acquisite nel mondo militare e il successo riscontrato nel mercato globale dalle imprese nate da *alumni* della suddetta Unità, ha richiamato l'attenzione di numerosi studiosi e giornalisti[480]. Molte delle imprese o delle *start-ups* nate in Israele, infatti, sono relazionate con persone che provengo dalla suddetta Unità. Questo stretto legame è decisamente vantaggioso per l'*ecosistema* difensivo del cyber-spazio nazionale per una serie di ragioni. Innanzitutto perché le Forze Armate e le istituzioni incaricate di occuparsi di difesa possono contare su affidabili partner nel panorama del settore privato, potendo affidare a loro importanti settori della sicurezza di network e infrastrutture, svolgendo una funzione di pura supervisione (limitando insomma le funzioni di monitoraggio). Inoltre, il fatto che molti responsabili di imprese private derivino dal mondo

[479] Tabanski (2013) op. citata p. 5

[480] Alcuni articoli possono essere ritrovati su http://www.businessinsider.com/best-tech-school-is-israels-unit-8200-2013-8, http://www.theguardian.com/world/2013/aug/12/israel-military-intelligence-unit-tech-boom, http://www.homelandsecuritynewswire.com/dr20120605-veterans-of-israel-s-secretive-unit-8200-head-many-successful-hightech-startups (ultimo accesso 28.02.2014)

militare fa sì che vi siano intatte strutture comunicative e di rapporti personali che agevolano il passaggio informale di informazioni e conoscenze.

Un esempio di questa facilità di interazione è la *Cyber Gym*[481] proposta dalla Israel Electric Corporation in collaborazione con le Forze Armate. L'esperimento ha un importante valore poiché perseguito attraverso la cooperazione tra i diversi elementi cruciali per la Difesa ed è inoltre legato all'idea ce l'esercitazione nella difesa dei network sia il modo principale per ottenere esperti capaci di gestire la sicurezza informatica.

La situazione non è così rosea come sembra*.* Nel report della Mc Afee sopracitato, si leggono ancora una volta le dichiarazioni del professor Ben-Israel: "*cyber security is not about saving information or data, but about something deeper than that. It's about securing different life systems regulated by computers. In Israel, we realised this 10 years ago"*[482]*. Le* autorità e l'accademia israeliana si sono perciò rese conto che per rendere operative la protezione delle infrastrutture critiche israeliane era necessario prendere in considerazione anche gli attori privati che molto spesso gestivano le stesse. Questo percorso non è privo di difficoltà, sia dal punto di vista delle basi legali che dell'implementazione.

In Israele però, con la sopracitata legge B784 del 2002, è stato istituito "a *legal framework to tell private industry what measures to take to secure the power, water and banking systems."*[483] *Questo sistema risulta perciò* sbilanciato verso la protezione di quelle infrastrutture che sono compatibili con il fatturato nazionale e con il mondo finanziario.

Un serio problema quando si parla di basi legali attraverso le quali gestire l'interazione tra settore privato e necessità pubbliche è quello del livello accettato di intrusività. Tabansky L.(2013) ne offre un perfetto esempio, citando la diatriba sulla sicurezza del network del Tel-Aviv Stock Exchange.[484] Secondo l'autore, il comitato di sicurezza della

[481]http://www.israelnationalnews.com/News/News.aspx/174712#.Uv-Jzvl5O4J
[482]Grauman B. (2012) op. citata p 68
[483]ibid
[484] Tabanski (2013) op. citata p. 3

NISA avrebbe identificato il TASE come infrastruttura critica e quindi proposto la supervisione nazionale sulla sua sicurezza, mentre l'Amministratore Delegato Ester Levanon la considerava un'opzione inaccettabile. Infatti, per l'AD della TASE le capacità in termini di sicurezza informatica degli addetti eramo sufficienti per garantire un'elevata protezione e, in aggiunta, la supervisione di un organo governativo, avrebbe fatto perdere credibilità alla Borsa di Tel-Aviv nel mercato internazionale. La conclusione di questa faccenda può servire a cogliere le insufficienze presenti nel sistema israeliano. Pochi anni dopo, lo scontro legale vide la vittoria della NISA e la supervisione di questa sull'operato della TASE ma solo in termini puramente legali perché dal punto di vista pratico, la NISA rimane tutt'oggi un'entità interpellabile solo in caso di attacco o diffusa difficoltà, non per un costante monitoraggio.

In conclusione, ancora una volta vorrei sottolineare che la ragioni per cui il modello israeliano funziona, anche in termini di Partnership tra settore privato e pubblico, sono strettamente legate allo sviluppo storico-sociale del paese. Ad ogni modo molte delle caratteristiche del sistema israeliano possono essere esportate ed utilizzate come modello, soprattutto quando si parla di investimenti per lo sviluppo e permeabilità del settore pubblico nella gestione privata. Come conclude Tabansky nel testo sopracitato, *there is no one-fits-all CIP blueprint.*[485]

5.6.3 Gli investimenti del settore pubblico e dell'esercito nel settore privato

La situazione fin qui analizzata è particolarmente positiva in prima analisi, però come sottolineano tutti gli esperti e i *policy-makers,* molti sforzi sono ancora necessari. Per concludere la parte di analisi relativa alle relazioni intra-statali, vorrei parlare di tre importantissime questioni che si stanno sviluppando ora in Israele. Il primo scenario è relativo al progetto **Magshimim**[486], intrapreso dalle Forze Armate in

[485]ibid

[486]Il sito del progetto: http://www.magshimim.net/ ultimo accesso 28.02.2014

collaborazione con il Ministero dell'istruzione e dell'Interno israeliani. Il progetto consiste nel selezionare studenti degli istituti superiori per immetterli in un programma in cui possono apprendere i fondamenti delle funzionalità del cyber-spazio e della sicurezza informatica, che li potranno poi agevolare nella selezione militare e nell'ammissione nei principali istituti universitari del Paese. Secondo Raya Bruk, la manager del progetto presso l'Unità 8200[487], il progetto ha una duplice funzione. Da una parte favorisce la scolarizzazione di tutte le aree del paese, infatti i fondi sono direzionati principalmente verso le aree periferiche del paese. Dall'altra fornisce un apporto alle richieste delle Forze Armate. È infatti attraverso l'educazione a determinati scenari e procedure che è possibile migliorare e sistematizzare la Difesa in ambito informatico nazionale.

Il secondo argomento che si deve menzionare è il programma di fondi governativi per lo sviluppo dell'Industria della Cyber Security israeliana[488] (**KIDMA**). Non esiste solo questo fondo, ma esso rappresenta l'esempio più chiaro e concreto di come il governo israeliano sia direttamente impegnato per aiutare il settore privato a contribuire alla crescita del settore economico e al miglioramento della situazione difensiva. In particolare si rifà a una delle indicazioni della Raccomandazione 3611 del 2011 in cui si richiedeva l'avanzamento delle capcità nazioanli nel campo della sicurezza cibernetica[489]. Il primo investimento è stato di appena 20 milioni di dollari (80 milioni di New Israeli Shekels), ma le agevolazioni avvantaggiavano le imprese più competitive, le più giovani, le più specializzate e coloro che riportavano la propria attività in Israele, dopo essersi specializzati, tutti questi meccanismi hanno prodotto una forte competizione e un crescita esponenziale del livello di specializzazione dell'industria israeliana. Il programma, inoltre favoriva chi elaborava nuove tecnologie e chi era in grado di dimostrare la possibilità di cooperare internazionalmente nello sviluppo dei propri progetti. Inutile dire che questo fondo, accompagnato

[487]L'Unità 8200 è stata incaricata di sviluppare e controllare il progetto Mashimim

[488]Ministry of Industry, Trade & Labor (2013) *R&D Incentives Programs,* consultabile www.moital.gov.il/madan.htm ultimo accesso 28.02.2014

[489]Ibid p. 11

da altri[490], ha creato un ulteriore corsa al settore cibernetico da parte di privati e imprese.

Infine, il progetto che riassume in sé tutte le nozioni appena discusse è quello che riguarda il deserto nel sud del paese, il Negev. È questa un'area da sempre poco abitata e poco sviluppata, nella quale si sono svolte numerose esercitazioni militari e dove sono nascosti alcuni siti militari nucleari (i.e. Dimona). Il progetto riguardante il *cyber-hub* di **Be'er Sheva** è un'iniziativa del tutto innovativa che potrebbe avere grandi ripercussioni nella gestione della sicurezza informatica. L'idea è quella di creare un centro nevralgico che combini tutte le entità incluse nell'*ecosistema* cibernetico: l'Università, il settore privato e le Forze Armate. Le tre componenti sono state già esaminate e anche le loro future componenti a Be'er Sheva, ciò che preme sottolineare in questa sede è che se il progetto dovesse funzionare potrebbe rappresentare il tante volte citato *force-multiplier* perché potrebbe essere davvero capace di far convergere gli sforzi di tutti gli attori coinvolti e creare il proverbiale *hub* che il Primo Ministro Netanyahu cerca di produrre da alcuni anni.

5.7 La cooperazione internazionale

Dopo aver ampiamente analizzato le linee della cooperazione intra-statale è ora necessario soffermarsi sulla collaborazione sovra statale israeliana. Come già detto, l'interazione internazionale sia fondamentale per la buona riuscita di un efficace sistema di protezione nazionale contro le minacce cibernetiche. Questo è maggiormente vero, per un paese come Israele che, è stato ricordato in precedenza, essere un'" isola politica", circondata da paesi ostili o al massimo neutrali. Risulta chiaro perciò che il Paese abbia cercato di fortificare le alleanze con quei paesi e organizzazioni che son più prossime alle esigenze di

[490]Ad esempio si veda l'Israeli Cyber Experimentation Center http://www.iucc.ac.il/wp-content/uploads/2014/01/ICE-brochure.pdf ultimo accesso 28.02.2014

sicurezza israeliane. Anche Eviatar Matania, il Direttore del Cyber Bureau, in un articolo pubblicato su Israel Defense[491], ha sottolineato come la cooperazione internazionale sia fondamentale in un dominio in cui l'attacco ha un chiaro vantaggio sulla difesa, soffermandosi sull'*information and data sharing,* sulle regolamentazione inter-statale (secondo processi simili agli accordi sulle armi non convenzionali).

In primo luogo Israele ha cercato di rafforzare il rapporto con gli **Stati Uniti**, storico e più importante partner militare del Paese. La questione cibernetica è solo una delle declinazioni di questa alleanza ma ha notevolissimi risvolti pratici ed economici e viene persino celebrata nel United States-Israel Enhanced Security Cooperation Act del 2012.[492]

Innanzitutto in termini militari[493], i più volte citati Stuxnet, Duqu e Flame sembrerebbero essere tutti produzione della collaborazione tra i due paesi. Inoltre, il sostegno dell'Unità 8200 per i rilevamenti di intelligence in territorio siriano e iraniano (anche in termini di *cyber-leaks*) sono un'altra importante casistica di cooperazione tra i due eserciti.

D'altra parte dal punto di vista commerciale, la cooperazione è sicuramente molto più visibile e meno segretata. La vantaggiosissima relazione economica vale sia per il settore pubblico che per quello privato. Di maggior eco internazionale sono sicuramente i milioni di dollari investiti dalle più importanti multinazionali statunitensi impegnate nel settore della sicurezza informatica (i.e. Google, Microsoft, Lockheed Martin).

Considerando gli alleati nel Mediterraneo, Israele non può che contare sull'Unione Europea e su alcuni dei membri dell'Organizzazione del Trattato del Nord Atlantico, dopo che i rapporti con la Turchia si sono guastati da due anni a questa parte. In particolare una grande rilevanza per Israele ha il rapporto di alleanza con l'**Italia**, sia per la questione dei cavi sottomarini, sia per l'elevato valore degli investimenti di

[491]Matania, E. e Goldstein, T. (2013) *Global Cyber Cooperation,* Israel Defense, Tel Aviv http://www.israeldefense.com/?CategoryID=512&ArticleID=2364 ultimo accesso 28.02.2014
[492]Per il documento ufficiale dell'accordo tra USA e Israele: https://www.govtrack.us/congress/bills/112/s2165/text
[493]Cfr. http://www.ynetnews.com/articles/0,7340,L-4239641,00.html

importazioni, esportazioni e servizi reciproci. A proposito, lo scorso dicembre è stato siglato tra i due governi un accordo bilaterale[494] sulla cooperazione in materia di *cyber-space*, nel quale si prevedono missioni periodiche di funzionari e tecnici degli enti competenti in materia di sicurezza informatica dei rispettivi Paesi, nonché la partecipazione ad eventi ed incontri a livello di esperti e funzionari governativi. Ha inoltre l'obiettivo di promuovere il dialogo, lo scambio di informazioni e i progetti tra imprese e esponenti del mondo accademico dei due paesi. Sarà inoltre istituito un advisory group composto, tra gli altri, da aziende e start up di questo settore nonché istituzioni accademiche ed enti di ricerca dei rispettivi Paesi.

A livello di organizzazioni internazionali, va ricordata l'appartenenza di Israele all'OSCE (Organization for Security and Co-Operation in Europe) e il suo contributo alla recente pubblicazione di una Decisione[495], la prima di questo tipo, sull'adozione di misure di *confidence-building* volte a ridurre le tendenze conflittive nel cyber-spazio.

Visione analitica e conclusioni

Dopo aver analizzato attentamente tutte le componenti del sistema di difesa e dell'ambiente in cui questo viene ad essere *in atto* è il momento di tirare delle conclusioni analitiche. Vi sono molte questioni che vanno studiate in maniera approfondita. La prima è la relazione unica che vige tra entità difensiva e offensiva dell'approccio israeliano al cyber-spazio. Come ripetuto numerose volte, le necessità legate alla realtà politica mediorientale rendono impellente per Israele il dotarsi di una struttura difensiva efficace. La predilezione per la difesa proattiva fa sì che il focus militare sia prevalentemente di tipo preventivo, anche se la differenziazione con un focus di matrice puramente offensiva spesso

[494] L'accordo tra Israele e Italia è parzialmente disponibile qui: http://moked.it/files/2013/12/vertice_ita_isr_intese_20131202.pdf

[495] Il testo della decisione è disponibile: http://www.osce.org/pc/109168 ultimo accesso 28.02.2014

è molto labile, data la natura *dual-use* di molte tecnologie. Sia nelle dichiarazioni politiche che militari, il cyber è ritenuto ormai un ulteriore dominio militare e, persino le alte cariche dello Stato hanno ammesso che Israele si sta dotando sia di capacità difensive che offensive.[496] Peraltro, è ormai ampiamente attribuito ad Israele l'attacco alla centrale nucleare di Natanz attraverso il contagio con il virus Stuxnet, episodio che mostra perfettamente quale sia il concetto di prevenzione per le Forze Armate israeliane. La questione, però, ha anche giocato in sfavore di Israele, perché l'ha allontanato dalla collaborazione con la NATO, i cui esperti di etica del Centro di eccellenza di Tallinn hanno definito come *un atto di forza*[497] e di conseguenza hanno condannato le azioni israeliane perché contrarie ai dettami della Carta delle Nazioni Unite. Senza entrare nel merito della questione legale, questo scenario evidenzia come il modello di difesa preventiva possa mettere in difficoltà le già risicate alleanze di Israele, complicando il progetto del paese di ampliare il sostegno internazionale alla lotta contro i cyber-attacchi.

Data la natura degli attacchi è estremamente variegata, il paese deve essere pronto a reagire a qualsiasi tipo di minaccia. Questo provoca una predisposizione da parte delle forze di sicurezza del paese a prevedere tutti i tipi di minaccia: *social engineering*, violazioni del cloud, il cyber-crimine, le minacce provenienti dall'interno, oltre che agli attacchi provenienti da altri paesi[498]. Con una media di oltre cento mila attacchi di molteplice natura al giorno, il paese ha sviluppato un livello di capacità di protezione e di *response readiness* uniche al mondo, caratterizzate dalla flessibilità e da una ampia capacità di previsione.

Per riguarda la *governance* e la gestione interna della cyber-sicurezza, invece il commento merita di essere più lungo. Innanzitutto, mi trovo in accordo con gli studiosi israeliani che come si è detto sin ora richiamano a gran voce la pubblicazione di una strategia chiara e trasparente. Questo perché come mi ha confidato Gil Baram, una

[496]In un pubblico intervento il Ministro degli Esteri ha commentato così sulla questione: http://www.pri.org/stories/2012-06-06/israels-defense-minister-confirms-cyber-warfare-campaign

[497]Cfr. http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all ultimo accesso 28.02.2014

[498]*Cyber threats Forecast for 2014:* http://www.israeldefense.com/?CategoryID=512&ArticleID=2654 ultimo accesso 28.02.2014

ricercatrice dello Yuval Ne'eman Workshop, "*anche se in Israele le cose funzionano decisamente bene, l'approccio è eccessivamente improntato a una reazione istantanea ad hoc, non esiste pianificazione a lungo termine, né chiara divisione dei compiti".*[499] Credo che in poche parole sia chiaro ciò che affligge la gestione interna del paese. Data la natura metodica della Difesa, vorrei avanzare l'ipotesi che sia la mancata divisione dei compiti, che la scarsa pianificazione, siano a loro volta delle conseguenze di un problema ancora più viscerale del paese: la costante divisione politica[500] e la volontà di mantenere un elevato livello di autorità e gestione da parte delle singole autorità governative. Questo è chiaramente un argomento che prescinde lo scopo di questa trattazione, ma va rimarcato nel momento in cui si analizza il funzionamento della difesa cibernetica nazionale e se ne identificano le limitazioni.

Considerando unicamente la divisione e la settorializzazione della difesa è inevitabile giungere all'analisi del National Cyber Bureau, delle sue funzioni e del suo scopo. Con la Raccomandazione 3611 del 2011 il Primo Ministro, supportato dal Comitato del Cyber National Initiative, hanno tentato di applicare in Israele uno di quei *best-practice model* di cui si è più volte parlato. L'idea è, secondo le parole di Oren Bratt della Isrel Military Industries[501], quella di standardizzare il sistema di protezione copiando modelli positivi intrapresi in altri paesi (e.g. Estonia) e adattandoli al sistema Isreliano. Pur non avendo dalla mia parte il favore del tempo per vedere gli esiti di questa scelta, mi sento di condividere nuovamente il pensiero del Colonnello Aaro Cederberg, ex responsabile della cyber-sicurezza al Ministro della Difesa finlandese, il quale alla domanda se credeva veramente che il modello comprensivo di difesa finlandese fosse esportabile ha risposto:"of *course not! But the idea of a general defense, that (…) you can try to implement in different ways depending on the country background."*[502] Lo stesso concetto

[499]Mia traduzione di una intervista che mi ha rilasciato Baram G. nel gennaio 2014
[500]Vercelli, C. (2008) *Breve Storia dello Stato d'Israele (1948-2008),* Carocci Ed., Milano; anche Tabansky (2013) op. citata
[501]Dichiarazione rilasciata durante un intervento alla confrenza Cyber Tech 2014, il 27 gennaio 2014
[502]Dichiarazione rilasciata da Aaro Cederberg a commento di un suo intervento alla conferenza Cyber Stability, indotta dall'UNIDIR a Ginevra nel Febbraio 2004

credo possa valere per la situazione israeliana. Per quanto il modello di accentramento del controllo del Sistema di difesa dipende anche da alcuni fattori politici che in Israele potrebbero essere difficili da ottenere, come la disponibilità delle forze politiche di autolimitare la propria autorità[503], o la permeabilità e la volontà di condividere informazioni non classificate ma di alto valore per la sicurezza del paese da parte delle forze armate.

Per queste ragioni credo che l'esperimento di Be'er Sheva sia di immenso valore, ma più dal punto di vista dello *spark*, ovvero per la potente confluenza di capitali, originati da investimenti diretti stranieri, da capitali di multinazionali o da fondi governativi allo sviluppo. La dimensione di *hub* della Difesa probabilmente sarà più difficile da raggiungere nel breve periodo, anche se va detto che il mondo si sta procedendo è ipoteticamente quello corretto.

Un altro problema deve essere risolto: l'eccessiva dipendenza dal fattore economico nelle analisi del rischio e delle entità che necessitano protezione. Il discorso è lungi dall'essere di carattere moralistico, ma è motivato da ragioni di concreto preminenza strategica. Infatti, se non si includono anche in pratica le infrastrutture che mettono a disposizione dei cittadini servizi essenziali e vitali, ma non remunerativi (i.e. servizi ospedalieri), il sistema resterà perennemente a un livello insufficiente di resilienza.

Un ulteriore questione, legata alla gestione delle infrastrutture è la protezione nazionale delle imprese. Abbiamo visto come questo argomento sia delicato perché incrocia l'attualissima diatriba del bilanciamento tra le necessità di sicurezza e l'intromissione delle strutture statali nella dimensione privata. A prescindere da questa spinosa questione, le istituzioni dovrebbero quanto meno includere l'idea di far rientrare le imprese private (al di là dei grandi gruppi che gestiscono i principali servizi nazionali) nella protezione fornita dallo stato, perché come si ricava da molte ricerche svolte in diversi paesi, le

[503]Va ricordato che nella Raccomandazione del 2011, la divisione di molti compiti tra la NISA e il Cyber Bureau era da decidere in base al dialogo tra le due entità. Il che banalmente significa che, con l'intercessione del Primo Ministro, il Cyber Bureau avrebbe acquisito funzioni solo se il NISA avesse acconsentito a rinunciarvi

debolezze al livello delle Piccole o Medie Imprese si possono ripercuotere facilmente a più ampi settori della rete nazionale.

Ancora una volta, il sistema di difesa nazionale funziona più per l'innata capacità di sopravvivere e per la limitata capacità offensiva dei nemici che per la capacità strategica di chi si occupa della pianificazione della Difesa. Per concludere, il sistema di protezione israeliano, per quanto perfettibile e migliorabile, mostra alcune caratteristiche uniche (difficilmente esportabili) che gli permettono di mantenersi ai massimi livelli mondiali, anche in confronto alle grandi potenze geopolitiche del mondo.

Considerazioni conclusive

Nonostante la presentazione dei due *case studies* non sia stata fatta per mostrare un'analisi comparativa, ci si può soffermare brevemente sulle discrepanze tra i due modelli per carpire quali siano le variabili e le caratteristiche che possono essere trasposte alla situazione di altri stati e quali quelle che invece sono uniche e difficilmente riproducibili.

Come abbiamo visto la principale differenza tra i due paesi sembra essere la postura strategica al cyber-spazio. Da una parte, Israele risulta essere indirizzato verso una prospettiva che contempla ampiamente un approccio offensivo, mentre l'Estonia sembra prediligere un'impostazione puramente difensiva. Questo, anche per ragioni circostanziali, che hanno poco a che vedere con la libera scelta. Infatti, nel caso di Israele l'essere circondato da nemici, ha portato il paese a sviluppare modalità militari coercitive che ha tentato di trasporre nel cyber-spazio. Anche l'entità dei nemici ha contribuito a formare questo tipo di modello. A differenza dell'Estonia infatti, i nemici che circondano Israele sono Stati che sono relativamente meno capaci militarmente e che non sono praticamente mai stati soverchianti. Il primo problema del paese baltico invece è la Federazione Russa, con la quale non ha nessuna speranza di competere militarmente. È questa una delle ragioni per cui l'approccio estone è molto più indirizzato alla difesa e alla cooperazione internazionale. Questa produce una dinamica del tutto simile anche nel cyber-spazio, *in primis* perché le dinamiche che si intaprendono in questo dominio non sono in alcun modo scindibili dalle altre, secondo perché le capacità dei due paesi sono sproporzionate anche in questo dominio.

La seconda notevole differenza è la relazione cooperativa con altri stati. Nel caso dell'Estonia, date le sue dimensioni e le sue

possibilità al principio degli anni Novanta, è stata una necessità puntare molto sul sostegno esterno, giunto prevalentemente da due direttrici: le alleanze nordiche (i.e. Svezia e Finlandia) e dalla NATO. In questa dinamica rientra anche la collaborazione per mantenere sicuro il cyber-spazio. Per Israele, invece, la dimensione cooperativa è una realtà relativamente recente. Se si tralascia la ferrea collaborazione con gli Stati Uniti, gli sforzi di siglare accordi con paesi europei e asiatici risale alle legislature di Nethanyahu e, tranne che nel caso italiano, ha più una rilevanza politica che "tecnica". Anche in questo caso la questione è fortemente condizionata da motivazioni circostanziali.

Spostando invece l'attenzione sulla dimensione interna, si notano prevalentemente due grosse differenze. La prima riguarda la presenza dei militari nella gestione della sicurezza e della difesa. In Israele la componente militare è decisamente più marcata a tutti i livelli istituzionali e, in particolare, risalta molto la differenza tra la NISA e la RIA, dove la NISA è un corpo del quale è difficile carpire informazioni sui componenti (sia da informazioni *open-source*, sia da testimonianze dirette), ma del quale si sa che la componente militare è decisamente alta. La RIA invece è un corpo interamente gestito da civili, totalmente trasparente che non risente delle influenze militari se non per vie indirette e che risponde a un Ministero del tutto "civile", come risulta essere quello degli Affari Economici e della Comunicazione.

La seconda differenza riguarda invece il livello di chiarezza delle regolamentazioni interne e la specificazione dei ruoli. In Estonia, la ECSS e l'Emergency Act combinati, chiariscono tutte le reciproche responsabilità[504] e spazi di manovra, se vi è poi della confusione deriva dall'implementazione e dalle diatribe politiche tra i diversi organismi adibiti alla difesa cibernetica. In Israele invece, la Raccomandazione 3611 non fornisce le sufficienti informazioni per cogliere i meccanismi interni di funzionamento della difesa. Come commenta Gil Baram, "*in Israele le cose funzionano bene, ma più per una capacità innata a*

[504] Nella versione di quest'anno della ECSS sarà inclusa anche la RIA, che fu formata nel 2009 e quindi non rientra nella ECSS 08-13

reagire a minacce esterne, che per una precisa organizzazione interna"[505].

A prescindere da queste importanti differenze, ciò che era più importante sottolineare erano le similitudini, ossia quelle variabili che non dipendono dal carattere nazionale o da particolari scelte politico-economiche momentanee, ma che possono rappresentare un modello per altri Stati. Nonostante i due paesi abbiano esigenze strutturalmente diverse, è possibile notare come gli incentivi esterni, provenienti dal cyber-spazio, abbiano generato un modello di gestione della difesa del tutto similare e espressione dell'ecosistema che si è voluto sostenere in questo elaborato. Entrambi i paesi infatti hanno dato una notevole rilevanza alla protezione delle infrastrutture critiche, migliorandone la gestione e le tecnologie impiegate. Sostenendo un fortissimo rapporto con il settore privato, facilitato dalla possibilità di intessere forti legami informali, al punto da riconoscere la preminenza dello sviluppo in molti settori della *cyber-security.* Entrambi i paesi inoltre sono una chiara dimostrazione di come vi sia un possibile legame tra crescita dell'innovazione tecnologica e del settore produttivo relativo, e una prospettiva di crescita economica.

Si può argomentare che le due realtà considerate abbiano anche in comune le modeste dimensioni in termini geografici e di popolazione. Questo è senz'altro vero, ma non inficia la correttezza del modello proposto, come possono dimostrare le esperienze di paesi notevolmente più grandi, quali Svezia, Finlandia e persino Stati Uniti. Infatti, la necessità di apportare modifiche importanti alla protezione informatica è avvertita globalmente. La percezione che le reti e i sistemi informatizzati siano decisamente troppo vulnerabili per continuare con una difesa statica, affidata a *firewalls,* anti-virus e filtri (Siboni 2013, 45-58), trascende le dimensioni geografiche o demografiche e si ritrova come minimo comun denominatore tra le diverse istanze presentate internazionalmente.

È infatti forse questa l'unica necessità condivisa da tutti i paesi

[505] Intervista gennaio 2014

che si sono costruiti un *cyber-power* a livello internazionale: la ricerca di massimizzazione della sicurezza, dato l'aumento delle potenzialità distruttive delle armi cibernetiche. Questa necessità si è manifestata concretamente in due modalità: il tentativo di ricorrere alle Organizzazioni internazionali per trovare un accordo sul controllo degli armamenti cibernetici, e il rafforzamento delle difesa interna. Quanto si è voluto affermare in questo elaborato è che, non potendo per il momento contare sulla possibilità di un accordo internazionale, è necessario sviluppare delle capacità difensive concrete a livello nazionale, tentando di evitare di innescare il pericoloso meccanismo della corsa agli armamenti. La maniera più prolifica di ottenere dei risultati, come si è visto, è quella di intraprendere un approccio olistico, in cui la dimensione strategica e gestionale sia accomapagnata da un percorso di condivisione delle responsabilità con il più ampio numero di attori e di educazione degli addetti alla sicurezza e della più vasta fascia possibile della cittadinanza, in modo da creare un modello resiliente nazionale competitivo e flessibile.

Per concludere, nello scenario della *cyber-warfare,* la necessità degli Stati di acquisire capacità difensive è legato anche alla multidimensionalità delle minacce. Infatti, nonostante lo stato sia li principale attore nel cyber-spazio, come si è visto, molte altre sono le entità che producono attacchi costanti ai sistemi nazionali. Per questo motivo una difesa è necessaria e il modello ecosistemico proposto sembra essere il più efficace sinora elaborato. La prospettiva del perfezionamento difensivo da sola non porterà però a risolvere il problema della conflittualità nel cyber-spazio, anzi potrebbe nel lungo periodo portare a un processo ulteriormente competitivo. A questo problema, l'unica vera contromisura rimane l'accordo internazionale per la limitazione delle *cyber-weapons*. Infatti, soltanto percorrendo la via aperta dalla Dichiarazione di Erice e dalla Raccomandazione dell'OSCE del dicembre scorso, sarà possibile intraprendere un cammino che possa portare alla riduzione del livello di conflittualità nel cyber-spazio.

Indice degli Acronimi

APT: Advanced Persistent Threat
ARPA: Advanced Research Projects Agency
CASIC**:** China Aerospace Science & Industry Cororation CBMs: Confidence-Building Measures
CCDCoE: Cooperative Cyber Defense Centre of Excellence
CDL: Cyber Defense League (estone)
CEIS: Center for Encryption and Information Security
CERN: Organizzazione Europea per la Ricerca Nucleare
CERTs: Computer Emergency Response Teams
CIIP: Critical Information Infrastructure Protection
CLUSIT : Associazione Italiana per la Sicurezza Informatica
CLUSIF: Club de la Securité de l'Information Français
CNCI: Comprehensive National Cybersecurity Initiative
C&C: Command and Control
C4I: Command, Control, Communications, Computers, And (Military) Intelligence
DDoS: Distributed Denial of Service
DNS: Domain Name System
DoS: Denial of Service
ECOSOC: UN Economic and social Council
ECSS: Estonian Cyber Security Strategy
ENISA: European Union Agency for Network and Information Security Agency
GCA: Global Cybersecurity Agenda 86
HTTP: Hypertext Transfer Protocol
IBM: International Business Machines
IAI: Israel Aerospace Industries
ICANN: Internet Corporation for Assigned Names and Numbers
ICDS: International Centre for Defense Studies
ICRG: Islamic Cyber Resistance Group
ICT: Information Communication Technology
ICT: Institute for Counter Terrorism
IDF: Israel Defence Forces
IDS: Intrusion Detection System

IETF: Internet Engineering Task Force
INSS: Institute for National Security Studies
ISP: Internet Service Provider
IT: Information Technology
ITU: International Telecommunication Union
MEAC: Ministero per gli Affari Economici e la Comunicazione (Estone)
MILNET: Military Network
NCIRC: NATO Computer Incident Response Capability
NCS: National Cyber Strategy
NCB: National Cyber Bureau
NCW: Net-Centric Warfare
NIPRNET: Non-classified Internet Protocol (IP) Router Network
NISA: National Information Security Agency (israeliano)
OSCE: Organization for Security and Cooperation in Europe
PPP: Public-Private Partnership
PSYOP: Psycological Operations
RIA/ EISA: Estonian Information System's Authority
SCADA: Supervisory Control and Data Acquisition
SEA: Syrian Electronic Army
TCBMs: Transparence and Cconfidence-Building Measures
TCP/ IP: Transport Control Protocol/ Internet Protocol
UAV : Unmanned Aerial Vehicle

Bibliografia

ACETI, L. (2012) *Time and Space Compression in Cyber Space,* LEONARDO Abstract Service

ANDREATTA, F. (2013) *Technology and War. An Historical Perspective*. Presentazione a Isodarco Winter School, Andalo http://www.isodarco.it/courses/andalo13/paper/Iso13-Andreatta.pdf ultima consultazione 28.02.2014

ARIMATSU, L. (2012) *A Treaty for Governing Cyber-Weapons* in *Proceedings of the 4th International Conference on Cyber Conflict*, Christian Czosseck, Rain Ottis and Katharina Ziolkowski eds., 2012

ARQUILLA, J. e RONFELDT, D. (1997) *In Athena's Camp*, RAND Corporation Pub., Washington

AUSTIN, G. and GADY, F-S. (2012) *Cyber Détente between the United States and China: Shaping the Agenda*, East-West
Institute, New York.

AVERBUCH, A. e SIBONI G. (2013) *The classic Cyber Defense Methods have failed: What Comes Next?*, Military and Strategic Affairs, No. 1, pp. 45-58

BARAM, G. (2013) *The Effect Of Cyberwar Technologies On Force Buildup: The Israeli Case,* Military and Strategic Affairs, Vol.5, No.1, pp. 23-43

BASELEY-WALKER, B.(2011) *Transparency and Confidence-Building Measures in Cyberspace: Towards Norms of Behaviour,* Disarmament Forum, United Nations Institute for Disarmament Research, n.4, p. 31-40

BELOVICH, S.G. (2012) *Cyber Security Briefing: Why what we are doing now won't work* consultabile: ultimo access il 28.02.2014

BEN-ISRAEL, I. e TABANSKY, L. (2011), *An interdisciplinary look at security challenges in the information age* In "Military and Strategic Affairs", Vol.3, No.3, pp.21-37

BETZ, D.J. e STEVENS, T. (2011) *Cyberspace and the State: Toward a Strategy for Cyber-Power,* Routledge, International Institute for Strategic Studies, Oxon.

BIKKENIN, R. (2003) *Information Conflict in the Military Sphere: Basic Elements and Concepts,* Morskoj Sbornik, no. 10

BLANK, S. (2008) *Web War I: Is Europe's First Information War a New Kind of War?*, Comparative Strategy, Vol. 27, No.3, pp.227-47.

BREHMER, B. (2006) *The Dynamic OODA LOOP: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control*, Department of War Studies Swedish National Defence College, Stockholm

BRUNNER, E.M. e SUTER, M. (2008), *International CIIP Handbook 2008 / 2009*. An *inventory of 25 national and 7 international critical information infrastructure protection policies*, Center for Security Studies (CSS), ETH Zurich

BUCCI, S.P. e INSERRA, D. (2013) *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace,* Backgrounder, No.2785, pp.1-16

BUCK, T. (2013) *Israel Army to Tech Start-up,* Financial Times, London

BUCKLAND B.S. e WINKLER T.H. (2013), *Public Private Cooperation: Challenges and Opportunities in Security Governance,* DCAF Horizon 2015 working paper No. 2, Geneva Centre for the Democratic Control of Armed Forces (DCAF);

BULL, H. (1977) *The Anarchical Society,* Macmillan, London.

CARR, J. (2011) *Inside Cyber Warfare*, O'Reillly, Sebastopol.

CAVELTY, M.D. (2012) *Cyber-security*, in Contemporary Security Studies, Oxford University Press, New York, pp. 363-377

CAVELTY, M.D. (2011) *Unraveling the Stuxnet Effect: of much persistence and little change in the Cyber Threats Debate,* Military and Strategic Affairs, Vol.3, No.3, pp. 11-19

CHADWICK, A. e HOWARD, P. eds (2009) *Routledge Handbook of Internet Politics,* Routledge, London and New York.

CHOO, K.K.R. (2011) *The cyber threat landscape: Challenges and future research directions,* Computers and Security, Vol.30, pp. 719-731

CHOUCRI, N. (2012) *Cyberpolitcs in International Relation*s, MIT Press, Chicago

CHOUCRI, N. e GOLDSMITH, D. (2012), *Lost in cyberspace: Harnessing the Internet, international relations, and global security,* Bulletin of the atomic scientists, Vol.68, No.2, pp. 70-77

CHOUCRI, N e al. (2008) *Mapping Sustainability. Knowledge e-Networking and the Value Chain*, The Alliance for global sustainability, Vol. 11, pp.1-16

CILLUFFO, F.J e CARDASH, S.L. e SALMOIRAGHi, G.C (2012) *A Blueprint for Cyber Deterrence: Building Stability through Strenght*, Military and Strategic Affairs, Volume 4, No. 3, p.3-23

CLARK, D. (2010) *Characterizing Cyberspace: past, present and future*, MIT Press, Chicago

COHEN, D. e ROTBART A. (2013) *The Proliferation of Weapons in Cyberspace*, Military and Strategic Affairs, No. 1, pp. 59-80

CORDANI, G. (2013) *Cyber Weapons: il controllo tra Stati Uniti, Russia e NATO*, tesi magistrale dell'Università di Bologna

CORNISH, P. e HUGHES, R. e LIVINGSTONE, D (2009) *Cyberspace and the National Security of the United Kingdom: Threats and Responses*, Chantam House Report, London

CROSSTON, M. (2013) *Duqu's Dilemma: the ambiguity assertion and the futility of sanitized cyberwar*, Military and Strategic Affairs, Vol.5, No.1, pp. 119-131

CROSSTON, M. (2011) *World gone Cyber MAD. How Mutually Assured Debilitation is the best hope for cyber deterrence,* Strategic Studies Quarterly, Vol 5, No.1, pp.100-16.

CZOSSEK, C. e OTTIS, R. e ZIOLKOWSKI K. (2012) *4th Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn

DEIBERT, R. (2009) *The Geopolitics of Internet Control: Censorship, sovereignty and cyberspace* in Chadwick, A. and
Howard, P. eds, *Routledge Handbook of Internet Politics*, Routledge, London and New York.

DEMCHAK, C. and DOMBROWSKI, P. (2011) *Rise of a Cybered Westphalian Age*, Strategic Studies Quarterly, Vol 5, No.1, pp.32-61.

DENNING, D. (2001) *Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign* Policy, in Arquilla J. e Ronfeldt D. (2001) *Networks and netwars: the Future of Terror, Crime and Militancy*, RAND Publications, Santa Monica. Consultabile http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf ultimo accesso 28.02.2014

DENNING, D. (2001), *Obstacles and Options for Cyber Arms Controls in Cyberspace*, Heinrich Böll Foundation, Berlin, Germany, June 29-30.

DENNING, D.(2000) *Reflections on Cyberweapons Controls*, Computer Security Journal, Vol. XVI, No4, Fall, pp.43-53

DENNING, P. J. (1989) *The ARPANET after Twenty Years*, American Scientists, No. 77, pp. 530-535

DI GANGI, C. (nd) *Il diritto internazionale umanitario,* Pegaso, Università telematica, consultabile http://www.unipegaso.it/materiali/PostLaurea/DiGangi/ModI/Lezione_I.pdf ultimo accesso 28.02.2014

DIPERT, R.P. (2010) *The Ethics of Cyberwarfare*, Journal of Military Ethics, Vol 9, No.4, pp.384-410.

DODGE, M. (2008) *Understanding Cyberspace Cartographies: a Critical Analysis of Inernet Structure Mapping,* Doctoral Thesis at UCL

DOMBROSKI, P. e TOSS, A. L. (2008) *The Revolution in Military Affairs. Transformation and the Defense Industry*, Security challenges, Vol. 4 No 4, pp.13-38

DONOVAN, K.M. (2011), *Expanding The Department Of Defense's Role In Cyber Civil Support*, Masters's thesis, Joint Forces Staff College

DOUHET, G. (1942) *Il dominio dell'aria*, consultabile, http://www.liberliber.it/mediateca/libri/d/douhet/il_dominio_dell_aria/pdf/il_dom_p.pdf ultimo accesso 28.02.2014

DUNN-CAVELTY, M. et.al (2007) Power and Security in the Information Age: *Investigating the role of the state in cyberspace*, Ashgate, Burlington.

DUTTA, S. (2007) *Estonia: A Sustainable Success in Networked Readiness*? Consultabile http://www.weforum.org/pdf/gitr/2.1.pdf ultimo accesso 28.02.2014

EFRATI, R. e YAFE, L. (2013) *The challenges and opportunities of National Cyber* Defense, ISRALE DEFENSE, Tel Av

ENSIGN, R.L. (2013) *Top Cyber Experts Talk Public-Private Cooperation,* The Wall Street Journal, New York

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (2012) *National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace,* ENISA Publications, Heraklion

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (2012) *Threat Landscape. Responding to the Evolving Threat Environment,* ENISA Publications, Heraklion

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (2011) *Measurement Frameworks and Metrics for Resilient Networks and Services*, ENISA Publications, Heraklion

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (2012) *National Cyber Security Strategies. Practical Guide on Development and Execution,* ENISA Publications, Heraklion

EVEN, S. e SIMAN-TOV, D. (2012), *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 INSS Publ., Tel Aviv

FARWELL, J. and ROHOZINSKI, R. (2011) *Stuxnet and the future of Cyber War*, Survival, Vol 53, No.1, pp.23-40.

FIREEYE, Inc. (2013) *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, consultabile: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf (ultimo accesso 28.02.2014)

FORD, C.A. (2010) *The Trouble with Cyber Arms Control,* The New Atlantis, N°29, pp. 52-67.

FRANZESE, P.W. (2009) *Sovereignty in Cyberspace: Can it exist?*, Air Force Law Review, Vol 64, pp.1-42.

GADY, F.S. e AUSTIN, G. (2010) *Russia, The United States, and Cyber Diplomacy: Opening the Doors,* EastWest Institute, New York

GARTZKE, E. (2013) *The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth,* International Security*,* Vol. 38, No. 2, pp. 41–73

GEERS, K. (2011a) *Sun Tzu and Cyber War*, NATO CCDCOE Publication, Tallinn

GEERS, K. *(*2011b) *Strategic Cyber Security,* CCD COE Publications, Tallinn

GEERS, K. (2010) *Cyber Weapons Convention*, Computer Law & Security Review 26(5):5

GEERS, K. (2008) *Cyberspace and the Changing Nature of Warfare*, Hakin9 E-Book, 19(3) No. 6; SC Magazine (27 AUG 08) 1-12.

GIACOMELLO, G. (2013) *Cybersecurity And Critical Information Infrastructures*, ISPI Analysis, No. 201 pp. 1-9 consultabile: http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_201_2013.pdf ultimo accesso 28.02.2014

GIACOMELLO G. E ERIKSON, J.E. (2006), *The Information Revolution, Security, and International Relations: (IR)relevant Theory?,* International Political Science Review*, Vol 27, No. 3,* pp. *221–244*

GILES, K. (2012) *Russian Cyber Security: Concepts and Current Activity*, Chatham House, London.

GOLDSTEIN, GP. (2012) *Cyber Weapons and International Stability: New Destabilization Threats Require New Security Doctrines* in Military and Strategic Affairs, Vol.5, No.2, pp.121-139

GORI U., GERMANI L.S. (a cura di) (2011) *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Franco Angeli, Roma.

GORTZAK, Y. e HAFTEL, Y.Z. e SWEENEY, K.(2005), *Offense-Defense Theory: An Empirical*

Assessment in “The Journal of Conflict Resolution”, Vol. 49, No. 1, pp.67-89

GRAMAGLIA, M. e PERNIK, P. e Thuoy, E. (2014) *Military Cyber Defense Structures of NATO Members: An Overview*, ICDS Pub, Tallinn

GRAUMAN B. (2012) *Cyber-security: the vexed question of global rules*, Security and Defense Agenda publications, Bruxelles.

HARE, F. (2012) *The Significance of Attribution to Cyberspace Coercion: A Political Perspective,* Paper presented at the Cyber Conflict (CYCON), 4th International Conference, June 5-8.

HARE, F. (2010) *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?*, in *Virtual Battlefield,* NATO CCDCOE Pub., Tallinn.

HATHAWAY O.A. et al. (2012) *The law of cyber-attack,* California Law Review, Berkeley, CA, EUA, v. 100, n. 4, p. 817-885.

HEALEY J. e VAN BOCHOVEN L. (2011) *NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow*, Atlantic Council Issue Brief , (p.2, http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf.

HERRERA, G.L (2007) *Cyberspace and Sovereignty: Thoughts of Physical Space and Digital Space,* in Dunn Cavelty, M. et al *Power and Security in the Information Age: Investigating the role of the state in cyberspace*, Ashgate, Burlington.

HERZ, J. (1950) *International Idealism and Security Dilemma*, World Politics, Vol. 2, No. 2 pp.157-180

HERZOG, S., *(2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, Journal of Strategic Security, 4 (2): 49-60.

HARBULOT, C. (2013) *La Piége technologique de la cyber*-guerre, Geopolitique, Vol.8 N.120 p. 64

HATHAWAY, M (2013) *Cyber Readiness Index 1.0*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge

HIRSCH, G. (2013) *The sixth Dimension has Taken off*, Israel Defense, Tel Aviv http://www.israeldefense.com/?CategoryID=411&ArticleID=2621 ultimo accesso 28.02.2014

HUGHES, R. (2010) *A Treaty for Cyberspace*, International Affairs, Vol 86, No.2, pp.523-41.

INFORMATION WARFARE MONITOR (2010) *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, JR03-2010, Shadowserver Foundation, web version http://shadows-in-the-cloud.net, ultimo accesso ottobre 2013

INSTITUTE FOR COUNTER- TERRORISM (2013) *Cyber-Terrorism Activities Report No. 5* . Consultabile: http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1254/currentpage/1/Default.aspx ultimo accesso 28.02.2014

INSTITUTE FOR COUNTER- TERRORISM (2013) *Cyber-Terrorism Activities Report No. 4* consultabile: http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1232/currentpage/1/Default.aspx ultimo accesso 28.02.2014

INSTITUTE FOR COUNTER- TERRORISM (2013) *Cyber-Terrorism Activities Report No. 3*

consultabile:
http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1187/currentpage/1/Default.aspx ultimo accesso 28.02.2014

INSTITUTE FOR COUNTER- TERRORISM (2013) *Cyber-Terrorism Activities Report No. 2* consultabile:
http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1172/currentpage/1/Default.aspx ultimo accesso 28.02.2014

INTERNATIONAL TELECOMMUNICATION UNION (2011) *The Quest for Cyber Peace* consultabile http://www.itu.int/pub/S-GEN-WFS.01-1-2011 ultim accesso 28.02.2014

INTERNATIONAL TELECOMMUNICATION UNION (2008) *ITU Impact Alert: Cyber Drill for Partner Countries* http://www.itu.int/ITU-D/eur/rf/cybersecurity/ITU-IMPACT-CYBER-DRILL.doc ultimo accesso 28.02.2014

JORDAN, D. et al (2008) *Understanding Modern Warfare*, *Cambridge University Press,*

JOUBERT, V. (2012) *Five Years after Estonia's cyber attacks: lessons learned for NATO*?, NATO Defense College*,* Rome, No. 26, pp. 1-8

JUNIO, T. (2012) *How Probable is Cyber War?: Bringing IR Theory Back In to the Cyber Conflict Debate*, The Journal of Strategic Studies 36/1 consultabile http://dx.doi.org/10.1080/01402390.2012.7395614 ultimo accesso 28.02.2014

JUVARA, R. (2013) Infrastrutture critiche, il centro dell'attenzione. A colloquio con Sandro Bologna, consultabile ultimo accesso
http://www.securindex.com/downloads/59c2917e6a227d408c18714306fa4f44.pdf 28.02.2014

KALDAS, K.H.(nd) *The evolution of Estonian security options during the 1990s,* tesi di Laurea Magistrale Università di Tartu. Consultabile*:*
http://www.ut.ee/ABVKeskus/sisu/publikatsioonid/2006/pdf/ESTsecur.pdf ultimo accesso

KAMP, K.H. (2013) *NATO 2014 Summit Agenda*, NATO Defense College*,* Rome, No. 97, pp. 4

KARIG, D. e Lee R. (2001) *Remote Denial of Service Attacks and countermeasures*, Princeton University Press*,* Princeton

KARATZOGIANNI, A. ed. (2009) *Cyber Conflict and Global Politics,* Routledge, London and New York.

KASKA, K. et al. (2013) *Cyber Defense Unit of the Estonian Defense League*, NATO CCDCOE Pub, Tallinn

KASKA K., TIKK E. e VIHUL L. (2010) *International Cyber Incidents: Legal considerations*, NATO CCDCOE Publication, Tallinn

KELLO, L. (2013a) *The Skeptics Misconstrue the Cyber Revolution: A Response to Commentators on ISSF/H-Diplo and elsewhere,* H-Diplo e Security Studies, International Security, Journal of Strategic Studies, e The International Studies Association's Security Studies Section (ISSS), pp.1-4

KELLO, L. (2013b) ,*The meaning of cyber revolution. Perils to theory and statecraft*, International Security, Vol. 38, No. 2, pp. 7–40

KLEINROCK, L.(1961*) Information Flow in Large Communication* Nets, RLE Quarterly Progress Report
KLIMBURG, A. (Ed.) (2012) *National Cyber Security Framework Manual*, NATO CCD COE

Publication,Tallinn

KLIMBURG, A. (2011) *Mobilizing Cyber Power*, Survival, Vol 53, No.1, pp.41-60.

KORNS, S.and KASTENBERG, J. (2009) *Georgia's Cyber Left Hook*", Parameters, Vol 38, No.4, pp.60-76.

KRAMER, D. F. e TEPLINSKY, M.J. (2013) *Cybersecurity and tailored deterrence* , The Atlantic Council of the United States, Washington, pp. 1-12

KRAMER, F.D. et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington D.C.

KRASNER, S.D. (1999) *Sovereignty: Organized Hypocrisy*, Princeton University Press, New Jersey.

KUEHL, D.T. (2009), *From Cyberspace to Cyberpower: Defining the Problem,* in Franklin D. Kramer, Stuart Starr & Larry K. Wentz, eds., *Cyberpower and National Security*, Washington D.C., *National Defense University Press, Potomac Books*

LAN T, ZHANG XIN, RADUEGE H. D. , Jr., Dmitry I. Grigoriev, Pavan Duggal and Stein Schjølberg*, (*2010*) "Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*" EastWest Institute (Andrew Nagorski ed. 2010). 90

LEED, M (2013) *Offensive Cyber Capabilities at the Operational Level*, Centre for Strategic and International Studies, Washington

LEINER, et al. (2012) *Brief History of the Internet*, Internet Society Publication

LEWIS, J. A. (2012) *In Defense of Stuxnet*, Military and Strategic Affairs, Vol.4 No. 3 pp.65-76

LEWIS, J. A. (2010) *The Electrical Grid as a Target for Cyber Attack,* Centre for Strategic and International Studies, Washington

LEWIS, J.A. e SAPORITO, L. (2013) *Cyber Incidents Attributed to China*, Centre for Strategic and International Studies, Washington

LEWIS, J.A. (2008) *Securing Cyberspace for the 44th Presidency,* CSIS, Washington

LEWIS, J. A.; Timlin, K. (2009*) Cybersecurity and cyberwarfare: preliminary assessment of National Doctrine and Organization,* EUA: Center for Strategic and International Studies, Washington, DC

LEWIS, J. A. (2002) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threat*s, Centre for Strategic and International Studies, Washington

LIAROPOULUS, A.N. (2013) *Exercising State Sovereignti in Cyberspace: an International Cyber-order under construction?*, paper presentato all 8th *Conference on Information Warfare and Security,* Denver

LIAROPOULOS, A.N. (2011a) *War and Ethics in Cyberspace: Cyber-conflict and Just War Theory*, in Ryan, J. ed, *Leading Issues in Information Warfare & Security Research*, vol.1, Academic Publishing International Ltd, Reading.

LIAROPOULOS, A.N. (2011b*) Power and Security in Cyberspace: Implications for the Westphalian state system*, in *Panorama of Global Security Environment*, Centre for European and North American Affairs, Bratislava.

LIBICKI, M. C. (2013) *Reflections on Cyberdeterrence*, ISPI Analysis, No. 201, consultabile: http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_202_2013_0.pdf ultimo accesso 28.02.2014

LIBICKI, M.C.(2011), *The Strategic Uses of Ambiguity in Cyberspace*, Military and Strategic Affairs, Vol.3, No.3, pp.1-12

LIBICKI, M.C (2009), *Cyberdeterrence and cyberwar,* RAND Corporation, Santa Monica, CA.

LIBICKI, M.C. (2007) *Conquest in Cyberspace: National Security and Information Warfare,* Cambridge University Press, New York.

LIBICKI, M.C. (1995) *What is Information Warfare?* Washington DC

LIFF, P.A. (2013) *The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio,* The Journal of Strategic Studies, Vol. 36, No. 1, pp. 134–138

LIMNÉLL J. e RID T. (2014), *Is Cyber Warfare Real? Gauging the threats*, Foreign Affairs, concultabile a http://www.foreignaffairs.com/articles/140762/jarno-limnell-thomas-rid/is-cyberwar-real ultimo accesso 28.02.2014

LIMNÉLL J. (2013a) "The Dangers of Mixing Cyber Espionage with Cyber Warfare" consultabile http://www.infosecisland.com/blogview/23165-The-Danger-of-Mixing-Cyber-Espionage-with-Cyber-Warfare.html ultimo accesso 28.02.2014

LIMNÉLL J. (2013b) "Cyberworld as a political domain" consultabile: http://www.infosecisland.com/blogview/23177-Cyderworld-as-political-domain.html ultimo accesso 28.02.2014

LIMNÉLL, J. (2013c) *Defining the quality of Cyber Warfare* consultabile: http://www.infosecisland.com/blogview/22924-Defining-the-Qualities-of-Cyber-Warfare.html ultimo accesso 28.02.2014

LINDSAY, J.R. (2013), *Stuxnet and the limits of cyber warfare,* Security Studies, Vol.22, No.3, pp.365-404;

LINDSAY J.E CHEUNG T.M. (2013), *The Greatest Transfer of Wealth in History? Exploring the Relationship between Chinese Cyber Espionage and Technological Innovation,* University of California Institute on Global Conflict and Cooperation (IGCC), pp.1-28

LINDSAY, J.R. (2013), *Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations*, International Studies Association annual meeting, San Francisco, pp. 1-24

LINDSAY, J. (2012), *China and cybersecurity: political, economic and strategic dimensions,* Report from Workshops held at the University of California, San Diego, pp. 1-36

LOCATELLI, A (2013) *The Offence/Defense Balance in Cyberspace*, ISPI Analysis*, No. 203* consultabile: http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_203_2013.pdf ultimo accesso 28.02.2014

LORENTS P. & OTTIS R. (2010), *Knowledge Based Framework for Cyber Weapons and Conflict* in C. Czosseck and K. Podins, Conference onCyber Conflict Proceedings, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, pp. 129-142

LUNAS F. W. (2011), *The Modern Application on Sun Tzu'z Art of War*, position paper per il Centre for Cyberspace Research, consultabile al http://www.afit.edu/en/ccr/docs/cyber_innovations/Lunas_The_Modern_Application_of_Sun_Tzu_Art_of_War.pdf, ultimo accesso 28.02.2014

LUNCEFORD, B. (2009) *Cyberwar: the future of war?*, in *War and the Media: Essays on News Reporting, Propaganda and Popular Culture*, di Paul M. Haridakis, Barbara S. Hugenberg, and Stanley T. Wearden, 238-251. Jefferson, NC: McFarland

LUPOVICI, A. (2011), *Cyber warfare and deterrence: trends and challenges in research,* Military and Strategic Affairs, Vol.3, No.3, pp. 49-62

LUTTWAK, E. N. (2001) *Strategy: the Logic of War and Peace,* the Belknap Harvard University Press, Cambridge P 157

LUTTWAK, E. N (1995) *Toward Post-Heroic Warfare*, *Foreign Affairs*, Vol. 74, No. 3, May-Jun, pp. 109-122.

LYNN W.J. (2010), *Defending a New Domain. The Pentagon's Cyberstrategy*, Foreign Affairs, Vol.89, No.5, pp. 97-108

MAHAN, A. T. (1890) *The Influence of sea Power upon History, 1660-1783*, Little Brown, Boston

MÄGI, E. (nd) *Tiger Leap Program As A Beginning Of 21-St Century Education.* Consultabile http://www.ut.ee/eLSEEConf/Kogumik/Magi.pdf ultimo accesso 28.02.2014

MANDIANT (2013) *APT1 Exposing One of China's Cyber Espionage Units* consultabile http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf ultimo accesso 28.02.2014

MATANIA, E. e GOLDSTEIN, T. (2013) *Global Cyber Cooperation,* Israel Defense, Tel Aviv http://www.israeldefense.com/?CategoryID=512&ArticleID=2364 ultimo accesso 28.02.2014

MAURER, T.(2011) *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass

McELROY, D. e VAHDAT, A. (2013) *Iranian Cyber Warfare Commander Shot Dead In Suspected Assassination*, The Telegraph; 2 October, Telegraph, London

MCGRAW, G. (2013), *Cyber War is Inevitable (Unless We Build Security In),* The Journal of Strategic Studies, Vol. 36, No. 1, pp. 109–119

MEARSHEIMER, J. (2001) *The Tragedy of Great Power Politics*, W.W. Norton & Co., New Yor

MELE, S. (2013a) *I principi strategici delle politiche di cybersecurity,* pubblicato su: http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/principi-strategici-delle-politiche-di-cyber-security.html ultimo accesso 28.02.2014

MELE, S. (2013b) *Cyber-Weapons: Legal and Strategic Aspects. Version 2.0*, Istituto Italiano di Studi Strategici Nicolò Machiavelli, Roma

MEYER, P (2012) *Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda, RUSI Journal*, Vol. 157, No. 1.

MCGUIRE, C. (2012) *Digital Apocalypse: the artillery of Cyber War*, consultabile http://www.infosecisland.com/documentview/22200-Digital-Apocalypse-The-Artillery-of-Cyber-War.html ultimo accesso 28.02.2014

MIHALACHE, A. (2002) *The Cyber Space–Time Continuum: Meaning and Metaphor,* The Information Society, No. 18, pp. 293-301

MILLER, R.T. (2009), "Morals in Market Bubble", University of Dayton Law Review, Vol. 35 pp

113-138

MILLER, R. A. and KUEHL, D.T. (2009). *Cyberspace and the "First Battle" in 21st-century war*, Defense Horizons, Center for Technology and National Security Policy. Consultabile: http://www.ndu.edu/press/lib/pdf/defense-horizons/DH-68.pdf ultimo accesso 28.02.2014

MORGENTHAU, H. (1948) *The Politics Among Nations: The Struggle for Power and Peace*, Alfred Knopf, New York

MOROZOV, E. (2011) *The Net Delusion. The Dark Side of Internet Freedom*, Public Affairs, New York.

NOMAN, H. (2011) *In the name of God: Faith-based Internet Censorship in majority Muslim Countries*, OpenNet Initiative.

NYE, J.S. (2011) *The Future of Power*, Public Affairs, New York.

NYE, J.S. (2010) *Cyber Power*, *Belfer Center, Harvard Kennedy School*, Cambridge

O'CONNEL, M. E (2012) *"Cyber security without cyber war"*, Journal of Conflict & Security Law, Oxford University Press, v. 17, n. 2, p. 187-209.

OREN, A (2010) "The IDF's New Battlefield is Found in Computer Networks," *Haaretz*, Gerusalemme

PERNIK, P. e THUOY, E. (2013) *Cyber Space in Estonia: Greater Security, Greater Challenges*, ICDS Pub, Tallinn

PETERSON, D. (2013), *Offensive Cyber Weapons: Construction, Development, and Employment* in "The Journal of Strategic Studies", Vol. 36, No. 1, pp. 120- 124

RADUEGE, H.D. (2013) *The Public/Private Cooperation We Need on Cyber Security*, HBR Blog Network

RATTRAY, G. J. (2009) *An Environmental Approach to Understanding Cyberpower* in Kramer, F.D., et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington D.C.p 256

RAUD, H. (2012) *Securitization and Governance of Cyberspace –Case study on cyber security policy and public administration capacity in Estonia,* Tesi Magistrale University of Tartu

RID, T. (2013), *More attacks, less violence,* The Journal of Strategic Studies, Vol. 36, No. 1, pp. 139–142

RID, T e MCBURNEY, P (2012) *Cyber-Weapons*, The RUSI Journal, 157:1, 6-13.

RID T. (2011) *Cyber War Will Not Take Place*, The Journal of Strategic Studies, Vol.35, No.1, 5-32

ROBINSON, N, et al. (2013) *Cyber-security threat characterisation. A rapid comparative analysis*, RAND Corporation Publications, Santa Monica

ROBINSON, N. (2013), *Cybersecurity Strategies Raise Hopes of International Cooperation,* , RAND Corporation Publications, Santa Monica

ROSCINI, M. (2010), *World Wide Warfare- Jus ad bellum and the use of cyber force,* Yearbook of United Nation Law, Vol.14, pp.85-130

RYAN, J. ed. (2011) *Leading Issues in Information Warfare & Security Research*, vol.1,

Academic Publishing International Ltd, Reading.

SCHMIDT, A (2013) *The Estonian Cyberattacks,* in *The fierce domain – conflicts in cyberspace 1986-2012*, di Healey, J. (ed), Atlantic Council , Washington, D.C.

SCHMITT, M.N. ed. (2013) *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge University Press, Cambridge.

SCHMITT, M.N. (2012) "*Attack" as a Term of Art in International Law: The Cyber Operations Context ,* in C. Czosseck and K. Podins, *Conference on Cyber Conflict Proceedings*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn

SCHWEITZER, Y. e SIBONI, G. e YOGEV E. (2011) *Cyberspace and Terrorist Organizations*, Military and Strategic Affairs, Vol. 3 No. 3, pp. 39-47

SECHRIST, M. (2012) *New Threats Old Technology: Vulnerabilities in Undersea Communication Cable Menagement System*s*,* Belfer Center Harvard Kennedy School, Cambridge

SEGAL, A. (2011) *Cyberspace Governance: The Next Step*, Council of foreign relations, New York, pp. 1-4

SETOLA, R. (2011*) La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici,* Centro Militare di Studi Strategici (CEMISS), pp. 1-107

SETOLA, R. (2003) *La protezione delle infrastrutture critiche informatizzate, Automazione e Strumentazione*.

SHELDON, J. B (2011) *Achieving mutual comprehension: why cyberpower matters to both developed and developing countries,* Disarmament Forum, United Nations Institute for Disarmament Research, n. 4, p. 41-50.

SHI, S. and Song, Y. (2012) *Identifying Speculative Bubbles with an Infinite Hidden Markov Model*

SHREIER, F. (2010) *On Cyber Warfare,* DCAF Publication, Geneva

SIBONI, G. e Y.R (2012) *What Lies Behind Chinese Cyber Warfare*, Military and Strategic Affairs, No. 2, pp. 49-64

SIBONI, G., KRONENFELD S. (2012) *Iran and Cyberspace Warfare*, Military and Strategic Affairs, No. 3, pp. 77-99

SIBONI, G. (2011) *Protecting Crititcal Assets and Infrastructures from Cyber Attacks*, Military and Strategic Affairs, Vol. 3 No. 1, pp. 93-101

SINKS, M. A. (2008) *Cyber Warfare and International Law*, *Air University*, Alabama.

SINGH, S. (2012) *NSA announces cyber security cooperation with private sector,* The Indu, New Dehli

SIROLI, G.P. (2012), *Cyberspazio e Cyberwar*, in *L'ABC del Terrore. Le armi di distruzione di massa del terzo millennio,* a cura di Giampiero Giacomello e Alessandro Pascolini, V&P, Bologna

SIROLI, G.P. (2003), *Computer a prova di hacker,* Le Scienze, Vol. 416, pp. 70-73

SKLENKA, S. D. (2007) *Strategy, National Interests, And Means to An End*, Strategic Studies Institute, U.S. Army War College, Carlisle, PA

SOBELMAN, A.T. (2000) *Is everyone an enemy in cyberspace?*, Strategic Assessment, Vol.2, No.4, pp. 26-28

SOBELMAN, A.T. (1998) *An information revolution in the Middle East?,* Strategic Assessment, Vol.1, No.2, pp.1-13

SPYKMAN, N. (1944) *Geography of the Peace*, Harcourt and Brace, New York

STARR, S. H. (2009) *Toward a Preliminary Theory of Cyber Power*, in Kramer, F.D., et.al (2009) *Cyberpower and National Security*, Potomac Books, Inc, Washington D.C.

STAVRIDIS J. E e FARKAS E.N. (2012), *The 21st Century Force Multiplier: Public–Private Collaboration,* The Washington Quarterly, Vol.35, No.2, pp.7-20

STEINBERG, G. M. (2011) *Israel Studies An Anthology: The Evolution of Israeli Military Strategy: Asymmetry, Vulnerability, Pre-emption and Deterrence*; Israel Studies Anthology.

STERNER, E. (2011) *Deterrence in Cyberspace: Yes, No, Maybe*, in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century,* George C. Marshall Institute, Washington, D.C.

SUN TZU (1963) "*The Art of War"* (tradotto da Samuel B. Griffith), Oxford University Press, New York

SWAN, D. (2012) *Cyber security Vulnerabilities Facing IT Managers Today*, Tesi Magistrale. Consultabile: https://www.academia.edu/1416741/Cybersecurity_Vulnerabilities_Facing_IT_Managers_Today ultimo accesso 28.02.2014

SYMANTEC (2013*) Internet Security Report 2013,* Symantec Corporation*,*

TABANSKY, L. (2013) *Critical Infrastructure Protection Policy: the Israeli Experience,* The Journal of Information Warfare, Vol. 13 issue No. 3

TABANSKY, L. (2012) *International Cooperation in Critical Infrastructure Protection Against Cyber Threats*, Atlantic Voices, Vol. 2, No. 9, pp. 6-9

TABANSKY, L. (2011a) *Critical Infrastructure Protection against Cyber threats*, Military and Strategic Affairs*,* Vol 3, No.2, pp.61-78

TABANSKY, L. (2011b) *Basic Concepts in Cyber Warfare*, Military and Strategic Affairs*,* Vol 3, No.1, pp.75-92.

THOMAS, T. (2010) "Google Confronts China's Three Warfares", *Parameters*, Vol 40, No.2, pp.101-113.

THOMASON, J (1981); "Dependence, risk,and vulnerability"; Professional Paper 307 http://www.cna.org/sites/default/files/research/5500030700.pdf ultimo accesso 28.02.2014

THOUY, E. e MALDRE, P. (2013) *Dynamic Challenges, enduring Institutions: Cyber Security and the Future of the Tansatlantic Alliance*, ICDS Publ, Tallinn.

TIKK, E., et.al (2010) *International Cyber Incidents: Legal Considerations*, NATO CCD COE Publications, Tallinn.

TIRMAA-KLAAR H. e KLIMBURg A. (2011) *Cybersecurity And Cyberpower: Concepts, Conditions And Capabilities For Cooperation For Action Within The Eu*

TORDJMAN, N (2012) *Facing Virtual Reality – European Union's response to Threats from the Cyber World*, Heinrich Heine Univertat, Düsseldorf.

TOURE, H. (2010a) *Securing Cyberspace*. in *Annual Meeting 2010 of the* World EconomicForum*,* Davos, Switzerland,

TOURE, H. (2010b) *Building Confidence and Security in the Use of ICTs*. in *Interactive Facilitation Meeting on WSIS Action Line C5: C*ybersecurity

TSAROUGIAS, N. (2012) *Cyber attacks, self-defense and the problem of attribution*, Journal of Conflict & Security Law, Vol. 17, No.2, pp.229-244.

UNGERLEIDER, N. (2011) *The middle east cyberwar: "new media fighters" battle attacks in Israel and Turkey*; Fast Company. Consultabile: http://www.fastcompany.com/1725909/middle-east-cyberwar-new-media-fighters-battle-attacks-israel-and-turkey ultimo accesso 28.02.2014

VAN CREVELD, M. (1999) *The Rise and Decline of the State*, Cambridge University Press, Cambridge

VAN CREVELD, M. (1991) *The Transformation of War*, The Free Press, New York

VERCELLI, C. (2008) *Breve Storia dello Stato d'Israele (1948-2008),* Carocci Ed., Milano

VERIZON (2013) *Data Breach Investigation* report consultabile: http://www.verizonenterprise.com/DBIR/2013/ ultimo accesso 28.03.2014

VIIK, L. (2003) *The Internet Connects People not Computers*.Estonian Ministry of Foreign Affairs: Modern Estonia. Consultabile: www.vm.ee/estonia/kat_175/pea_175/2079.html ultimo accesso 28.02.2014

VON CLAUSEWITZ, C. (1832) *Vom Kriege*, trad.Howard M.

VON HEINEGG, W.H. (2012) *Legal Implications of Territorial Sovereignty in Cyberspace*, in Czosseck, C. et.al, 2012 *4th International Conference on Cyber Conflict*, NATO CCD COE Publications*,* Tallinn.

WADDELL, B. (2011*) That's What I'm Talkin' About* http://www.evolvingexcellence.com/blog/2011/01/thats-what-im-talkin-about.html#ixzz2pKNLKSrG ultimo accesso 28.02.2014

WALT, S. M. (2010), Is the cyber threat overblown?, Foreign Policy. Consultabile http://www.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown 28.02.2014

WALTZ, K. N. (1979) T*he Theory of International Politics*, Mc Graw-Hill, New York

WAMALA, F. (2011) *National Cybersecurity Strategy Guide*, ITU Publications , Geneva.

WILSHUSEN, G.C. (2013) *CYBERSECURITY:A Better Defined And Implemented National Strategy Is Needed To Address Persistent Challenges*, United States Government Accountability Office Publications, Washington

WILSHUSEN, G.C. (2012) *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage*, United States Government Accountability Office Publications, Washington

WINKEL, M. (2013) *The Global Social Network Landscape*, pag 30. Consultabile

http://www.optimediaintelligence.es/noticias_archivos/719_20130715123913.pdf ultimo accesso 28.02.2014

WOLFERS, A. (1962) *Discord and Collaboration: Essays on International Politics,* The Johns Hopkins Press, Chapter Five, "The Goals of Foreign Policy," pp. 67- 80

WU, T.S. (1997) *Cyberspace Sovereignty? The Internet and the International System*, Harvard Journal of Law &
Technology, Vol 10, No.3, pp.647-66.
ZALMAN, F. S (May 1986) *Adjusting to High Inflation: The Israeli Experience*; Federal Reserve Bank Of St. Louis

ZAMBERNARDI, L. (2010) *The Counterinsurgency's impossible Trilemma*, Washington Quarterly, 33:3 pp. 21-34

Strategie cibernetiche nazionali e documenti ufficiali

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION - *Information systems defence and security. France's Strategy*, July 2009

AUSTRALIAN GOVERNMENT – *Cyber Security Strategy*, 2009

COUNCIL OF EUROPE – *Cybercrime Strategies (version 14)*, October 2012

COUNCIL OF EUROPE (2001) "*Convention on Cybercrime*," Budapest, November 23.

ESTONIAN INFORMATION SYSTEM'S AUTHORITY – *Emergency Act*, 15 June 2009

EUROPEAN COMMISSION (2013) - *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*

DUTCH MINISTRY OF SECURITY AND JUSTICE – *The National Cyber Strategy (NCSS). Strenght Through cooperation*, July 2011

FEDERAL MINISTRY OF INTERIOR – *Cyber Security Strategy for* Germany, February 2011

GENERAL ASSEMBLY, *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmamen*t, UN document A/S-15/3, 28 May 1988, pp. 28–33

GOBIERNO DE ESPAÑA – *Spanish Security Strategy. Everyone's Responsibility*, Madrid 2011

GOUVERNMENT DU GRAND-DUCHE DU LUXEMBOURG – *Stratègie Nationale en matière de cyber sécurité*, Nov 2011

GOVERNMENT OF CANADA – *Canada's Cyber Security Strategy,* 2010

GOVERNMENT OF FINLAND – *Finland's Cyber security Strategy*, January 2013

GOVERNMENT OF JAPAN - *Information Security Strategy for Protecting the Nation, 2010*

GOVERNMENT OF SWEDEN - *Enhancing Internet freedom and human rights through responsible business practices*, April 2012

GOVERNMENT OF THE REPUBLIC OF TRINIDAD & TOBAGO - *National Cyber Security Strategy*, December 2012

GOVERNMENT OF THE UNITED STATES OF AMERICA – *The National Strategy to Secure Cyberspace, 2003*

GOVERNMENT OF THE UNITED STATES OF AMERICA – *Cyberspace Policy Review*, 2011

GUVERNUL ROMÂNIEI - *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*, May 2013

MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY OF INDIa – *National Cyber Security Policy*, 2013

MINISTRY OF DEFENSE OF ESTONIA – *Cyber security* Strategy, Tallinn 2008

NORWEGIAN MINISTRIES - *Cyber Security Strategy for Norway*, December 2012

OECD (2012) *The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy,* OECD Digital Economy Papers, No. 209, OECD Publishing, pp.1-14

PRESIDENZA DEI MINISTRI – *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico,* Gennaio 2014

PRESIDENZA DEI MINISTRI – *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica,* Gennaio 2014

REPUBLIK ÖSTERREICH - *Austrian Cyber Security Strategy*, 2013

RUSSIAN FEDERATION'S PRESIDENT - Information Security Doctrine of the Russian Federation, ottobre 2000. http://www.mid.ru/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b?OpenDocument

SECRETARIAT GENERAL DE LA DEFENSE NATIONAL DE LA REPUBLIQUE FRANÇAIS – *Menaces sur les systèmes informatiques,* september 2006

SHANGHAI COOPERATION ORGANIZATION (2009) *Agreement on Cooperation in the Field of Ensuring International Information Security* (based on unofficial translation), Yekaterinburg, June 16, 2009. Members: China, Kazakhstan, Kyrgystan, Russia, Tajikistan, and Uzbekistan.

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (2011) "Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities" consultabile: http://www.gao.gov/new.items/d1175.pdf ultimo accesso 28.02.2014

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (2010) "Critical Infrastructure Protection: Key Private and Public Key Expectations" consultabile: http://www.gao.gov/new.items/d10628.pdf ultimo accesso 28.02.2014

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (2010) "Cyberspace: United States faces challenges in addressing global Cybersecurity and Governance" consultabile: http://gao.gov/assets/310/308401.pdf ultimo accesso 28.02.2014

WORLD ECONOMIC FORUM (2013) *ICT for Economic Growth: A Dynamic Ecosystem Driving The Global Recovery*, consultabile: http://www3.weforum.org/docs/WEF_IT_DynamicEcosystem_Report_2009.pdf ultimo accesso: 28.02.2014

WORLD FEDERATION OF SCIENTISTS (2009) *The Erice Declaration of Principles for Cyber Stability and Cyber Peace was drafted by the Permanent Monitoring Panel on Information Security of the World Federation of Scientists*.

Conferenze:

"Information Warfare 2012", Rome, Italy (8 November 2012)

"*Cyber Dialogue: What is Stewardship in cyberspace*?" Toronoto, Canada (18-19 Marzo)

"Workshop Protezione Infrastrutture Critiche", Roma, Italia (26 novembre 2014)

"Baltic Defense Innovation Conference" , Tallinn, Estonia (3 Dicembre 2013)

"DiploHack", Tallinn, Estonia (6-8 Dicembre 2013)

“IPRED III: International Preparedness & Response to emergences and Disasters”, Tel Aviv, Israele (13 gennaio 2014)

“Cyber Tech 2014” Tel Aviv, Israele (27-28 gennaio 2014)

“INSS Annual Conference” Tel Aviv, Israele (28-29 gennaio 2014)

“UNIDIR Cyber Stability Seminar: Preventing Cyber Conflict” Geneva, Svizzera (10 Febbraio 2014)

Sitografia

http://abcnews.go.com/blogs/politics/2011/05/cyber-attack-on-us-electric-grid-gravest-short-term-threat-to-national-security-lawmakers-say ultimo accesso 28.02.2014

http://gigaom.com/2013/03/27/undersea-cable-cut-near-egypt-slows-down-internet-in-africa-middle-east-south-asia/ ultimo accesso 28.02.2014

http://www.wired.com/gadgetlab/2013/04/how-vulnerable-are-undersea-internet-cables/ ultimo accesso 28.02.2014

http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/ ultimo accesso 28.02.2014

http://www.youtube.com/watch?v=FcJawnKzi3s ultimo accesso 28.02.2014

https://www.clusif.asso.fr/index.asp ultimo accesso 28.02.2014

http://clusit.it/rapportoclusit/ ultimo accesso 28.02.2014

http://www.fas.org/irp/doddir/army/fm3-38.pdf ultimo accesso 28.02.2014

http://www.atlanticcouncil.org/publications/books/a-fierce-domain-conflict-in-cyberspace-1986-to-2012
ultimo accesso 28.02.2014

http://www.ccdcoe.org/publications/books/legalconsiderations.pdf ultimo accesso 28.02.2014

http://www.huffingtonpost.com/2011/10/31/nitro-attacks-china-hacker-chemical-firms-symantec_n_1067978.html ultimo accesso 28.02.2014

http://www.mcafee.com/it/threat-center/operation-aurora.aspx ultimo accesso 28.02.2014

http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?hpid=z1 ultimo accesso 28.02.2014

http://blog.foreignpolicy.com/posts/2010/09/27/6_mysteries_about_stuxnet ultimo accesso 28.02.2014

http://hackmageddon.com/2011/06/22/2011-cyberattacks-timeline/ ultimo accesso 28.02.2014

http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/ ultimo accesso 28.02.2014

http://www.globalresearch.ca/israeli-intelligence-report-us-drone-downed-by-iran-cyber-attack/28114 ultimo accesso 28.02.2014
http://www.kaspersky.com/flame ultimo accesso 28.02.2014

http://freebeacon.com/the-cyber-dam-breaks/ ultimo accesso 28.02.2014

http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?_r=0 ultimo accesso 28.02.2014

http://dx.doi.org/10.1080/01402390.2012.7395614 ultimo accesso 28.02.2014

http://www.foreignaffairs.com/articles/140762/jarno-limnell-thomas-rid/is-cyberwar-real ultimo accesso 28.02.2014

http://www.securitychallenges.org.au/ArticlePDFs/vol4no4DombrowskiandRoss.pdf ultimo accesso 28.02.2014

http://www.isodarco.it/courses/andalo13/paper/Iso13-Andreatta.pdf ultimo accesso 28.02.2014

http://www.afit.edu/en/ccr/docs/cyber_innovations/Lunas_The_Modern_Application_of_Sun_Tzu_Art_of_War.pdf ultimo accesso 28.02.2014

http://freebeacon.com/the-cyber-dam-breaks/ ultimo accesso 28.02.2014

http://securityaffairs.co/wordpress/17875/hacking/undetectable-hardware-trojan-reality.html ultimo accesso 28.02.2014

http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf ultimo accesso 28.02.2014

http://www.liberliber.it/mediateca/libri/d/douhet/il_dominio_dell_aria/pdf/il_dom_p.pdf ultimo accesso 28.02.2014

http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf ultimo accesso 28.02.2014

http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/ ultimo accesso 28.02.2014

http://www.colossus-computer.com/colossus1.html ultimo accesso 28.02.2014

http://www.investintech.com/content/historyinternet/ ultimo accesso 28.02.2014

http://www.edn.com/electronics-blogs/edn-moments/4399541/ARPANET-establishes-1st-computer-to-computer-link--October-29--1969 ultimo accesso 28.02.2014

http://denninginstitute.com/pjd/PUBS/AmSci-1989-6-arpanet.pdf ultimo accesso 28.02.2014

http://www.lk.cs.ucla.edu/data/files/Kleinrock/Information%20Flow%20in%20Large%20Communication%20Nets1.pdf ultimo accesso 2014

http://denninginstitute.com/pjd/PUBS/AmSci-1989-6-arpanet.pdf ultimo accesso 28.02.2014

http://www.defensenews.com/article/20100118/DEFFEAT01/1180306/Mapping-Pentagon-s-Networks ultimo accesso 28.02.2014

http://www.strategypage.com/htmw/htiw/articles/20100123.aspx ultimo acceso 28.02.2014

https://www.cs.duke.edu/courses/spring01/cps049s/class/html/mp.history.html ultimo accesso 28.02.2014

http://www.youtube.com/watch?v=2d7sPPlefok ultimo accesso 28.02.2014

http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf ultimo accesso 28.02.2014

http://www.internetworldstats.com/stats.htm ultimo accesso 28.02.2014

http://www.techterms.com/definition/cyberspace ultimo accesso 28.02.2014

http://www.leoalmanac.org/time-and-space-compressio%E2%80%8Bn-in-cyberspace/ ultimo accesso 28.02.2014

http://personal.lse.ac.uk/whitley/allpubs/timespecialissue/time06.pdf ultimo accesso 28.02.2014

http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/ ultimo accesso 28.02.2014

http://www.technollama.co.uk/open-web-vs-closed-internet ultimo accesso 28.02.2014

http://gigaom.com/2012/03/23/open-vs-closed-what-kind-of-internet-do-we-want/ ultimo accesso 28.02.2014

http://www.greatfirewallofchina.org/ ultimo accesso 28.02.2014

http://www.freedomhouse.org/report/freedom-net/2012/egypt#.UwNeIfl5O4I ultimo accesso 28.02.2014

http://surveillance.rsf.org/en/syria/ ultimo accesso 28.02.2014

http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf ultimo accesso 28.02.2014

http://www.dhs.gov/topic/cybersecurity ultimo accesso 28.02.2014

http://www.arcyber.army.mil/ ultimo accesso 28.02.2014

http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf a ultimo accesso 28.02.2014

http://www.fas.org/irp/doddir/army/fm3-05-30.pdf ultimo accesso 28.02.2014

http://www.psywar.org/ ultimo accesso 28.02.2014

http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument ultimo accesso 28.02.2014

http://cryptome.cn.com/2014/uscc-chinas-cyber-activities.pdf ultimo accesso 28.02.2014

http://icds.ee/fileadmin/failid/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf ultimo accesso 28.02.2014

http://www.wassenaar.org/ ultimo accesso 28.02.2014

http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html ultimo accesso 28.02.2014

http://www.osce.org/pc/109168 ultimo accesso 28.02.2014

http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf ultimo accesso 28.02.2014

http://www.citizenlab.org/cybernorms/letter.pdf ultimo accesso 28.02.2014

http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg;jsessionid=QI0W7ckcZt5e7NUAX7Rj3Q__.ntc-as1-guri2a ultimo accesso 28.02.2014

https://www.ria.ee/facts-about-e-estonia/ ultimo accesso 28.02.2014

http://e-estonia.com/e-estonia/how-we-got-here ultimo accesso 28.02.2014

http://e-estonia.com/components/x-road ultimo accesso 28.02.2014

http://estonianworld.com/technology/starting-scratch-case-e-government-estonia/ ultimo accesso 28.02.2014

http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf ultimo accesso 28.02.2014

http://lencd.com/data/docs/186-Bk3PartB_ESTONIA%20Tiger%20Leap.pdf ultimo accesso 28.02.2014

http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf ultimo accesso 28.02.2014

http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-asummary-to-date ultimo accesso 28.02.2014

http://www.riso.ee/et/files/InfoturbeRaamistik.pdf ultimo accesso 28.02.2014

https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf ultimo accesso 28.02.2014

http://www.kaitseministeerium.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf ultimo accesso 28.02.2014

http://www.hs.fi/english/article/Cyber-attacks+in+Estonia+Finland+observes+from+a+distance/1135227745145 ultimo accesso 28.02.2014

http://www.ccdcoe.org/423.html ultimo accesso 28.02.2014

http://www.ccdcoe.org/37.html ultimo accesso 28.02.2014

https://www.ria.ee/about-estonian-information-system-authority/ ultimo accesso 28.02.2014

https://www.ria.ee/activities-of-ria/ ultimo accesso 28.02.2014

http://www.state.gov/r/pa/prs/ps/2013/218234.htm ultimo accesso 28.02.2014

http://www.iiss.org/en/events/gsr/sections/global-strategic-review-2010-946c/sixth-plenary-session-6e03/q-6d98 ultimo accesso 28.02.2014

https://www.ccdcoe.org/334.html ultimo accesso 28.02.2014

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe ultimo accesso 28.02.2014

http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html ultimo accesso 28.02.2014

http://www.upi.com/Science_News/Technology/2012/10/27/Israel-shuts-down-police-computers/UPI-77211351363492/2012 ultimo accesso 28.02.2014

http://www1.cbs.gov.il/reader/?MIval=cw_usr_view_SHTML&ID=423, ultimo accesso 28.02.2014

http://urdunmubdi3.ning.com/profiles/blogs/financing-the-startup-nation?xg_source=activity ultimo accesso 28.02.2014

http://147.237.72.58/Tehila1/english_site ultimo accesso 28.02.2014

http://www.shabak.gov.il/english/Pages/default.aspx ultimo accesso 28.02.2014

http://www.shabak.gov.il/about/units/reem/pages/default.aspx ultimo accesso 28.02.2014

http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf ultimo accesso 28.02.2014

http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html ultimo accesso 28.02.2014

http://rt.com/news/iran-israel-cyber-war-899/ ultimo accesso 28.02.2014

http://www.ynetnews.com/articles/0,7340,L-4423968,00.html ultimo accesso 28.02.2014

http://electronicintifada.net/content/cyberwarfare-us-israels-electronic-attacks-iran-and-palestinians/11453 ultimo accesso 28.02.2014

http://www.israeldefense.com/?CategoryID=512&ArticleID=1557 ultimo accesso 28.02.2014

http://www.thewire.com/global/2012/03/israels-iron-dome-anti-missile-system-scary-efficient/49769/ ultimo accesso 28.02.2014

http://www.israeldefense.com/?CategoryID=512&ArticleID=2675 ultimo accesso 28.02.2014

http://www.israeldefense.com/?CategoryID=483&ArticleID=2492 ultimo accesso 28.02.2014

http://www.statisticbrain.com/social-networking-statistics/ ultimo accesso 28.02.201

http://in.bgu.ac.il/en/hsi/Pages/Movie.aspx ultimo accesso 28.02.2014

http://www.atp-israel.com/ ultimo accesso 28.02.2014

http://www.phantomreport.com/israel-invests-millions-in-drive-for-elite-cyber-warriors-unit-8200 ultimo accesso 28.02.2014

http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html ultimo accesso 28.02.2014

http://www.israeldefense.com/?CategoryID=483&ArticleID=2594 ultimo accesso 28.02.32014

http://portal.idc.ac.il/en/main/pages/newsDetails.aspx?idcid=142&idclang=English ultimo accesso 28.02.2014

http://heb.inss.org.il/index.aspx?id=4494 ultimo accesso 28.02.2014

http://www.businessinsider.com/best-tech-school-is-israels-unit-8200-2013-8 ultimo accesso 28.02.2014

http://www.theguardian.com/world/2013/aug/12/israel-military-intelligence-unit-tech-boom ultimo accesso 28.02.2014

http://www.homelandsecuritynewswire.com/dr20120605-veterans-of-israel-s-secretive-unit-8200-head-many-successful-hightech-startups ultimo accesso 28.02.2014

http://www.magshimim.net/ ultimo accesso 28.02.2014

http://www.iucc.ac.il/wp-content/uploads/2014/01/ICE-brochure.pdf ultimo accesso 28.02.2014

https://www.govtrack.us/congress/bills/112/s2165/text ultimo accesso 28.02.2014

http://moked.it/files/2013/12/vertice_ita_isr_intese_20131202.pdf ultimo accesso 28.02.2014

http://moked.it/files/2013/12/vertice_ita_isr_intese_20131202.pdf ultimo accesso 28.02.2014

http://www.osce.org/pc/109168 ultimo accesso 28.02.2014

http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all ultimo accesso 28.02.2014

http://www.israeldefense.com/?CategoryID=512&ArticleID=2654 ultimo accesso 28.02.2014