GRUPPO DI LAVORO AIIC

PROSPETTIVE STRATEGICHE DELLA PROTEZIONE CIBERNETICA

FEBBRAIO 2016

With the support of the Associazione italiana esperti infrastrutture critiche (AIIC)

Il Gruppo di Lavoro AIIC

- S. BRUSCHI, AIIC, SOCIO
- M. D'ORAZIO
- E. FIORITI, AIIC, SOCIO, COORDINATORE
- G. VILLAROSA , AIIC, SOCIO

Figura 1. L'Italia dal satellite.

LISTA DELLE TAVOLE

LISTA DELLE ABBREVIAZIONI

AIIC: Associazione italiana esperti delle infrastrutture critiche
PA: Pubblica amministrazione
CI: Critical Infrastructures
CII: Ceitical Information Infrastructure
Bce: Banca centrale europea
DHS: Department of Homeland Security
CERT: Computer Emergency Response Team
IC: Infrastrutture critiche
SW: software
Sys Admin: System Admnistrator
ICT: Information and Communication Technology
SCADA: Supervisory Control and Data Acquisition
EU: European Union
SC: Sistema Cibernetico
UE: Unione Europea
LAN: Local Area Network
SO: Sistema Operativo
IDS: Sistema di detezione intrusi
CAO: Criticalità auto-organizzata

Roma, 30 Ottobre 2015

Il presente documento si rivolge ai tecnici del settore, senza trascurare il pubblico non specializzato ma comunque interessato per motivi professionali o culturali. Per questo motivo si è cercato di renderlo di facile lettura e comprensione, il più possibile breve e sintetico; tuttavia siamo stati costretti a dare per acquisite alcune nozioni informatiche di base. I Riferimenti sono limitati al Settembre 2015.

SIMONE BRUSCHI,
MARIO D'ORAZIO,
ENZO FIORITI,
GIOVANNI VILLAROSA.

Note biografiche degli autori

Simone Bruschi, membro del Progetto Winston Smith, socio Clusit, AIIC, AEIT Segretario e Tesoriere di AMES Society - Microelettronica, Elettronica, Semiconduttori. Da molti anni studio le problematiche dell' underground di Internet cercando di diffondere una chiara conoscenza dei mezzi e del loro corretto utilizzo. Nelle mie ricerche ho come obiettivo di trovare una forma di comunicazione semplificata, per dimostrare che non vi è una vulnerabilità che non sia gestibile e che ogni sistema ha un suo linguaggio di interpretazione.

Mario D'Orazio è laureato in Ingegneria Elettronica presso l'Università La Sapienza di Roma. Ha lavorato nel settore della difesa e della pubblica amministrazione prima di passare ad occuparsi di reti di telecomunicazioni in particolare di gestione e integrazione dei sistemi. Affianca il lavoro di consulente alla attività di insegnamento dell'informatica presso la Pontificia Università Antonianum di Roma.

Enzo Fioriti è laureato in ingegneria dei controlli automatici all'Università La Sapienza di Roma. Ha lavorato nel settore privato e poi all'ENEA nel campo delle Infrastrutture Critiche e della robotica degli sciami. Si è occupato di cibernetica, reti neurali, caos, sistemi dinamici, sicurezza informatica, pattern recognition, oscillatori non lineari, reti complesse, diffusione epidemica del malware, swarm intelligence. Attualmente è consulente nel settore delle Infrastrutture Critiche.

Giovanni Villarosa, Security Manager (Università Roma tre), Chief Security Officer (Campus Biomedico Roma), Data Protection Officer (Luiss Business School). Laureato in scienze dell'intelligence, sicurezza e difesa alla Fondazione Universitaria Multinational Intelligence College di Lugano. Esperto di sicurezza e protezione fisica per infrastrutture complesse. Corsi di alta formazione (Università Roma Tor Vergata) in geopolitica, intelligence, eversione e terrorismo, competitive intelligence, esplosivi nella gestione della security, intelligence CBRNe.

1 Introduzione

La cibernetica è l'insieme di tre discipline: la teoria dell'informazione, la teoria del controllo automatico, l'elettronica. L'importanza della sicurezza delle infrastrutture cibernetiche, genericamente chiamate informatiche, è tale ormai da condizionare le altre Infrastrutture Critiche e lo sviluppo economico nel suo insieme. Ciò ha comportato la produzione di un grandissimo numero di studi, pubblicazioni, rapporti su programmi informatici difensivi, strutture specialistiche di supporto, addestramento del personale, analisi vulnerabilità e minacce, dispositivi hardware. La stessa Commissione Europea continua a finanziare studi analoghi, parcellizzando ulteriormente il lavoro.

Il risultato è che ogni istituzione continua a seguire propri criteri e metodologie, i quali, seppure di alto livello tecnico, sono fortemente carenti dal punto di vista della sintesi e del coordinamento. Di conseguenza, le risorse disponibili sono disperse in interventi *per se* corretti, ma privi di una sovrastante logica *che li renda efficaci* a fronte di un ambiente in grande cambiamento qualitativo.

Il Gruppo di Lavoro AIIC non si propone di colmare autonomamente le lacune esistenti, ma più modestamente di *evidenziare* una strada da percorrere. Non discuteremo di questioni politiche che competono agli organi istituzionali, l'analisi sarà limitata elle modalità generali di soddisfacimento delle indicazioni *ricevute* dalla politica, da inserire nel novero delle cose attuabili dati i mezzi disponibili.

Un esempio concreto varrà a chiarire il concetto basilare analizzato nel presente lavoro. Prima del II conflitto mondiale il Governo francese costruì la famosa "linea Maginot", per garantire la sicurezza dei confini. Il livello tecnico delle fortificazioni era indiscutibilmente eccellente, ma non evitò il disastro, da addebitarsi proprio alla alta qualità delle difese che infatti non furono superate. Furono semplicemente evitate, sviluppando una innovativa metodologia *ad hoc* compatibile con le risorse disponibili. La causa del disastro è da ricercarsi proprio nel *successo completo* della linea Maginot, che costrinse gli avversari ad elaborare soluzioni alternative.

Tali circostanze si ripetono sistematicamente in tutti i campi: quando ci si affida completamente a soluzioni tecnologiche molto avanzate, si sottovaluta l'aspetto metodologico sovrastante (qui chiamato "*dottrina*"). Non sono peraltro rari i casi in cui il progredire tecnico-scientifico finisce anzi col peggiorare i termini iniziali del problema, si pensi agli antibiotici che selezionano ceppi di batteri sempre più resistenti.

A nostro avviso, *il punto focale è l' assenza di riflessioni fondamentali su obiettivi, metodologie, impiego degli strumenti relativi alla protezione cibernetica, cioè appunto una "dottrina", che viene poi ad essere implementata nelle varie "strategie".*

Al proposito, è interessante il caso di un grande Paese orientale. Considerazioni geopolitiche della dirigenza nazionale hanno ivi determinato la elaborazione di una dottrina resa parzialmente pubblica in un articolo semi-ufficiale. La base della dottrina cibernetica desumibile da esso è che i targets *non* sono quelli comunemente considerati della massima importanza, in quanto saranno opportunamente protetti. Perciò le *scarse risorse disponibili devono essere dirette altrove,* ottenendo il conseguimento degli scopi prefissati *ad un minore costo*. Per esempio, una azione con risvolti psicologici potrebbe essere più efficiente di una distruttiva azione hacker contro una infrastruttura industriale.

Sempre nell' articolo citato, si sostiene inoltre la necessità di inserire le metodologie cibernetiche in un contesto di per se formale, ma non militare. Gli scenari futuribili sono quindi *profondamente diversi da quelli immaginati nella pianificazione attuale della protezione delle IC.*

In Italia invece esiste una tendenza a tralasciare ogni discussione in merito. Trattandosi di una questione anche culturale, non si può pensare di alleviare il problema con un semplice incremento dei finanziamenti, né ci si possono attendere indicazioni dai Paesi con disponibilità economiche e tecniche superiori, viste le peculiari necessità dei singoli membri UE.

Infine una importantissima osservazione di carattere macroeconomico. A nostro avviso, qualsiasi provvedimento teso a stabilizzare la protezione cibernetica nazionale deve contemporaneamente esercitare una rilevante influenza sull'economia, da cui trarre i mezzi per proseguire l'azione nel futuro.

La protezione cibernetica deve essere un *investimento reale*, con effetto immediato sulla fiscalità generale. Come ha fatto notare M. Draghi, presidente della Bce, a New York il 9 Ottobre 2014: << In Europa c'è bisogno di investimenti nel digitale e nell'istruzione, più che investimenti infrastrutturali>>.

Quindi è necessario avviare *subito* un dibattito concreto nel Paese, superando gli aspetti meramente tecnici, per estendere l'analisi alle prospettive generali ricordando lo scopo finale: garantire all'Italia una *adeguata sovranità cibernetica in ogni circostanza*.

2 La situazione attuale

2.1 Criticità ed assenza del dibattito interno

Finalità di una qualsivoglia dottrina cibernetica per l'Italia dovrebbe **essere garantire alla nazione una adeguata sovranità cibernetica in ogni circostanza.** Oggi è evidente la mancanza di tale garanzia, con conseguente rischio di compromissione delle iniziative politiche, economiche, sociali come indicato in [1.1, 1.2, 1.3, 2.1].

Si noterà l'ambiguità del termine "adeguata", che implica in effetti l'impossibilità di garantire la completa disponibilità e sicurezza di ogni elemento della rete cibernetica nazionale in ogni istante ed in ogni circostanza. Ne deriva la necessità di adottare una dottrina funzionale al livello di sovranità desiderata ed al livello di risorse disponibili realmente nel breve-medio periodo (3 -10 anni), il che implica una scelta, più o meno giusta che sia, ma esplicita. Diversamente si andrebbe incontro a spreco di risorse, inefficacia, inefficienza. Qui il dibattito è aperto e da approfondire.

Poco è noto al pubblico sui rischi legati alle organizzazioni in grado di manomettere Internet, i collegamenti telematici, le banche dati, i mainframe e le IC che usano estesamente l'informatica senza misure precauzionali serie. Il pubblico associa i rischi alla figura del giovinastro hacker per noia, senza percepire le dimensioni del problema. Del resto, anche l'allarmismo periodicamente presente sui mezzi di comunicazione di massa ha ormai prodotto una diffusa mitridizzazione, relegando le crisi informatiche nel novero dei disastri naturali.

Anche gli addetti ai lavori sembrano ignorare le proporzioni assunte dalle difficoltà da affrontare, limitandosi ad auspicare interventi sovranazionali e a sfornare analisi di vulnerabilità. Per esempio la dipendenza della disponibilità di energia dalle CII è stata drammaticamente sottolineata nel nostro Paese nel 2003 (Figura 1) col famoso blackout, dovuto peraltro a cause accidentali. In altre nazioni si sono però avuti incidenti non occasionali (ormai si contano a decine) ma tutto ciò non ha prodotto alcun serio dibattito.

La consapevolezza delle mutate relazioni internazionali contemporanee all'affermarsi di una tecnologia capace di ribaltare l'assioma della superiorità della difesa è lungi dall'affermarsi perfino nelle Nazioni più avanzate, con conseguenze potenzialmente gravi.

Ancora maggiormente perniciosa è la dipendenza del settore finanziario dalla ICT, per quanto fino ad oggi non si sono conosciuti episodi rilevanti. Le implicazioni durante momenti di instabilità finanziaria sono ancora da valutare, ma alcuni precedenti ne attestano le insidie.

Non è qui il caso di fare una ennesima disamina delle vulnerabilità che affliggono il sistema cibernetico; basti dire che in questo lavoro si intende semplicemente prendere in considerazione lo scenario del caso peggiore, cioè un opponente in grado di disporre di grandi risorse e della volontà di usarle per i propri fini al di fuori della legalità interna ed internazionale.

In estrema sintesi, questo è lo scenario da affrontare, facendo rilevare ancora una volta la mancanza di attenzione al riguardo, con la eccezione di un piccolo numero di addetti ai lavori.

2.2 Prolegomeni

Lo scopo di questa trattazione introduttiva e semplificata, prolegomeni appunto, è focalizzare gli aspetti peculiari della sicurezza di un sistema cibernetico, individuare gli elementi invarianti di uno scenario in rapidissima evoluzione.

Gli elementi di un sistema cibernetico possono essere ricondotti a due entità principali: un sistema informatico, genericamente chiamato server, interconnesso con l'esterno tramite una rete di telecomunicazione. Il sistema informatico può fornire sia l'accesso ad un insieme di informazioni, sia consentire il controllo remoto di altri sistemi.

I sistemi cibernetici tra loro interconnessi costituiscono il cyberspazio, uno spazio concettuale che fa da collante tra le diverse reti e infrastrutture di comunicazione e di servizi che sono alla base della società tecnologica moderna.

Lungi dall'essere un'astrazione concettuale il cyberspazio è una realtà con cui si interagisce ogni giorno; dalla semplice ricerca di informazioni via internet, la lettura del giornale on-line, le previsioni del tempo, gli orari degli autobus o dei treni, alle interazioni più elaborate: acquisto on line di servizi e/o merci, videochat tramite social network, telecontrollo.

La pervasività del cyberspazio è tale da essere diventato un elemento caratterizzante la società odierna e un'esperienza tanto comune nella nostra quotidianità quanto lo era negli anni novanta guardare la televisione.

Un server connesso ad internet fornisce ad utenti un insieme di determinati servizi, per esempio lo scambio di messaggi email. Gli utenti del servizio possono accedere ai loro messaggi da casa usando un computer e la rete internet cablata, o da ovunque usando uno smartphone e un'apposita *app*. Il server risponde alle richieste visualizzare o recapitare i messaggi degli utenti dopo averli identificati, in modo da garantire ad ogni utente la privacy. Inoltre il server deve essere accessibile in ogni momento dagli amministratori per poterlo gestire. Per accedere al server sia gli utenti che gli amministratori usano delle credenziali, tipicamente username e password, che consentono al server di identificarli e presentare le funzioni appropriate per ognuno. Utenti e amministratori condividono lo stesso mezzo di accesso al server, la rete internet, ciò che li distingue dal punto di vista del server sono le credenziali. Se un utente A si presenta al server usando le credenziali dell'utente B il server lo riconoscerà come utente B e gli fornirà i messaggi di B. Se l'utente A si presenta con le credenziali di un amministratore il server gli consentirà di aver accesso alle funzioni di amministrazione del server.

Un sistema informatico è un pezzo di elettronica e software che riconosce non l'utente ma le sue credenziali, allo stesso modo con cui la serratura del portone non riconosce il padrone di casa, ma solo la chiave che la apre.

Sempre nel caso del server di email, chiunque abbia accesso alla rete su cui è esposto il nostro server potrebbe cercare di presentarsi con le credenziali di un amministratore e se le indovinasse avrebbe completo accesso al sistema.

Se il server è su Internet, chiunque abbia accesso ad Internet, indipendentemente da quanto fisicamente vicino o lontano sia dal server, sia che si trovi nella stessa nazione, o nello stesso

continente, dove è fisicamente installato il server può provare ad accedervi presentando le credenziali di amministratore.

Lo scenario che ne deriva è quello di un assedio continuativo al nostro server da parte di una pluralità di attaccanti difficilmente localizzabili e non neutralizzabili. Per difendere il nostro server potremmo investire in contromisure per contrastare i tentativi di accesso illecito al sistema. Tipicamente i costi necessari alla difesa sono di gran lunga superiori a quelli necessari per l'attacco: migliaia di euro in tecnologie e software difensive contro poche centinaia per l'acquisto di un pc, un tablet o uno smartphone per provare a forzare il sistema.

Una classificazione delle tipologie di attaccante è complessa:

- l'utente casuale che cerca di ottenere un vantaggio aggirando le restrizioni del server: ad esempio la ragazza gelosa che vuole leggere i messaggi del fidanzato.
- l'hacker solitario che vuole sfidare le difese del sistema
- il gruppo organizzato di hacker che cerca informazioni sensibili o vuole bloccare la fornitura del servizio
- la struttura offensiva di un paese straniero interessato ad avere accesso alle infrastrutture informative e tecnologiche (banche dati, data center di banche o aziende multinazionali, rete energetica, ferroviaria, aerea, etc etc per spionaggio o per supporto alle operazioni militari convenzionali.

Altrettanto complessa la classificazione delle finalità di un attacco:

- attacchi tesi a distruggere la capacita di interconnessione o di fornire servizi del sistema;
- attacchi tesi a penetrare nel sistema per carpirne informazioni o assumerne il controllo;
- attacchi tesi a ad avere accesso ad una seconda rete cui il sistema è connesso.

Per quanto si investa nel rendere sicuri e inviolabili i server, restano sempre una serie di problemi che possono aprire brecce nei sistemi più sicuri: la presenza di errori o difetti: il software che gestisce un server è un sistema complesso fatto di vari sottosistemi nel cui processo di progettazione sviluppo e realizzazione sono passibili di errori o difetti che se sfruttati possono permettere ad un attaccane di aggirare le difese del sistema; il fattore umano: un server è un sistema usato a vario titolo da una pluralità di persone che se non sufficientemente preparate addestrate e sorvegliate, possono commettere errori od omissioni che lascino spalancate le porte di accesso al sistema, esempio tipico username e password scritte su un post-it vicino alla postazione di lavoro, leggibili dal personale che effettua la pulizia degli uffici la notte; infine, il paradosso tecnologico: quanto più progredisce la tecnologia di difesa tanto più progredisce la tecnologia degli attaccanti. Ovvero tutti i server che ritardino l'aggiornamento del software di difesa, e non si parla di settimane ma di giorni o di ore, rispetto all'aggiornamento degli attaccanti sono vulnerabili.

La sicurezza è un concetto dinamico: deve essere continuamente controllata e verificata, seguendo un piano che deve sempre essere aggiornato.

L'esito con cui il piano di sicurezza deve necessariamente confrontarsi, perché più probabile sul lungo termine, è la sconfitta. Qualunque strategia di difesa deve prevederla e definire i criteri e le modalità per ripristinare le capacita del sistema attaccato limitando le conseguenze sugli altri sistemi cui il server è connesso.

Passando dall'esempio di un singolo server agli scenari reali in cui una molteplicità di server gestiscono reti nevralgiche, per esempio la rete di distribuzione elettrica, la rete telefonica, la rete ferroviaria, i server e le reti che gestiscono i dati e le informazioni delle società quotate in borsa o delle banche, quanto detto sopra si amplifica e comporta impatti sociali ed economici rilevanti. Si pensi alla compromissione della rete ferroviaria, che avvenga tramite l'accesso al server che espone sul web gli orari.

La compromissione della rete di gestione e telecontrollo delle centrali idroelettriche potrebbe portare un aggressore ad avere accesso al sistema di apertura delle saracinesche di una diga provocando un'inondazione i cui effetti sarebbero gli stessi di un attacco militare convenzionale.

La caratteristica di interconnessione del cyberspazio fa si che la compromissione di un sistema abbia ripercussioni anche sugli altri, sia dirette che indirette. Per esempio un attacco diretto a bloccare la distribuzione di energia della rete elettrica ha una ripercussione diretta sulla rete telefonica, in quanto lascia senza alimentazione le antenne della rete mobile. Un attacco diretto a penetrare il sito web con l'orario ferroviario potrebbe indirettamente consentire l'accesso al server della rete ferroviaria che fornisce al sito web l'orario e da questo a tutta la rete ferroviaria. In questo caso l'attacco al sito web indirettamente compromette anche la rete ferroviaria.

Da quanto precede segue che la sicurezza è un concetto globale, non solo del soggetto attaccato ma anche di quanti direttamente o indirettamente ad esso sono interconnessi. Gli esiti di un attacco informatico non sono limitati al cyberspazio, ma hanno implicazioni nella vita reale delle persone e della società.

Si rende necessaria allora una dottrina per il cyberspazio, le cui iniziative dei singoli attori del cyberspazio siano coordinate e integrate in un piano strategico di più ampio respiro.

3 Aspetti teorici: il modello azione - reazione

La sicurezza cibernetica implica l'analisi delle interazioni fra i soggetti operanti in un certo ambiente, analisi da sviluppare in modo scientifico o quantomeno rigoroso. A tale scopo la Teoria dei Sistemi, ha sviluppato degli strumenti concettuali molto utili, quali *feedback* (in italiano *retroazione*) e la *stabilità* strutturale. In figura 2 è rappresentato un esempio di *feedback* dall'uscita:

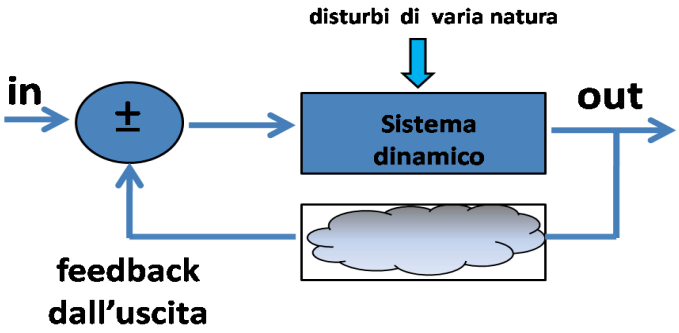

Figura 2. Rappresentazione concettuale di un sistema dinamico non-lineare. Una causa (in) produce un effetto (out), che a sua volta influisce sulla causa iniziale del processo. Il tutto è stabile se l'uscita si mantiene entro valori ritenuti accettabili. Si noti che questo modello vale anche se il Sistema cibernetico è fisicamente sconnesso da Internet.

come si osserva, le uscite sono riportate in ingresso, ma possono essere sommate o sottratte all'ingresso attuale, producendo un risultato di stabilizzazione o destabilizzazione. I sistemi in grado di stabilizzarsi si adattano agli ingressi dinamicamente, ossia modificandosi entro certi limiti.

I sistemi instabili invece incontrano delle modifiche difficili da sostenere, per cui il funzionamento subisce pesanti alterazioni. Anche un Sistema Cibernetico (SC) è un sistema del tipo indicato in Figura 2 e possiede quindi un feedback.

Nelle interazioni cibernetiche l'opponente esercita appunto delle reazioni alle difese approntate da un System Admin, reazioni che sono difficili da prevenire con immediatezza a causa della fantasia creativa dell' hacker.

Per fissare le idee con un piccolo esempio, pensiamo ad un hacker che cerca di entrare nel SC, agli amministratori che cercano di scoprirne i tentativi e tappare le falle per salvaguardare il sistema, alla ulteriore reazione dell'hacker cercherà a sua volta di migliorare la tecnica di intrusione e cosi via. Questo ciclo, definito "*detect and mitigate*", rappresenta la procedura standard per buona parte delle protezioni cibernetiche.

3.1 Il sistema informatico sicuro

La ricerca di un Sistema informatico sicuro è l'ideale di ogni pianificazione. Molte sono state le proposte al riguardo, fino a giungere ad un orientamento, oggi prevalente, di tipo "*detect and mitigate*" ossia scopri l'intrusione, tappa la falla e riduci il danno.

Purtroppo di recente (M. Adam, T. Clancy et al., 2013) si è scoperto che un SC basato su metodologie di sicurezza *detect and mitigate* **è intrinsecamente instabile,** perché il feedback (la reazione dell'hacker) adatterà gli attacchi alle difese. Quindi la maggior parte delle tecniche in uso sono, almeno teoricamente, inadeguate a prescindere dai programmi software impiegati o dalla bravura dei tecnici.

Il significato fisico di Figura 2 è che il sistema Hacker si adatta a seconda degli input ricevuti e a sua volta agisce sul sistema Sys Admin, un po' come accade nei film Star "Trek Next Generation" con i Borg e ciò anche se il SC è disconnesso da Internet. Ma se le misure adottate in difesa del SC nello schema di Figura 2 vengono più o meno rapidamente assimilate e superate, esiste una valida strategia da opporre? La risposta è si, posto che si riesca ad eliminare gli accessi di bassa complessità informatica quali l'accesso fisico, il phishing, il social engineering etc etc e contemporaneamente a variare spesso i parametri interni del sistema Sys Admin. Lo sforzo di superare barriere ad alto contenuto tecnologico che cambiano continuamente ribalta il vantaggio iniziale dell'Hacker a favore del Sys Admin. "Continuamente" può significare anche **ogni giorno**, ma soprattutto significa evitare con cura la **periodicità** delle variazioni.

Si noti attentamente la necessità dell' assenza di canali di bassa complessità informatica (attacchi fisici, elettromagnetici, social engineering etc etc) e della non-stazionarietà dei canali ad alta complessità (gli attacchi informatici molto evoluti): solo allora il SC diviene sicuro anche a fronte di attacchi adattativi avanzati.

Naturalmente ci sono delle controindicazioni: troppa non-stazionarietà induce instabilità nel sistema da proteggere, ossia avremo un sistema sicuro da interferenze e disturbi, ma che funziona male. Fortunatamente la teoria del controllo automatico ha analizzato anche questa situazione e l'ha risolta attraverso la previsione dell'uscita per prevenire in anticipo l'instabilità. Una analoga soluzione vale per la protezione cibernetica.

In sintesi, un sistema del tipo di Figura 2 **è *teoricamente* messo in sicurezza** da tre fattori:

1) **assenza di canali di bassa complessità**,
2) **non-stazionarietà dei canali ad alta complessità**,
3) **capacità previsionali significative.**

La prima proprietà è trattata nel paragrafo 5 come protezione fisica, la seconda è considerata nel paragrafo 4 nell'ambito dell'approccio indiretto, la terza nei paragrafi 3.2 e 3.3.

3.2 L'infrastruttura cibernetica come sistema complesso

Proseguiamo con un ulteriore raffinamento del nostro modello di SC immaginando l'infrastruttura cibernetica come in Figura 3, come un sistema di sistemi connessi. Notiamo subito che lo scambio di comunicazioni è la natura stessa del sistema, quindi non si può staccare la spina per risolvere eventuali problemi. Tranne alcuni casi particolari, saremo costretti a rimanere in gioco alle condizioni poste dagli altri soggetti.

La seconda caratteristica che avvicina l'infrastruttura cibernetica ad un sistema complesso è la presenza di feedback non lineari, cioè qualitativamente diversi da quelli descritti in Figura 2. Una delle conseguenze è la scomparsa della proporzionalità fra causa ed effetto, come dire che un semplice PC potrebbe generare un gigantesco blackout.

Un terzo elemento è la natura dell'equilibrio globale nel Sistema cibernetico, che non è statico ma evolve lentamente verso un punto critico oltre il quale si produce un collasso molto rapido. Fenomeni di questo tipo si verificano spesso nel Sistema produzione/distribuzione dell' elettricità (SE) e sono chiamati criticalità auto-organizzate (CAO).

Quest'ultimo elemento merita una considerazione particolare. Se già di per se il SC si avvicina ad un punto di collasso, le azioni distruttive deliberate saranno pericolosamente favorite. Nell'ambito degli studiosi di IC questo fenomeno è chiamato effetto domino o delle inter-dipendenze e ne costituisce l'argomento di investigazione principale nonché la principale preoccupazione. Pertanto, la protezione cibernetica non potrà prescindere dalla analisi quantitativa delle inter-dipendenze con le altre IC.

Negli ultimi decenni la ricerca sui sistemi complessi ha prodotto interessanti risultati. Oggi i maggiori centri di ricerca del mondo lavorano sulla analisi di problemi di grande e grandissima scala, che coinvolgono la sicurezza cibernetica ed offrono l'opportunità di soluzioni concrete. Il paradigma del sistema complesso è parte integrante della elaborazione della dottrina, perché non è pensabile un controllo umano diretto sui molteplici fattori da prendere in considerazione prima di prendere una decisione operativa. Qui non è il caso di entrare nel dettaglio, basterà tener presente la necessità di affrontare il problema della protezione cibernetica con un metodo scientifico aggiornato come nell'esempio concreto che segue, tratto dalla letteratura scientifica recente.

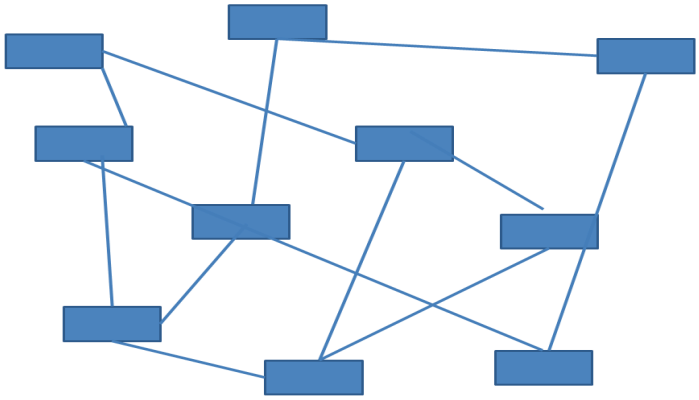

Figura 3. Rappresentazione concettuale di un insieme di Sistemi dinamici interconnesi (del tipo di Figura 2) a formare un Sistema complesso.

La diffusione di malware (mal-icious soft-ware) nelle reti di dispositivi elettronici ha sollevato profonda preoccupazione, poiché dalle reti ICT le infezioni potrebbero propagarsi ad altre Infrastrutture Critiche, producendo il ben noto effetto domino.

Esistono due strategie di base per la diffusione del malware di prossima generazione: l'intrusione mirata e la ricerca cooperativa. La prima prevede l'approccio tradizionale al bersaglio, la seconda richiede un controllo distribuito e uno schema decisionale complesso con ricerca di una decisione consensuale.

Come diretta conseguenza il malware si diffonderà come una epidemia vera e propria. Tuttavia, mentre un worm convenzionale cerca di infettare il maggior numero possibile di macchine il più rapidamente possibile, un malware avanzato infetterà poche macchine opportunamente selezionate in un tempo relativamente lungo. Comunque in entrambi i casi l'infezione procede seguendo le stesse equazioni usate per studiare la dinamica delle epidemie biologiche.

Per comprendere come la matematica dei sistemi complessi può essere d'aiuto presentiamo questo esempio tratto da [3.2]. Bisogna proteggere una LAN di computer da una infezione di malware sofisticato. Si è reso disponibile un antivirus, ma c'è il problema della esiguità delle risorse che impedisce ai computer di ricevere il trattamento in tempi ridotti tramite i tecnici specializzati che sono pochi. Perciò bisogna scegliere con cura i computer (i nodi di Figura 4) cui somministrare l'antivirus.

Si può arrestare la diffusione del virus vaccinando solo il 4% dei computer ma scegliendoli in modo ottimale, secondo precisi criteri ?
Comprendere questo modello significa avere la possibilità di contrastare la diffusione del malware nei suoi stadi iniziali, quando i costi sono ancora limitati. I ricercatori stanno cercando quindi di sviluppare una analisi di alto livello della propagazione del malware *tralasciando i dettagli software* per generalizzare il più possibile le strategie difensive, *scegliendo in modo ottimale i nodi più importanti da proteggere*.

Allo scopo gli autori (A. Arbore e E. Fioriti, 2012) hanno progettato un algoritmo applicato al caso di una rete LAN reale infettata da un vero virus. Le simulazioni numeriche effettuate su tale rete mostrano che l'algoritmo è in grado di fermare la diffusione del virus.

In Figura 4 si mostra il risultato ottenuto dalla vaccinazione dei soli computer scelti dall'algoritmo. I nodi (o computer) scelti dall'algoritmo per la vaccinazione sono mostrati in Figura 4 con colore verde (rappresentano 4% del totale dei computer della LAN), mentre i punti in rosso sono i nodi su cui la diffusione ha avuto successo. Sono rimasti infetti il 23% del totale dei nodi; il numero può apparire grande ma si deve considerare l'esiguo budget disponibile.

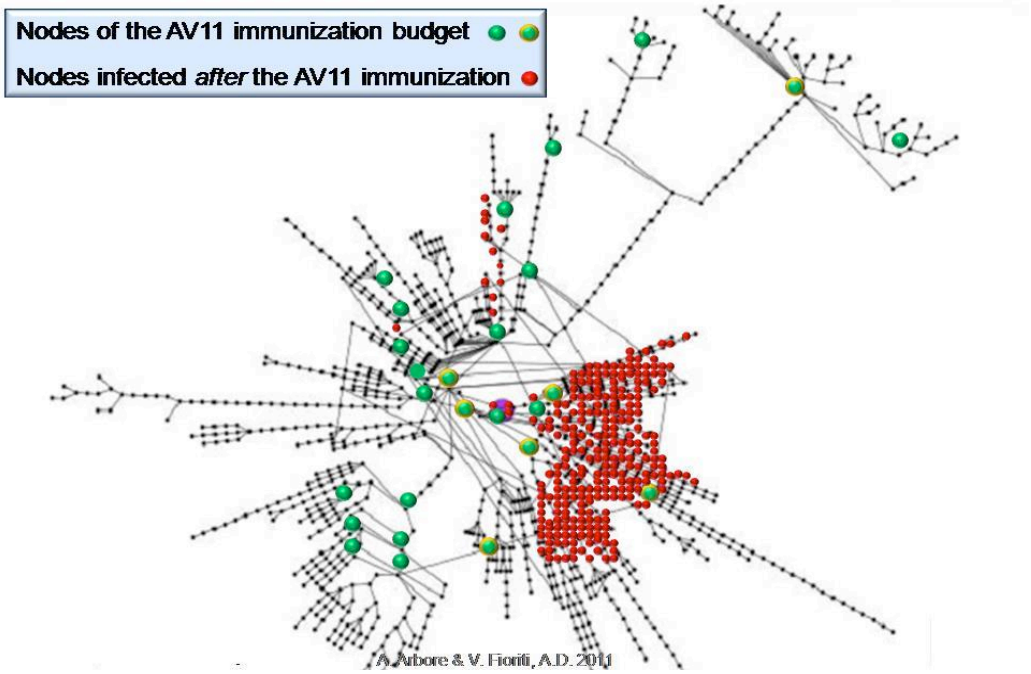

Figura 4. Una rete LAN dopo la vaccinazione (nodi verdi grandi, 4% del totale). I punti rossi indicano i computer rimasti infetti, mentre i punti neri piccoli sono stati salvaguardati dalla vaccinazione.

Oggi la resilienza e protezione delle CI sono temi centrali per molti programmi di ricerca in tutto il mondo; in particolare per le infrastrutture ICT sottoposte a devastanti attacchi. Sfortunatamente le dipendenze fra le CI sono ormai giunte ad un livello tale di complessità da necessitare di una trattazione formale, di cui, peraltro, ancora non si dispone completamente. D'altro canto i codici software di attacco sono sempre più sofisticati e si associano a strategie complesse in grado di apprendere ed analizzare la rete di computer target in modo intelligente ed organizzato.

Per affrontare questa non facile situazione, gli studiosi stanno sviluppando tool matematici di ispirazione biologica. Fra questi il modello epidemiologico ha ricevuto molte attenzioni ed ha prodotto risultati concreti attraverso l'analisi spettrale che ci consente di stabilire se una rete sarà soggetta ad essere infettata, quali sono i nodi critici, cosa fare per ridurre o annullare i danni, come aumentarne la resilienza.

Non è immediato né semplice per gestori delle reti tecnologiche accettare il fatto che la topologia della rete abbia delle proprietà nascoste ed imprevedibili all'analisi meccanico-funzionale, ma con ogni probabilità questa è la strada da percorrere per padroneggiare gli sviluppi futuri.

3.3 Il paradosso tecnologico

A fronte di un input quale potrebbe essere un nuovo tipo di software, come abbiamo detto in precedenza il sistema cibernetico produce un *feedback* che, di solito, tende a neutralizzare la prima innovazione e cosi via. Può accadere che si ottenga così un risultato opposto a quello desiderato per cui si era prodotta la prima innovazione, generando un paradosso insieme ad uno spreco di risorse. Il progresso tecnologico dei mezzi tecnici, per quanto rilevante, non è un fattore decisivo.

Questo è appunto il paradosso della linea Maginot, creata per garantire la sicurezza perimetrale tramite uno spiegamento di risorse finanziarie e tecniche notevolissimo. Come noto, produsse un disastro dovuto proprio al *successo completo* della infrastruttura, che costrinse gli avversari ad elaborare contromosse alternative migliori, originali e meno costose.

Tali circostanze si ripetono sistematicamente in tutti i campi, quando ci si affida completamente a soluzioni tecnologiche avanzate, si sottovaluta l'aspetto metodologico sovrastante (la *dottrina*). Avendo a che fare con avversari in grado di elaborare strategie complesse (il modello *azione-reazione* o del *feedback*) questo è lo scenario che si presenta. Bisogna considerare l'opponente come capace di reagire ed adattarsi opportunamente tramite il feedback, non supporre a priori che si comporterà secondo uno schema fisso e prevedibile, seppure molto sofisticato. Qualche volta viene presentato il paragone con gli scacchi, ma è un paragone estremamente fuorviante. Non si gioca alla pari nella realtà, non ci sono regole e sopratutto l'ambiente può essere modificato. In conseguenza di ciò gli esiti non sono predicibili.

Per sfuggire al paradosso tecnologico la soluzione consiste nell'adottare *metodologie* di impiego dei mezzi che siano di altissimo livello a fronte di *mezzi* tecnici sufficientemente efficaci anche se non eccezionali. Apparentemente questa soluzione appare semplice, in realtà richiede un continuo processo dinamico di aggiornamento/addestramento non banale. L'idea di fondo è che non sono i picchi di eccellenza a produrre risultati apprezzabili, ma un buon livello medio complessivo.

Scendendo nel dettaglio, il paradosso tecnologico per la sicurezza cibernetica richiede di evitare la ricerca delle soluzioni tecniche più popolari ed attraenti per l'alto livello scientifico e tecnologico, anche per gli elevati costi inevitabilmente connessi e specialmente in situazioni di risorse scarse quale l'attuale. Ma il motivo principale è che si rivelerebbero inadeguate e vulnerabili nel giro di poco tempo.

Ciò che serve è strutturare un processo dinamico piuttosto che implementare progetti di grande impegno economico, soluzione che ricorda il metodo linea Maginot. Un processo significa una metodologia organizzata secondo una dottrina condivisa ed implementata da opportune strategie, addestramento continuo e verifiche indipendenti.

Inizialmente la cosa potrebbe essere molto onerosa, ma sul medio periodo il rapporto costi/benefici si ristabilirebbe grazie ai ritorni economici indotti, cfr. il paragrafo 6. In ogni caso a prescindere dalla dottrina scelta è mandatorio evitare la trappola del paradosso tecnologico.

3.4 Modelli matematici

Recentemente sono stati introdotti diversi strumenti formali per lo studio della sicurezza nel Sistema cibernetico. Il loro impiego su vasta scala è necessario per monitorare e prevedere eventuali azioni aggressive, scoprire punti deboli nelle infrastrutture, ottimizzare le difese.

Dato l'enorme numero delle installazioni, dispositivi, reti di computer etc etc non è pensabile eseguire un controllo su basato sulla sorveglianza diretta, diventa necessario elaborare sistemi automatizzati previsionali tramite modelli matematici molto sofisticati, ossia *anticipare* gli eventi con un ragionevole margine di tempo.

Elenchiamo ora alcune metodologie matematiche e le loro applicazioni pratiche, tratte dal libro bianco 2009 dei Sandia Labs sulla cybersecurity [3.1]:

Malicious code detection

Detection methods beyond simple signature detection are required for long-term proactive detection and analysis. Moreover, methods are needed that can identify mutations or variations of malicious code with high accuracy and low false positive rates.

Malicious behaviour detection
Methods are needed for aggregating information (locally and across networks) to detect complicated multi-stage attacks, analyzing systems for identification of potential vulnerabilities, and detecting rare events

Machine Learning
Online learning methods for dynamic modelling of network data and malware.
Modelling data with skewed class distributions to handle rare event detection.
Feature selection/extraction for data with evolving characteristics.

Optimization
Large-scale optimization for graph searching/analysis and model parameter estimation (e.g., in learning models and descriptive analysis models).
Sub-optimal optimization in the presence of data sampling or other uncertainties.
Optimization under uncertainty applied to discrete models and/or data.

Statistics and Probability
Data analysis in the presence of missing values.
Modelling uncertainty: reliability and risk versus noise and sampling error.
Sampling streaming or distributed data, and determination of how and to what extent such samples differ from real data.

Linear Algebra
Updating matrix- or tensor-based models when data is added or changed.
Simultaneous modelling of heterogeneous data types and relationships.
Tensor models for analyzing complicated, multi-way relationships in data

L'uso di queste tecniche sarebbe estremamente auspicabile all'interno di una moderna protezione cibernetica ed è sicuramente una delle aree di ricerca da focalizzare nell'immediato futuro.

4 Dottrine per la protezione cibernetica

Finalità di una dottrina cibernetica è **garantire alla nazione una adeguata sovranità cibernetica in ogni circostanza.**

Questo punto è centrale e non scontato, sia perché sono plausibili altre scelte, sia per le implicazioni. Alcuni Stati hanno già riconosciuta la sovranità cibernetica alla stregua di ogni altro tipo di sovranità, molti altri Stati invece non ne hanno recepito l'esigenza, limitandosi a generiche affermazioni sulla necessità economica di proteggere le proprie CII. La differenza è evidente: mentre gli asset economici sono in qualche modo negoziabili, la sovranità è inalienabile.

Si noterà poi l'ambiguità del termine "adeguata", che implica l'impossibilità di garantire la completa disponibilità e sicurezza di ogni elemento della rete cibernetica nazionale sempre e comunque. Ne deriva la necessità di adottare una dottrina funzionale consona al livello di sovranità desiderata ed al livello di risorse disponibili effettivamente nel breve-medio periodo, il che costringe ad una scelta, più o meno discutibile, ma esplicita. Diversamente si andrebbe incontro a spreco di risorse, inefficacia, inefficienza.

Ne paragrafo 6 si darà conto dei notevoli costi legati alla implementazione pratica di una dottrina e delle sue strategie derivanti. Insieme alle difficoltà finanziarie si intravede però l'opportunità di fornire una "spinta" al sistema economico proprio grazie agli investimenti richiesti.

4.1 Il nuovo paradigma

Si vengono oggi a delineare dei *principi operativi* diversi rispetto a quelli che si conoscevano nel passato, evidentemente a causa delle innovazioni tecnologiche introdotte. Tali innovazioni sconvolgono molti convincimenti ormai abituali e dovrebbero far riflettere sulle difficoltà di armonizzare le metodologie "digital immigrant" con quelle "digital native" .

Ne raccogliamo alcuni:

I) L'attacco cyber è *favorito* rispetto alla difesa in quanto le metodologie difensive tipo "detect and mitigate" sono *intrinsecamente instabili.* Si ribalta un assioma che ha retto per secoli.

II) La *mobilità* (cosa diversa dalla velocità) è completa. Microchip sotto pelle, occhiali google, satelliti, Internet etc etc garantiscono la totale dislocazione degli asset anche nello spazio reale.

III) La velocità delle azioni è massima, per cui bisogna *prevedere* anticipatamente eventuali interferenze nel normale funzionamento del Sistema cibernetico.

IV) Gli aspetti *psicologici* divengono prevalenti.

I principi operativi sono alla base delle varie strategie che implementano le dottrine più comuni esposte di seguito nel paragrafo 4.2.

Nel paragrafo 7 invece si esporranno le dottrine in vigore in vari importanti Paesi. Si noterà come spesso la dottrina *de facto* sia un prolungamento della politica nazionale estera. In alcuni casi la scelta potrebbe essere corretta, ma in generale le novità introdotte dai principi operativi esposti dovrebbero dissuadere da simili semplificazioni.

4.2 Le dottrine

Esponiamo ora alcune tipologie standard di dottrine (naturalmente sono possibili combinazioni di due o più di esse).

La classificazione adottata, pur non essendo arbitraria, non va considerata fissa. Al momento lo stato dell'arte non consente alcuna strutturazione della materia ed anche il presente documento costituisce soltanto una sistematizzazione provvisoria.

Poiché la priorità è proteggere le infrastrutture ed il pubblico, punto di partenza sarà la scelta di *cosa* proteggere e conseguentemente con quali mezzi e quante risorse. Diamo pure per scontato che: tutti gli asset (aziendali, della PA, di privati, etc etc) provvedano ai dettagli locali della protezione cyber: firewall, crittografia, Intrusion Detection System, antivirus, VPN, etc etc; che sia già in opera la protezione contro i piccoli gruppi hacker; che esistano CERT e centri raccolta dati nazionali. La dottrina si considera quindi in relazione ad interventi di maggiore portata ed entità.

Perimetro singolo

Questa dottrina indica chiaramente una scelta di protezione ad oltranza. E' peraltro ben nota la difficoltà estrema di racchiudere entro un perimetro difensivo tutti gli asset di un qualche valore.

Per esempio, si potrebbe imporre che tutto il traffico Internet sia limitato a strutture collocate fisicamente in Italia o nell'Unione Europea, ma con conseguenti problemi commerciali. Il vantaggio evidente è di limitare i rischi, non dover fare esclusioni inevitabilmente impopolari e di giovarsi delle prerogative psicologiche della difesa.

Gli svantaggi sono numerosi: alti costi, uso di tecnologie molto avanzate (che spingono verso il "paradosso tecnologico"), la quasi certezza di non realizzare quanto ci si era proposti, mancanza di iniziativa, sindrome permanente da linea Maginot (o da firewall, per rimanere in tema). Ancora peggio: ci si potrebbe rendere conto troppo tardi della frantumazione del perimetro a causa della fiducia accumulatasi nel tempo, ma mai testata seriamente in precedenza dagli opponenti. La spiegazione risiede nel fatto che, come osserva un esperto statunitense:

"[. . .] experts have long noted that cyberspace provides an inherently asymmetrical threat that leaves defenders at a tremendous disadvantage. Attackers need only find one vulnerability to exploit, whereas defenders must protect large ungainly systems at every point of entry ".

La scelta ricade su questa dottrina quando mancano riflessioni approfondite, essendo comoda e rassicurante per tutti i soggetti.

Naturalmente il perimetro singolo comporta costi monetari elevati e diffusa vulnerabilità.

Perimetri multipli

Si ripete il concetto prima esposto con la differenza di suddividere gli asset protetti in perimetri difensivi multipli, che vedono come ostile tutto quello che c'è fuori. La caduta di uno non compromette gli altri. Naturalmente si sottointende una gerarchia degli asset da proteggere

Questa opzione non esclude di rispondere con azioni controffensive *ex post*, ma sostanzialmente si ricade nella metodologia "*detect and mitigate*" che risulta essere intrinsecamente instabile.

Si moltiplicano i centri di controllo e la burocrazia relativa, restano le precedenti obiezioni, ma i costi sono più contenuti rispetto al perimetro singolo e l'efficacia elevata.

Difesa di profondità

Si basa sull'irrobustimento a strati concentrici delle difese globali, in modo che le difficoltà per l'attaccante aumentino proseguendo la penetrazione. Quando gli asset non sono numerosi è una buona soluzione, anche se impiega metodologie tipo "*detect and mitigate*".

E' la scelta di chi è conscio di non essere in grado di attuare una protezione perimetrale totale ed essere contemporaneamente oggetto di pesanti minacce e si affida alla elasticità delle proprie strutture per limitare i danni. Prevede azioni di ritorsione.

Svantaggi principali, gli alti costi.

Difesa preventiva e deterrenza

Quando gli asset sono troppo estesi e numerosi ci si basa sulla capacità di restituire eventuali azioni dannose come deterrente o preventivamente, se si gode della superiorità. Dal punto di vista tecnico, stante la difficoltà di attribuire con la dovuta precisione gli attacchi ai responsabili reali, risulta quasi impossibile applicare in toto la deterrenza mentre l'azione preventiva viene ad essere facilitata oltremodo e pericolosamente.

Trattandosi di una strategia offensiva impiegata a scopo difensivo costa poco in termini di risorse, ma incontra difficoltà legali e politiche poiché potrebbe essere considerata come puramente offensiva, come è in realtà. Sebbene i costi monetari non siano eccessivi, sono elevatissimi i rischi di tipo politico, a causa dell'inevitabile escalation conseguente. Tuttavia numerosi Stati non nascondono di adottare l'attacco preventivo addirittura a scopo di deterrenza, riservandosi la decisione di cosa debba considerarsi attacco informatico.

Gli aspetti legali della difesa preventiva sono estremamente problematici e poco si prestano ad una sistematizzazione legislativa.

Approccio indiretto

Nella sua versione offensiva sembra sia la scelta fatta della Cina.

La finalità è di prevalere prima ancora di iniziare un confronto, convincendo l'opponente a non rischiare azioni ulteriori.

Poiché la difesa è difficile e richiede l'impiego di una maggiore quantità di risorse, l'approccio indiretto è una scelta economicamente valida. Inoltre evita di concentrare la maggior parte delle

risorse su una sola costosa pianificazione e di conseguenza non incorre nel paradosso "linea Maginot". Non potendo affidarsi ad una singola infrastruttura si è in qualche modo costretti a riesaminare continuamente problemi e soluzioni, affinando le capacità di apprendimento. G. Pili riassume cosi l'approccio indiretto:

1. vincere l'opponente senza combattere (razionalità globale) e con
2. il minor numero di risorse e il minimo tempo (razionalità strumentale);
3. lo scopo tattico è il controllo di un "cyber-territorio",
4. lo scopo strategico è l'ottenimento dei vantaggi desiderati, non la distruzione delle infrastrutture opponenti (razionalità strategica).

Un esempio banale: per superare uno stateful firewall non necessariamente serve un complicato procedimento software, forse basta entrare da un accesso fisico non protetto e guadagnare l'accesso logico al server direttamente dalla tastiera (la password è sul post-it in alto a sinistra, di solito).

L'approccio indiretto realizza (in teoria) la gestione dei canali a bassa ed alta complessità di cui si è parlato nel paragrafo 3 che assicurano la completa protezione cibernetica nei modelli azione-reazione più avanzati.

Il maggior svantaggio è di non poter proteggere tutti i propri asset direttamente, il che comporta grossi problemi a livello decisionale superiore.

5 Identificazione strategica degli asset critici

Generalmente si è portati a considerare soltanto gli aspetti informatici della protezione cibernetica, sottovalutandone altri. Eppure la sicurezza di un server non si limita ad evitare contaminazioni col malware. Avvicinarsi fisicamente ad esso è senz'altro più redditizio ed economico, come è stato dimostrato nel passato. Un asset critico non è solo un asset importante: una infrastruttura secondaria potrebbe consentire un facile accesso a quelle vitali oppure essere essa stessa fondamentale.

Oggi la protezione fisica in senso lato è considerata un "canale di bassa complessità" e di conseguenza è trascurato nelle pianificazioni. Pertanto questo aspetto della protezione cibernetica va rivalutato ed inserito in un giusto contesto.

5.1 Ruolo strategico della protezione fisica

Come integrare la protezione fisica a livello strategico ? Quali sono i vantaggi e gli svantaggi ? In Italia si lamenta da sempre la mancanza di un piano strategico nazionale in materia di ***"Phisical Security"*** per le c.d. "Infrastrutture sensibili"**,** nel cui ambito andrebbe ricompresa anche la protezione delle "Infrastrutture critiche. Ad oggi, in Italia, vi è un *piano strategico* per quanto riguarda il perimetro della "Cyber Security", la c.d. ***"Logical Security"*** che però, da sola, non basta certamente per una corretta protezione delle Infrastrutture nazionali. Ebbene, detto ciò, si parta da un punto fermo: la sicurezza assoluta non esiste; esiste piuttosto una formula abbastanza accettabile di protezione e sicurezza altamente performante dal punto di vista dei risultati.

La grande maggioranza dei servizi essenziali di un Paese sono regolati e gestiti totalmente con sistemi automatizzati, e alti tassi di informatizzazione. Questo fa comprendere come, ormai, tutto è interdipendente dall'elettronica e dall'informatica; due discipline moderne, due settori (economico-industriale) che vanno strettamente a braccetto, dipendendo intrinsecamente l'uno dall'altro. E dunque, accanto alla sicurezza logica, sta assumendo una valenza strategica in tutti gli Stati dell'unione anche il "perimetro infrastrutturale", oggi generalmente sottovalutato, della sicurezza, della protezione fisica delle installazioni. Ricordiamo sempre che le infrastrutture, specialmente se critiche, garantiscono la disponibilità di beni e servizi vitali come l'approvvigionamento energetico, i trasporti, le telecomunicazioni. Interruzioni su vasta scala avrebbero certamente gravi ripercussioni sulla popolazione e sull'economia, compromettendo la sicurezza e il benessere dello Stato.

Dicevamo degli alti tassi di automazione: con la tecnologia e con la globalizzazione è cresciuta anche l'importanza delle infrastrutture critiche: un blackout generalizzato, ad esempio, nella distribuzione di energia elettrica metterebbe a "terra" l'intera economia del Paese colpito; causerebbe interruzioni (cd effetto domino) anche nell'ambito delle altre infrastrutture interdipendenti (es. telecomunicazioni, approvvigionamento idrico o traffico ferroviario) comportando gravi disagi per la popolazione (mancato funzionamento di illuminazione, sistemi di refrigerazione, riscaldamenti, ascensori).

Peraltro le catastrofi naturali (evento incidentale da non sottovalutare, come quelli antropici), che si manifestano con sempre maggiore frequenza, gli attacchi cibernetici e l'invecchiamento dei sistemi tecnologici hanno fatto sì che negli ultimi anni i rischi per le infrastrutture siano cambiati.

Come già sottolineato, le forti interdipendenze in caso d'evento richiedono, ormai, una netta collaborazione sempre più stretta di tutti gli attori coinvolti. Per questi motivi è più che mai necessario, tramite una corretta strategia nazionale, rafforzare in modo significativo la resilienza "fisica" (capacità di resistenza e di risposta) in relazione alle infrastrutture da salvaguardare dai rischi.

Le migrazioni sistematiche delle multinazionali, verso i paesi emergenti e in via di sviluppo, ha fatto delle aziende mondiali un target di una vasta gamma di minacce. Il numero crescente degli attacchi e delle intrusioni nascoste stanno spingendo le imprese ad adottare un approccio più sofisticato alla sicurezza fisica. Non è più solo la necessità di salvaguardare i propri asset; oggi è garantire la continuità del business sotto il profilo fisico, delle persone, delle informazioni, delle infrastrutture. Questo più ampio perimetro della "security fisica" e l'emergere della consapevolezza che le "infrastrutture IT" sono risorse critiche rendono necessaria una sempre più stretta integrazione tra gli ambiti della sicurezza fisica e una maggiore convergenza tra sicurezza logica e fisica.

Considerato tutto ciò, si pone d'obbligo la domanda: che modello di sicurezza attuare? La tecnologia da sola, evidentemente, non può bastare: deve essere integrata con mirate politiche di "security" generali, che coinvolgano sempre di più pubblico e privato. E' stato ampiamente dimostrato che in diverse situazioni incidentali dovute a attacchi logici, e portati a compimento finale, ebbene la grande maggioranza dei casi era da ricondurre solo a grossolane carenze proprio in ambito della c.d. ***"Phisical Security":*** Ced non presidiati, controlli degli accessi mal progettati e peggio ancora mal gestiti, sistemi di videosorveglianza inefficienti, difese fisiche passive improprie, sistemi antintrusione non progettati alle effettive misure di protezioni necessarie, scarsa vigilanza di polizia privata, errate policy di security.

Argomenti e argomentazioni, questi, affrontati ormai da anni: se ne parla, da sempre, ma senza raggiungere una concreta soluzione; sono anni che si rimandano pericolosamente le decisioni finali da attuare. Per i modelli di sicurezza contemplati nel nostro ordinamento occorre premettere che nel corso degli anni lo Stato ha dovuto misurarsi con la difficoltà sempre crescente di far fronte all'esigenza di tutela della collettività, trovandosi, pertanto, costretto ad ammettere e regolare il concorso degli enti locali e dei soggetti privati in alcune attività (quelle "sussidiarie") volte a garantire la sicurezza dei cittadini.

Tali soggetti, o meglio taluni operatori privati della sicurezza, infatti, hanno reclamato nel tempo ruoli di partecipazione attiva nella costruzione di modelli volti a rafforzare tra i cittadini il sentimento di tranquillità o a placarne le ansie alimentate da una diffusa percezione di insicurezza.

Ciò ha contribuito alla nascita della c.d. sicurezza "integrata", quale strumento attuativo di politiche che vedono integrarsi le competenze esclusive dello Stato in materia di ordine e sicurezza pubblica, con quelle riconducibili agli enti locali ed ai privati operanti sul piano della prevenzione, quali governi territoriali di prossimità.

La sicurezza "sussidiaria" indica l'insieme delle varie attività, poste in essere professionalmente da soggetti privati (singoli od associati), integrative o complementari della sicurezza approntata dalle forze di polizia.

La possibilità per i privati di assumere in sussidiarietà una funzione pubblica, è legata non solo alla natura dell'attività da svolgere, ma soprattutto alla capacità di dar vita ad un sistema adeguato che consenta, nel caso specifico, di contemperare le esigenze della sicurezza con la garanzia dei cittadini. Il termine sussidiarietà è stato scelto al fine di evidenziare il carattere complementare delle attività sopra citate, rispetto alle funzioni di pubblica sicurezza che restano istituzionalmente affidate alle forze di polizia, avendo esse qualifiche correlate a specifici poteri di polizia giudiziaria o di pubblica sicurezza.

Pertanto, poiché oggi la "sicurezza" viene aggettivata nelle più disparate norme come pubblica, integrata, sussidiaria, complementare e partecipata, per evitare il generarsi di una certa confusione e conflittualità, ebbene bisognerebbe che il legislatore assegnasse, senza equivoci, ruoli di partecipazione attivi/passivi precisi per ognuno e non limitarsi a descrivere sommarie istruzioni nelle circolari ministeriali, prive peraltro di efficacia legale.

E dunque per mettere in sicurezza le infrastrutture è giunto il momento che tutti i soggetti pubblici e privati devono concorrere alla produzione di quell'inestimabile bene comune che è la "sicurezza": una security "integrata, partecipata e condivisa", dove lo Stato ed Enti locali, ma soprattutto pubblico e privato, lavorano insieme.

6 Dottrine nei paesi UE e non UE

Osserviamo che mancano riferimenti espliciti alla dottrina nel senso inteso nel nostro documento, perciò è necessario inferire gli aspetti teorici dalle pratiche di cui si ha notizia e dal materiale pubblicato a vario titolo sotto forma di "strategia nazionale". Vantaggi e svantaggi delle varie dottrine sono stati già descritti nel paragrafo 4.

6.1 Paesi UE

Unione Europea

La Commissione UE ha sviluppato numerosi programmi: "i2010 strategy, an information strategy for growth and employment, 2005", “Strategy for a secure information society”, 2006, European Programme for Critical Infrastructures Protection, 2004 to 2007, Programme for crisis prevention, preparation and management in matter of terrorism and other security-related risks (CIPS), 2013.

Esistono poi numerosi attori nel campo informatico:

- Directorates-General from the European Commission (DG Infso, DG Justice, DG Home, DG Entr, DG HR, DG JRC),
- General Secretary of the Council,
- EU External Action Service, Parliament,
- European Data Supervisor, European Network and Information Security Agency (ENISA), European Defence Agency (AED),
- Europol e i “common enterprises” (Galileo and Artemis).

naturalmente l' ENISA (European Network and Information Security Agency) recita la parte principale in qualità di CERT - EU.

In particolare ENISA indica sul suo sito i seguenti documenti [7.8]:

Austria
Austrian Cyber Security Strategy (2013)
Belgium
Belgian Cyber Security Strategy (2014) (Dutch) (available also in French)
Czech Republic
Cyber Security Strategy of Czech Republic for the 2011-2015 Period (2011)
Estonia
Cyber Security Strategy (2008)
Finland
Finland's Cyber Security Strategy (2013)
France
Information systems defence and security, France's strategy (2011)
Italy
National strategic framework for cyberspace security (2013)

Germany
Cyber Security Strategy for Germany (2011)
Hungary
National Cyber Security Strategy (2013)
Latvia
Latvia's Cyber Security Strategy (2014)
Lithuania
Programme for the development of electronic information security (cyber security) for 2011-2019 (2011)
Luxembourg
National strategy on cyber security (2011)
The Netherlands
The national cyber security strategy (2013)
Poland
Cyberspace Protection Policy of the Republic of Poland (2013)
Romania
Cyber Security Strategy in Romania (2011)
Slovak Republic
National Strategy for Information security in the Slovak Republic (2008)
Spain
The National Security Strategy (2013)
United Kingdom
Cyber Security Strategy of the United Kingdom (2011).

Una analisi similare è contenuta anche in [7.9], a firma di una agenzia indipendente di Washington.

Infine, il *Joint Communication* [1.2] dell' Alto Rappresentante Ashton (2013) sulla cybersecurity nell'UE è forse il più recente documento ufficiale emesso dalla Commissione. Purtroppo non è possibile, data la varietà di interessi in gioco e la complessità delle relazioni nella UE, parlare, neanche genericamente, di una dottrina comune UE.

Di seguito comunque analizzeremo alcuni dei maggiori paesi europei che si avvicinano maggiormente alla elaborazione di una dottrina.

Francia

La Francia riconosce come parte della propria sovranità lo spazio cibernetico [7.6]. Le responsabilità sono chiaramente indicate:

"According to the Constitution, the Prime Minister is responsible for national defence. Under his direct authority, a Secretary General for Defence and National Security (SGDSN6) organises and coordinates all the ministries' policies relevant to this field."

L' ANSSI è l'autorità nazionale francese per la protezione dei sistemi informatici, con giurisdizione sul settore pubblico e privato ed ha dotato la nazione di quattro obiettivi:

- sovranità informatica
- indipendenza strategica informatica
- produzione interna dei prodotti attinenti l'informatica

- obbligo per gli attori pubblici e privati di collaborare alla sicurezza e resilienza delle IC.

Per ora manca una autentica consapevolezza della necessità di elaborare una risposta organica alle contingenze. Sembrerebbe tuttavia che la Francia si stia dirigendo verso una **dottrina di difesa di profondità**, probabilmente in conseguenza di incidenti che hanno compromesso importanti IC di recente [7.6].

UK

Il Regno Unito d'Ighilterra ha lanciato nel 2011 un programma di protezione cyber da 800 milioni di euro a fronte di un costo dei danni prodotti da ciber-attacchi stimato in 34 miliardi di euro. Un professore dell' Istituto di sicurezza e resilienza dell' University College di Londra ed ex ministro dell'Interno, J. Reid, coautore del rapporto [7.7] ha affermato alcuni anni fà:

"We desperately need a doctrine, a set of agile policies that shape the way we approach the challenges. If we get that, we will maximise the opportunities and minimise the dangers but we will never have complete security and control."

In effetti il rapporto intitolato *Cyber Doctrine* [7.7] sembra voler colmare il gap e nella prefazione dichiara:

"The proposed Doctrine is founded on the recognition that resilience is competitiveness. It should be synonymous with entrepreneurship. At its centre is the vital principle of the easy integration of competent authorities and capabilities with the capacity to manage and innovate "

per cui una parte preminente è singolarmente assegnata all'aspetto commerciale piuttosto che a quello proprio della protezione vera e propria.

Poiché comunque gli autori dichiarano la coincidenza fra "dottrina" e "resilienza" e ne suggeriscono l'adozione come dottrina ufficiale per il Regno Unito, ci pare di poter concludere che questi studiosi suggeriscano una dottrina elastica a metà fra la difesa di profondità e quella a perimetri multipli. Tuttavia le attività di ricerca delle informazioni che UK pratica estesamente a 360° suggeriscono invece la pratica **di una dottrina di difesa preventiva.**

Germania

In Germania il centro di Ciberdifesa Nazionale accorpa le maggiori responsabilità. La dottrina prevede l'assenza di attività offensive, il rafforzamento delle infrastrutture ed investimenti nella ricerca. Le risorse impiegate al momento della stesura del documento [7.9] da cui sono tratte queste informazioni (2011) sembrano essere estremamente scarse. Data la crisi di sicurezza del 2014, è da prevedere una radicale modifica di queste impostazioni.

Si configura chiaramente il caso di una **dottrina di perimetro singolo**.

6.2 Paesi non UE

USA

Iniziamo con gli USA, che rivestono una importanza particolare per l'avanzamento tecnologico all'avanguardia. La dottrina USA prevede di difendere le infrastrutture critiche ed informatiche in particolare, riservandosi il diritto di azioni cibernetiche preventive o ritorsive e destinando allo scopo diversi miliardi di dollari all'anno (ulteriori dettagli non sono noti). La deterrenza sembra essere la principale risorsa difensiva della dottrina *de facto* USA. Si noti la netta differenza con l'approccio cinese, che non sembra ritenere efficaci le minacce di ritorsione, e la costante ricerca della superiorità tecnologica in ogni circostanza [7.3]:

"While it is possible military outcomes can be determined by cyber operations alone, CyberOps are not generally an end to themselves [...].
It is focused on winning the cyber-electromagnetic contest through three concurrent lines of effort: gaining advantage, protecting that advantage, and placing adversaries at a disadvantage. Commanders conduct CyberOps to retain freedom of action in cyberspace, while at a time and place of their choosing, denying freedom of action to adversaries, thereby enabling other operational activities.
These lines of effort to prevail in the cyber-electromagnetic contest nest with and contribute to the joint force's construct of cyberspace superiority. CyberOps leverages cyberspace [...] throughout all the domains" .

La dichiarazione seguente di un importante funzionario USA chiarisce come la gestione in piena sicurezza non sia considerata impossibile, anzi:

“We’re never going to get rid of 100 percent; so when I say solvable, what I mean is we can mitigate most of the problems that we’re seeing on the network today. The cyber threat is not going away, but it is something that if we organize ourselves well, implement needed defenses and standards on both the public and private side, and, most of all, just keep our heads about us, then it is quite manageable” (K. Alexander, [7.2]).

Non mancano tuttavia le difficoltà; secondo S. Mele [7.1], infatti:

" Occorre evidenziare come la rapida evoluzione del pensiero strategico americano in materia di cyber-security, abbia fatto sì che nell’ultimo decennio si siano

- La difficoltà per le Agenzie federali di effettuare una corretta valutazione dei rischi derivanti dal cyber-spazio attraverso lo sviluppo e l’implementazione dei principi **e** delle direttive in materia di *cyber-security* impartite dal governo centrale.

- La difficoltà da parte delle Agenzie deputate alla protezione delle infrastrutture critiche di comprendere correttamente quali siano le norme e i regolamenti in materia di cyber-security da applicare al loro specifico settore (criticità a cui Obama ha provato a dare una risposta attraverso il recente *Presidential Executive Order on Improving Critical Infrastructure Cybersecurity*)

- La persistente difficoltà di rilevare, contrastare e mitigare gli attacchi informatici, soprattutto a causa della mancanza in seno al *Department of Homeland Security (DHS)* di un efficace sistema di analisi predittiva delle minacce derivanti dal cyber-spazio e di un sistema centrale per la condivisione delle informazioni tra settore pubblico/governativo e i principali attori privati."

Tali osservazioni attestano chiaramente delle incongruenze di fondo, mai chiarite, quantomeno a livello ufficiale, nella dottrina USA [7.3].

Riassumendo**:** le attuali indicazioni delle istituzioni USA richiedono una totale difesa del perimetro, peraltro ancora da definire compiutamente**, basata sulla costante supremazia tecnologica da mantenere ed estendere.** Si conta sulla **deterrenza** per dissuadere dal porre in essere attacchi di **vasta portata** e sulla incentivazione di politiche di ***resilience*** per ridurre il danno eventuale. Pertanto la dottrina *de facto* USA è quella del **perimetro singolo** insieme **ad azioni preventive e dissuasive**.

Cina

Una trattazione teorica ufficiosa è disponibile in [7.4]. La base della dottrina cibernetica cinese desumibile da tale documento, che comunque *non* riveste carattere ufficiale, è che i targets *non* sono quelli comunemente considerati di massima importanza in quanto è molto probabile siano opportunamente protetti. Perciò le scarse *risorse disponibili devono essere dirette altrove, ottenendo il conseguimento degli scopi prefissati ad un minore costo*. Per esempio, una azione con risvolti psicologici potrebbe essere più efficiente di una distruttiva azione hacker contro una infrastruttura industriale.

Inoltre i funzionari cinesi sembrano sostenere la necessità di inserire informalmente le metodologie cibernetiche in un contesto di per se militare ma non ad esso subordinato, in quanto le azioni hacker oggi sono tollerabili dal punto di vista politico e non c'è una restrizione di principio o pratica, se non quella dell'anonimato ufficiale.

Cade quindi la separazione tra l'aspetto militare e l'azione di influenza diplomatica, anzi l'opzione militare tradizionale è considerata ormai largamente obsoleta. Gli scenari futuribili sono quindi profondamente diversi da quelli immaginati nella pianificazione attuale della protezione delle IC in UE e USA.

In sintesi, da [7.4] abbiamo i seguenti principi generali:

- Omnidirectionality -- 360 degree Observation and Design, Combined Use of All Related Factors
- Synchrony -- Conducting Actions in Different Spaces within the Same Period of Time
- Limited Objectives -- Set a Compass to Guide Action within an Acceptable Range for the Measures

- Unlimited Measures -- The Trend is Toward Unrestricted Employment of Measures, but Restricted to the Accomplishment of Limited Objectives

- Asymmetry -- Seek Nodes of Action in the Opposite Direction from the Contours of the Balance of Symmetry

- Minimal Consumption -- Use the Least Amount of Combat Resources Sufficient to Accomplish the Objective

- Multidimensional Coordination -- Coordinating and Allocating All the Forces which can be Mobilized in the Military and Non-Military Spheres

- Multidimensional Coordination -- Coordinating and Allocating All the Forces which can be Mobilized in the Military and Non-Military Spheres

Nell'articolo [7.5] G. Kanwal, un analista indiano, riassume la dottrina cinese con queste parole:

"Underpinning the new professionalism of the PLA is the basic doctrine of 'active defence' (jiji fangyu) that seeks to conduct 'people's war under modern conditions' (better understood as 'local wars under hi-tech conditions'—gaojishu tiaojian xia de jubu zhanzheng)."

In quanto sopra si ravvisa chiaramente la completa struttura **dell'approccio indiretto.**

Russia

La Russia ha sviluppato un approccio prevalentemente militare alle questioni della sicurezza informatica, sostituendo i mezzi classici con attacchi cibernetici allo scopo di ottenere fini politici. I mezzi impiegati sono stati molto vasti e lasciano intendere una struttura estesa e ben addestrata alle spalle.

La produzione di documenti ufficiali è minima, per cui le inferenze sono ottenute da azioni monitorate dalla UE. Infatti, in diverse occasioni la Federazione russa è stata accusata di operazioni cibernetiche aggressive nei confronti dei vicini. Ufficialmente la dottrina contempla delle strategie di controllo, prevenzione, soluzione delle crisi esposta nel documento *Conceptual Views Regarding the Activity of the Armed Forces of the Russian Federation in the Information Space* (2011) ove non si discutono le strategie preventive delle crisi.

Nondimeno, la dottrina *de facto* appare essere quella della **difesa preventiva e deterrenza.**

Paese	PERIMETRO SINGOLO	PERIMETRO MULTIPLO	DIFESA PREVENTIVA, DETERRENZA	DIFESA DI PROFONDITA	APPROCCIO INDIRETTO
UE					
Francia					
Germania					
Estonia					
Finlandia					
RegnoUnito					
USA					
Cina					
Russia					
India					
Canada					
Giappone					
Corea Sud					

Tavola 4. Alcune delle dottrine in vigore.

Nella Tavola 4 si è sintetizzata graficamente la situazione nei maggiori Paesi interessati ai problemi della protezione cibernetica. Come si nota facilmente, la maggior parte dei Paesi si è orientata verso il perimetro singolo o multiplo e/o verso la deterrenza.

7 Raccomandazioni

7.1 Provvedimenti generali

La responsabilità delle azioni di protezione cibernetica e delle risorse deve essere assegnata ad un unico soggetto, l'Autorità nazionale.

Sarebbe *auspicabile* che le imprese private, abilitate da apposito regolamento, siano controllate a tutti i livelli da cittadini italiani residenti in Italia e proprietari al 100% .

Tutte le azioni suggerite nel presente documento, pur avendo un orizzonte temporale ampio godrebbero di maggior efficacia se realizzate come *crash program*, ossia entro cinque anni al massimo.

Il quadro legislativo dovrà essere ridotto per evitare il tipico proliferare di circolari e specifiche, lasciando alla Autorità la maggior libertà di azione, come indicato nel paragrafo che la riguarda.

Istituzione di un data-base obbligatorio nazionale delle azioni deliberate e degli incidenti cibernetici

Inserimento nella Costituzione del concetto di sovranità nazionale dello spazio cibernetico.

7.2 Provvedimenti strategici e tecnici

Far si che le informazioni vitali, i dati, etc. etc. europei circolanti sulla rete Internet circolino solo sul territorio europeo su server fisicamente collocati nella UE e non come accade attualmente, rimbalzando su più punti in tutto il globo terreste,

Per una maggioranza molto rilevante, i sistemi operativi, risultano non essere Italiani, con le problematiche che si possono immaginare, dalla non proprietà degli stessi, sino ad arrivare a situazioni in cui i sistemi sono completamente chiusi, rendendo impossibile fare una analisi del reale contenuto. Quindi è necessario produrre SO italiani e relative applicazioni.

Utilizzo esclusivo di server per email e social networks residenti sul suolo nazionale.

Utilizzo massivo di sistemi crittografici basati su algoritmi nazionali, sia per quanto concerne la parte delle mail, che per quanto concerne la protezione dei dati contenuti al interno dei server/storage stessi.

Istituzione di un sistema nazionale alternativo di cyber-comunicazione protetto dalle interferenze elettromagnetiche.

Adozione dell'approccio indiretto come dottrina di protezione cibernetica nazionale.

Monitoraggio continuo tramite mezzi fisici e previsionali di tutte le attività cibernetiche.

Impiego delle tecniche matematiche delle reti complesse nella gestione del cyberspazio.

Corsi di formazione per programmi open source di crittografia forte gratuiti.

Tutela dei device fissi o mobili, in caso gli stessi vengano compromessi da eventuali infezioni di malware.

Nei SC ricercare ove possibile l'assenza di canali di bassa complessità (attacchi banali) e la non-stazionarietà dei canali ad alta complessità.

Analisi appropriata della sicurezza fisica nelle infrastrutture indispensabile per la sicurezza logica delle IC e la corretta pianificazione della continuità operativa.

7.3 Provvedimenti organizzativi

Assicurare la massima priorità a massicci investimenti nel settore informatico, anche a scapito di altri programmi di investimento di simile impegno finanziario in corso o preventivati.

Elaborazione di una giurisdizione cibernetica concernente gli Enti nazionali e le relazioni internazionali.

8 Riferimenti

8.1 Riferimenti nel documento

[1.1] Presidenza del Consiglio dei Ministri, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf., (2013)

[1.2] High representative of the EU for foreign affairs and security policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, EU Commission, (2013).

[1.3] Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate della PCdM, *Protezione delle infrastrutture critiche informatizzate: la realtà Italiana,* (2004) http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=2832

[2.1] Presidenza del consiglio dei Ministri, *Quadro strategico nazionale*, https://www.google.it/#q=+Quadro+Strategico+Nazionale+ed+il+Piano+Nazionale+Protezione+Cibernetica+della+Presidenza+Consiglio+Ministri, (2013).

[3.1] D. Delavy et al, *Mathematical Challenge in Cybersecurity*, Sandia Labs Reports, (2009).

[3.2] A. Arbore and E. Fioriti, *Suboptimal topological protection from advanced malware*, CRITS 2011, Luzern, (2011).

[3.3] M. Adams, T. Clancy et al., rXiv:1311.0257v1 [cs.CR], (2013).

[3.4] Star Trek Next Generation, *L'attacco dei Borg*, (1997).

[4.1] European Commission: Communication on Critical Information Infrastructure protection (CIIP); 30.3.2009 European Commission *Communication on CIIP on "Achievements and next steps: towards global cyber-security*"; 31.3.2011.

[4.2] DPCM 24 gennaio 2013 - *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*.

[4.3] Presidenza del Consiglio dei Ministri - *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico* -Dicembre 2013.

[4.4]http://books.google.it/books?id=wligOmsgQEIC&pg=PA107&lpg=PA107&dq=sistema+cibernetico&source=bl&ots=qOTmk8_B4U&sig=HAiKnBO_tiTrF_IpZrQctV8h6jw&hl=it&sa=X&ei=0bo4VPziN4HfOITUgNgB&sqi=2&ved=0CF8Q6AEwCw#v=onepage&q=sistema%20cibernetico&f=false

[7.1] S. Mele, http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html, (2003).

[7.2] Defense News, http://www.defensenews.com/article/20121013/DEFREG02/310130001/DoD-8217-s-New-Cyber-Doctrine

[7.3] TRADOC manual Pam 525-7-8, (2010)

[7.4] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, (1999).

[7.5] G. Kanwal, *China's Emerging Cyber War Doctrine*, Journal of Defence Studies, (2010).

[7.6] P. Tromparent, *Franch cyberdefence policy*, Int. Conf. NATO Tallin 2012, (2012).

[7.7] J. P. Mac Intosh et al, *Cyber doctrine*, Institute for security studies, London, (2011).

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

[7.9] S. Deitz et al., *Cybersecurity*, CSIS (2011).

[7.10] http://www.bankinfosecurity.com/cyber-priorities-unveiled-in-fy-2015-budget-a-6600/op-1

8.2 Bibliografia generale

Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models Intelligence and National Security Alliance, 2009

Applicability of the Additional Protocols to Computer Network Attacks Knut Dormann International Committee of the Red Cross (ICRC), 2004

Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats James A. Lewis CSIS, 2003

Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks Jason Healey Cyber Conflict Studies Association, 2010

In the Crossfire: Critical Infrastructure in the Age of Cyber War McAfee and CSIS, 2010 Cyberdeterrence and Cyberwar Martin C. Libicki RAND, October 2009

Thresholds for Cyberwar James A. Lewis CSIS, October 2010

Cyberpower and National Security Franklin D. Kramer, Stuart H. Starr, Larry Wentz (eds.) National Defense University, 2009

Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks Paul Cornish , Chatham House, 2009

Cybersecurity and National Policy Dan Geer ,Harvard National Security Journal, 2010 Cyber Security and the Intelligence Community

Eric Rosenbach and Aki J. Peritz ,Belfer Center for Science and International Affairs, 2009

Cyber War: The Next Threat to National Security and What to Do About It Richard A. Clarke and Robert Knake New York: HarperCollins, 2010

Defending a New Domain William J. Lynn III Foreign Affairs, Sept / Oct 2010

Defending Against Cyber Terrorism: Preserving the Legitimate Economy Olivia Bosch, Alyson J.K. Bailes and Isabel Frommelt (eds.) Business and Security: Public–Private Sector Relationships in a New Security Environment. SIPRI and Oxford University Press, 2004. 187-196.

Freedom on the Net: A Global Assessment of Internet and Digital Media Freedom House, 2009

The Future of the Constitution: The Cyberthreat, Government Network Operations, and the Fourth Amendment Jack Goldsmith The Brookings Institution, 2010

Google Confronts China's "Three Warfares" Timothy Thomas Parameters, Summer 2010. 101-113.

A Human Capital Crisis in Cybersecurity Karen Evans and Franklin Reeder CSIS Commission on Cybersecurity for the 44th Presidency, November 2010

International Cyber Incidents: Legal Considerations Eneken Tikk, Kadri Kaska, Liis Vihul NATO Cooperative Cyber Defence Centre of Excellence, 2010

Internet Governance in an Age of Cyber Insecurity Robert K. Knake Council on Foreign Relations, 2010

An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies Isabelle Abele-Wigert and Myriam Dunn International CIIP Handbook 2006, Vol. 1, Center for Security Studies, ETH Zurich

The "Korean" Cyber Attacks and Their Implications for Cyber Conflict James A. Lewis CSIS, October 2009

Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008 U.S. Cyber Consequences Unit, 2009

Plan for Enhancing Internet Security, Stability, and Resiliency Internet Corporation for Assigned Names and Numbers (ICANN), 2009

Project Grey Goose Phase 1: Russia/Georgia Cyber War – Findings and Analysis Phase II: The Evolving State of Cyber Warfare Greylogic, 2008-2009

Russia and the Cyber Threat Kara Flook Critical Threats, 13 May 2009

Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency CSIS, 2008

Shadows in the Cloud: Investigating Cyber Espionage 2.0 Joint Report: Information Warfare Monitor and Shadowserver Foundation, 2010

Strategic Advantage: Why America Should Care About Cybersecurity Melissa E. Hathaway Belfer Center for Science and International Affairs, October 2009

Surviving Cyberwar Richard Stiennon Government Institutes, 2010

Targeting Information Infrastructures Ian Dudgeon and Gary Waters (eds.) Australia and cyber-warfare. Australian National University, 2008. 59-84.

Tracking Ghostnet: Investigating a Cyber Espionage Network Ron Diebert and Rafal Rohozinski Information Warfare Monitor, 2009

Unrestricted Warfare, Qiao Liang and Wang Xiangsui PLA Literature and Arts Publishing House, 1999

Virtual Criminology Report 2009 – Virtually Here: The Age of Cyber Warfare McAfee and Good Harbor Consulting, LLC, 2009

Government Publications and Policy Documents

An Assessment of International Legal Issues in Information Operations Office of General Counsel, May 1999

Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress Congressional Research Service, 2008

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation U.S.-China Economic and Security Review Commission, 2009

Cornerstones of Information Warfare US Air Force, 1997

Critical Foundations: Protecting America's Infrastructures Report of the President's Commission on Critical Infrastructure Protection, 1997

Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities Government Accountability Office, 2008

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed Government Accountability Office, July 2010

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience Government Accountability Office, July 2010

Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats Government Accountability Office, 2007

Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats Government Accountability Office, 2010

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative Government Accountability Office, 2010

Cyber Security Strategy Cyber Security Strategy Committee Estonian Ministry of Defense, 2008

Cyber Security Strategy for Germany German Federal Ministry of the Interior, 2011

Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space UK Office of Cyber Security, 2009

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance Government Accountability Office, 2010

Cyberspace Policy: Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership is Needed Government Accountability Office, 2010

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure The White House, 2009

Economics of Malware: Security Decisions, Incentives and Externalities Directorate for Science, Technology, and Industry Organisation for Economic Co-operation and Development (OECD), 2008

French Strategy for the Defense and Security of IT Systems (French) French Republic, February 2011

Governing the Internet: Freedom and Regulation in the OSCE Region Organization for Security and Co-operation in Europe (OSCE), 2007

Information Security Doctrine of the Russian Federation: Approved by President Vladimir Putin on September 9, 2000 Russian Federation, 2000

The IT Security Situation in Germany in 2009 Federal Office for Information Security, 2009 The IT Security Situation in Germany in 2011 Federal Office for Information Security, 2011

ITU Global Cybersecurity Agenda: High-Level Experts Group Chairman's Report International Telecommunication Union, 2008

ITU Study on the Financial Aspects of Network Security: Malware and Spam ICT Applications and Cybersecurity Division, International Telecommunication Union, 2008

Japanese Information Security Status: Environment and Policies IT Security Center Information-technology Promotion Agency

National Cybersecurity Strategy The Netherlands, 2011

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture Government Accountability Office, 2009

The National Military Strategy for Cyberspace Operations The US Joint Chiefs of Staff, 2006

National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy (Draft) The White House, 2010

NATO and Cyber Defence NATO Parliamentary Assembly, North Atlantic Treaty Organization, 2009

Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy Committee on Deterring Cyberattacks National Research Council, 2010

Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security, and Resilience European Commission, 2009

Reducing Systemic Cybersecurity Risk OECD/IFP Project on “Future Global Price Shocks”

Organisation for Economic Co-operation and Development (OECD), 2011

The Second National Strategy on Information Security: Aiming for Strong "Individual" and “Society” in IT Age National Information Security Policy Council, 2009

Security Issues and Recommendations for Online Social Networks European Network and Information Security Agency (ENISA), 2007

Technology Policy Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities Committee on Offensive Information Warfare, National Research Council, 2009