Il Futuro della Cyber Security in Italia

Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni

Laboratorio Nazionale di Cyber Security
Consorzio Interuniversitario Nazionale per l'Informatica

Ottobre 2015

A cura di:

Roberto Baldoni, Università degli Studi di Roma "La Sapienza"
Rocco De Nicola, IMT, Institute for Advanced Studies, Lucca

Il volume è stato realizzato da:

con il supporto del
Dipartimento delle Informazioni per la Sicurezza
della Presidenza del Consiglio dei Ministri

ISBN 9788894137309

Titolo: Il Futuro della Cyber Security in Italia

Stampato in Italia, Ottobre 2015

A cura di: Roberto Baldoni e Rocco De Nicola

Autori in ordine alfabetico:

Luca Allodi
Alessandro Armando
Roberto Baldoni
Antonio Barili
Sandro Bologna
Matteo E. Bonfanti
Silvia Bonomi
Francesco Buccafurri
Enrico Cambiaso
Costantina Caruso
Michele Colajanni
Luigi Coppolino
Fabrizio d'Amore
Salvatore D'Antonio
Sabrina De Capitani di Vimercati
Rocco De Nicola
Carolina De Stefano
Tommaso De Zan
Federica Di Camillo
Giorgio Di Natale
Andrea Di Nicola
Andrea Dimitri
Gianluca Dini
Riccardo Focardi
Giuseppe F. Italiano
Giovanni Lagorio
Antonio Lioy
Michele Loreti
Federico Maggi
Marco Mayer
Alberto Marchetti Spaccamela
Luigi Martino
Fabio Massacci
Massimo Mecella
Luca Montanari
Gian Domenico Mosco
Ida Panetta
Vincenzo Piuri
Paolo Prinetto
Luigi Romano
Pierangela Samarati
Donatella Sciuto
Fabio Scotti
Stefano Silvestri
Maurizio Talamo
Alberto Trombetta
Fiamma Terenghi
Aaron Visaggio
Stefano Zanero

Prefazione

Internet sta rivoluzionando la nostra società e la nostra economia, favorendo l'interazione, lo scambio di idee, la condivisione delle informazioni, creando nuove modalità di coinvolgimento politico e sociale e di scambio economico e commerciale. *Spazio cibernetico* (*Cyberspace*) è il termine convenzionalmente usato per riferirsi all'ambiente all'interno del quale avvengono le operazioni che fanno uso di Internet. La riduzione dei costi di accesso alla rete e lo sviluppo della banda larga comporteranno un'ulteriore crescita del cyberspace, rendendolo un fattore sempre più cruciale per la crescita economica e sociale.

L'aumento della dipendenza dal cyberspace, da un lato offre nuove opportunità, dall'altro introduce nuove minacce. Il cyberspace rende possibili mercati nazionali e transnazionali più aperti; tale apertura rende però i sistemi informatici su cui esso si basa più vulnerabili agli attacchi di quanti (criminali, hacker, terroristi) intendono comprometterli, danneggiarli o sfruttarli per ottenere, in modo fraudolento, informazioni personali o commerciali. Va anche considerato che questi eventi malevoli possono accadere in modo quasi istantaneo a livello planetario e avere origini in luoghi fisicamente lontani o comunque esterni alle organizzazioni colpite; reati come la frode e il furto di segreti industriali oggi possono essere commessi a distanza e su larga scala in pochi secondi.

Quanto appena detto fa capire che sviluppare nuove capacità e nuovi strumenti per migliorare la sicurezza cyber del sistema Paese rappresenta una sfida nazionale della massima importanza per la crescita e per il benessere e la sicurezza dei cittadini. La correlazione tra prosperità economica di una nazione e la qualità delle sue infrastrutture cyber sarà sempre più stretta e un paese, per stare nel gruppo delle nazioni più sviluppate, dovrà migliorare la sicurezza cyber nella società, nel sistema industriale e nella pubblica amministrazione.

Il miglioramento delle difese del cyberspace sarà pertanto uno dei requisiti che guiderà gli investimenti da parte di operatori internazionali, i quali non sono interessati a insediamenti industriali in assenza di un'adeguata organizzazione e capacità difensiva cyber. Ma tale miglioramento contribuirà anche ad assicurare una maggiore protezione della privacy dei cittadini e delle infrastrutture critiche che sempre più dipendono da strumenti informatici. Proprio per questa ragione, molti paesi avanzati stanno progettando e realizzando piani strategici nazionali che coinvolgono pubblico, privato e ricerca e puntano a rafforzare la difesa delle infrastrutture critiche nazionali, delle organizzazioni governative, delle aziende e dei singoli cittadini dagli attacchi cibernetici.

A partire da queste considerazioni, il *Laboratorio Nazionale di Cyber Security* del CINI (Consorzio Interuniversitario Nazionale per l'Informatica) ha coinvolto numerosi esperti accademici per la redazione di un documento che, a due anni dalla pubblicazione del *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico*, mira a evidenziare le sfide che l'Italia dovrà affrontare nei prossimi anni per aumentare, a tutti i livelli, la consapevolezza della minaccia cyber e le capacità difensive del nostro Paese. Le sfide proposte sono poi accompagnate da una serie di raccomandazioni agli organi preposti per rispondere ad esse in modo adeguato, migliorando nel contempo la politica digitale del paese.

Nel volume, il capitolo 1 fornisce una breve introduzione alle problematiche di sicurezza, mentre nel capitolo 2 vengono analizzati l'evoluzione del cyber crime, gli scenari di alcuni stati e la situazione italiana, con particolare attenzione al panorama normativo in materia di cyber security. I capitoli 3 e 4 contengono rispettivamente le sfide e le raccomandazioni. L'Appendice presenta una panoramica delle politiche di cyber security adottate da alcuni stati nazionali.

In conclusione, ringraziamo tutti i colleghi che hanno contribuito a questo libro bianco: un gruppo unico per numerosità, eccellenza e multidisciplinarità, che rappresenta il meglio della ricerca in Italia nel settore della cyber security. Un grazie speciale va ad Alberto Marchetti-Spaccamela e a Paolo Prinetto, che hanno contribuito alla revisione finale del manoscritto. Tra i ringraziamenti dobbiamo aggiungere anche il supporto ottenuto dai membri dei progetti TENACE e CINA, finanziati dal MIUR. In ultimo, diciamo che il nostro lavoro editoriale ha comportato la rielaborazione di parte dei testi che i colleghi ci hanno fornito, questa rielaborazione potrebbe aver travisato in parte il loro messaggio o ignorato qualche aspetto importante, ce ne scusiamo in anticipo.

Lucca, Ottobre 2015

Roberto Baldoni
Rocco De Nicola

Indice

CAPITOLO

1 Introduzione

Internet sta rivoluzionando la nostra società e la nostra economia, favorendo l'interazione, lo scambio di idee, la condivisione delle informazioni, e creando nuove modalità di coinvolgimento politico e sociale e di scambio economico e commerciale. *Spazio cibernetico* (*Cyberspace*) è il termine convenzionalmente usato per riferirsi all'ambiente all'interno del quale avvengono le operazioni che fanno uso di Internet. La riduzione dei costi di accesso alla rete e lo sviluppo della banda larga comporteranno un'ulteriore crescita del cyberspace, rendendolo un fattore sempre più cruciale per la crescita economica e sociale.

Tuttavia l'adozione del cyberspace porta con sé problemi di vulnerabilità delle applicazioni e dei sistemi informatici, dovute anche al fatto che la stragrande maggioranza delle reti e dei sistemi che formano il cyberspace sono stati progettati e realizzati pensando a criteri di usabilità e al più di resilienza, senza tenere in debito conto fin dall'inizio aspetti di sicurezza.

Queste vulnerabilità sono sempre più utilizzate da singoli e da gruppi a fini criminali per ottenere guadagni illeciti. A questo scopo vengono ad esempio sottratte, a imprese e organizzazioni, informazioni riservate, quali elenco clienti, brevetti o asset strategici. La cronaca recente evidenzia che attacchi di questo tipo sono stati condotti in molti stati. Proprio per questa ragione, molti paesi stanno progettando e realizzando piani strategici nazionali che coinvolgono pubblico, privato e ricerca. Questi prevedono non solo la messa a punto di adeguate misure di contrasto ai crimini cibernetici, ma anche azioni di sensibilizzazione e di coordinamento. Lo scopo finale è arrivare, in breve tempo, all'innalzamento delle difese delle infrastrutture critiche nazionali, delle organizzazioni governative, delle aziende e dei singoli cittadini.

L'implementazione di un piano strategico è un processo molto complesso che richiede una relazione stretta tra pubblico, privato e mondo della ricerca. Se si considerano, a titolo di esempio, le infrastrutture critiche nazionali (reti elettriche, idriche, informatiche, ...), si vede che esse sono gestite da soggetti privati, pur essendo pubbliche, e necessitano delle competenze avanzate dei ricercatori per poter fronteggiare in modo adeguato minacce sempre più complesse e sofisticate.

Tutti i soggetti coinvolti devono essere consapevoli della minaccia e, per quanto di propria competenza, migliorare i propri livelli di protezione. Anche un soggetto apparentemente marginale all'interno di un'organizzazione e non dotato di adeguate protezioni di sicurezza, può essere utilizzato come base per portare attacchi al cuore dell'organizzazione stessa. A sua volta, un'organizzazione "compromessa" può mettere a repentaglio organizzazioni a essa collegate che, seppur dotate di difese evolute, condividono informazioni grazie alla reciproca fiducia di relazione commerciale.

In un sistema economico globale nel quale le informazioni hanno un valore essenziale, la sicurezza delle reti è diventata una delle sfide più serie per l'economia. Questa consapevolezza è emersa in tutta la sua drammaticità nel 2007, quando in Estonia una serie di attacchi cibernetici ha rischiato di abbattere l'intera infrastruttura informatica del Paese [73]. Come ha rilevato il presidente Obama nel 2009 [57], l'interdipendenza tra i sistemi informatici delle economie mondiali che utilizzano la stessa infrastruttura di base, gli stessi software, hardware e standard, con miliardi di dispositivi connessi, è alla base del carattere di universalità del *cyber crime* e lo rendono un fenomeno del quale è impossibile prevedere con esattezza le conseguenze nel medio-lungo termine. La vera differenza tra il *cyber crime* e la criminalità tradizionale non risiede tanto nella tipologia di aggressioni che li caratterizza, quanto nella circostanza che le violazioni perpetrate tramite il *cyber space* sono di fatto prive di confini fisici e di limiti geografici; spesso il crimine informatico è dunque più conveniente, anche per via della mancanza della sua percezione fisica da parte della vittima.

Non può quindi stupire il progressivo incremento, quantitativo e qualitativo, di attacchi e minacce criminali con le finalità più disparate, in quella "terra di mezzo" che è oramai diventato il cyberspace: dalle frodi e dalle estorsioni informatiche ai furti di identità e di dati sensibili, fino ad arrivare allo spionaggio e al sabotaggio, compresi gli atti vandalici meramente emulativi. Attacchi che possono anche non essere mirati a colpire un soggetto preciso, selezionato in base a determinate caratteristiche, ma a danneggiare in modo casuale un numero indefinito di soggetti sensibili alla minaccia predisposta dal criminale. Non bastano singole misure protettive. Occorre mettere in atto vere e proprie strategie difensive in mancanza delle quali, secondo il Report Global risks 2014 del World Economic Forum [29], nel 2020 le perdite economiche causate da attacchi cyber potrebbero arrivare fino a tremila miliardi di dollari.

Sotto il profilo delle vittime potenziali, un rilievo particolare hanno le istituzioni pubbliche di ogni dimensione e le imprese multinazionali, già più volte oggetto di crimini informatici dai quali sono derivati danni ingenti. Tuttavia, anche le imprese di piccole e medie dimensioni, che costituiscono il fulcro del tessuto economico italiano, sono un potenziale bersaglio di attacchi informatici, sia casuali sia mirati. Le imprese di piccole e medie dimensioni appaiono anzi le più vulnerabili e per loro le conseguenze negative sono in proporzione ancora maggiori, a causa delle ridotte risorse organizzative ed economiche delle quali dispongono. Il dato dimensionale accentua l'asimmetria informativa della vittima rispetto all'attaccante, in quanto l'impresa di dimensioni minori deve sopportare costi più rilevanti per dotarsi di un sistema di protezione e ha maggiori difficoltà a reagire ai danni, economici e reputazionali, causati da una violazione informatica. È quindi indispensabile che gli interventi di *regulation* volti a tutelare le vittime degli attacchi informatici tengano conto delle diverse caratteristiche dei destinatari. Altrettanto importante è che le imprese minori siano concretamente incoraggiate a incrementare la cultura della sicurezza, che stentano ancora a fare propria. La *cyber security* costituisce, del resto, una componente essenziale del "valore" che l'impresa è istituzionalmente chiamata a generare per i propri *stakeholders*, nei confronti dei quali l'impresa ha precisi obblighi di protezione.

L'assenza di una politica digitale in un Paese può produrre danni gravissimi nel breve e nel medio periodo, esponendolo al rischio di perdere rilevante opportunità di crescita, quali posti di lavoro qualificati in tutti i settori industriali e nei servizi, ricerca universitaria e privata, produzione di know how, imprese innovative e startup [23]. La sicurezza informatica non va dunque considerata un costo superfluo, o peggio un freno all'attività, ma, al contrario, una precondizione indispensabile per il suo esercizio, che per le imprese si traduce in un vantaggio in termini di competitività. Il diffondersi di una cultura della sicurezza informatica è un fattore decisivo per il Paese, in chiave non solo difensiva ma soprattutto di crescita economica.

CAPITOLO

2 Quadro di riferimento

Questo capitolo introduce le problematiche legate alla evoluzione della minaccia, mostrando come diversi fattori, quali l'aumento continuo della pervasività dei dispositivi, la vulnerabilità dei sistemi software, l'abbattimento dei costi e la diminuzione della necessità di abilità informatiche elevate per portare attacchi di una certa complessità, creeranno le condizioni per un aumento enorme della minaccia in termini di qualità degli attacchi e del numero degli stessi. Il capitolo contiene anche una breve descrizione delle dinamiche del cyberspazio e del governo mondiale di Internet e pone in evidenza come lo spazio cibernetico non sia escluso dalle logiche geopolitiche e della competizione, sia economica che militare, a livello internazionale.

Il capitolo si chiude analizzando brevemente la situazione sicurezza in Italia mettendo in evidenza come nel nostro paese, la presa di coscienza dell'importanza della cybersecurity è quasi inesistente sia nel mondo imprenditoriale sia in quello della politica, per non parlare del vasto pubblico. Solo di recente sono stati registrati importanti passi in avanti nell'individuazione di una road map per l'implementazione di una strategia nazionale per la sicurezza; di questo diamo conto nella parte finale del capitolo. Un'analisi del quadro normativo e delle politiche pubbliche che definiscono le misure di cyber security adottate da altri Stati per far fronte alle minaccia cibernetiche è invece riportata in Appendice. Tale analisi identifica i principali attori coinvolti nell'organizzazione della cyber security, esamina la loro struttura e le loro funzioni nonché l'interazione e il coordinamento di questi ultimi con altri attori rilevanti su scala internazionale.

2.1 Evoluzione della minaccia cyber

L'evoluzione digitale della società ha favorito e incrementato l'interazione tra individui, aziende e istituzioni per finalità sociali, economiche e finanziarie, ma ha, al contempo, creato nuove opportunità per attività criminali di vario tipo, portando a nuovi modelli di strutturazione e organizzazione della criminalità. Da un lato sono infatti comparse attività criminali completamente nuove, quali le frodi finanziarie online e l'abuso di credenziali, dall'altrosi è visto che attività criminali tradizionali possono essere perpetrate con strumenti nuovi e pervasivi.

Studiando queste trasformazioni è possibile delineare degli scenari criminologici di rischio, anche al fine di indicare ai governi nazionali e ai servizi di intelligence dove allocare gli sforzi e le risorse non solo a fini di contrasto ma soprattutto a fini di prevenzione. Tali scenari si possono decomporre nei seguenti elementi: 1) Chi, ovvero attori, strutture e modelli organizzativi emergenti della criminalità; 2) Cosa, ovvero i rischi in termini di target e vittime; 3) Come, ovvero il modus operandi.

I professionisti nel crimine come servizio

La presenza di un mercato virtuale che offre prodotti e servizi altamente specializzati per perpetrare attività criminali e/o minacce informatiche (*Crime-as-a-service*) sta modificando e modificherà sempre più i modelli organizzativi della criminalità. Le più recenti trasformazioni sono caratterizzate dal declino delle forme più tradizionali e gerarchiche dei gruppi criminali organizzati, a favore di network estremamente fluidi, mutevoli e transitori. Questi si formano sulla base di azioni/progetti circoscritti, limitati nel tempo e finalizzati a obiettivi specifici, avvalendosi di cyber-criminali professionisti *freelance* che, guidati dal profitto, vendono competenze e strumenti (malware, exploit zero-day, o accesso a botnet) a gruppi criminali e terroristici. Il *Crime-as-a-Service*, oltre a favorire la crescente specializzazione dei cyber-criminali, incrementa le capacità offensive di altri soggetti criminali sprovvisti di competenze e know-how tecnologici.

Il mercato sommerso è strutturato in ruoli e funzioni (venditori, acquirenti, intermediari...), e si svolge tramite forum online di varia accessibilità e tecnologia. Il mercato è stratificato in livelli di conoscenze: da cyber-criminali con competenze base che vendono principalmente beni finanziari o contraffatti (80-90%), fino al grado più alto della gerarchia, composto da cyber-criminali (10-20%) altamente qualificati che offrono prodotti e strumenti tra i più avanzati e sofisticati, capaci di colpire singoli individui, aziende, organizzazioni, enti governativi. È oggi possibile ipotizzare che il mercato sia suddiviso in "cyber-professionisti" singoli o strutturati in piccoli gruppi (70%), organizzazioni criminali (20%), cyber-terroristi (5%), cyber-criminali afferenti/assoldati da enti

governativi (4%), attivisti (1%). Nonostante questo mercato sia globale, i cybercriminali di maggiore rilievo e con specifiche competenze appartengono prevalentemente a: Cina, America Latina, e Europa dell'Est per gli attacchi attraverso malware; Russia, Romania, Lituania, Ucraina e altri paesi dell'Est Europa per gli attacchi alle istituzioni finanziarie; Vietnam per le minacce relative all'e-commerce, Stati Uniti d'America (trend più recente) per i reati finanziari. Un business fiorente (300 miliardi circa il costo per l'economia globale) che rappresenta il motore principale delle trasformazioni prossime e future delle minacce informatiche.

Lo scenario complessivo si muove verso la strutturazione di una nuova generazione di cyber-organizzazioni criminali sofisticate, di ampie dimensioni e più specializzate. Queste trasformazioni avranno un impatto anche sui gruppi criminali organizzati, i gruppi terroristici e i gruppi di attivisti. Si assisterà al passaggio dalla fase attuale di reclutamento di cyber-criminali freelance a quella di "internalizzazione" con la nascita di joint ventures strutturate e stabili o con sviluppo di cyber-risorse interne ai gruppi. Di conseguenza, il rischio emergente sarà quello di una maggiore convergenza di interessi criminali e un maggiore scambio di competenze e servizi tra questi gruppi.

Comportamenti e vittime: pervasività e vulnerabilità

I trend generali del cybercrime indicano attacchi più sofisticati e multiscopo, un aumento della numerosità e delle tipologie di attacco, così come del numero di obiettivi e delle vittime e dei danni economici conseguenti. Quali, quindi, i principali cyber-comportamenti e i target prossimi e futuri?

Furto e manipolazione di dati sensibili: I dati sensibili rappresentano un bene che sarà sempre più sfruttato dai cyber-criminali per commettere attività criminali. La crescente digitalizzazione delle informazioni e l'aumento della raccolta, elaborazione e archiviazione di dati (causato dalla crescita dei servizi cloud e dalla Internet of Things) ovviamente aumenta il livello di rischio connesso alle intrusioni. L'abuso di tali dati spazia dal tradizionale schema di frode (e.g. relativamente a carte di credito o credenziali bancarie), alle attività di estorsione o di cyber-spionaggio (industriale/governativo). In modalità "crime as a service" si possono acquistare dati che sono ripuliti e rivenduti in blocchi sulla base delle esigenze degli acquirenti. Le intrusioni all'interno delle infrastrutture di aziende di logistica e trasporti rappresentano un trend in aumento, in quanto perpetrate per facilitare attività criminali tradizionali. È ipotizzabile che, più le aziende introdurranno sistemi automatizzati gestiti da remoto, più i gruppi criminali organizzati li sfrutteranno a questo scopo.

Business della contraffazione: I differenti mercati illegali presenti nel *Surface Web* e nel *Deep Web* porteranno alla quasi esclusiva dislocazione della vendita di prodotti contraffatti online che, a loro volta, diventeranno più mirati alle necessità prossime e future dei consumatori. Questi mercati illegali saranno sempre più sofisticati, ovvero predisposti replicando fedelmente le caratteristiche dei siti web legali, diminuendo le possibilità di riconoscimento da parte dei potenziali acquirenti. In aumento quindi la contraffazione e la vendita online di prodotti di consumo quotidiano, dai dentifrici ai detersivi, di medicinali e vaccini di cui saranno contraffatte sempre più tipologie, e di apparecchiature mediche.

Criptovalute e riciclaggio: Le criptovalute, tra le quali Bitcoin è sicuramente la più conosciuta e diffusa, rappresentano oggi un sistema di pagamento in via di espansione, a seguito dell'adozione crescente da parte di aziende con servizi e-commerce e della diffusione di Bitcoin-Bancomat. Se da un lato questo tipo di valute espone gli utilizzatori al rischio di violazione dei propri e-wallet o degli "exchange" (le entità che provvedono alla conversione della criptovaluta in moneta "fiat"), dall'altro potrebbe modificare le attività criminali prossime e future. La possibilità di scambi monetari protetti da pseudonimato e esterni ai controlli dei circuiti finanziari rende possibile una maggiore espansione del commercio illegale di materiale o prestazioni professionali (incluse quelle del "crime as a service"), sia online, sia a fronte di scambi offline (e.g. come supporto per attività di contrabbando o traffico di droga). Da segnalare inoltre il fenomeno delle criptomonete "di nicchia" che offriranno maggiore sicurezza e anonimato rispetto a quelle più tradizionali e saranno funzionali per determinate attività criminali.

Modus operandi e servizi diversificati e personalizzati

La progressiva specializzazione dei cyber-criminali corrisponde specularmente alla creazione di una rete di servizi diversificati e personalizzati per attività criminali da parte di attori privi di competenze informatiche specifiche. Ad esempio, è possibile acquistare o affittare, a prezzi accessibili, pacchetti di malware, soprattutto Trojan bancari (e.g. Zeus), exploit *Zero-day*, ma anche tutorial e consulenza online per l'implementazione: nel 2013 gli exploit kit costavano tra i 1.000-2.000 oppure potevano essere affittati al costo dii 200-600 a settimana o di 600-1.200 al mese. Alternativamente, viene offerta come servizio la disponibilità di Botnet, facilitando attacchi di Denial of Service distribuito finalizzato a compromettere la funzionalità di servizi online di vario tipo (da quelli bancari a quelli di e-commerce). Le Botnet vengono anche usate per attività quale l'invio di mail di spam e di phishing, o per anonimizzare attacchi e frodi online.

In particolare, sono questi ultimi i target prossimi e futuri delle minacce cibernetiche, soprattutto a fronte delle tendenze emergenti nelle ICT, ovvero *Internet of Things*, *Internet of Everything* e *Bring Your Own Device* (BYOD) grazie al quale sempre più individui saranno connessi alla rete delle loro aziende/istituti diventando, a loro volta, veicolo per attacchi su più vasta scala. Combinazioni di malware capaci di infettare computer e dispositivi mobili, ad esempio, si stanno sviluppando a seguito del crescente utilizzo di smartphone per autenticarsi a servizi online (e.g. Zitmo, Zeus in the mobile, compagno del noto troiano bancario *United Payment System* "tradizionale"). Similmente, si assiste al crescente sviluppo di fake app, ovvero applicazioni di servizi, giochi, ecc., contenenti malware ingannevoli.

2.2 Dinamiche del Cyberspace e Governance di Internet

Fin dalla sua creazione, Internet è stata intesa come un *ungoverned space* [15], ovvero un luogo non regolamentato dalle autorità politiche nazionali e internazionali. Inoltre, vista la sua conformazione "artificiale" e tecnologica, gran parte delle responsabilità oggettive ricadevano sulle iniziative intraprese da aziende private. Questa "libertà dallo Stato" ha prodotto i suoi effetti fino a quando il cyberspazio ha iniziato a espandersi e ha prodotto dinamiche geopolitiche.

Attualmente, l'architettura della governance di Internet è basata sull'*Internet Corporation for Assigned Names and Numbers* (ICANN)[1] - con sede negli Stati Uniti - composta da un'associazione privata *multi-stakeholder*. Tale impostazione è stata messa in discussione da due principali eventi: le dinamiche geopolitiche che interessano l'odierno sistema internazionale tendenzialmente multipolare e, in secondo ordine, lo scandalo mediatico verificatosi dopo il cosiddetto "Snowden Leaks". Gli USA promettono di rivedere, in chiave più inclusiva, la politica decisionale in seno all'ICANN attraverso le dichiarazioni del Segretario del Dipartimento del Commercio Penny Pritzker, il quale ha dichiarato "non permetteremo che la rete globale venga cooptata da singole persone, entità o Nazioni e che subentri la loro visione campanilistica. Il modello condiviso non è quindi in discussione, perché garantisce il maggiore potenziale sia per l'innovazione sia per l'inclusione" [61]. L'impostazione "americano-centrica" dell'ICANN viene, però, oggi messa in discussione da altri attori rilevanti come Russia e Cina che puntano al ridimensionamento del ruolo di ICANN e spingono sulla necessità di un maggiore coinvolgimento inclusivo internazionale e multipolare attraverso l'agenzia delle Nazioni Unite l'International Telecommunications Union (ITU). A tal proposito, durante la Conferenza mondiale sulle telecomu-

[1] https://www.icann.org/

nicazioni internazionali, tenutasi a Dubai nel 2012, sono emerse posizioni contrastanti per il futuro del cyberspazio. L'ITU ha cercato di espandere la propria autorità su Internet; gli operatori di TLC europei hanno voluto garantire più ricavi cambiando le regole per lo scambio di informazioni tra le reti; Cina, Russia e India hanno avanzato proprie idee relative alla diffusione di controlli governativi su Internet; gli Stati Uniti e l'Europa hanno preferito appoggiare il modello multi-stakeholder di ICANN.

Gli effetti di un passaggio della *governance* da parte di uno stato-Nazione come gli Stati Uniti a un organismo che risponda direttamente alle Nazioni Unite, da un punto di vista strettamente strategico, provocherebbero uno spostamento del baricentro del potere decisionale a favore soprattutto dei Paesi che in seno al Consiglio di Sicurezza delle Nazioni Unite hanno diritto di veto. La conseguenza potrebbe essere, nel medio e lungo periodo, una vera e propria "balcanizzazione" dove a prevalere sarebbero solo gli interessi particolari dei singoli Stati, piuttosto che l'interesse collettivo. È pur vero, come dimostrano gli ultimi avvenimenti internazionali, che l'attuale impostazione di Internet, ma in larga misura anche del cyberspace, non può essere mantenuta come un luogo anarchico e caotico. A causa dell'intrinseca asimmetria, il dominio cibernetico si presta ad azioni che minano la "sicurezza nazionale" degli Stati, soprattutto se a utilizzare il cyberspace sono attori non statali (terroristi e/o la criminalità organizzata). Allo stesso tempo, l'elevata informatizzazione, interconnessione e interdipendenza, oltre a far emergere le *Information and Communications Technologies* (ICT) come il vero "centro di gravità" delle società industrializzate, ha portato anche all'escalation del confronto tra gli Stati il quale si concentra sempre di più sull'utilizzo dei sistemi informatici piuttosto che sugli armamenti convenzionali.

Ci sono tre aspetti fondamentali legati al cyberspazio che richiedono decisamente una maggiore cooperazione internazionale: la sicurezza informatica, la governance di Internet, la libertà di espressione che richiedono un approccio multilaterale e cooperativo tra gli attori delle relazioni internazionali.

La sicurezza informatica: necessita di un partenariato pubblico-privato a livello mondiale, che prevede diverse fasi cooperative. Infatti, data l'ubiquità del cyberspazio e l'interdipendenza e interconnessione delle varie infrastrutture critiche a livello internazionale, gli Stati dovrebbero impegnarsi formalmente a combattere le minacce che provengono dallo spazio cibernetico e che producono effetti reali (si pensi ad esempio alle *Botnet*, tipici attacchi informatici, che se sponsorizzati da uno Stato possono provocare anche *excalation* militari). In risposta alle minacce provenienti da attacchi informatici, gli Stati (attraverso un partenariato pubblico-privato) dovrebbero costituire delle strutture di *alert* che ricevono la notifica da parte di soggetti pubblici e privati, per garantire al meglio la re-

silienza dell'intero sistema *Internet-based*. In questo settore sarebbe opportuno prevedere dei "tavoli di dialogo" aperti alla comunità internazionale in modo tale da prevedere, ad esempio delle Confidence Building Measures (CBM) applicabili al cyberspazio, per riuscire a mitigare sia il rischio di *excalation* militare così come il rischio di proliferazione di *cyber weapons*. A tal proposito è da segnalare l'iniziativa intrapresa dall'OSCE "Confidence building measures to enhance cybersecurity", che prevede attraverso il dialogo aperto tra gli Stati Membri, l'applicazione delle CBM anche al cyberspace, in modo tale da prevenire escalation militari.

La governance di Internet: dovrebbe essere basata esclusivamente sul modello *multi-stakeholder*. Gli Stati dovrebbero raggiungere la consapevolezza che le principali attività legate a Internet (e in generale al cyberspazio) non dovrebbero essere controllate esclusivamente da imprese o entità private. Più in generale, l'ICANN dovrebbe diventare più trasparente, strutturato, responsabile e inclusivo, in modo tale da rendersi capace di rappresentare un quadro *multi-stakeholder* se vuole sopravvivere come un regolatore privato.

La libertà di espressione: dovrebbe essere garantita attraverso l'elevata capacità inclusiva delle Nazioni Unite che, atttraverso la comunità scientifica, dovrebbero spingere verso una sicura e diffusa *awerness* legata alla cultura di Internet e al superamento del *digital divide* [3]. L'accesso universale a Internet dovrebbe sempre essere preservato come garanzia per la libertà e per il mantenimento del cyberspazio inteso come *global common*. Questo aspetto potrebbe entrare in contrasto con le tesi favorevoli alle iniziative di una "sorveglianza" nazionale di Internet in modo tale da contrastare l'anonimato [46]. Una nazionalizzazione di Internet porterebbe alla "balcanizzazione di Internet" che, mentre da un lato renderebbe più facile il contrasto ai criminali, dall'altro lato significherebbe la fine della libertà di Internet.

2.3 Multipolarità e Cyber-war

Lo spazio cibernetico non è escluso dalle logiche geopolitiche e della competizione internazionale. Dal momento che include sia elementi digitali sia fisici - cavi, satelliti, routers, computer di amministrazioni pubbliche e privati - esso contiene elementi che hanno una collocazione geografica precisa e dati che hanno rilevanza economica, politica e strategica per la sicurezza nazionale. Le attività nello spazio cibernetico sono dunque influenzate dalla realtà delle vicende internazionali e viceversa. Gli ultimi sviluppi legati alla sicurezza nello spazio cibernetico hanno infatti riportato i governi al centro dell'azione. Ne sono esempio la nuova strategia di cybersecurity degli Stati Uniti (2015) e l'inten-

sificarsi del dialogo con l'UE, che si è dotata di una strategia per la cybersecurity per la prima volta nel 2013. A livello internazionale si susseguono inoltre iniziative formali e informali per la descrizione di definizioni e norme condivise, a fronte della presenza di numerosi attori e differenti contesti normativi e tecnologici che implicano importanti limitazioni in termini di governance mondiale.

I rischi associati allo spazio cibernetico sono di diversa natura, legati alle relazioni internazionali fra stati e alla presenza di attori non statuali. Alcuni stati dispongono già da tempo di unità offensive e difensive per la cyber-war, diretta a infrastrutture economiche e civili, oltre che militari, anche se la realtà suggerisce che si tratta di uno scenario ancora remoto. È però vero che situazioni di confronto, o conflitto, fra stati rendono oggi meno impossibili, seppur improbabili, atti di cyber-war, mentre rendono molto probabile un incremento dello scontro relativo al cyber-spionaggio a danno di apparati governativi, civili e militari, ma anche di imprese private. Attualmente, dunque, le minacce più probabili nello spazio cibernetico di uno stato provengono da attacchi di gruppi sostenuti o tollerati da governi e dallo spionaggio informatico di reparti di intelligence, che cercano di penetrare i sistemi informatici di paesi esteri a fini politici, economici e militari.

Anche l'utilizzo dello spazio cibernetico da parte di organizzazioni terroristiche è una possibile minaccia alla sicurezza nazionale, in primis per lo sfruttamento della rete a fini di propaganda, addestramento, autofinanziamento e pianificazione. La capacità di questi gruppi di rappresentare un pericolo reale alle infrastrutture critiche resta più limitata, ma destinata a crescere nel medio-lungo termine, anche a causa dell'aumento della loro competenza tecnica.

In Italia, le Relazioni al Parlamento dei Servizi d'Informazione hanno da alcuni anni incluso la minaccia cibernetica per l'Italia. L'ultima relazione (2014), individua due aspetti principali: cyber-spionaggio per fini industriali e cyber-jihad, giudicati una minaccia concreta attuale e con proiezione a medio-lungo termine. Lo spionaggio industriale ha colpito in particolare aziende italiane ad alto valore tecnologico. La cyber-jihad si è concretizzata soprattutto in attività di propaganda, addestramento, autofinanziamento e pianificazione, ma non in attacchi a infrastrutture critiche o a sistemi informatici di rilevanza strategica.

Al costante rischio di cyber-spionaggio si aggiunge dunque un incremento della minaccia cyber-terroristica, a maggior ragione in relazione a manifestazioni quali l'EXPO 2015 - il primo evento "fully cloud powered", la cui alta visibilità potrebbe rendere il proprio sistema IT particolarmente appetibile da attaccare, e il Giubileo straordinario che inizierà a dicembre 2015.

Come e in che misura il diritto internazionale possa regolare la conflittualità fra stati nel dominio cibernetico e il problema dell'attribuzione degli attacchi informatici sono oggi tra i fattori che influenzano maggiormente la cooperazione internazionale fra stati.

A tal proposito, rimane una questione aperta se un attacco cibernetico costituisca o meno un attacco armato e in che misura si possa rispondere. Il "Tallinn Manual on the International Law Applicable to Cyber Warfare" (2013) - espressione di opinioni di un gruppo di esperti indipendenti senza valore vincolante - afferma che il diritto internazionale dei conflitti armati si applica alle operazioni cibernetiche. Durante il vertice NATO del settembre 2014, i capi di stato dei paesi membri hanno avallato l'Enhanced Cyber Defence Policy, approvata il giugno precedente dai ministri della difesa dei paesi dell'Alleanza. Secondo la Policy, la NATO riconosce che il diritto internazionale si applichi al cyberspace e che la difesa dello spazio cibernetico sia inclusa nel compito fondamentale di difesa collettiva dell'Alleanza. Afferma inoltre che l'eventuale attivazione dell'articolo 5 in seguito ad un attacco cibernetico verrà decisa caso per caso.

Una delle maggiori sfide relative alla cyber-war e al cyber-terrorismo resterà, nel breve-medio termine, l'assenza di un quadro giuridico certo e condiviso.

Iniziative per lo sviluppo di "Confidence Building Measures" (CBM) - come l'"Initial Set of OSCE CBMs to Reduce the Risks of Conflict Stemming from the Use of ICT" (OSCE, 2013) - o codici di condotta, contribuiscono alla cooperazione istituzionale e operativa, ma solo in parte concorrono a definizioni normative. Nonostante le iniziative internazionali volte alla descrizione di fattispecie e norme condivise, ad esempio sull'attribuzione della responsabilità legale, l'assenza di un quadro giuridico di riferimento certo continuerà a pesare sulla possibilità di governance.

La collaborazione è rallentata dalla volontà di molti stati di mantenere la massima libertà d'azione per le proprie attività di intelligence o per i propri attacchi cibernetici. Alla ritrosia degli Stati sembra fare eccezione la gestione del contrasto al cyber-crime, ritenuto di primaria importanza per i forti impatti economici, perché gli opposti interessi di tutti i maggiori attori economici, costringe alla collaborazione. Una sfida potrebbe essere quella di considerare una selezione di strumenti tecnici e giuridici volti al contrasto al cyber-crime per valutare l'adattabilità in ambito cyber-war e cyber-terrorismo (stante la mancanza di differenze tecniche tra le varie categorie) così da riuscire a internazionalizzare la trattazione dei temi cyber-war e cyber-terrorismo in un'ottica più collaborativa.

2.4 Politica digitale e sicurezza informatica in Italia

Analizzando la situazione sicurezza in Italia, emerge che, a differenza di molti altri Paesi, nel mondo imprenditoriale (fatta eccezione per le grandi banche e pochi grandi gruppi) e in quello della politica, per non parlare del vasto pubblico, la presa di coscienza dell'importanza della cyber security (*cyber security awareness*) è quasi completamente inesistente persino a livello dei manager

aziendali. Politica digitale, crescita e sicurezza sono in realtà facce della stessa medaglia, in quanto una strategia digitale competitiva e orientata allo sviluppo non può non comprendere una dimensione *security* caratterizzata dai più elevati standard internazionali [20].

In Italia, un ulteriore elemento di debolezza è rappresentato dal processo di digitalizzazione della Pubblica Amministrazione che in teoria potrebbe rappresentare uno straordinario volano di crescita per il sistema Paese, ma che risulta viceversa assai frammentato e privo di una visione unitaria capace di garantire interoperabilità tra le diverse amministrazioni e dalle amministrazioni verso i cittadini e le imprese. Le stesse consistenti forniture pubbliche di servizi digitali (via Consip o senza Consip) non hanno a monte un piano di riorganizzazione della Pubblica Amministrazione capace di sfruttare in modo efficiente e creativo la vasta gamma di soluzioni offerte dalla rivoluzione digitale. Non si intendono qui negare alcuni progressi (fatturazione elettronica, ricettari medici digitali in alcune regioni, ecc.), tuttavia la dispersione di energie e la frammentazione istituzionale sono ancora elevatissime, come peraltro ha dimostrato il recente dibattito parlamentare sull'emendamento Quintarelli[2] in sede di riforma costituzionale.

L'ambiguità normativa e gestionale che ha contraddistinto il ruolo e le attività dell'Agenzia per l'Italia Digitale (AgID) è un altro esempio delle difficoltà esistenti. In linea di principio, non sarebbe difficile delineare una politica governativa, investimenti pubblici e una legislazione all'altezza delle nuove sfide, anche perché oggi è possibile far tesoro delle esperienze di altri paesi. In appendice viene riportata una breve descrizione delle politiche di cyber security di altri stati, scelti per evidenzare "best practices", si vedano anche [44] e [45].

La rivoluzione prodotta dallo spazio digitale nuove sfide alla responsabilità politica dello stato moderno in termini di strutture amministrative, processi decisionali, diritti civili, sicurezza e servizi al cittadino. Su questo punto si registra in Italia un grave ritardo culturale e politico. Il tema è sostanzialmente assente dallo spazio pubblico, così come scarsa è la partecipazione delle università e delle imprese nazionali ai grandi appuntamenti internazionali sulla governance e sul futuro di Internet e del cyberspace[3].

[2] L'emendamento 31.26 presentato dall'On. Stefano Quintarelli ed approvato il 12 febbraio 2015 propone una modifica all'articolo 117 della Costituzione Italiana. Il *comma r* recita: "Lo Stato ha legislazione esclusiva nelle seguenti materie: [...] pesi, misure e determinazione del tempo; coordinamento informativo statistico e informatico dei dati, dei processi e delle relative infrastrutture e piattaforme informatiche dell'amministrazione statale, regionale e locale". Questo riporta, in modo chiaro, la competenza delle piattaforme informatiche al governo centrale, dopo la modifica del titolo quinto della Costituzione Italiana fatta nel 1999 con la legge costituzionale n. 1/1999.

[3] Global Conference on CyberSpace, `https://www.gccs2015.com/programme`

In Italia, la molteplicità delle autorità politiche deputate (Ministero dello Sviluppo Economico in primis, Ministero della Funzione Pubblica, Ministero degli Interni, altri Ministeri, Regioni, ASL, grandi comuni, ecc.) è in palese contrasto con la natura stessa della rivoluzione digitale. Questa, infatti, per essere efficace, richiede di rompere i compartimenti stagni, le isole di potere e impone una visione trasversale e unitaria che consenta di agire con velocità, con una catena di comando chiara e secondo una logica modulare coerente con una visione a lungo termine dell'intero sistema Paese.

La distinzione tra virtuale e reale non esiste più, se mai è esistita in precedenza. In ogni caso siamo oggi di fronte a una nuova e gigantesca "rivoluzione industriale" che ha riflessi dirompenti sulla vita di tutte le imprese di ogni settore, delle pubbliche amministrazioni e di ogni singolo cittadino, sia sul piano lavorativo sia su quello della vita privata. È sbagliato pensare alla crisi economica come un effetto esclusivo della crisi finanziaria, anche se essa ne ha costituito un rilevante acceleratore; la crisi è dovuta a un cambiamento sistemico dove i modelli organizzativi aziendali, i prodotti, le metodologie di produzione stanno cambiando rapidamente, spazzando via alcune categorie di lavori e creandone di nuovi più qualificati [23]. Di conseguenza, sul piano economico vinceranno i paesi più avanzati sul piano digitale e più aperti all'innovazione, i paesi che sapranno mantenere i propri cervelli e attirarne di nuovi.

Per queste ragioni è necessario e urgente dotare l'Italia di una strategia digitale ben definita, di una struttura di governance e di una capacità organizzativa all'altezza delle sfide della rivoluzione digitale[4].

Nonostante il tema della cyber security e della sua governance sia dibattuto nel nostro paese sin dai primi anni 2000, solo di recente sono stati registrati importanti passi in avanti nell'individuazione di una road map per l'implementazione di una strategia nazionale. Tra il 2012 e il 2013, infatti, venne completato il quadro degli interventi di natura strategica nazionale a tutela delle Infrastrutture Critiche, con riguardo alla protezione cibernetica e alla sicurezza informatica nazionale. Dopo la Legge n. 133 del 7 agosto 2012, che attribuisce al comparto intelligence nuove e specifiche competenze in materia di protezione cibernetica e sicurezza informatica, e dopo il decreto Legge del 18 ottobre 2012, n.179 "Ulteriori misure urgenti per la crescita del Paese", provvedimento Crescita 2.0, che nasce con l'obiettivo di dare attuazione all'implementazione della Agenda Digitale, venne emanato il DPCM del 24 gennaio 2013 [60] che getta le basi per la definizione della strategia nazionale. Tale decreto definisce tre diversi livelli di intervento: indirizzo politico e coordinamento strategico, supporto e raccordo tra gli enti competenti, gestione della crisi ed in particolare prevede che:

A. Il Presidente del Consiglio dei Ministri:

[4] Per ulteriori approfondimenti si veda anche [30, 13, 40, 41, 11].

1. adotti il Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico [58];
2. adotti il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionale [59];
3. emani le direttive e ogni atto d'indirizzo necessari per l'attuazione del Piano; impartisce (sentito il CISR) le direttive al DIS e alle Agenzie.

B. si assegnino al Comitato Interministeriale per la Sicurezza della Repubblica (CISR) le seguenti attività:

1. esercizio dell'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico;
2. approvazione delle linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, per la condivisione delle informazioni e per l'adozione di best pratices e di misure rivolte all'obiettivo della sicurezza cibernetica;
3. elaborazione degli indirizzi generali e gli obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali da perseguire nel quadro della politica dell'informazione per la sicurezza da parte degli organismi di informazione per la sicurezza, ciascuno per i profili di rispettiva competenza;
4. promozione dell'adozione delle iniziative necessarie per assicurare, in forma coordinata, la piena partecipazione dell'Italia ai diversi consessi di cooperazione internazionale (sia in ambito bilaterale sia multilaterale, sia dell'UE sia della NATO), al fine della definizione e adozione di politiche e strategie comuni di prevenzione e risposta;
5. formulazione delle proposte di intervento normativo e organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi;
6. partecipazione, con funzioni di consulenza e di proposta, alle determinazioni del Presidente, in caso di crisi.

C. si rinforzi il ruolo del Dipartimento delle informazioni per la sicurezza (DIS), che coordina le agenzie di intelligence per incrementare il livello di cyber security.

Per coordinare tutte le attività implicite nelle funzioni del CISR, l'art. 4 del decreto instaura l'Organismo collegiale di coordinamento, guidato dal Direttore Generale del DIS. Tale Organismo, chiamato anche *CISR tecnico*, ha, tra gli

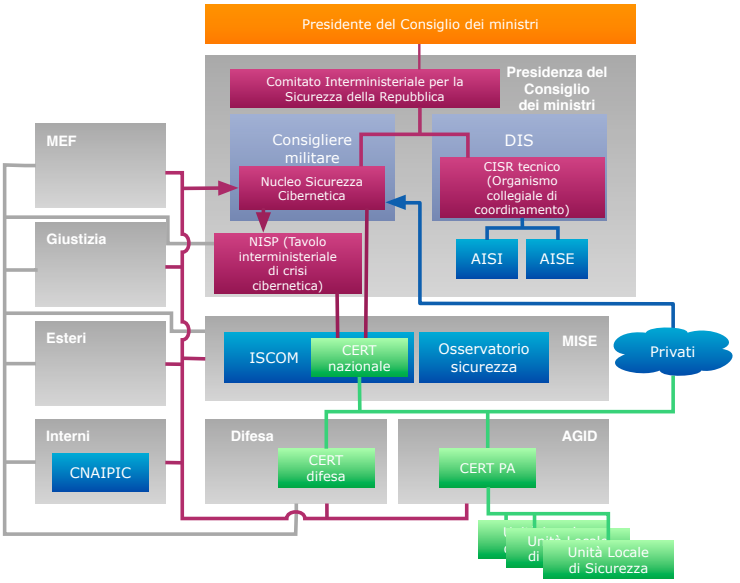

Figura 2.1: Panorama operativo italiano per la gestione della cyber security.

altri, anche il compito di identificare minacce e vulnerabilità potenziali dei sistemi nazionali (sia pubblici sia privati) e di definire le best practice con l'aiuto di un comitato scientifico. Formazione e cultura della sicurezza rientrano anche tra compiti dell'Osservatorio Permanente per la Sicurezza e Tutela delle Reti, in forza presso il MISE. Il decreto, inoltre, istituisce presso l'Ufficio del Consigliere militare, il Nucleo per la sicurezza cibernetica (NSC), avente funzioni di coordinamento delle varie componenti (Ministeri, Polizia postale attraverso il CNAIPIC, CERT e AgID) e di supporto per le attività del Presidente del Consiglio, per quanto riguarda la preparazione e la prevenzione delle crisi. L'NSC, in caso di crisi, attiva il Nucleo Interministeriale Situazione e Pianificazione (NISP) (quale tavolo interministeriale di crisi cibernetica) che avvalendosi del supporto del CERT Nazionale, assicura le attività di stabilizzazione e reazione. Il CERT nazionale, avvalendosi delle unità locali di sicurezza e cooperando con CERT-PA, presso AgID e CERT-difesa presso il Ministero della Difesa, incrementa la capacità del Paese di rispondere alle crisi cyber. Ulteriori dettagli in [58, 16]. Quanto accuratamente descritto nel DPCM è stato inglobato nel "Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico" [58], pubblicato nel dicembre 2013. In tale documento viene fornita una descrizione dei ruoli e compiti dei soggetti pubblici definiti pocanzi. La Figura 2.1 riporta le interazioni tra tutti i vari attori e riassume l'intero panorama italiano.

CAPITOLO

3 Le Sfide

Questo capitolo introduce una serie di sfide, viste da una angolazione accademica, che l'Italia dovrà affrontare nei prossimi anni per rimanere al passo degli altri paesi sviluppati. L'insieme delle sfide, certamente non esaustivo mira a fornire una panoramica della complessità e della multimensionalità del mondo in cui siamo entrati da ormai alcuni decenni. Queste sfide, per poter essere affrontate, avrebbero bisogno di un ecosistema in cui ricerca, ambiente produttivo e ambiente governativo lavorino in sinergia. Ecosistema che sarebbe favorito dalla attuazione di alcune raccomandazioni che riportiamo nel capitolo successivo.

È importante sottolineare che le sfide non hanno solo carattere tecnologico, ma investono la sfera economica, sociale e organizzativa di un sistema complesso come una nazione. Le prime sezioni del capitolo mettono in evidenza gli ambienti dove gli attacchi cyber saranno più insidiosi, segnatamente Internet of Things e Infrastrutture Critiche. La Sezione 3.3 mostra come gli attacchi tendano a utilizzare il fattore umano per superare le barriere difensive di una organizzazione. La sezione 3.4, oltre a presentare gli attacchi principali a cui sono soggette le componenti hardware di un sistema, è la prima di una serie di sezioni dedicate a strumenti atti a rendere più resilienti i sistemi informatici, quali le tecnologie biometriche (Sezione 3.5) e quelle crittografiche (Sezione 3.6).

Le sezioni successive affrontano le problematiche relative alla protezione di componenti fondamentali del cyber space, quale la Internet Nazionale (Sezione 3.7) e le informazioni memorizzate nei sistemi (Sezione 3.8). Una soluzione efficace per la protezione dei sistemi è la riduzione della loro superficie d'attacco, attraverso il consolidamento delle sale server (Sezione 3.9). La parte dedicata alla protezione si conclude con le nuove competenze da fornire a progettisti di

sistemi informativi complessi, al fine di creare sistemi tolleranti alle intrusioni (Sezione 3.10).

L'ultimo gruppo di sezioni tratta aspetti collaterali, ma non meno importanti nel contesto cyber di attacco e difesa, quali: esercitazioni per migliorare la preparazione rispetto ad attacchi (Sezione 3.11), investigazioni digitali per migliorare le tecniche forensi post attacco (Sezione 3.12), operazioni di intelligence nel cyberspace per anticipare possibili attacchi (Sezione 3.13), condivisione delle informazioni per migliorare la risposta ad attacchi informatici (Sezione 3.14) e infine nuove tecniche di valutazione del rischio cyber per migliorare, in termini di costi ed efficienza, i processi di gestione della conformità a standard di sicurezza di una organizzazione (Sezione 3.15).

3.1 Internet delle Cose

Uno dei temi più caldi del mondo ICT è l'evoluzione verso la cosiddetta *Internet delle Cose* ("Internet of Things" – IoT), a volte anche detta *Internet di ogni Cosa* ("Internet of Everything") per evidenziarne il carattere pervasivo. Si tratta della naturale evoluzione di varie tendenze concorrenti: la miniaturizzazione e specializzazione dei dispositivi digitali, la loro costante connessione alla rete - sempre più necessaria per sfruttarne al meglio le funzionalità - e la pervasiva interazione tra questi oggetti "intelligenti e connessi".

Ad esempio, le auto moderne non sono più dei dispositivi meramente meccanici, ma sono computerizzate in modo pervasivo, monitorate e controllate da reti di elaboratori interne al veicolo. Prossimamente, un'auto sarà connessa a Internet e potrà cooperare con l'infrastruttura stradale e con le auto vicine. Questo tuttavia significa anche che un avversario che sia in grado di infiltrare uno qualunque degli elaboratori interni all'autoveicolo si trova nella posizione di poter attaccare i sistemi safety-critical di bordo [34]. Questa minaccia è ancora più seria se si considera che l'attacco può essere eseguito remotamente attraverso le varie interfacce di comunicazione del veicolo con il mondo esterno [12] quali i dispositivi mobili e gli smartphone [17].

In modo simile, nell'aviazione civile e commerciale si sta affermando l'idea dell'*e-enabled aircraft*, secondo la quale un aeromobile opera come un nodo mobile e intelligente in una rete multi-link globale di sistemi posizionati in aria, a terra e nello spazio [70]. In questa visione, le minacce derivanti da attacchi cibernetici si fanno sempre più concrete [69], sia verso gli aeromobili, sia verso le infrastrutture di controllo del traffico aereo. Ad esempio, sono state sollevate perplessità in merito all'architettura informatica di alcuni nuovi aeromobili, quali il Boeing 787 Dreamliner o gli Airbus A350 e A380, che hanno una singola rete di bordo utilizzata sia per il controllo del velivolo sia per il sistema di intrattenimento accessibile dai passeggeri. La prova della pericolosità di questo stato

di cose è stata fornita recentemente da un hacker americano che, attraverso il sistema di intrattenimento di bordo, per venti volte avrebbe superato i meccanismi di sicurezza degli aerei sui quali viaggiava, giungendo persino a controllare un motore di uno dei velivoli[1].

La gestione di dispositivi IoT, incluso l'aggiornamento del software alla base del loro funzionamento, diventa fondamentale per la sicurezza dell'IoT stessa e di tutto ciò che a essa è correlato. Infatti, l'aggiornamento del software non solo permette il rilascio di nuove funzionalità, ma spesso consente anche di risolvere dei problemi di sicurezza attraverso delle "patch": è quindi fondamentale che questi aggiornamenti avvengano in maniera estremamente sicura e tempestiva. L'attuale tendenza a richiedere che ciascun dispositivo si colleghi a un server centrale introduce evidenti colli di bottiglia prestazionali [9] e non è scalabile in funzione del numero di dispositivi connessi. Alcuni ricercatori stanno investigando la possibilità di impiegare metodologie innovative per la distribuzione efficiente e sicura degli aggiornamenti software a dispositivi IoT [1, 2].

A livello di iniziative e progetti in corso, l'Unione Europea e Eurocontrol, nel 2007, hanno attivato un programma cooperativo di ricerca dal nome Single European Sky ATM Research (SESAR) per la modernizzazione del controllo del traffico aereo (ATM) in Europa. Il programma è gestito da SESAR Joint Undertaking (SESARJU), un partenariato pubblico-privato (PPP) che comprende i principali attori del settore. Nell'ambito del Programma Quadro H2020, SESARJU ha stanziato 20 milioni di euro per il 2015 per ricerca, sia di base sia applicata, nel settore dell'ATM. Una delle aree di ricerca individuate è "Information Management in ATM", nell'ambito della quale la cyber security viene considerata una delle sfide principali.

Dietro questa importante minaccia i vari stakeholder si stanno muovendo. Nell'ambito automotive, a livello internazionale, AUTOSAR (AUTomotive Open System ARchitecture), un partenariato internazionale tra produttori OEM e fornitori Tier 1, ha iniziato a standardizzare soluzioni architetturali per la comunicazione sicura end-to-end tra i processori connessi in rete a bordo degli autoveicoli. A livello europeo, la Commissione ha finanziato sia programmi di ricerca specificamente incentrati su cyber security nel settore automobilistico, tra cui EVITA[2] e PRESERVE[3], sia programmi di ricerca, quali SESAMO[4] e SAFURE[5], in cui la cyber security nel settore automobilistico è uno dei casi di studio del progetto.

[1] `http://www.repubblica.it/tecnologia/sicurezza/2015/05/18/news/hacker%_voli_aerei-114625489/`

[2] `http://www.evita-project.org/`

[3] `https://www.preserve-project.eu/`

[4] `http://sesamo-project.eu/`

[5] `http://www.safure.eu/`

In ogni momento della nostra vita saremo quindi sempre più circondati da migliaia di dispositivi connessi miniaturizzati, potenzialmente vulnerabili, e che per noi diventeranno allo stesso tempo sempre più necessari. Oltre alle smart cars, le smart cities e le smart houses completano il quadro. Tuttavia questi dispositivi in genere vengono progettati tenendo conto di aspetti come costo e design e la sicurezza non viene certo considerata un punto rilevante. Quindi possiamo attenderci attacchi che tenderanno a rendere inutilizzabili i nostri smartphone, televisori, frigoriferi oltre che le nostre auto e poi chiedere un riscatto (ransomware) per permetterci di riutilizzarli. Possiamo addirittura pensare ad attentati ad-personam attraverso la compromissione di componenti software di vetture o di dispositivi casalinghi.

3.2 Infrastrutture Critiche e Sistemi Cyber-Fisici

Sempre più frequentemente i dispositivi fisici con cui interagiamo giornalmente o su cui si basano i servizi fondamentali per la nostra vita quotidiana – le automobili, le televisioni, gli smartphones, ma anche i servizi di fornitura di energia elettrica o acqua, l'assistenza sanitaria e le telecomunicazioni – sono controllati da sistemi informatici. Si parla di Cyber-Physical System (CPS) [62] per riferirsi al singolo sistema o sottosistema e di Infrastruttura Critica (Critical Infrastructure - CI) per indicare un sistema complessivo controllato informaticamente. Questa dualità espone i CPS e le CI a una vasta gamma di nuovi attacchi che sono possibili anche in assenza di un collegamento, diretto o indiretto, del dispositivo alla rete.

In questi sistemi, sfruttando il legame tra il mondo fisico e quello informatico, un hacker può riuscire a ottenere il controllo della porzione fisica del sistema e quindi a far sì che un attacco informatico abbia effetti sul mondo fisico, con possibili conseguenze sull'ambiente o addirittura sulla vita delle persone. Un esempio degno di nota è il malware Stuxnet [39], che ha rappresentato (nel 2010) il primo attacco cyber fisico a un'infrastruttura critica e ha portato alla rottura di oltre trecento centrifughe della centrale nucleare Iraniana di Natanz. Ciò ha rallentato notevolmente il programma nucleare Iraniano, probabilmente più di quanto avrebbe potuto fare un attacco militare[6].

A partire dall'11 settembre 2001, la protezione delle CI da attacchi informatici ha acquisito un'elevatissima priorità nei programmi di molti governi. A livello Europeo la materia è stata affrontata a partire da una comunicazione del

[6] `http://web.archive.org/web/20120602025727/http://www.telegraph.co.uk/technology/news/9305704/Barack-Obama-ordered-`

2006[7], recepita con Direttiva 2008/114/CE[8], con la quale si propone un programma europeo per la protezione delle infrastrutture critiche (European Programme for Critical Infrastructure Protection, EPCIP) e si costituisce una rete informativa di allarme sulle infrastrutture critiche (Critical Infrastructure Warning Information Network, CIWIN).

A livello nazionale, l'Italia già nel 2003 creava, in seno al Ministero per l'Innovazione Tecnologica, un gruppo di lavoro sulla protezione delle Infrastrutture Critiche di Comunicazione (Critical Information Infrastructure - CII)[9]. Con il decreto legge n. 155 of 31/7/05 (legge Pisanu), la responsabilità per la protezione delle CII nazionali veniva affidata alla Polizia di Stato e in particolare al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC). Il 24 gennaio 2013 viene emanato invece il DPCM del 24 gennaio 2013 [60] già discusso nella Sezione 2.4. Oltreoceano, negli USA, la cybersecurity delle infrastrutture critiche ha ricevuto una particolare attenzione sotto le presidenze G. W. Bush e B. Obama attraverso una serie di azioni che culminano con tre executive orders promulgati nel triennio 32013-2015 come riportato nell'Appendice A.5.

Malgrado queste iniziative, le infrastrutture critiche sono soggette ad attacchi informatici sempre più frequenti e sempre più sofisticati, come dimostrato da alcuni recenti report di Symantec[10] e McAfee[11]. Difatti, per una loro efficace protezione occorre intervenire a diversi livelli, sul piano tecnico-scientifico e su quello normativo.

Sul piano tecnico-scientifico, si devono far evolvere le tecniche progettuali dei sistemi cyber-physical al fine di considerare i requisiti di affidabilità e sicurezza, spesso tra di loro contrastanti, in un unico processo produttivo (tipicamente i sistemi fisici controllati sono progettati con la logica dell'affidabilità rispetto a possibili guasti, mentre mancano le necessarie misure di sicurezza rispetto ad attaccanti malevoli). Ciò richiederà necessariamente l'inclusione di esperti dello specifico settore applicativo in tutte le fasi del ciclo produttivo (dalla specifica alla validazione e al test sul campo), in un approccio che veda il focus dell'ingegnerizzazione spostarsi dai dispositivi informatici considerati in isolamento (IT-Engineering) al sistema nella sua globalità (System Enginee-

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:IT:PDF

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:IT:PDF

[9] http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=2832

[10] http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_intelligence_qtrly_oct_to_dec_WP_21169903.en-us.pdf

[11] http://www.mcafee.com/in/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

ring)[12]. È importante notare che un tale approccio consentirebbe di risolvere, a livello architetturale, una serie di problematiche di sicurezza derivanti dall'elevato impiego di sistemi legacy da un lato e commerciali (Components Off The Shelf - COTS) dall'altro, entrambi – per motivazioni diverse – in generale non progettati né realizzati secondo specifiche di sicurezza adeguate all'impiego in applicazioni critiche. Occorre infine evidenziare che, come si vedrà nella prossima sezione, i problemi posti dall'impiego di componenti legacy nella realizzazione di infrastrutture critiche non si limitino alle sole componenti software, ma coinvolgono, in modo del tutto analogo, anche le componenti hardware.

Sul piano normativo, occorrerebbe imporre che i sistemi finali, in fase di esercizio, garantiscano livelli prestabiliti di sicurezza. Alcune recenti tendenze di mercato infatti, tra cui innanzitutto la progressiva privatizzazione del settore, hanno portato gli operatori di infrastrutture critiche a privilegiare logiche di mercato e di riduzione dei costi a discapito della sicurezza. Per fronteggiare questo problema alcuni paesi hanno imposto, per la realizzazione delle infrastrutture critiche nazionali, l'acquisto di solo hardware certificato, altri l'impiego di prodotti realizzati da ditte nazionali, più facilmente controllabili e monitorabili[13]. Si ritiene che avrebbe una grande valenza strategica la creazione di un ente certificatore – verosimilmente strutturato come una rete di attori qualificati impegnati localmente sul territorio nazionale – che possa monitorare in maniera sistematica tutte le fasi del ciclo produttivo delle infrastrutture critiche nazionali – nonché valutare accuratamente le inevitabili interdipendenze con le infrastrutture critiche estere – e fornire quindi garanzie concrete sul livello effettivo di sicurezza in fase di esercizio.

3.3 Organizzazione, Fattore Umano e Ingegneria Sociale

La maggior parte degli attacchi perpetrati ai sistemi informatici viene effettuata grazie a una componente di fattore umano (fattore H). La componente umana può essere sia di natura consapevole sia di natura inconsapevole, ma in entrambi in casi è spesso decisiva per portare a termine un attacco con successo. È chiaro che le soluzioni tecnologiche non possono da sole assicurare la sicurezza di un sistema. Innanzitutto le organizzazioni devono definire e istituzionalizzare al loro interno una cultura della sicurezza informatica, in modo tale che siano scongiurati comportamenti, consapevoli o inconsapevoli, inappropriati per la sicurezza. Stabilire come gli essere umani dovrebbero interagire correttamen-

[12] `http://publications.jrc.ec.europa.eu/repository/bitstream/JRC90412/lbna26808enn.pdf`

[13] Ciò è stato fatto in particolar modo per le infrastrutture critiche di tipo militare.

te con i sistemi informatici e con i flussi informativi per scongiurare il rischio che creino falle di sicurezza, è una materia complessa e ardua da affrontare. Per esempio, è importante tenere in conto le differenze tra gli individui, quali: le abilità cognitive, la percezione che il singolo ha del rischio, la conoscenza degli strumenti e dei processi e, non in ultimo, le attitudini personali.

Naturalmente sia la percezione del rischio sia le differenze individuali sono condizionate e a volte determinate dall'ambiente in cui gli incidenti di sicurezza accadono. La cultura e il clima nell'organizzazione possono avere un impatto significativo. Una delle componenti più importanti del fattore H è la cosiddetta *Ingegneria Sociale* (Social Engineering SE): un insieme di tecniche atte a raggirare l'essere umano al fine di ottenere informazioni riservate. Queste possono essere poi utilizzate per portare a termine un attacco utilizzando strumenti e tecnologie.

Nel seguito si affronteranno i seguenti temi: i più comuni tipi di errori causati dal fattore H; come si possa aumentare la consapevolezza del rischio; come si possa instaurare una cultura della sicurezza all'interno dell'organizzazione; come si svolgono gli attacchi di ingegneria sociale e come ci si possa difendere

Dal punto di vista psicologico, il social engineering si basa sulla consapevolezza che, in determinati contesti, il comportamento umano mostra una certa tendenza alla fiducia verso gli altri. Tuttavia, ciò si somma alla abilità tecnica dell'attaccante di impersonare il ruolo di entità fidata e al livello di vulnerabilità della vittima. Il concetto di vulnerabilità del comportamento della vittima è legato a diversi aspetti, connessi da un lato al grado di competenza tecnica e procedurale delle attività connesse ai sistemi oggetto di attenzione, dall'altro al supporto che tali sistemi forniscono all'utente per la protezione rispetto ad attacchi di SE, ma, nel caso di organizzazioni, anche dall'adozione di adeguati protocolli di sicurezza procedurale.

Gli obiettivi finali degli attacchi di SE sono quelli tipici del cybercrime, quindi, in generale, la compromissione dei requisiti di confidenzialità, integrità o disponibilità di un sistema, spesso attraverso la strutturazione di un attacco di tipo APT (Advanced Persistent Threat). L'attacco di SE è cioé spesso solo una fase di un attacco o di una serie di attacchi complessi che si possono protrarre nel tempo. In alcuni casi gli attacchi di SE sono specificamente progettati per una specifica vittima, intesa come singola persona o come organizzazione. Un esempio di attacco di questo tipo è lo *spear phishing*, in cui la vittima riceve una e-mail fortemente personalizzata, contestualizzata rispetto a dettagli reali della sua vita. L'apertura dell'e-mail comporta ad esempio l'installazione di un malware che a sua volta può controllare l'ulteriore installazione di malware attraverso opportuno download da server web controllati dall'attaccante. L'obiettivo è spesso quello di installare backdoors multiple all'interno dell'organizzazione che possano garantire all'attaccante la possibilità di accedere all'interno del perimetro dell'organizzazione, anche nel caso in cui i precedenti attacchi vengono

rilevati e contrastati. Attraverso le backdoors l'attaccante ha quindi la possibilità di scaricare informazioni relative ad account, password, codici di accesso e di costruire la base per realizzare attacchi complessi e persistenti volti tipicamente al prelievo abusivo di informazioni. Talvolta gli attacchi di social engineering sono mirati per operare su larghissima scala, con vari obiettivi criminali, spesso legati all'alimentazione dei blackmarket di dati personali, codici di accesso, numeri di carte di credito, etc.

In funzione della tipologia di attacco, e quindi del target considerato, gli attacchi di SE includono un certo grado di personalizzazione, che, sempre più frequentemente, appare anche nel caso di attacchi su larga scala, complicando pertanto le azioni di contrasto, e aumentando il livello atteso di fiducia da parte della vittima.

I dati sull'efficacia degli attacchi di SE, più di quanto accade per altri attacchi informatici, sono affetti da elevata imprecisione, presumibilmente tendente a sottostimare il fenomeno, sia per la resistenza di aziende o enti pubblici di rivelare di essere stati vittima di attacchi di questo tipo, sia perché non sempre essi si rendono palesi. Vi sono infatti utenti che si dimostrano vulnerabili rispetto ad attacchi di SE ma acquisiscono consapevolezza di avere subito un attacco immediatamente dopo il suo verificarsi ma anche utenti che non percepiscono nulla. Tra i primi, vi è una parte maggioritaria che non denuncia l'incidente subito per il timore di andare incontro a sanzioni o semplicemente per il rischio della perdita di reputazione.

Alcuni degli standard e delle linee guida di riferimento per arginare i rischi di attacchi di SE sono contenute in [51, 52, 53, 54, 37].

Le sfide da intraprendere nel prossimo futuro per mitigare i rischi legati agli attacchi di social engineering possono essere riassunte nelle seguenti azioni:

- Definire politiche e standard condivisi per il rilascio di informazioni sensibili e definire best practices e standard per l'addestramento dei dipendenti e per l'identificazione delle contromisure nei processi organizzativi;

- Realizzare soluzioni software per impedire comportamenti rischiosi dell'utente per offrrire protezione a livello dei provider di servizi internet;

- Adottare strategie di monitoraggio e di verifica della vulnerabilità nei processi aziendali, anche attraverso simulazioni di attacchi, e automatizzare le tecniche per il rilevamento degli attacchi di tipo phishing;

- Definire procedure standard per realizzare sessioni di addestramento personalizzate e specializzate sulle diverse tipologie di attacco.

3.4 Componenti e Sistemi Hardware

Una delle sfide che, come sistema Paese, non possiamo permetterci di ignorare è quella posta dalla "qualità" (dal punto della cyber security) delle componenti hardware impiegate nella realizzazione dei sistemi ai vari livelli, dalla IoT alle Infrastrutture Critiche, dai sistemi Cyber Fisici ai server dalle Pubbliche Amministrazioni centrali e periferiche. È infatti fondamentale accrescere la consapevolezza sul ruolo che le strutture hardware possono giocare, e di fatto già giocano, sia nella fase di difesa dei sistemi in cui sono impiegate, sia come possibili sorgenti o mezzi di attacco verso le medesime.

L'hardware esegue il software e costituisce, di fatto, l'ultima linea di difesa: se un attaccante corrompe l'hardware, tutti i meccanismi introdotti per rendere sicuro il software (a qualsiasi livello) possono rivelarsi inutili. Anche in presenza dei migliori algoritmi crittografici, dei più sofisticati software di intrusion detection, dei più potenti firewall e dei più aggiornati antivirus, un hardware non opportunamente protetto, indipendentemente dal contesto in cui opera, può costituire l'anello debole della catena, diventando una facile porta di accesso al sistema, alle sue funzionalità e ai suoi dati.

Analogamente a quanto avviene per il software, anche nel caso dell'hardware sono state registrate diverse tipologie di attacchi con finalità diverse:

- Attacchi per recuperare dati memorizzati all'interno dei dispositivi: hanno come obiettivo un sistema specifico, al fine di scoprire o recuperare dati segreti e/o sensibili;
- Attacchi per modificare le funzionalità di un sistema: hanno come obiettivo la modifica di un dispositivo (chip) o di una sua peculiare funzionalità (IP core) all'interno del sistema. Esempi tipici sono costituiti da denial of service, aggiunta di funzionalità per fare dello sniffing, etc.;
- Attacchi per recuperare informazioni relative alla progettazione e/o alla fabbricazione di un chip o di un IP core: hanno come obiettivo la contraffazione, la reverse engineering e, in generale, la sottrazione di componenti di proprietà intellettuali (IP) e di informazioni strategiche dal punto di vista industriale.

Ne consegue che anche l'hardware deve essere progettato, costruito, collaudato, usato e manutenuto tenendo conto dei possibili attacchi e delle possibili minacce.

I problemi connessi con la sicurezza dell'hardware (*Hardware Security*) differiscono da quelli dalla sicurezza dei dati, del software, delle reti e delle infrastrutture proprio a causa della diversa natura dell'hardware stesso, qui inteso sia ai vari livelli gerarchici di astrazione (blocchi logici, IP core, chip, piastre, sistemi, ...) sia ai vari tipi di componenti (processori, memorie, dispositivi di in-

gresso/uscita, sensori, attuatori, reti di interconnessione, ...) sia di complessità del sistema (sistemi embedded, mobile, personal, server, cluster, HPC, ...).

Gli aspetti di sicurezza vanno inoltre considerati in tutte le fasi del ciclo di vita dell'hardware stesso (*Hardware Trust*): dalla progettazione alla fabbricazione, dal collaudo (sia a fine produzione sia sul campo) alla dismissione. Occorre al riguardo anche evidenziare come, tranne che in casi molto particolari (tipo quelli rappresentati da sistemi basati su FPGA, con o senza meccanismi di riconfigurazione dinamica parziale), la "vita operativa" dell'hardware sia tipicamente molto maggiore di quella del software, il quale può venire aggiornato, anche con interventi in remoto. Nel caso dei sistemi basati su FPGA con trasmissione dei file di configurazione, tali file sono soggetti alle stesse problematiche della sicurezza del software.

L'hardware, infine, può rilevarsi critico anche al di là della sua "vita operativa" in almeno due contesti diversi. Da un lato, componenti e dispositivi dismessi possono essere attaccati per prelevare dati: è noto, al riguardo, il caso di informazioni riservate estratte in modo fraudolento da fotocopiatrici dismesse dal Pentagono. Dall'altro lato, i dispositivi possono essere ricuperati da apparati dismessi (tipicamente dissaldandoli dalle piastre) ed essere riciclati, ri-immettendoli in modo fraudolento sul mercato, eventualmente dopo averne opportunamente contraffatto il package. Occorre evidenziare come, al di là del danno economico, l'uso di questi componenti "riciclati" abbia gravi conseguenze sulla affidabilità (dependability) dei sistemi in cui vengono ri-impiegati, in quanto, avendo essi ormai raggiunto il termine previsto dal costruttore per la "vita operativa" nominale, la loro probabilità di guasto raggiunge valori tali da compromettere le funzionalità dei sistemi.

Come visto nella sfida a essa dedicata, la Internet-of-Things (IoT) porta ad avere una gran quantità di sistemi hardware immersi (embedded) nei sistemi più disparati e tutti fortemente connessi, tramite interfacce di natura e caratteristiche tra loro molto diverse. Bachi nella sicurezza o eventuali backdoor presenti in uno qualsiasi degli "oggetti" della IoT, al limite anche semplicemente un interruttore "intelligente" per il controllo dell'illuminazione di un locale, o l'interfaccia di un frigorifero, possono, di fatto, diventare una facile porta di accesso a tutto il sistema. D'altro canto, come già evidenziato, eventuali backdoor non sono necessariamente sempre introdotte in modo fraudolento: si pensi, a titolo di esempio, alla necessità di accessi per interventi diagnostici e/o manutentivi remoti).

Non si deve commettere l'errore di ritenere che l'attacco a sistemi hardware sia possibile solo nel caso in cui tali sistemi si trovino fisicamente nelle mani degli attaccanti (come nel caso di cellulari, smart card o sistemi embedded) e che quindi soluzioni Cloud e in generale di Hardware-as-a-Service (HaaS) ne siano immuni. Sono stati infatti recentemente registrati attacchi a server virtuali sfruttando caratteristiche fisiche misurabili del server reali, quali temperature,

frequenze dei clock, cache miss, etc.

Per quanto riguarda le infrastrutture critiche, sono già stati evidenziati, nella sezione precedente, i problemi di sicurezza derivanti dall'impiego di componenti di tipo legacy. Recenti studi hanno evidenziato come l'uso sia di dispositivi hardware non particolarmente innovativi in infrastrutture critiche di tipo "classico" sia di sistemi più moderni e sofisticati in "smart grid" diverse possano rendere tali infrastrutture facilmente vulnerabili ad attacchi esterni anche molto semplici ed elementari.

In conclusione, riteniamo importante incrementare nei policy maker e negli stakeholder la consapevolezza della gravità della minaccia e della rilevanza, anche economica, del problema connessi con l' *Hardware Security and Trust* e sensibilizzare attivamente quanti, a livello nazionale, sono a vario titolo coinvolti nella progettazione, nella produzione e nel collaudo di sistemi hardware. Questo implica coinvolgere, da un lato, i produttori di chip (le Silicon Foundry) e i vari centri di progettazione (i Design Center) attivi sul territorio nazionale e, dall'altro, gli ormai numerosissimi soggetti che impiegano componenti di tipo FPGA sia nella IoT sia in infrastrutture critiche. È importante anche sia sensibilizzare i gestori di infrastrutture critiche e sistemi critici ai vari livelli sia formare esperti (laureati magistrali, specialistici, dottori di ricerca) sulle tematiche di cui sopra.

Riteniamo, infine, che, in linea con quanto già è stato fatto in numerosi paesi, sia importante e non più temporalmente dilazionabile intraprendere le azioni necessarie per dotare il Sistema Paese di due iniziative del tutto innovative, almeno per il panorama italiano:

- La creazione di una struttura (alliance) in grado di fornire, al pubblico e ai privati, analisi, valutazioni qualitative e quantitative, misure dei livelli di sicurezza di componenti, sistemi e infrastrutture hardware, nonché certificazioni e consulenze nella gestione di tutte le fasi del ciclo di vita (definizione dei requisiti, procurement, progettazione, produzione, test, analisi, ...) di infrastrutture hardware.
- L'attivazione di una filiera nazionale completa che, coinvolgendo tutti i soggetti necessari, sia in grado di produrre dispositivi e apparati hardware certificati o comunque dotati delle necessarie garanzie di sicurezza richieste per applicazioni critiche specifiche.

3.5 Biometria

Il riconoscimento di persone o classi di persone o loro comportamenti mediante tecniche biometriche sta assumendo un ruolo crescente in un'ampia varietà di applicazioni nell'ambito della sicurezza fisica e dei sistemi informativi. Il riconoscimento biometrico si basa sull'analisi di tratti biologici (ad esempio:

impronte digitali, volto, iride) o comportamentali (ad esempio: voce, modo di camminare, gesti, firma). Dai tratti raccolti da appositi sensori vengono estratte rappresentazioni (template) che contengono le caratteristiche essenziali dei tratti stessi in modo sostanzialmente invariante rispetto all'acquisizione. In fase di registrazione, il template della biometria selezionata viene archiviato insieme al nominativo della persona e a eventuali altre sue informazioni personali. In fase operativa, il template acquisito per una persona da identificare viene confrontato con i template archiviati: il template uguale, entro una tolleranza predefinita, a quello acquisito in fase operativa identifica la persona in esame. L'accuratezza dell'identificazione si basa sull'unicità del tratto biometrico considerato e sulla possibilità di distinguere template di persone diverse. I tratti biometrici hanno diverse capacità di identificazione: tipicamente, iride, impronte digitali e volto sono i più accurati. La biometria da adottare per una specifica applicazione dipende, in particolare, dal grado di accuratezza nell'identificazione che si desidera ottenere, dalla criticità dell'applicazione stessa, dall'intrusività e dal costo dell'acquisizione, e dalle normative vigenti sulla privacy.

Il riconoscimento biometrico facilita enormemente e rende molto più accurato e sicuro il *controllo degli accessi logici* a sistemi informativi, applicazioni e servizi informatizzati. L'utente non deve più disporre di un oggetto per l'identificazione o ricordarsi un'informazione, ma deve presentare soltanto la propria biometria richiesta per essere identificato. I settori applicativi che possono beneficiare di queste tecniche per facilitare l'accesso, anche attraverso internet, sono numerosi, tra cui commercio elettronico, pagamenti in esercizi commerciali, servizi bancari, sportelli bancari automatici, amministrazione pubblica digitale, sistemi informativi sanitari, sistemi biomedicali, sistemi di assistenza a disabili e anziani, sistemi informativi e di gestione aziendale, sistemi di gestione produzione industriale, sistemi logistici, sistemi per la formazione a distanza, sistemi informativi turistici e culturali, ambienti a realtà aumentata e virtuale, intrattenimento e giochi, e accesso a computer e dispositivi mobili. Tecniche di identificazione biometrica continua o periodica possono essere adottate per assicurare la continuità dell'interazione della persona identificata inizialmente con il sistema informatizzato.

Le tecnologie biometriche sono usate efficacemente anche per il *controllo degli accessi fisici* e per *videosorveglianza*, ad esempio per aree critiche o ad accesso ristretto, controllo delle frontiere (in particolare in porte per controllo automatizzato), aree pubbliche, edifici pubblici, attività di polizia, attività forensi, impianti sportivi, caveau bancari, mostre e fiere, servizi e infrastrutture di trasporto (in particolare in aereoporti).

Un'ulteriore area applicativa emergente e di crescente impatto sulla vita dei cittadini è costituita dall'*intelligenza ambientale*. Le tecniche biometriche possono semplificare l'identificazione della singola persona, di classi di persone o di comportamenti per facilitare l'interazione con l'ambiente e la personalizza-

zione dell'ambiente stesso adattandolo alle loro necessità, preferenze e desideri, proteggendone al contempo le informazioni. L'ambiente che ci circonda è infatti sempre più pervaso da dispositivi, applicazioni e sistemi informatizzati e connessi in sistemi informativi complessi, con i quali interagiamo per utilizzare servizi e gestire situazioni della vita quotidiana. La personalizzazione di tali applicazioni e servizi, e persino la loro costruzione ritagliata esattamente sulle esigenze di ogni persona, è sempre più importante per migliorare la qualità della vita e assicurare una semplice interazione. L'intelligenza ambientale è diretta a sviluppare soluzioni auto-adattative per l'ambiente stesso, mediante apprendimento automatico delle richieste dell'utente, profilazione adattativa dell'utente e memorizzazione delle conoscenze acquisite per il riuso successivo. Applicazioni tipiche possono essere ad esempio in domotica, assistenza a disabili e anziani, smart city, servizi sanitari e farmaceutici personalizzati.

Il riconoscimento biometrico si basa su solide esperienze internazionali, sviluppate anche con il contributo della ricerca italiana. Alcune sfide per il futuro saranno però critiche per assicurare il mantenimento del livello di eccellenza della ricerca italiana nello scenario internazionale e l'uso capillare dei risultati della ricerca in questo settore per la realizzazione di applicazioni avanzate, a beneficio dello sviluppo economico del sistema Italia e delle imprese italiane anche a livello internazionale, nonché del miglioramento della qualità della vita dei cittadini. Le principali sfide da affrontare sono:

Tecniche biometriche con ridotti vincoli operativi: L'obiettivo è la minimizzazione dei vincoli ambientali e operativi imposti per la raccolta di tratti biometrici necessari per assicurare una elevata accuratezza nel riconoscimento. Tra queste sono le tecniche con ridotti vincoli di illuminazione, quelle con procedure di acquisizione minime o assenti (ad esempio sul posizionamento del soggetto da identificare), quelle senza contatto e quelle a distanza.

Approcci multi-modali: L'uso integrato di più biometrie e di tecniche per la loro fusione intelligente può aumentare l'accuratezza e rendere il sistema più robusto e sicuro contro eventuali attacchi.

Protezione dei dati biometrici: L'impossibilità di modificare i tratti biometrici in caso di furto delle biometrie archiviate rende estremamente critica la salvaguardia della sicurezza dei dati biometrici, che non dovrebbero essere conservati o trasmessi se non in modo protetto. Per garantire tale protezione e permettere un'elaborazione efficiente ptranno tornare utili le tecniche di crittografia omomorfa presentate nella prossima sezione.

Privacy biometrica: L'associazione univoca dei tratti biometrici con l'individuo rende sempre più importante dare all'individuo il controllo dell'uso

delle proprie biometrie, specificatamente in applicazioni che non rivestono aspetti critici dal punto di vista della sicurezza nazionale. Lo sviluppo di approcci che trasferiscano all'individuo la proprietà della protezione delle proprie biometrie diventa quindi importante per la diffusione di applicazioni per la vita quotidiana.

Miglioramento dell'accettabilità e dell'usabilità: I cittadini spesso percepiscono l'uso di biometrie come eccessivamente invasivo o di difficile uso o pericoloso in aree geografiche critiche per la diffusione di malattie, anche a causa delle tecniche per la raccolta delle biometrie stesse. Lo sviluppo di tecniche senza contatto e a distanza può ridurre questa percezione e favorire la diffusione dell'uso in applicazioni quotidiane.

Nuovi tratti biometrici: Lo studio dell'uso di nuovi tratti biometrici o di nuovi approcci per l'acquisizione di tratti biometrici noti può aiutare a migliorare l'interazione con i sistemi di acquisizione dei tratti o la non riproducibilità dei tratti biometrici. Tra questi sono i tratti elettrocardiografici, il monitoraggio cardiaco ottico, i tratti elettroencefalografici, l'impronta del palmo, l'analisi iperspettrale di strutture corporee, o il DNA.

Interoperabilità: La confluenza di diverse banche biometriche in sistemi informativi complessi richiede l'adozione di tecniche per la gestione dell'interoperabilità in modo da rendere trasparente l'accesso alle singole banche dati, la gestione flessibile della fusione multimodale in funzione delle biometrie disponibili, la certificazione dinamica dell'accuratezza in funzione della qualità delle informazioni raccolte.

Tecniche biometriche per dispositivi mobili La diffusione di dispositivi mobili (ad esempio: smart phone, tablet) introduce vincoli sull'uso di sensori e tecniche di acquisizione. La disponibilità di tecniche biometriche adeguate permetterà di assicurare l'accesso ad applicazioni in modalità avanzata mediante identificazione biometrica.

Ulteriori dettagli su queste tematiche possono essere trovati in [21] e [26].

3.6 Sistemi Avanzati di Crittografia

La crittografia è uno strumento fondamentale per la sicurezza dei sistemi e delle reti, che permette di trasformare i dati in modo che siano accessibili solo se si conosce una *chiave segreta*. Ogni sistema connesso a una rete accessibile "in chiaro", o senza un adeguato sistema crittografico, può essere vittima di un attaccante di rete, in grado di intercettare tutte le informazioni scambiate, incluse password e numeri di carte di credito.

La crittografia, oltre a proteggere la confidenzialità dei dati, permette di realizzare meccanismi di identificazione forte, non basati su password. Gli *immobilizer* delle moderne automobili, ad esempio, si basano su uno schema di sfida-risposta in cui una sfida casuale inviata dalla centralina viene cifrata dalla chiave fisica dell'automobile utilizzando una chiave di cifratura condivisa con la centralina. La centralina verifica che la risposta cifrata corrisponda e, solo in tale caso, disattiva l'immobilizer. In questo modo, anche se interponiamo una antenna che intercetta lo scambio di messaggi, non siamo in grado di rubare la chiave di cifratura perché essa non viene mai inviata alla centralina.

Tantissimi oggetti che utilizziamo ogni giorno sono, di fatto, dispositivi crittografici: bancomat, carte di credito, smartcard, chiavette per macchine distributrici, SIM dei telefoni, generatori di password usati dalle banche, etc. Quali sono quindi le sfide per i prossimi anni?

Vulnerabilità crittografiche: Nonostante esistano cifrari tuttora inviolati, l'utilizzo della crittografia è complesso e anche una sola componente debole può compromettere tutto il sistema. Un solo meccanismo vulnerabile può permettere di rompere cifrari robusti come RSA in poche ore o minuti [7]. È necessario fare chiarezza e eliminare i meccanismi vulnerabili da dispositivi e librerie crittografiche una volta per tutte. Questo è una sfida particolarmente complessa perché, tra le altre cose, richiede la migrazione di applicazioni datate per le quali non è sempre semplice capire i meccanismi crittografici che utilizzano.

Transizione a cifrari standard: Molti dispositivi crittografici in commercio si basano su cifrari proprietari, tipicamente insicuri. Negli ultimi anni sono stati violati innumerevoli dispositivi tramite tecniche di ingegneria inversa che hanno permesso di ricavare l'algoritmo crittografico, per poi analizzarlo [24, 78]. Le industrie si stanno muovendo verso cifrari standard come AES e RSA ma la transizione non è semplice. È noto che le implementazioni di cifrari standard possono essere soggette a diversi attacchi basati su effetti collaterali, quali il tempo di esecuzione e il consumo energetico [77]. Questa sfida richiede un'analisi accurata delle implementazioni dei cifrari ed è un ambito di potenziale collaborazione tra industria e mondo accademico.

Hardware crittografico: Qualsiasi ente o azienda che faccia uso importante della crittografia ne delega la realizzazione a sistemi hardware, noti come Hardware Security Modules (HSMs). Sono sistemi resistenti all'intrusione progettati per proteggere le chiavi crittografiche eseguendo tutte le operazioni sensibili direttamente all'interno del dispositivo. Un attacco su questi dispositivi, noto come *wrap-decrypt* [14], si basa sulla richiesta al dispositivo di esportare una chiave cifrandola con un'altra chiave di cifratura (wrap), allo scopo, per esempio, di importarla in un altro dispo-

sitivo. L'attacco procede chiedendo di decifrare il testo cifrato (decrypt) ottenendo la chiave in chiaro. In [10] è stato dimostrato che questi attacchi sono possibili su dispositivi commerciali e c'è evidenza che questi attacchi siano stati sferrati negli ultimi anni[14]. Abbiamo avuto modo di constatare che, a livello internazionale, sta aumentando la sensibilità per i problemi legati all'uso della crittografia, soprattutto in ambito bancario e governativo[15]. In Italia, questo tipo di problematiche è ancora considerato secondario rispetto a vulnerabilità più classiche a livello di rete, sistemi e applicazioni.

Crittografia nel cloud: I problemi di sicurezza nel cloud ricevono sempre più attenzione e si ha sempre più consapevolezza dei possibili rischi e minacce impliciti nel loro uso. In tale scenario, infatti, i propri dati e la loro riservatezza, sono interamente affidati al provider del cloud. La soluzione ovvia di cifrare i propri dati prima di trasferirli nel cloud e di decifrarli nel trasferimento inverso, anche se già offerta in soluzioni commerciali, presenta diverse criticità. In primo luogo, è assolutamente essenziale che il fruitore di un servizio cloud non affidi le proprie chiavi private al provider del cloud ma le gestisca all'interno dei propri sistemi. Affidare la gestione delle proprie chiavi al provider del cloud è un po' come come lasciare oggetti di valore in una camera di hotel: sono al sicuro fintanto che il personale dell'hotel si comporta onestamente.

Ma la sfida più complessa resta quella di utilizzare o analizzare tali dati sul cloud: nelle soluzioni attuali è necessario decifrarli o spostarli all'interno dei propri sistemi, senza quindi sfruttare a pieno le capacità offerte dal cloud. Esistono nuovi approcci che risolverebbero questo problema, come ad esempio la cifratura omomorfica di Craig Gentry [27], che consente di operare su dati cifrati, ottenendo gli stessi risultati delle medesime operazioni svolte sui dati in chiaro. Utilizzando tali tecniche, si potrebbe quindi fare in modo di operare ed eseguire applicazioni su dati memorizzati nel cloud senza doverli mai decifrare o spostare. Sfortunatamente, tali tecniche sono molto complesse a livello computazionale, e quindi rimangono ancora di interesse puramente teorico. Gli esperti prevedono però che nel futuro saranno disponibili implementazioni di cifratura omomorfica di interesse pratico utilizzabili in scenari concreti.

In conclusione, riteniamo strategiche le seguenti sfide:

1. Attivarsi, a livello nazionale e internazionale, affiché ci sia un uso più consapevole dei sistemi crittografici, che porti a una eliminazione pro-

[14] Famoso il caso RBS WorldPay `http://www.wired.com/2009/11/rbs-worldpay/`. Si veda `http://cryptosense.com/real-hsm-breaches/` per una panoramica su questi attacchi.

[15] `http://www.cryptosense.com`

gressiva di meccanismi obsoleti e vulnerabili e a una adozione, sempre maggiore, di sistemi di cifratura standard;

2. Elevare lo standard di sicurezza dei sistemi crittografici presenti sul mercato tramite strumenti di analisi, verifica e certificazione, riconosciuti a livello governativo;

3. Continuare, all'interno della comunità scientifica, la ricerca teorica di nuovi algoritmi crittografici che permettano di applicare la crittografia in ambiti finora inesplorati quali, ad esempio, la computazione su dati cifrati nel cloud.

3.7 Protezione di Internet

La rete Internet, una volta usata quasi solo per scopi di ricerca o di svago, è ormai diventata una componente indispensabile di qualunque servizio informativo, inclusi quelli a supporto delle infrastrutture critiche. Purtroppo il progetto iniziale di Internet ha privilegiato la funzionalità alla sicurezza e quindi ci troviamo ad affrontare molteplici rischi dovuti a questa insicurezza di base insita nella rete stessa. Questo problema è tipicamente poco compreso da chi sviluppa e gestisce i servizi informativi ed è quindi ancora più grave perché trascurato.

Come ben noto, Internet non è una rete reale ma un'astrazione logica. In realtà i dati vengono trasmessi tra reti adiacenti che hanno accordi specifici (cosiddetti di "peering") per inoltrare il traffico verso una certa destinazione. Questo comporta la necessità di protocolli per scambiarsi le informazioni circa la strada migliore da seguire per raggiungere una certa rete (cosiddetti annunci di "routing"). I protocolli si basano sulla fiducia e la buona fede, ossia assumono che gli apparati di rete (i router) non forniscano informazioni false ma annuncino solo ed esclusivamente le reti a cui sono effettivamente collegati. Purtroppo nell'odierno scenario mondiale, carico di tensioni sociali, economiche e politiche, queste assunzioni sono spesso non verificate. È eclatante il caso avvenuto ad Aprile 2010 in cui un router di China Telecom (il maggiore fornitore Internet della Cina ed uno dei più grandi al mondo) ha fatto un annuncio errato che per circa 20 minuti ha obbligato il 15% del traffico totale di Internet a passare attraverso la Cina, con ovvie possibilità di lettura e anche manipolazione. Questo problema ha colpito molti paesi al mondo, tra cui circa 10.000 reti USA (incluse quelle militari) e 100 reti italiane. È argomento di discussione se si sia trattato di un errore di un sistemista o di un attacco deliberato, comunque questo evento è una prova dell'insicurezza nell'instradamento dei pacchetti in Internet.

A partire dall'anno 2000 sono state proposte varie estensioni di sicurezza (quali SBGP, soBGP e IRV) al protocollo BGP usato per gli annunci di routing, ma la comunità scientifica non ha ancora deciso quale sia la soluzione più efficiente

e ciò ne ritarda l'adozione su larga scala. Attualmente i gestori delle reti effettuano localmente un filtraggio degli annunci ricevuti, cercando di individuare annunci errati o "illogici" (ad esempio dovrebbe risultare illogico che il traffico tra Roma e Milano passi attraverso un paese diverso dall'Italia). Questi filtraggi sono però insufficienti a garantire la completa protezione delle informazioni di instradamento ed è quindi necessaria una protezione più strutturata. Per il governo USA la messa in sicurezza del routing è una parte imprescindibile della strategia nazionale per proteggere la rete, ma non risulta in corso uno sforzo analogo a livello Europeo e tanto meno Italiano, esponendo così a grossi rischi sia i servizi sia gli utenti di questi paesi.

Anche il percorso fisico dei dati dovrebbe essere oggetto di particolari attenzioni: quando si acquisisce un servizio di comunicazione, rivolto a un servizio critico o sensibile, sarebbe opportuno verificare o imporre contrattualmente che il traffico passi esclusivamente su cavi e apparati di rete collocati in territorio Italiano, ma questa è una cosa a cui pochi prestano attenzione, esponendo così le comunicazioni ad attacchi da parte di persone situate all'estero.

Un ulteriore problema di Internet è la falsificabilità delle informazioni relative al mittente di un pacchetto o di un messaggio per effettuare attacchi verso un bersaglio nascondendo l'autore dell'azione. Quest'abilità viene sfruttata negli attacchi di tipo DDOS (Distributed Denial Of Service) che mirano a generare così tanto traffico o richieste di servizio da rendere un server inutilizzabile. Ad esempio, nel 2014 questi attacchi sono stati capaci di generare in media un traffico di 59 Gbps (miliardi di bit al secondo) e di 15 Mpps (milioni di pacchetti al secondo) contro un singolo bersaglio, cosa difficilmente sopportabile anche dai server più robusti e dalle reti più moderne. Giganti commerciali, quali Microsoft e Sony, sono stati oggetto di questi attacchi: a Natale 2014 le reti di gioco legate alle console Xbox e Playstation sono state rese inutilizzabili da un attacco DDOS, rovinando le feste ai giocatori e colpendo la reputazione delle aziende. Gli attacchi DDOS colpiscono anche i server legati a enti governativi, talvolta come parte di azioni di disobbedienza civile in rete (il cosiddetto "hacktivism", cui in Italia in passato è stato soggetto il sito del Ministero della Giustizia).

Contro questi attacchi, oltre a filtrare tempestivamente il traffico "anomalo" (in base alla quantità generata e alla sua tipologia), sarebbe molto utile poter individuare gli autori dell'attacco e disporre di capacità di calcolo e di trasmissione aggiuntiva, per far fronte ai picchi dovuti agli attacchi.

Per il primo punto, i fornitori di accesso Internet dovrebbero filtrare i pacchetti di rete con mittente palesemente falso (ossia non appartenente a una delle reti del fornitore) nonché attivare meccanismi di "traceback" per permettere di tracciare in tempo reale il percorso dei pacchetti usati per l'attacco. Purtroppo questi meccanismi sono implementati da pochi fornitori di accesso Internet mentre, data la composizione come rete-di-reti di Internet, sarebbe necessario che venissero adottate da tutti i fornitori in modo coordinato. Un attacco tipi-

camente attraversa varie reti prima di raggiungere il bersaglio finale, anche allo scopo di far perdere le proprie tracce.

Per il secondo punto, data l'attuale tendenza a usare sempre più servizi cloud (facilmente riconfigurabili) si potrebbe pensare a un accordo di cooperazione tra amministrazioni diverse per supportarsi reciprocamente in caso di attacchi DDOS, condividendo la banda di rete e/o la capacità di calcolo, così da aumentare tempestivamente la resistenza all'attacco (nell'attesa che venga identificata e bloccata la sorgente dello stesso).

Non si può fare poi a meno di citare un ultimo rilevante problema di Internet, relativo all'identificazione dei nodi di rete. In Internet i server sono identificati da nomi simbolici (come `www.agid.gov.it`) per facilitarne la comprensione da parte degli utenti, ma le comunicazioni in rete usano i cosiddetti indirizzi IP, sequenze di quattro numeri (come `89.97.56.10`) che identificano univocamente un nodo di rete. È compito del sistema DNS (Domain Name System) effettuare la traduzione da nomi a indirizzi. Purtroppo i messaggi scambiati tra i componenti del DNS non sono protetti ed è quindi possibile per un attaccante falsificare le risposte. In questo modo le comunicazioni degli utenti vengono dirottate verso server fraudolenti che forniscono informazioni errate oppure catturano informazioni sensibili (ad esempio i codici di accesso a un sistema, sostituendosi alla sua pagina di login).

Per risolvere questo problema è stato sviluppato il sistema DNSSEC, un'estensione del DNS che sfrutta una struttura di firme digitali per garantire l'autenticità e l'integrità delle associazioni nome-indirizzo e impedire quindi i succitati attacchi. L'attivazione di DNSSEC è in forte crescita. Nel 2008 gli USA hanno deciso che tutti i domini governativi (ossia quelli sotto `.gov`) devono obbligatoriamente essere protetti da DNSSEC: la zona radice è stata firmata nel 2010, così come avvenuto per il dominio Europeo `.eu`. L'Italia purtroppo non ha ancora provveduto ad attivare DNSSEC sul dominio `.it`, lasciando così vulnerabili tutti i sottodomini registrati in quest'ambito, fra cui `.gov.it`.

È infine utile menzionare alcune preoccupazioni relative all'infrastruttura logica su cui poggiano molte applicazioni fruibili attraverso Internet (le applicazioni Web), che sono soggette a utilizzi impropri, se non attacchi, da parte di numerosi soggetti operanti sulla rete. Oltre alle classiche esigenze della sicurezza delle informazioni (confidenzialità, integrità, autenticazione), ne emergono ulteriori, legate alle vulnerabilità delle applicazioni Web derivanti da input impropri, inattesi o maliziosi. Tramite l'opportuna somministrazione di input "avvelenati", soggetti malintenzionati potrebbero ottenere funzioni non legittime dalle applicazioni, mandarle in errore, effettuare furti di credenziali e, più in generale, attaccare altri utenti della stessa applicazione. Lo standard TLS (evoluzione dell'obsoleto SSL) è un utile strumento per supportare la sicurezza delle informazioni nelle applicazioni Web, e permette la modalità di interazione "sicura" nota come HTTPS. Questa modalità può essere utilmente impiegata anche per

contrastare abusi che, attraverso la somministrazione di input avvelenati o specifiche tecniche di scripting, possono portare al furto di credenziali e al furto di identità. L'impiego di una interazione completamente basata su HTTPS che si interrompe in presenza di comunicazioni, anche parziali, non basate su TLS può utilmente limitare l'occorrenza di questi attacchi. Tale politica è l'oggetto dello standard HSTS (HTTP Strict Transport Security), attualmente utilizzato in modo non sistematico, ma su base volontaria. Uno strumento collegato è la CSP (Content Security Policy), che permette all'applicazione Web di elencare esplicitamente le terze parti autorizzate a far parte dell'applicazione, stabilendo implicitamente che tutte le altre possibili terze parti non sono autorizzate.

In conclusione, per migliorare il livello di sicurezza della Internet italiana, si raccomanda di:

- Attivare il DNS sicuro sui principali domini, non solo governativi, ma anche quelli di servizi pubblici o privati importanti, come quelli bancari o dei trasporti;
- Creare un sistema di monitoraggio sui percorsi di rete (ossia gli annunci di routing) per verificarne l'attendibilità, nell'attesa di un protocollo sicuro relativo a questa problematica, da implementarsi non appena disponibile;
- Definire sistemi di cooperazione e ridondanza (anche tra amministrazioni o fornitori diversi) per incrementare dinamicamente la capacità di trasmissione e di elaborazione a fronte di attacchi massicci;
- Creare sistemi per il tracciamento degli attacchi, sia per bloccarli alla fonte sia per perseguire i responsabili;
- Definire clausole contrattuali per garantire che il traffico interno all'Italia transiti su cavi e apparati collocati sul suolo Italiano e verificare periodicamente il rispetto di questa clausola;
- Individuare categorie di applicazioni e di organizzazioni istituzionali che dovrebbero essere obbligate a fornire applicazioni Web basate su HSTS e CSP, obbligandole all'impiego di tali standard.

3.8 Protezione dell'Informazione

La rapida evoluzione che negli ultimi anni ha caratterizzato l'ICT (Information and Communication Technology) ha avuto, e continua ad avere, un profondo impatto sulla società in cui viviamo, sul modo in cui lavoriamo, sulle nostre relazioni sociali e perfino su aspetti della vita quotidiana non immediatamente visibili. La disponibilità pressoché ovunque di reti wireless aperte al pubblico

ha favorito lo sviluppo e una continua e rapida diffusione di dispositivi di vario tipo in grado di connettersi a Internet, dagli smartphone fino ai più recenti dispositivi indossabili (wearable device). Questi dispositivi sono in grado di generare, raccogliere e condividere grandi quantità di dati spesso personali. In aggiunta a questo fenomeno, Internet e l'uso che ne facciamo è mutato notevolmente negli anni. Siamo, infatti, passati da uno scenario dove Internet era visto come un grande archivio di dati e di servizi a disposizione degli utenti, a uno scenario dove gli utenti hanno un ruolo attivo di produttori di contenuti personali (foto, video, blog). Questo cambiamento è stato facilitato anche dallo sviluppo di applicazioni sociali che permettono, ad esempio, la creazione di comunità online nelle quali gli utenti possono trovare altri utenti con interessi simili, discutere di problemi comuni o semplicemente memorizzare o rendere accessibili risorse personali. Facebook, Twitter e i vari servizi di Google, da Google+ a YouTube, sono solo alcuni degli esempi maggiormente noti di questa tendenza. Tutto questo ha portato allo sviluppo di una società digitale nella quale uno dei pilastri è l'*informazione*.

La quantità di dati e informazioni disponibili in rete è in costante aumento anche per lo sviluppo di nuovi modelli e tecnologie di memorizzazione, elaborazione e condivisione delle stesse. Basti pensare alla tendenza – destinata ad aumentare nel prossimo futuro – a trasferire dati, documenti e informazioni sul cloud. I vantaggi che derivano dall'utilizzo di queste nuove tecnologie sono molteplici: la facilità di fruizione delle informazioni che diventano disponibili con un semplice click del mouse, le economie di scala di cui si usufruisce e la maggiore sicurezza e affidabilità dei servizi offerti da terze parti. Questa propensione nell'utilizzare le nuove tecnologie del cloud non riguarda esclusivamente gli utenti ma coinvolge anche soggetti pubblici, banche e operatori telefonici (solo per nominarne alcuni), con la conseguenza che banche dati con informazioni sensibili e di valore strategico sono trasferite in server che sono al di fuori del nostro controllo diretto, spesso senza sapere né dove i dati siano effettivamente memorizzati né quali organizzazioni siano coinvolte nella loro gestione. Tutto questo introduce numerosi interrogativi sulla sicurezza e sulla protezione dei dati e delle informazioni. Quali garanzie abbiamo che le nostre informazioni sensibili siano propriamente protette? Quali mezzi abbiamo per controllare chi accede alle nostre informazioni? Qual'è la reale consapevolezza degli utenti sui rischi che potenzialmente derivano dall'uso delle nuove tecnologie?

L'importanza del tema si evince anche da una relazione pubblicata nel Marzo 2015 dal Garante Europeo per la Protezione dei Dati Personali (European Data Protection Supervisor) che identifica i tre obiettivi strategici alla base delle sue azioni per i prossimi cinque anni (2015-2019)[16]. Tra questi obiettivi figura la *protezione dei dati personali nell'era digitale*, prestando anche attenzione ai

[16] `https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Strategy2015`

fenomeni del Cloud Computing, dei Big Data e dell'Internet of Things. La protezione dei dati è, infatti, fondamentale per dare agli utenti un senso di fiducia nei servizi online, favorendo così la crescita economica e la competitività delle imprese.

È interessante osservare che il tema della protezione dei dati e delle informazioni deve essere affrontato considerando anche aspetti legali, economici e sociali di sensibilizzazione degli utenti, tutti aspetti che hanno comunque bisogno di poggiarsi sulla disponibilità di soluzioni tecnologiche. La comunità di ricerca e sviluppo ha dedicato diversi sforzi per la realizzazione di queste soluzioni tecnologiche, molte delle quali si basano sull'assunzione che sia sufficiente criptare i dati proteggendoli così da occhi indiscreti [18, 68]. Esistono, ad esempio, diverse applicazioni che permettono agli utenti di criptare i dati e di tenere nascosta la chiave di crittazione per poi trasferire i dati crittati nel cloud. Se da un lato queste soluzioni proteggono i dati anche dal provider che li memorizza, dall'altra è più difficile sfruttare le funzionalità del cloud, per l'impossibilità, da parte del provider, di accedere ai dati in chiaro. Per ovviare a questo inconveniente è possibile consegnare tutti i nostri dati in chiaro a un provider che potrà poi usare la crittografia per proteggerli in memorizzazione o durante il loro trasferimento da una parte all'altra della rete. Questo però richiede di porre *piena fiducia* nel provider e nella sua capacità di gestire correttamente i dati. La sfida che dovrà essere affrontata negli anni a venire avrà quindi come obiettivo primario, quello di superare le limitazioni di queste soluzioni. In particolare, alcuni aspetti chiave che dovranno essere affrontati sono i seguenti.

Empowerment degli utenti: I proprietari dei dati dovranno diventare cittadini di primo livello della società digitale. A tal fine, l'obiettivo sarà lo sviluppo di soluzioni che permettano loro di definire delle politiche di accesso in modo da porre delle restrizioni su chi può accedere ai propri dati personali, per quale scopo e come, e se questi dati possono essere condivisi con terze parti. Tali restrizioni dovranno tenere in considerazione diversi fattori quali, ad esempio, il contesto applicativo, la sensibilità delle informazioni stesse e il grado di fiducia del ricevente dei dati. Inoltre, dovranno essere considerati aspetti peculiari dello specifico scenario nel quale si troveranno a operare i proprietari dei dati. Ad esempio, nell'ambito di applicazioni sociali, alcune informazioni (quali, ad esempio, una foto di gruppo) possono riferirsi a più persone, che dovranno poter regolamentare l'accesso alla informazione condivisa, prevedendo così meccanismi di composizione di politiche e di risoluzione di conflitti.

In aggiunta alla protezione delle informazioni da chi non ha i permessi per conoscerle, sono aspetti altrettanto importanti quelli legati all'integrità dei dati e alla verifica del soddisfacimento dei requisiti di sicurezza (i dati devono sempre essere memorizzati con una cifratura robusta ad attacchi basati su frequenza) e alla qualità dei servizi adottati per la ge-

stione dei dati. Questo richiederà lo sviluppo di tecniche che permetteranno agli utenti di verificare in ogni istante l'integrità e la disponibilità dei propri dati e il soddisfacimento dei requisiti di sicurezza e di qualità concordati con il fornitore dei servizi utilizzati.

Gestione sicura dei dati: La presenza sul mercato di molteplici provider che offrono servizi di memorizzazione e di computazione può essere vista come un'opportunità da sfruttare per ottenere servizi migliori e più sicuri. Tale diversificazione introduce comunque nuovi problemi. Infatti, diversi provider offrono servizi che variano per il grado di affidabilità, scalabilità, disponibilità e sicurezza e diventa quindi difficile scegliere il servizio più vantaggioso e sicuro rispetto alle proprie esigenze. Sarà quindi necessario disporre sia di modelli per esprimere e ragionare sui requisiti di protezione dei propri dati, sulle garanzie di sicurezza, sulla fiducia dei provider e sulla funzionalità e convenienza economica, sia di tecniche per la scelta del provider che meglio risponde a tali requisiti.

Consapevolezza dei rischi di privacy: Alcuni dei problemi di violazione della privacy degli utenti derivano dal fatto che spesso gli utenti stessi non si rendono conto dei rischi a cui vanno incontro quando decidono di rendere pubbliche certe informazioni. L'obiettivo sarà quindi quello di sviluppare delle soluzioni che possano segnalare agli utenti i possibili rischi derivanti dal rilascio di specifiche informazioni personali, tenendo conto delle informazioni già rilasciate, della conoscenza e dei mezzi che un potenziale osservatore potrebbe sfruttare per violare la privacy o per inferire informazioni sensibili.

Accesso ed elaborazione sicura dei dati: L'uso della crittografia per proteggere i dati rende più difficoltosa e complicata da parte del provider detentore dei dati l'esecuzione di elaborazioni. Sarà quindi necessario sviluppare soluzioni efficienti e sicure di accesso ai dati crittati che possano essere adottate in scenari moderni, dove gli utenti possono utilizzare un "thin client" con, ad esempio, limitata capacità computazionale e che siano in grado di adattarsi dinamicamente allo specifico contesto di interazione tra utente e provider detentore dei dati. In aggiunta al problema dell'accesso sicuro ed efficiente dei dati, c'è anche da considerare che spesso i risultati di un'elaborazione sono alla base di decisioni che possono avere un forte impatto economico. Per questo motivo, sarà fondamentale avere tecniche in grado di verificare la correttezza, completezza e la freschezza di elaborazioni anche complesse che coinvolgono più parti e che sfruttano architetture distribuite che, tipicamente, sono al di fuori del controllo di chi poi utilizza i risultati di tali elaborazioni.

Protezione della privacy delle interrogazioni: In alcuni scenari né i dati né gli utenti che accedono a tali dati hanno particolari requisiti di protezione,

mentre sono le interrogazioni che devono essere protette. Si pensi, ad esempio, al caso in cui un utente sia interessato ad accedere a informazioni sulle cure per una specifica malattia. Sapendo il tipo di dati ricercati, un osservatore potrebbe facilmente inferire che l'utente (o una persona a esso vicina) soffre della malattia oggetto dell'interrogazione. L'obiettivo sarà quindi quello di sviluppare tecniche che siano in grado di proteggere sia il singolo accesso sia sequenze di accessi, nascondendo così quali sono i dati cui è stato fatto accesso agli occhi di un qualsiasi osservatore, incluso il provider che memorizza i dati stessi.

3.9 Riduzione delle superfici di attacco

La scomparsa dei perimetri aziendali e la permeabilità degli stessi costituisce una delle principali vulnerabilità dei sistemi informatici di tutte le aziende e organizzazioni. Il consolidamento consente una razionalizzazione dei costi e migliora, se ben realizzato, il livello di sicurezza e affidabilità dei sistemi e dei servizi informatici. Tale processo si muove su scale diverse: dalla riduzione di molteplici centri di elaborazione in pochi data center ben presidiati, al consolidamento infrastrutturale all'interno di ciascun data center, fino al consolidamento del sistema informatico a livello logico e gestionale.

La diffusione degli strumenti e applicazioni informatiche dei decenni passati ha portato a una distribuzione dei server e dei servizi che, non potendo godere al tempo di reti a elevata capacità, robustezza e capillarità, sono stati replicati e installati in prossimità dei clienti. Tale situazione ha creato problemi di gestione, di inaffidabilità e di insicurezza oggi non più tollerabili. Il trend si è potuto invertire grazie al miglioramento infrastrutturale di Internet e alle accresciute capacità computazionali dei server, che stanno portando a un consolidamento delle infrastrutture e dei servizi in aree protette, con connessioni e alimentazioni ridondate e con personale competente preposto alla gestione [25]. Tutte le grandi organizzazioni, a esclusione di quelle che erogano servizi a milioni di utenti, si stanno concentrando su non più di 3-4 data center espandibili. I Dipartimenti del Governo Federale degli Stati Uniti e grandi aziende, quali Lockheed Martin e Boeing, rappresentano esempi guida. Simili azioni stanno avvenendo in nord Europa. Direttive da parte della Commissione Europea (ad esempio, "Sfruttare il potenziale del cloud computing in Europa" – Comunicazione COM 529 del 27.9.2012) e iniziative AgID ("Razionalizzazione del Patrimonio ICT PA" – dicembre 2014) vanno nella medesima direzione. Nel momento in cui la digital transformation sta coinvolgendo tutti i settori privati e pubblici, il trend di mercato conferma una preferenza verso il consolidamento. In pratica, la trasformazione in atto sarà realizzata prevalentemente mediante servizi implementati da cloud privati (on premise o esterni) e pubblici. In Italia, si scon-

ta qualche ritardo storico, ma anche nel nostro Paese il mercato del cloud è in continuo aumento, con una crescita tendenziale superiore al 30% negli ultimi tre anni, che ha consentito si superare il miliardo di euro nel 2014[17].

Nell'ambito del singolo data center, i processi di consolidamento sono tipicamente basati sull'adozione di soluzioni di virtualizzazione, inizialmente a livello di server, più recentemente anche a livello di rete e storage. Tali sistemi consentono di concentrare in un numero limitato di dispositivi fisici una quantità elevata di servizi precedentemente erogati da server dedicati e utilizzati al di sotto del 25%. I benefici che ne derivano, valutabili in termini di riduzione dei costi, maggiore utilizzazione delle risorse, bilanciamento automatico, alta affidabilità, minori consumi energetici, semplificazione di gestione, sono evidenti. Gli effetti positivi di un simile trend si riverberano sulla sicurezza, in quanto virtualizzazione e concentrazione degli asset in pochi data center ben presidiati facilitano il controllo delle informazioni a livello fisico e logico. Al contrario, in assenza di consolidamento, le architetture dei sistemi informatici diventano rapidamente complesse e frastagliate e anche il mantenimento di un database aggiornato del patrimonio IT può diventare proibitivo: in assenza di informazioni sulle risorse da proteggere e della relativa importanza e criticità per le linee di business, la sicurezza è impossibile da garantire.

Il consolidamento delle risorse fisiche, tuttavia, è solo un primo passo, del tutto insufficiente se non integrato con azioni di consolidamento logico in termini di maggiore controllabilità, separazione di competenze e omogeneità di gestione. I sistemi consolidati si prestano più facilmente all'integrazione di strumenti di logging e auditing centralizzato in grado di garantire una visibilità completa delle attività di tutti gli utenti. Simili soluzioni sono fondamentali per rilevare tentativi di attacco, sia esterni sia interni, e per azioni di gestione incidenti e investigazioni successive a un incidente informatico. Un auditing a granularità fine delle attività degli utenti consente di censire, limitare o proibire l'utilizzo di canali di comunicazioni spesso utilizzati da utenti interni anche per uso lavorativo, quali servizi di chat, file sharing e cloud storage. Il ridotto numero e concentramento di sistemi hardware e software consente una limitazione del numero di amministratori dotati di privilegi elevati con possibilità di accesso ad aree critiche e aumenta l'efficacia dell'assessment. Analoghi benefici derivano dalla minore necessità di intervento di aziende esterne e di consulenti su cui è difficile esercitare un controllo accurato. Questa impossibilità sta correttamente portando le aziende a una radicale riduzione del numero di fornitori, che saranno tipicamente rappresentati da poche grandi aziende, cui si chiedono certificazioni e adeguamenti a standard, e piccole aziende per servizi verticali molto specialistici.

[17] Dati Assinform, Marzo 2015.

3.10 Progettazione di Sistemi Informativi Complessi

La riduzione della superficie d'attacco rappresenta certamente un passo importante per aumentare la protezione dei sistemi informatici. Un'altro caposaldo è la progettazione resiliente di questi ultimi. Un sistema informatico resiliente ad attacchi deve, infatti, essere in grado di mantenere la disponibilità dell'informazione anche quando è sotto attacco. A tal fine, è necessario replicare l'informazione e mai tenerla centralizzata in un sol luogo. In questo modo il servizio può essere comunque erogato anche se un attaccante prende il controllo di alcune repliche. Un attacco può avere molteplici scopi: bloccare un servizio o, peggio, comprometterne l'integrità dei dati gestiti.

Nel primo caso, per l'avversario può essere sufficiente impossessarsi di una replica per riuscire a bloccare il servizio simulando il guasto di una macchina. Infatti, a seconda dello schema di replicazione utilizzato, può essere necessario dover garantire che tutte le repliche siano allineate per garantire la corretta esecuzione del servizio. Tuttavia, se il servizio viene replicato poggiandosi su un'infrastruttura di comunicazione che non è in grado di garantire ritardi certi nella comunicazione, la verifica dell'allineamento delle repliche è impossibile e il servizio si blocca non appena una replica diventa silente.

Nel caso in cui l'avversario voglia compromettere l'integrità dei dati, se le repliche si scambiano messaggi su sistemi che assicurano limiti netti ai tempi di comunicazione, la perdità di integrità del dato avviene quando l'attaccante è in grado di controllare la maggioranza delle repliche. Da notare che questo valore decresce a un terzo delle repliche quando queste sono interconnesse attraverso canali di comunicazione che non garantiscono certezze sui tempi di consegna dei messaggi. In conclusione, più il sistema di comunicazione ha latenze non predicibili, più l'attaccante è facilitato nell'opera di compromissione dell'integrità dei dati.

La replicazione di dati introduce un'ulteriore problematica correlata alla gestione della coerenza delle repliche. In genere, se si vuole alta disponibilità di servizio, la coerenza delle repliche deve essere più lasca. Questo implica che degli utenti che chiedono accesso al dato, potrebbero leggere dati che non sono aggiornati (coerenza debole). Se si vuole fare in modo che il dato ritornato possa essere sempre l'ultimo scritto (coerenza forte), il sistema si dovrà bloccare se, ad esempio, per qualche motivo, in un determinato istante, solo una minoranza delle repliche sono interconnesse. Ritardando l'esecuzione della lettura o scrittura del dato fino a quando una maggioranza di repliche si riconnette. Da notare che se le repliche sono controllate da un'attaccante questa riconnessione potrebbe non avvenire mai e quindi portare a un blocco del servizio anche nel caso in cui il sistema di comunicazione sottostante assicuri tempi di comunicazione veloci tra le repliche.

Tutto ciò che è stato descritto in modo semplice appena sopra non è che un insieme di principi fondamentali su cui si basano applicazioni distribuite come i moderni Data Center e tutti i sistemi informativi complessi.

Tra questi principi fondamentali va sicuramente menzionata l'impossibilità di raggiungere un consenso in un sistema distribuito asincrono in presenza anche di un singolo nodo guasto (FLP impossibility result [22]) e l'impossibilità di raggiungere un consenso in un sistema distribuito asincrono in presenza di un terzo o più di nodi controllanti da un'attaccante (Byzantine Generals [38]) o il risultato che lega l'interrelazione tra consistenza e disponibilità in sistemi distribuiti soggetti a partizionamenti della rete, noto come CAP Theorem [28], che mostra l'impossibilità di avere sistemi disponibili e a consistenza forte se il sistema distribuito si può partizionare. Estreme semplificazioni di questi concetti portano ai sistemi di disaster-recover dei quali solo adesso si inizia a sentire l'importanza per la continuità di servizio.

Benché alcuni di questi risultati siano noti a tutta la comunità scientifica da trent'anni, essi non fanno ancora parte del bagaglio culturale dell'ingegnere e dell'informatico medio che definiscono i requisiti o peggio progettano grandi sistemi informativi complessi. Questo rende particolarmente agevole il ruolo degli attaccanti che possono riuscire a entrare nei sistemi e a bloccare i servizi in modo relativamente semplice grazie alla loro conoscenza di questi risultati e alla loro capacità di volgerli a proprio vantaggio.

Capire e padroneggiare questi concetti non è semplice e porta alla creazione di sistemi sempre più complessi in funzione del tipo di minaccia alla quale si vuole resistere. Questo non piace alle aziende informatiche poiché questo richiede l'assunzione di personale con abilità molto elevate, aumentando così i costi e diminuendo i profitti nel breve periodo. D'altra parte a volte le aziende non hanno colpe, poiché queste cose molto spesso vengono ignorate all'interno di capitolati di gara redatti, a volte, da persone senza competenze informatiche che così provocano danni elevatissimi al sistema paese. La colpa di questa mancanza di trasferimento tecnologico ricade però anche sul corpo accademico poiché spesso questo si richiude in un atteggiamento elitario senza confrontarsi con le sfide importantissime che la realtà propone.

3.11 Poligoni Virtuali per Esercitarsi sulla Sicurezza

L'aggiornamento degli strumenti e del personale preposto alla difesa dello spazio cibernetico è necessario ma non sufficiente: a causa dell'incessante evoluzione tecnologica si impone anche l'innovazione continua delle tecniche e delle strategie di difesa al fine di anticipare le minacce future.

Il problema non è limitato alla sfera civile, ma interessa in modo importante anche la Difesa. Già nel 2010 il NATO Strategic Concept [49] osservò che gli at-

tacchi cyber "stanno diventando più frequenti, meglio organizzati e più costosi" e "possono raggiungere un livello tale da minacciare la prosperità, la sicurezza e la stabilità nazionale ed Euro-Atlantica". In risposta a questa sfida, la NATO organizza annualmente e coordina lo svolgimento di Locked Shields, un'esercitazione finalizzata a potenziare le capacità di difesa cibernetica delle nazioni partecipanti. All'ultima edizione di Locked Shields (2015) hanno partecipato 16 squadre di esperti in rappresentanza di altrettante nazioni (inclusa l'Italia). Le esercitazioni vengono condotte utilizzando il Cyber Range del Cooperative Cyber Defence Centre of Excellence (CCDCOE) della NATO in Estonia.

I *Cyber Range – Poligoni Virtuali* – sono sofisticati sistemi di elaborazione che grazie alla tecnologia della virtualizzazione consentono di simulare sistemi ICT di complessità reale. Oltre a supportare le esercitazioni, i Cyber Range possono essere sfruttati per attività fondamentali per lo sviluppo e il potenziamento delle capacità di difesa, quali ad esempio:

- la formazione individuale sui vari aspetti della cybersecurity, anche attraverso corsi di livello universitario e di formazione continua del personale;
- l'addestramento di operatori preposti alla difesa dei sistemi ICT;
- il testing e valutazione degli strumenti di difesa;
- la progettazione e sviluppo di tattiche, tecniche e strategie per contrastare le minacce;

La costituzione di un Cyber Range nazionale può contribuire in modo determinante a rafforzare la difesa dello spazio cibernetico del Paese. Un Cyber Range nazionale consentirebbe alle Forze Armate e alla Pubblica Amministrazione di formare e addestrare i propri operatori, alle università e ai centri di ricerca di stimolare lo sviluppo e la validazione sperimentale di nuove tecniche di cyber security e alle aziende che lavorano nel campo della cyber security di sviluppare e testare nuove soluzioni tecnologiche.

La costruzione di un Cyber Range, le cui linee guida sono tracciate in [50], pone tuttavia un insieme di sfide tecniche importanti, che possono essere sinteticamente riassunte nell'esigenza di sviluppare:

- strumenti software per la generazione automatica di scenari virtuali di complessità reale da utilizzarsi nelle simulazioni;
- tecniche e strumenti per la simulazione delle attività (sia benigne che ostili) in esecuzione nei dispositivi simulati e per la generazioni del traffico di rete;
- tecniche e strumenti per la definizione e l'esecuzione di strategie di attacco e di difesa;
- metodologie e strumenti per supportate le attività di formazione, anche in modalità e-learning;

- metodologie e strumenti per valutare le capacità dei singoli e delle squadre di operatori durante le attività di formazione e le esercitazioni.

Va infine osservato che gli stessi attori che beneficerebbero del Cyber Range nazionale potrebbero dare un contributo importante per vincere tali sfide: le Forze Armate fornendo le competenze operative maturate nella partecipazione alle esercitazioni NATO e le università, i centri di ricerca e le aziende identificando soluzioni e sviluppando nuove tecnologie.

3.12 Investigazioni Digitali

Quando – alla fine dell'800 – Edmond Locard (1877-1966) elaborava il principio di interscambio che lo avrebbe reso famoso tra tutti gli scienziati forensi del mondo (nella vulgata "ogni contatto lascia una traccia") aveva ben presenti gli scambi di energia e materia che avvengono inevitabilmente tra l'autore di un crimine e la sua vittima e tra costoro e la scena dei fatti. Di certo non poteva immaginare che un giorno non lontano a quegli scambi fisici si sarebbero aggiunti – fino a diventare preponderanti – gli scambi di informazione che avvengono tra gli attori e uno spazio non fisico, il cyber spazio, che al suo tempo non esisteva neppure.

Oggi ogni investigatore sa bene che, sia in presenza di reati informatici in senso stretto, quali l'accesso abusivo a un sistema informatico, sia in presenza di reati comuni, quali la truffa, potrà acquisire informazioni utili al proseguimento delle indagini e mezzi di prova da computer e cellulari, dalla documentazione del traffico telefonico, da pubblici registri informatizzati e da sistemi di comunicazione come la posta elettronica e i social network.

L'individuazione, l'acquisizione, la conservazione nel tempo e l'analisi di tutta questa grande quantità di informazioni, nonchè la loro presentazione in sede dibattimentale, rappresentano l'ambito di studio tradizionale e consolidato dell'Informatica Forense.

I diversi aspetti del problema sono stati analizzati in passato soprattutto con riferimento ai dati "at rest" presenti su supporti di memorizzazione tradizionali (hard disk magnetici o a stato solido) o che siano pervenuti a seguito di operazioni di intercettazione su dati "in transit", mentre per quanto riguarda gli ambienti di esecuzione, grande attenzione è stata dedicata ai sistemi basati sui sistemi operativi Microsoft, che tutt'ora rappresentano oltre il 90% dei sistemi client tradizionali in circolazione.

Più recentemente, con la diffusione dei sistemi mobili, gran parte delle attività di ricerca si è rivolta ai problemi connessi con l'acquisizione di informazioni da questo tipo di dispositivi, che presentano una grande eterogeneità di configurazione e – a differenza dei computer tradizionali – non consentono in genere un facile accesso privilegiato "dall'esterno" alle informazioni in essi contenute.

Il progressivo trasferimento delle applicazioni e dei dati nel cloud ha aggiunto un ulteriore elemento di complessità alle investigazioni digitali: applicazioni e dati "in cloud" infatti non sono materialmente presenti nei luoghi oggetto di eventuali perquisizione e spesso sono memorizzati al di fuori della giurisdizione italiana. Inoltre, in presenza di sistemi di archiviazione distribuiti, non è neppure chiaramente individuabile una collocazione fisica dei dati e delle applicazioni, con conseguenze che è facile intuire per sistemi giuridici costruiti sostanzialmente sul principio di territorialità.

Parallelamente alla diversificazione delle piattaforme oggetto di indagine (tradizionali, mobili e cloud) si è assistito a un incremento impressionante della capacità di memorizzazione dei sistemi e della velocità delle linee di comunicazione.

In considerazione dell'evoluzione tecnologica appena accennata (da sistemi tradizionali a sistemi mobili e in cloud, incremento della capacità di memorizzazione) è possibile tratteggiare le maggiori sfide che dovranno necessariamente essere affrontate nei prossimi anni:

- La prima e principale sfida è certamente rappresentata dal puro e semplice volume delle informazioni da acquisire e analizzare; già oggi le procedure operative consolidate – che prevedono l'esecuzione di una copia "bitstream" dei dati – richiedono molte ore per essere portate a termine anche su sistemi di modeste dimensioni e sono assolutamente improponibili per basi di dati di media capacità, Alcuni autori – soprattutto negli USA – hanno tra l'altro visto in questa pratica una forma di illecita "overreaching seizure" in quanto inevitabilmente si vengono ad acquisire anche informazioni per le quali non era stata fornita espressa autorizzazione o comunque estranee alle indagini. Nuovi metodi e protocolli investigativi dovranno essere messi a punto al fine di acquisire tutti – e soli – gli elementi di interesse investigativo "in situ" senza per questo dover acquisire l'intera massa dei dati.

- La seconda sfida è rappresentata dall'eterogeneità delle piattaforme, soprattutto mobili, che richiederanno lo sviluppo di metodologie di acquisizione e analisi molto flessibili e tali da poter agevolmente seguire la continua evoluzione tecnologica dei prodotti commerciali. In questo senso la diffusione della Internet of Things non potrà che rendere le operazioni di acquisizione sempre più complesse, ma anche più interessanti per i risultati potenzialmente ricavabili.

- La terza sfida investe i sistemi cloud, per i quali non solo dovranno essere sviluppati sistemi e protocolli di analisi che tengano conto del volume dei dati e della loro frequente inaccessibilità fisica, ma dovrà anche essere sviluppato e adottato un impianto normativo idoneo per stabilire quali

siano i limiti di intervento legittimo degli investigatori e a quali condizioni le informazioni così acquisite siano ammissibili come mezzi di prova in giudizio.

Le problematiche e le conseguenti sfide appena delineate investono un ambito sostanzialmente nazionale, sebbene sollevino delicate problematiche di giurisdizione quando - come nel caso de sistemi in cloud - i dati non siano materialmente presenti sul territorio nazionale.

Un diverso ordine di problemi è rappresentato dalla criminalità informatica internazionale, con ciò intendendo gli autori di azioni delittuose in danno a cittadini e imprese italiane, ma pianificate e condotte dall'estero. Rientrano in questa categoria ad esempio il phishing e fenomeni estorsivi come quelli condotti a mezzo di malware tipo cryptolocker, in grado di rendere inaccessibili le informazioni ai legittimi titolari fino a pagamento di un riscatto (pagamento che spesso viene richiesto in criptovalute difficilmente tracciabili come i bitcoin).

La sostanziale impunità di cui godono gli autori di questi reati, che operano da Stati verso i quali non esistono accordi internazionali in materia investigativa, li rende estremamente pericolosi e potenzialmente in forte crescita sia in termini assoluti sia in percentuale rispetto agli altri reati informatici. Il contrasto di questo tipo di criminalità implica differenti sfide, sul piano tecnologico e sul piano organizzativo.

Sul piano tecnologico sono necessari lo sviluppo e la diffusione di tecnologie idonee a riconoscere le minacce su base comportamentale, e non semplicemente delle firme statiche, del malware eventualmente utilizzato.

Sul piano organizzativo è importante innalzare il livello di consapevolezza e sensibilità del pubblico e degli operatori professionali riguardo questa particolare tipo di minaccia, unito alla creazione di una rete di early warning diffusa sul territorio; quest'ultima dovrebbe essere in grado di raccogliere e valutare le segnalazioni di eventi potenzialmente criminosi e – se del caso – diffondere appropriati avvisi.

Sempre sul piano organizzativo è indispensabile diffondere la conoscenza e l'applicazione delle best-practices nella gestione delle informazioni e delle comunicazioni informatiche, soprattutto a livello di Pubblica Amministrazione e imprese private. Si consideri che la minaccia rappresentata dal citato malware cryptolocker sarebbe stata completamente vanificata dalla sola adozione di corrette procedure di backup dei dati.

Su tutte queste sfide prevale quella che potremmo definire la "sfida zero": gli organi investigativi sono tradizionalmente strutturati su un livello operativo "di primo intervento" e su un secondo livello "specialistico" che interviene solo al realizzarsi di particolari condizioni. È a nostro parere di fondamentale importanza che le capacità di investigazione digitale – almeno quelle di base – siano diffuse in modo più ampio e capillare possibile, utilizzando ogni mezzo per adeguare la *formazione professionale degli operatori.* Questo permetterebbe

di acquisire tempestivamente le informazioni che sono soggette a rapida volatilità facendo in modo di non compromettere la successiva utilizzabilità del dato digitale in giudizio.

3.13 Intelligence e Big Data Analytics

Con l'espressione *big data* ci si riferisce a raccolte di dati così estese in termini di volume, velocità e varietà (cosiddetto modello delle "3V") da richiedere tecnologie e metodi analitici specifici. Il progressivo aumento dei dati è legato alla necessità di analisi su un unico insieme di dati, con l'obiettivo di estrarre appunto informazioni aggiuntive rispetto a quelle che si potrebbero ottenere analizzando piccole serie. Big data significa anche interrelazione di dati provenienti da fonti eterogenee, quindi non soltanto i dati strutturati, come i database, ma anche quelli non strutturati, come immagini, email, dati GPS, informazioni prese dai social network. La mole dei dati può diventare facilmente dell'ordine dei Zettabyte – miliardi di Terabyte – sono quindi necessari metodi e tecnologie che eccedono la capacità di elaborazione delle tecnologie tradizionali di trattamento dei dati, ovvero una potenza di calcolo parallelo e massivo con strumenti dedicati eseguiti su decine, centinaia o anche migliaia di server. I governi e le imprese stanno ponendo la massima attenzione allo studio di come queste grande moli di dati possono aiutare ad avere una migliore "situational awarenes" di un fenomeno e una migliore predicibilità di situazioni future. Raccolta informativa e analisi sono i capisaldi di un processo di intelligence strutturato ed è per questo che l'elaborazione di grandi moli di dati è destinato a diventare un game changer nel settore dell'intelligence. Per dare una dimensione anche economica si noti come il solo Dipartimento della Difesa degli Stati Uniti abbia assegnato, nel 2012, 250 milioni di dollari a progetti big data in ambito sicurezza[18].

A puro scopo esemplificativo si considerino i seguenti esempi in cui possono essere applicate tecniche di analisi di big data (*big data analytics*) per la prevenzione di minacce o in applicazioni di intelligence:

- Gli APT – Advanced Persistent Threat – rappresentano minacce molto gravi alla sicurezza delle informazioni; in genere un attacco APT ha come obiettivo il furto di proprietà intellettuale, l'accesso a dati sensibili o a informazioni strategiche che potrebbero essere utilizzate a scopo di lucro, ricatto, danno all'immagine, falsificazione dei dati, *insider trading* illegale o per causare una interruzione nelle attività di un'organizzazione. Gli

[18] Fact Sheet: Big Data Across the Federal Government - `https://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_fact_sheet_final.pdf`

APT sono gestiti da attaccanti altamente qualificati, ben finanziati e motivati, che agiscono su periodi di mesi o anni. L'obiettivo ultimo dell'attacco è restare il più a lungo possibile all'interno di una organizzazione al fine di avere un accesso costante a informazioni strategiche. Le tecniche utilizzate sono tali da risultare pressocchè invisibili agli usuali sistemi di rilevamento delle intrusioni. Tracce degli APT sono però presenti all'interno dei log di server, IDS – Intrusion Detection System, firewall e router dell'organizzazione attaccata, ma la massiccia quantità di dati da setacciare alla ricerca di anomalie può rappresentare un ostacolo. Utilizzando un sistema big data, gli RSA Labs hanno ottenuto ottimi risultati nell'individuazione di APT, elaborando, in una sola ora, un miliardo di messaggi, pari ai log di un intero giorno.

- I cosiddetti "terroristi isolati" (lone wolf terrorist) sono persone che agiscono in maniera autonoma senza prendere ordini da, o essere connessi a, organizzazioni specifiche. I terroristi isolati sono difficili da individuare con le tecniche tradizionalmente usate per il terrorismo organizzato, ma lasciano spesso tracce digitali che, se individuate e correlate, possono essere usate come indicatori di un comportamento potenzialmente interessante. Gli studi dimostrano infatti che il processo di radicalizzazione di un *lone wolf* avviene quasi totalmente su Internet, nelle sue pagine Web o nei suoi account di social network dove compaiono segnali, quali ammissioni di voler colpire un obiettivo, interesse ossessivo verso qualcosa o qualcuno, identificazione in un gruppo o una causa. La sfida è quella di poter continuamente tracciare e monitorare pagine Web e account di social network alla ricerca dei possibili soggetti interessanti.

- Nell'*intelligence strategica* il compito è di anticipare opportunità e sfide, analizzare le loro implicazioni e fornire ai decisori tutti gli elementi per lo sviluppo di una strategia in modo da trarre il maggiore vantaggio competitivo per il Paese. I dati di osservazione devono essere rilevati principalmente tramite un processo di *horizon scanning* per monitorare il cambiamento e le sue cause, trasversalmente su tutti gli aspetti della società. I dati rilevati vengono tipicamente classificati in quattro gruppi, in base al loro grado di evoluzione e di maturità quali indicatori di cambiamento: *(i)* weak signal, *(ii)* trend e sviluppi, *(iii)* driver (o megatrend), e *(iv)* wild card. I trend e i driver rappresentano cambiamenti in uno stadio avanzato, una wild card è un evento singolo che ha un forte impatto nel contesto in cui si realizza. Un weak signal[19], invece, è una variazione presente inizialmente in poche osservazioni ma che potrebbe moltiplicarsi in un numero tale di punti da diventare un trend (in termini epidemiologici, rappresenta il "paziente zero"). I weak signal sono strutturabili in tre

[19] Suoi sinonimi sono early warning, early detection, seed of change.

categorie di sorgenti di informazioni: sorgenti online (homepage di singoli, giornali digitali, blog, forum e social network, gruppi di discussione e newsletter), testuali e umane. I weak signal possono rappresentare quindi dei veri rivelatori di cambiamento; quando anticipano cambiamenti futuri, sono strumenti di grande valore perchè permettono di effettuare analisi previsionali utili alla elaborazione di policy e programmi di sviluppo.

Gli esempi precedenti (APT, lone wolf terrorist e weak signal) condividono la stessa caratteristica: sono rintracciabili solo collegando (pochi) elementi presenti in grandi quantità di dati e richiedono l'analisi di volumi di dati enormi, dinamici ed eterogenei: i big data, appunto.

Molte sono le sfide, tecnologiche ed organizzative, da affrontare per mettere in atto una strategia big data [5, 42], le principali sono le seguenti:

Interdisciplinarietà: Sistemi per l'elaborazione di big data devono proporre soluzioni tecnologiche e metodologiche, che mettono insieme data mining, machine learning, information retrieval, natural language processing (NLP), statistica, matematica applicata, oltre a un interfacciamento stretto con esperti di dominio (analisti). Sono quindi sistemi complessi da progettare e realizzare [6].

Quantità vs Qualità dei dati: La visione comune dei big data predilige la quantità a discapito della qualità del dato, sostenendo che la vastità dei dati è sufficiente a compensare eventuali distorsioni o difetti che potrebbero contenere. Questa visione è troppo semplicistica e un primo aspetto da affrontare è sviluppare una base statistica forte per valutare la qualità dei dati e l'affidabilità delle deduzioni (inferenze) effettuate tramite algoritmi quality-aware.

Affidabilità delle predizioni: Nelle applicazioni tradizionali statistiche, gli studiosi dividono l'analisi dei dati in statistica descrittiva, analisi dei dati esplorativa (ADE) e analisi dei dati di conferma (ADC). L'ADE si concentra sullo scoprire nuove caratteristiche presenti nei dati, mentre l'ADC nel confermare o falsificare le ipotesi esistenti. Viceversa, nell'analisi predittiva ci si concentra sull'applicazione di modelli statistici o strutturali per la classificazione o il forecasting predittivo. Se da un lato lavorare su grandi quantità di dati per scopi descrittivi (o comunque per confermare ipotesi pre-esistenti) è comunque complesso, modelli e tecniche predittive devono ancora essere migliorate per arrivare a livelli di affidabilità sufficienti.

Variabilità temporale dei dati e tempestività delle predizioni: Molto spesso, i big data sono dinamici e descrivono fenomeni che cambiano con il tempo (*streaming*); analizzare questo tipo di dati richiede di sviluppare mo-

delli analitici che siano nativamente *time-aware*, che siano sensibili a improvvisi cambiamenti nei dati e rapidamente li riflettano nei modelli costruiti. Infine la tempestività nella produzioni delle analitiche o della formulazione di predizioni è un requisito rigoroso. Non è sufficiente essere in grado di analizzare i dati che abbiamo, ma occorre fornire risposte entro un arco di tempo ristretto. Spesso questo significa che non si è in grado di eseguire un processo di analisi completo, ma vanno trovati dei meccanismi per ottenere approssimazioni dei risultati buone e veloci. Questo tipo di approccio copre tutte quelle applicazioni che prevedono un processo interattivo in cui debbano essere prese decisioni in modo tempestivo.

3.14 Condivisione delle Informazioni

La diffusione e la complessità degli attacchi informatici ad aziende, istituzioni governative e finanziarie sottolineano la necessità di risposte bene organizzate. Gli attacchi informatici sono trasversali ai settori pubblico e privato e, pertanto, le corrispondenti risposte richiedono il coinvolgimento di differenti entità, oltre a quelle precedentemente citate, quali le autorità regolatrici, le autorità giudiziarie e, nei casi più gravi, le autorità militari o l'intelligence. Per rendere le risposte il più efficaci possibile, la condivisione delle informazioni tra tali entità è fondamentale. Uno dei maggiori benefici derivanti dalla condivisione di informazioni (e risorse) consiste nel costo nettamente inferiore rispetto alla loro raccolta individuale, e il supporto a tale condivisione può avvantaggiarsi di vari strumenti giuridici, organizzativi o contrattuali, quali i consorzi, le società consortili o il contratto di rete. Le difficoltà riguardano principalmente la tutela delle informazioni scambiate, la violazione di restrizioni legali, il rischio di rilascio di informazioni sensibili, la scarsa interoperabilità e la mancanza di fiducia delle entità coinvolte. Le tecniche utilizzate per una condivisione sicura delle informazioni beneficiano dell'enorme mole di risultati provenienti dagli ambiti di ricerca sia informatico sia giuridico. Tuttavia, molti aspetti rimangono solo parzialmente risolti o perfino irrisolti. Le maggiori sfide riguardanti la condivisione sicura di informazioni che si presentano nell'immediato e nel medio termine possono essere riassunte nei seguenti punti:

- fornire una maggiore integrazione e sinergia tra soluzioni tecnologiche e strumenti giuridici;
- garantire maggiore usabilità strumenti per condivisione;
- sviluppare la consapevolezza e la cultura della sicurezza.

Gli organi di governo e l'amministrazione statunitense hanno riconosciuto da tempo che l'accresciuta frequenza e complessità degli attacchi informatici

pongono una serie di difficili sfide per le organizzazioni che devono difendere le proprie informazioni e infrastrutture. Una recente analisi effettuata dal National Institute of Standards and Technology (NIST) riconosce che la tipologia degli avversari varia da singoli individui a gruppi facenti parte di organizzazioni criminali o operanti per conto di stati. La quasi totalità degli avversari è motivata, ben finanziata e molto abile nell'impiego di tattiche, tecniche e procedure rivolte alla compromissione di sistemi, esponendo informazioni sensibili e sottraendo proprietà intellettuale.

Al fine di accrescere le loro capacità di risposta nei confronti di tali avversari, le organizzazioni sia pubbliche sia private hanno la necessità di mettere a fattor comune la conoscenza derivante dalle loro singole esperienze. Le modalità di condivisione dell'informazione all'interno del governo federale seguono un'architettura centralizzata e gerarchica, secondo cui i team operanti presso le differenti agenzie federali riportano le loro informazioni al Computer Emergency Readyness Team statunitense (US-CERT) oppure al Industrial Control System Cyber Emergency Team (ICS-CERT). La condivisione di informazioni riguardanti incidenti informatici, minacce e vulnerabilità tra differenti settori privati è coordinata dai cosiddetti Information Sharing and Analysis Center (ISAC). Recentemente, tale coordinamento è stato esteso alle istituzioni governative attraverso le Information Sharing and Analysis Organization (ISAO).

A livello europeo, la condivisione di informazioni è riconosciuta come un'area strategica e lo European Union Agency for Network and Information Security (ENISA) ha stilato linee guida per la creazione e gestione di organizzazioni quali l'Information Sharing and Alert System (EISAS), il cui principale compito è l'armonizzazione e il coordinamento delle azioni di differenti realtà, chiamati Information Exchanges. Tali organizzazioni, nelle intenzioni di ENISA, si debbono occupare di creare e mantenere a livello nazionale lo scambio sicuro di informazioni tra entità pubbliche e private.

In Italia, la rilevazione e il censimento degli attacchi informatici è svolto dal CERT Nazionale, presso il Ministero dello Sviluppo Economico. Tale struttura ha tra i suoi compiti il potenziamento dei meccanismi di risposta agli attacchi e degli strumenti per la loro rilevazione e contrasto. In particolare, è previsto uno strumento per la collaborazione tra enti privati, denominato piattaforma di infosharing, per la condivisione delle informazioni relative ai problemi e alle loro eventuali soluzioni. Sul lato istituzionale sono attivi stretti contatti con altre strutture, quali CERT-PA (Pubbliche Amministrazioni), CERT-Difesa e CNAIPIC (Ministero dell'Interno).

Dall'analisi delle documentazioni relative alle iniziative statunitensi ed europee, le linee guida di carattere generale per un'efficace condivisione sicura delle informazioni possono essere brevemente riassunte dicendo che ogni organizzazione deve:

- tenere un catalogo aggiornato dei dati e delle informazioni mantenute, accanto a una chiara ed esaustiva rappresentazione delle politiche sotto cui tali informazioni possono venire condivise;
- essere in grado di difendersi dai vari tipi di attacchi alle proprie infrastrutture digitali e di rispondere prontamente e flessibilmente, acquisendo informazioni sugli attacchi da sorgenti sia interne sia esterne;
- garantire una valida ed efficiente condivisione di informazioni mediante un adeguato supporto logistico, tecnologico e finanziario;
- assicurare, attraverso opportuni controlli, il rispetto delle politiche di condivisione delle informazioni, con particolare attenzione alla confidenzialità e alla privacy.

Le priorità che emergono in riferimento allo scenario italiano sono la razionalizzazione dei differenti CERT, ad esempio organizzandoli su base regionale e delegando il loro coordinamento ai corrispondenti CERT di livello nazionale, nonché l'armonizzazione delle comunicazioni tra i differenti CERT, attraverso la creazione di una piattaforma di condivisione sicura delle informazioni secondo le linee guida sopra accennate.

3.15 Metriche e Valutazione del Rischio

La normativa vigente in materia di sicurezza cyber prevede una serie di regole gestionali e tecniche di protezione la cui attuazione è a carico dei diversi soggetti coinvolti, ciascuno esposto a livelli di rischio diversi. In un contesto di risorse limitate, questi soggetti si trovano spesso in difficoltà nel rispettare le prescrizioni normative, con un'adesione meramente formale al dettato normativo, l'adozione di misure inefficaci e il conseguente dispendio delle già limitate risorse.

Per queste ragioni, una calcolata gestione del rischio diventa di primaria importanza per un'efficiente allocazione di risorse e una efficace protezione dagli attacchi informatici. È dunque necessario:

- proporre un modello realistico di valutazione del rischio informatico, facilmente attuabile da ogni soggetto all'interno del proprio ambiente produttivo e efficacemente regolamentabile con strumenti legislativi;
- proporre linee guida per la mitigazione del rischio conformi alla normativa, che tengano conto del rapporto costi/benefici desiderato dal soggetto e atteso dalla collettività;
- identificare a livello legislativo le informazioni condivisibili dai diversi attori (imprese e PA) in modo da consentire una valutazione sintetica del

rischio economico e sociale dovuto ad attacchi informatici, tenendo conto delle giuste riserve dei vari attori in termini di vantaggio competitivo, reputazione, etc.

La gestione del rischio dei sistemi informativi sta progressivamente acquisendo una posizione di primaria importanza all'interno di ogni organizzazione che gestisce dati o comunicazioni sensibili ed è oggetto di norme tecniche, regolamenti e leggi che enti pubblici e imprese private devono rispettare. Questo insieme di normative ha spesso respiro internazionale e può essere integrato da ulteriori normative locali (nazionali) per la gestione del rischio.

Le normative definiscono obblighi di gestione a fronte di diversi tipi di rischio: ad esempio i rischi operativi, legali, strategici e reputazionali. Il comitato di Basilea definisce il rischio operativo come "*Il rischio di perdite risultante dall'esistenza di inadeguati od inefficaci processi interni, sistemi o personale, o da eventi esterni*".

Sotto tale definizione ricade gran parte del rischio tecnologico e infrastrutturale associato a fenomeni naturali e ad errate considerazioni strategiche e organizzative; vi ricadono inoltre anche eventi dolosi come, ad esempio, gli attacchi informatici. Facendo riferimento a quest'ultima tipologia di attacchi, sono di particolare interesse i rischi associati alle transazioni finanziarie e alla gestione dei sistemi sensibili e delle infrastrutture critiche.

Tra gli standard che coprono questo tipo di rischi sono ben noti l'ISO 27001 per la gestione delle infrastrutture, PCI-DSS per la gestione della sicurezza di sistemi finanziari e *Basilea II* per i sistemi bancari. A livello nazionale italiano, la *circolare 263* del 27 dicembre 2006, e successivi aggiornamenti, si pone come strumento addizionale per la gestione del rischio operativo delle banche (ivi incluso il rischio di credito, di mercato, e altri).

Questi standard richiedono che venga attuata una serie di controlli sulla base di "regole" e che le eventuali "eccezioni" a tali "regole" siano appropriatamente giustificate e prevedano misure di controllo alternative.

Ogni organizzazione è diversa: l'imposizione di una "regola normativa" valida per tutti semplifica il processo di standardizzazione, ma può avere, in termini di effettiva riduzione del rischio, effetti largamente diversi a seconda della realtà dove viene applicata. Di conseguenza le organizzazioni sono costrette a investire per la certificazione senza avere un riscontro diretto del beneficio in termini di *incremento della sicurezza*, cioè di quanto il loro rischio operativo si è effettivamente ridotto per effetto dei controlli implementati.

In mancanza di una misura del rischio residuo l'organizzazione rimane sprovvista di uno strumento fondamentale per pianificare operazioni future: non ha strumenti per decidere se ridistribuire, mitigare ulteriormente o accettare tale rischio, così come non può pianificare razionalmente l'eventuale allocazione di ulteriori risorse per la sua gestione. Un ulteriore ostacolo a questa valutazione è la mancanza di una piattaforma comune che - coinvolgendo l'industria, la

Pubblica Amministrazione e il Governo nella condivisione di informazioni su incidenti di sicurezza e minacce informatiche - porterebbe a una più precisa stima del rischio condiviso.

La sfida è dunque quella di fornire strumenti scientifici capaci di indirizzare la produzione normativa verso la redazione di linee guida volte alla valutazione e alla riduzione effettiva del rischio operativo. Questa sfida si articola su tre elementi qualificanti:

1. identificare una metodologia di valutazione del rischio normativamente attuabile e di facile verifica che permetta una misura consistente del rischio proprio di ogni organizzazione;
2. tenere conto del livello di costo-beneficio desiderato dal soggetto, nel rispetto comunque dei legittimi interessi della collettività in cui il soggetto è inserito;
3. permettere la condivisione di informazioni tra attori industriali, gestori di infrastrutture critiche e pubblica amministrazione, allo scopo di permettere al Governo una efficace misura dell'esposizione collettiva al rischio economico e sociale del sistema Italia.

CAPITOLO

4 Raccomandazioni

Questo capitolo presenta una serie di raccomandazioni che, se seguite, permetteranno di rispondere con successo alle sfide elencate nel capitolo precedente. Le raccomandazioni non intendono essere esaustive, ma vanno a toccare dei punti ritenuti essenziali per una corretta implementazione di un *piano di sicurezza cibernetica* a livello nazionale. Piano che, per sua natura, dovrà necessariamente essere dinamico e in continua evoluzione in base ai cambiamenti tecnologici, normativi, sociali e geopolitici.

Prima di passare alla presentazione delle nostre raccomandazioni, riteniamo utile evidenziare che le strategie per la garantire la sicurezza cibernetica vanno considerata parte integrante della *politica digitale nazionale* che, coinvolgendo il governo nel suo insieme, dovrebbe dipendere direttamente dalla responsabilità politica del Presidente del Consiglio. Nel mondo cyber e nella realtà tecnologica contemporanea e futura, occorre infatti dotarsi di uno strumento in grado sovrintendere, attuare e concretizzare le priorità dell'agenda politica digitale evitando logiche campanilistiche e sovrapposizioni. La politica cyber sta diventando tanto importante quanto la geopolitica ed è, tra l'altro, improcrastinabile garantire una *rappresentanza italiana istituzionale e coordinata a tutti i tavoli di governance di Internet*.

Sarebbe quindi auspicabile la creazione, da parte della Presidenza del Consiglio, di una nuova struttura dedicata alla politica digitale, dotata di competenze chiare e di poteri effettivi su servizi, settori produttivi e Pubbliche Amministrazioni. Questa struttura dovrebbe rappresentare per l'intero paese quello che l'Agenzia per l'Italia Digitale (AgID) rappresenta per la Pubblica Amministrazione. La nuova struttura dovrà però essere organizzata in modo tale da non rappresentare, come è purtroppo spesso accaduto in Italia, un livello burocra-

tico aggiuntivo teso a verificare adempimenti procedurali in chiave legalistico-giuridica, ma, al contrario, dovrà essere in grado di fornire input strategici che consentano di disegnare l'architettura complessiva di un sistema modulare ed effettivamente competitivo a livello internazionale. Tale struttura sarebbe, tra l'altro, in linea con quanto già avvenuto in altri Paesi industrializzati (non solo le grandi potenze, ma anche Regno Unito, Germania e Francia, per non parlare di piccoli Paesi come Israele ed Estonia), dove la digitalizzazione ha costituito un rilevante fattore di crescita economica[1].

4.1 Strategia, pianificazione e controllo

Il quadro legislativo italiano delineato nella sezione 2.4 evidenzia, nella prevenzione, gestione e risposta ad attacchi cyber, uno scenario di competenze e responsabilità distribuito e frastagliato. La velocità con cui gli attacchi si dispiegano richiede invece un forte coordinamento tra rilevazione della minaccia e risposta. A questo va aggiunta la carenza di esperti di sicurezza che sconsiglia la dispersione di queste competenze tra i tanti attori partecipanti al quadro strategico nazionale. Una revisione del piano strategico allo scopo di centralizzare competenze e responsabilità relative specificamente alla sicurezza cibernetica è sicuramente auspicabile. Molti paesi come Francia, Germania, Israele e Olanda hanno già concentrato queste attività in apposite agenzie o enti.

Uno dei compiti fondamentali di un ente centrale per la sicurezza cibernetica è quello di delineare obiettivi strategici che permettano all'Italia di entrare nel gruppo dei Paesi "sicuri", cioé di diventare un Paese in cui sia mimino il rischio di furto di informazioni digitali e massima la sicurezza nelle transazioni on-line. Ovviamente, questo richiede il coinvolgimento di molteplici attori che possano agire all'interno di uno specifico quadro di riferimento, quale ad esempio il Piano nazionale per la protezione cibernetica e la sicurezza informatica [59]. In questo scenario è però fondamentale che l'ente per la sicurezza abbia poteri non solo di indirizzo ma di controllo del raggiungimento degli obiettivi. Infine questo ente dovrebbe supportare altri enti governativi nella definizione di requisiti, regole e vincoli da inserire all'interno di capitolati di gare in modo da avere soluzioni tecnologiche e organizzative di sicurezza all'avanguardia mondiale, in grado anche di evitare lock-in tecnologici e di servizio.

4.2 Sicurezza come investimento

Garantire luoghi sicuri dove mantenere e scambiare informazioni è sicuramente condizione necessaria per assicurare la prosperità economica di un Paese e

[1] `http://www.tau.ac.il/~liort/Cybersecurity%20in%20Israel.html`

la sicurezza fisica dei suoi abitanti; la messa in sicurezza del cyber space nazionale è quindi un obiettivo strategico. Finanziare ricerca e industria in questo settore all'interno di un progetto strategico è quindi prioritario anche per poter raggiungere il maggior grado di indipendenza possibile nella prevenzione e gestione di rischi relativi ai nostri dati, alle nostre transazioni e alle nostre infrastrutture critiche. Ovviamente la sicurezza costa, ma essa va vista come un investimento e come precondizione indispensabile per garantire la competitività del nostro sistema produttivo.

Guardando la cosa da un punto opposto, bisogna evitare di sprecare anche i pochi investimenti che vengono fatti sulla sicurezza. Le figure professionali legate alla sicurezza hanno un mercato mondiale e spesso in Italia ci troviamo a competere con realtà che offrono condizioni salariali di gran lunga migliori. È pertanto necessario mettere a punto delle strategie di *brain retention* che rendano più attraente lavorare su tematiche di sicurezza informatica nel nostro Paese. Israele, ad esempio, è riuscita a frenare l'emorragia attraverso la creazione di un ecosistema Industria-Università-Governo basato su parchi tecnologici e politiche incentivanti per le spin-of, riuscendo in questo modo a trasformare una debolezza endemica in un fattore di crescita.

4.3 Cyber Security Center - un'alleanza nazionale tra accademia, pubblico e privato

Per le particolari caratteristiche del settore della sicurezza cibernetica, che può richiedere riservatezza, se non segretezza, nel trattamento delle informazioni, ampiezza di conoscenze e dati, personale di altissima qualificazione e infrastrutture hardware e software rilevanti, le relazioni tra accademia, pubblico e privato dovrebbero evolvere in qualcosa di più articolato rispetto alle relazioni puntiformi presenti in questo momento sul territorio.

È necessaria una struttura leggera centralizzata multidisciplinare, in parte governativa, in parte privata e in parte legata al mondo della ricerca, in grado sia di far fronte a una serie di servizi e attività di ricerca sia di giocare un ruolo primario nelle linee attuative del processo dinamico di implementazione del Piano Strategico Nazionale di Sicurezza Cibernetica, insieme alle altre componenti del sistema governativo nazionale.

Il centro attrarrebbe ricercatori e investitori pubblici e privati per sviluppare ricerche di punta su tematiche di interesse strategico nazionale nel settore della sicurezza cibernetica e per fornire servizi al sistema governativo e produttivo del Paese, ivi comprese le infrastrutture critiche. Ricerche che non potrebbero essere portate avanti nel solo ambito accademico. Inoltre il centro potrebbe gestire l'evoluzione di standard e framework nazionali di cyber security, proporre

metodologie e procedure per approvigionamento sicuro di hardware e software, formazione e disseminazione culturale.

Il centro dovrebbe rappresentare il collante tra Università e centri di ricerca italiani, il settore produttivo e il settore governativo garantendo all'Italia, nel tempo, un luogo dove creare competenze di alto profilo, generare spinoff di settore, sviluppare la ricerca universitaria e contribuire alla definizione degli obiettivi strategici del Paese nel settore. All'estero esistono tali alleanze, segnatamente l'iniziativa NCSA (National Cyber Security Alliance) americana o l'alleanza security made in Germany, tuttavia hanno finalità diverse da quelle proposte in questo documento perché si muovono in un contesto dove già esistono organi governativi che si occupano di sicurezza informatica: NSA, NIST, DHS negli Stati Uniti e BSI in Germania.

4.4 Razionalizzazione del patrimonio informativo della Pubblica Amministrazione

È importante rimarcare che un piano di sviluppo organico delle infrastrutture informatiche della PA rappresenterebbe un asset strategico per il nostro Paese, nonché per la sicurezza dei nostri dati. Elemento centrale di questo piano dovrebbe essere la razionalizzazione dei data center della PA. Tale scelta non porrebbe ostacoli alla proprietà, alla riservatezza o alla operatività delle organizzazioni locali e ridurrebbe sensibilmente i costi di gestione attraverso la condivisione di applicazioni e dell'infrastruttura stessa. Quindi razionalizzare l'infrastruttura tecnologica della pubblica amministrazione, passando dalle attuali decine di migliaia di centri spesa, a un numero di almeno due (se non tre) ordini di grandezza inferiore, avrebbe il triplo vantaggio di (i) realizzare risparmi nell'ordine di centinaia di milioni di euro, (ii) aumentare sensibilmente i livelli di sicurezza e di disponibilità dei servizi della PA e (iii) realizzare un vero e proprio asset infrastrutturale tecnologico necessario per lo sviluppo del Paese. Questa rete di data center qualificati potrebbe essere usata anche per ospitare i sistemi informativi di piccole e medie imprese e getterebbe le basi per la creazione di una nuvola "made in Italy", sulla base del modello tedesco, che permetta lo sviluppo di tali imprese, sempre garantendo la riservatezza delle informazioni trattate, in accordo alle normative vigenti nel nostro Paese.

4.5 Formazione

Formare ogni settore della società a capire il cambiamento storico avvenuto con lo sviluppo di Internet, che ha aggiunto una nuova dimensione al nostro modo di vivere, è strategico. Per rispondere ai problemi posti dal crescente utilizzo del

cyberspace e dalle criticità in termini di sicurezza dei sistemi informatici è necessario promuovere la cultura della sicurezza e rendere consapevoli i cittadini e i lavoratori che la mancanza di attenzione può mettere a rischio un'intera comunità. Ogni singolo lavoratore deve comprendere che, come vittima di attacchi, può facilitare accessi ai sistemi informatici della sua organizzazione, senza che le tecnologie preposte siano in grado di rilevarli.

Per raggiungere tale obiettivo è necessario potenziare l'educazione specialistica, innalzando la sicurezza a obiettivo strategico; considerando l'educazione di base, la formazione universitaria e la formazione professionale.

Per l'*educazione di base*, la strategia di lungo termine deve prevedere l'arricchimento dei programmi di tutte le scuole superiori con adeguate nozioni di sicurezza che li mettano in guardia dall'uso poco accorto di programmi eseguiti sui loro computer o smartphone. Per la *formazione universitaria*, la strategia a medio termine, rivolta alla generazione attuale e prossima ventura di programmatori e ingegneri, deve prevedere un curriculum nazionale che contenga un insieme minimo di argomenti di base sulla sicurezza dei sistemi [72]. Ciò può essere facilitato dall'istituzione di laboratori virtuali dove professori e ricercatori possano contribuire o attingere esercizi pratici di sicurezza applicativa, rete e web [79].

Il problema della *formazione professionale* è ampio e complesso perché, come avviene per la sicurezza sul lavoro, investe non solo tecnici del settore, ma anche cittadini, imprese e pubbliche amministrazioni. La formazione e l'aggiornamento professionale di lavoratori e dei dirigenti attraverso una formazione professionale permanente assume pertanto un ruolo cruciale. Addestrare sul campo i lavoratori attraverso formazione ed esercitazione è tanto importante quanto acquisire nuova tecnologia. Questo addestramento va pianificato non solo per i professionisti informatici ma anche per i dirigenti, gli operatori tecnici ed il personale esecutivo.

In ultimo, ma non sicuramente perché meno importante, va sottolineata la necessità di rendere *tutti i cittadini* consapevoli dei rischi relativi a furto di identità, privacy, intercettazioni, operazioni bancarie, ..., ai quali essi sono esposti quando utilizzano strumenti informatici dallosmarthphonealla rete wifi di casa, dal tablet al computer in ufficio. Questo consapevolezza va formata attraverso opportune campagne di informazione e di formazione sia sui media tradizionali (giornali, radio, tv) sia sui social.

4.6 Certificazioni, Best Practices e Framework di Sicurezza Nazionale

Certificazioni e best practices di sicurezza sono una pratica importante e da diffondere all'interno del panorama industriale e governativo nazionale ed è fon-

damentale che il quadro normativo nazionale sia chiaro e coerente. In particolare, la creazione di certificazioni deve ispirasi a un framework pubblico condiviso, per creare le condizioni migliori a una diffusione uniforme e controllata degli attestati. Va pertanto seguita l'attività dell'ente normatore UNI con le sue articolazioni nel settore ICT (UNINFO) che emana norme anche sulla sicurezza, norme che possono condizionare in particolare le attività di formazione continua e i rapporti fra professionisti ICT e i fruitori di servizi di sicurezza, anche nella Pubblica Amministrazione.

È altrettanto importante che le problematiche legate alla sicurezza informatica non rimangano un fattore solo tecnico e tecnologico ma, come ripetuto più volte in questo documento, pervadano tutti i settori di un'organizzazione. In particolare si deve portare l'argomento rischio informatico all'interno dei consigli di amministrazione delle aziende e dei comitati direttivi delle organizzazioni pubbliche, in modo che il rischio informatico venga trattato e gestito come un qualsiasi altro rischio aziendale. In questo è importante la sensibilizzazione degli enti governativi per fare comprendere che questo rischio è sistemico, oltre che specifico per l'organizzazione.

Per facilitare questo passaggio, molti paesi avanzati stanno introducendo e favorendo l'adozione di *framework nazionali di sicurezza cyber*, per permettere sia di valutare in modo *semplice* le capacità cyber di una organizzazione sia di aiutare la definizione di una roadmap verso una capacità cyber adeguata al tipo di business dell'organizzazione, garantendo opportuna programmazione temporale. Questo ha il vantaggio di stimare il rischio del sistema Paese e di alzarne il livello delle difese. L'Italia dovrebbe muoversi in modo deciso in questo settore, favorendo l'introduzione di framework nazionali di sicurezza cyber, tenendo conto della specificità del settore produttivo italiano formato in stragrande maggioranza da piccole e medie imprese. Questo strumento è essenziale anche per formulare adeguate politiche e normative per migliorare la *supply chain* di aziende e organizzazioni governative e per essere strumento principe in un sistema di *due diligence* di relazioni tra stati [71].

APPENDICE

A Quadro Internazionale di Riferimento

Questa appendice si propone di presentare il quadro normativo e le politiche pubbliche che definiscono e organizzano la cyber security di Repubblica Ceca, Francia, Paesi Bassi, Federazione Russa e Stati Uniti. Si tratta di Stati Europei (UE e extra UE) e non Europei che si distinguono o per la loro rilevanza strategica a livello internazionale/regionale ovvero per l'attualità di alcune misure da questi adottate in materia di sicurezza cibernetica. Per ciascuno Stato, vengono individuati ed esaminati sia le principali fonti normative e di policy che definiscono la cyber security a livello nazionale, sia i principali attori che vi contribuiscono. La scelta degli Stati oggetto di studio è avvenuta sulla base di criteri che hanno permesso di facilitare l'esame comparato dei risultati dell'indagine ed hanno consentito di individuare best practice la cui adozione potrebbe essere d'interesse anche per altri Stati.

A.1 La cyber security nella Repubblica Ceca

Nella Repubblica Ceca, la cyber-security rappresenta sia un obiettivo sia un elemento essenziale dell'organizzazione della sicurezza nazionale. Essa viene perseguita dalle autorità governative ceche con il contributo di diversi attori nazionali, tanto pubblici quanto privati, attraverso l'adozione di specifiche misure volte a dare esecuzione alle linee d'indirizzo che sono stabilite da rilevanti strumenti di policy adottati progressivamente nel tempo [47]. Tra questi figurano: la "Strategia in Materia di Sicurezza Nazionale" [63] e il "Libro Bianco della Difesa" del 2011 [64] i quali, seppur in modo non approfondito, fanno riferimento al dominio cyber quale dimensione rilevante della sicurezza dello Stato; la "Strategia di Cyber Security della Repubblica Ceca" [65] e il relativo "Piano d'Azione" del

2012 riguardanti, rispettivamente, gli indirizzi in materia di sicurezza cibernetica per il triennio 2012-2015 e le misure per darvi attuazione; infine, la recente "Strategia di Cyber Security della Repubblica Ceca per il periodo 2015-2020" [66] e, di nuovo, il relativo piano d'azione, tuttora in fase di definizione[1]. Occorre osservare che nella Repubblica Ceca la cyber security è materia regolata anche da alcuni strumenti giuridici e cioè la "Legge sulla sicurezza cibernetica" n. 181[2] adottata nel 2014 ed entrata in vigore nel 2015 alla quale è stata data attuazione attraverso i Regolamenti n. 316/2014 e n. 317/2014, quest'ultimo riguardante le infrastrutture e sistemi informativi critici[3]. Unitamente a quanto previsto dalla Decisione N. 781 adottata dal Governo nel 2011, i suddetti strumenti giuridici organizzano la cyber security nella Repubblica Ceca e stabiliscono i ruoli, le funzioni e le responsabilità dei principali attori coinvolti in questa materia.

Avendo innanzitutto riguardo alla Strategia di Cyber Security 2015-2020, si tratta di un documento redatto dall'Autorità per la Sicurezza Nazionale della Repubblica Ceca che definisce il quadro di riferimento per le iniziative che dovranno essere intraprese dai vari attori nazionali per far fronte alle minacce cyber che originano sia da eventi di natura antropica che naturale [66]. In particolare, il documento presenta la visione delle autorità ceche in materia di cybersecurity, specifica gli obiettivi da queste perseguiti, i principi che ne informano l'azione e le sfide che si apprestano ad affrontare per il periodo 2015-2020. Gli obiettivi vengono dettagliati come segue:

a) il rafforzamento delle strutture nazionali preposte alla sicurezza del cyber e lo sviluppo di processi e pratiche volti a favorire un'efficiente cooperazione tra questi ultimi;

b) la promozione di un'efficiente e rafforzata collaborazione con i rilevanti attori su scala internazionale a livello universale, regionale, multilaterale e/o bilaterale;

c) il consolidamento delle azioni volte alla protezione delle infrastrutture critiche nazionali (infrastrutture informatiche e sistemi informativi);

d) l'intensificazione della cooperazione con il settore privato volta anche a consolidare la reciproca fiducia;

e) il sostegno ad iniziative di ricerca e sviluppo secondo un approccio multidisciplinare;

f) il sostegno a campagne informative e di sensibilizzazione in materia di cyber-security rivolte al grande pubblico, nonché la promozione di iniziative di carattere educativo e formativo rivolte a specifici destinatari;

g) il supporto in termini di risorse e strumenti ai principali attori nazionali impegnati nella prevenzione del, e contrasto al, cyber-crime;

[1] L'adozione del Piano d'Azione è prevista per agosto/settembre 2015.

[2] Act No. 181 on Cyber Security and Change of Related Acts, 23 July 2014.

[3] Entrambe i regolamenti sono disponibili in lingua ceca su `https://www.govcert.cz/cs/`.

h) la promozione di misure di carattere legislativo in materia di sicurezza cibernetica da adottarsi sia a livello sia nazionale che internazionale ed il loro continuo vaglio al fine di monitorarne l'efficacia [66].

I sopra citati obiettivi saranno perseguiti attraverso strumenti e azioni la cui adozione e attuazione dovranno essere informate ad alcuni principi o requisiti base, ovvero consistere in specifiche misure. Si tratta di principi o misure volte a: garantire la protezione dei diritti e delle libertà fondamentali degli individui (e.g. libertà di espressione, diritto alla privacy e alla protezione dei dati personali, principio della trasparenza e non discriminazione), nonché il rispetto del principio dello stato di diritto; favorire un approccio olistico e integrato alla cyber-security nonché basato sul principio di sussidiarietà che dovrebbe evitare possibili sovrapposizioni o duplicazioni di ruoli e responsabilità da parte degli attori coinvolti; stimolare la reciproca fiducia tra i diversi attori pubblici e privati, società civile inclusa, che contribuiscono alla sicurezza cyber; promuovere un approccio basto sull'acquisizione delle capacità conoscitive nonché degli strumenti tecnici e tecnologici, che siano anche il risultato di iniziative di ricerca e sviluppo, idonei a salvaguardare l'integrità del dominio cyber e a proteggerlo dalle minacce [47].

Sul piano organizzativo e a livello di direzione strategica, la responsabilità principale in materia di cyber security viene attribuita all'Autorità per la Sicurezza Nazionale[4] e, in particolare, al Centro Nazionale di Cyber-Security (CNCS)[5]. Il CNCS ha il compito di gestire il Computer Emergency Response Team (CERT) Governativo (GovCERT.CZ)[6] e di coordinare la cooperazione tra i vari Computer Security Incident Response Team (CSIRT) operanti tanto a livello nazionale quanto internazionale. Esso, inoltre, stabilisce gli standard di sicurezza previsti per determinati enti pubblici e privati nazionali, promuove campagne di informazione e sensibilizzazione in materia di cyber-security e sostiene iniziative di ricerca e sviluppo nel settore. Sempre a livello strategico opera il Consiglio di Cyber Security[7], un organo a rappresentanza allargata che è responsabile del coordinamento tra le varie agenzie e amministrazioni sia civili sia militari che operano nell'ambito cyber. Alle sue riunioni possono partecipare, se necessario e richiesto, anche rappresentanti del settore privato in particolare degli enti che sono responsabili della gestione delle infrastrutture critiche.

A livello operativo e in ambito di sicurezza civile, spetta al `GovCERT.CZ` il compito di raccogliere le notifiche di incidenti che coinvolgono la dimensione cyber e che interessano le infrastrutture critiche nazionali, quelle governative ovvero gli internet exchange points che consentono la connessione diretta con

[4] `http://www.nbu.cz/en/.`

[5] `http://www.govcert.cz/en/.`

[6] `http://www.govcert.cz/en/govcertcz/.`

[7] `http://www.govcert.cz/en/csc/cyber-security-council/.`

tali infrastrutture[8]. Una volta ricevuta la notifica di incidente cyber da parte dell'ente governativo interessato o gestore dell'infrastruttura critica, il GovCERT.CZ provvede ad esaminare l'incidente e offrire la sua assistenza. In base a quanto stabilito dalla Legge n. 181, gli enti di cui sopra hanno l'obbligo di adottare misure di sicurezza idonee a difendersi dagli incidenti cibernetici e farvi fronte, nonché l'obbligo di riportare la notizia di avvenuto incidente o attacco al CERT Governativo. Per quanto invece riguarda gli incidenti o attacchi che interessano enti di natura non governativa o privata, vige l'obbligo per questi ultimi di darne notifica al CERT nazionale (CSIRT.CZ). Sempre in base a quanto disposto dalla Legge n. 181, l'Autorità Nazionale per la Sicurezza ha facoltà di dichiarare lo "stato di emergenza cibernetica" è della durata massima di 7 giorni e rinnovabile fino ad un massimo di 30 - e richiedere l'adozione di particolari e ulteriori misure di sicurezza anche a enti privati[9].

Per quanto invece riguarda il settore militare, la difesa cibernetica della Repubblica Ceca è attribuita all'Agenzia per i Sistemi di Comunicazione e Informazione che è parte delle Forze Armate. L'Agenzia è responsabile dell'attuazione delle politiche in materia di cyber-security per quanto riguarda le forze Armate e il Ministero della Difesa. Il coordinamento tra le iniziative in materia di cyber-security adottate rispettivamente nel settore civile e militare è assicurato sul piano organizzativo dal Consiglio di Cyber Security e ulteriormente stabilito da un memorandum concluso tra il Ministero della Difesa e l'Autorità Nazionale per la Sicurezza.

Da notare che l'ordinamento ceco non prevede espressamente la possibilità di adottare misure di sicurezza o difesa cibernetica "attive" o "proattive", anche se sono attualmente in corso discussioni tra l'Autorità Nazionale per la Sicurezza e il Ministero della Difesa sull'argomento. Inoltre, va osservato che sebbene gli attori che nella repubblica ceca si occupano o hanno responsabilità in materia di cyber security siano formalmente definiti, esiste anche una comunità informale di esperti che potrebbe essere organizzata come "riserva".

A.2 La cyber security in Francia

La strategia nazionale francese in materia di cyber-security e l'apparato istituzionale-organizzativo al quale ne viene demandata l'attuazione sono definiti da una serie di strumenti normativi e di policy adottati progressivamente nel

[8] Act No. 181, cit., par. 8.

[9] "State of cyber emergency means a state, during which information security in information systems or security and integrity of services or electronic communication networks is seriously endangered and the interests of the Czech Republic may thus be violated or endangered according to the law on protection of classified information." [66]

tempo[8]. Si tratta de: il "Libro Bianco sulla Difesa e Sicurezza Nazionale"[10] del 2008 che, oltre ad annoverare per la prima volta la minaccia cyber proveniente da attori sia statuali che non tra i principali pericoli alla sicurezza nazionale, propone una serie di azioni per farvi fronte; la "Strategia Francese sulla Difesa e Sicurezza dei Sistemi Informativi"[11] del 2011 che si propone l'obiettivo specifico di tutelare e promuovere la sicurezza del dominio cyber al fine generale di garantire la sovranità e l'integrità della nazione; il "Libro Bianco sulla Difesa e Sicurezza Nazionale"[12] del 2013 che da rilievo alla necessità di allocare ulteriori risorse, sia finanziarie sia umane, alla protezione del ciberspazio e alla prevenzione di/reazione a attacchi coinvolgenti detto dominio, nonché stabilisce l'obiettivo della Francia di sviluppare capacità e soluzioni cyber tanto difensive quanto offensive[13]; il "Patto di Cyber Defence"[14] adottato dal Ministero della Difesa francese nel 2014 come seguito del Libro Bianco del 2013 e della Legge n. 2013-1168 riguardante la programmazione militare per il quinquennio 2014-2019[15]. Quest'ultima ha emendato il Codice della Difesa Militare integrandolo con disposizioni che fanno riferimento alla difesa da minacce cibernetiche che interessino, soprattutto, infrastrutture o sistemi informativi critici[16]. Non da ultimo, occorre ricordare che la strategia francese in materia di difesa cibernetica viene definita anche nella Dottrina Inter-Forze di Cyber Defence[17]. Avendo riguardo alla tipologia e, come emergerà tra breve, ai contenuti dei principali documenti richiamati sopra, emerge chiaramente il ruolo centrale assunto dall'Amministrazione della Difesa e alle Forze Armate francesi nella prevenzione e contrasto delle minacce cibernetiche. In altre parole, è possibile osservare che l'approccio francese alla protezione della nazione da pericoli che originano

[10] http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf.V.pp.53,96

[11] Adottata dall'Agenzia Nazionale per la Sicurezza dei Sistemi Informativi (vedi infra nel testo e nelle note), disponibile in inglese su http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

[12] In inglese su http://www.rpfrance-otan.org/White-Paper-on-defence-and.

[13] http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf.

[14] http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf.

[15] LOI n. 2013-1168 du 18 dicembre 2013 relative alla programmation militaire pour les annes 2014 - 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, disponibile in francese su http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825.

[16] Ibid., Ch. IV "Dispositions relatives a la protection des infrastructures vitales contre la cybermenace" e Ch. IX "Article Annexe".

[17] Documento classificato.

o si sviluppano da e attraverso il cyberspazio sembrerebbe inquadrarsi meglio nell'ambito della cyber-defence piuttosto che della cyber-security.

Tuttavia, a prescindere da eventuali categorizzazioni concettuali, il modello francese di sicurezza e difesa del cyber-spazio si basa su una visione strategica che si articola in chiari obiettivi di medio termine da perseguirsi attraverso l'adozione di specifiche misure. Secondo quanto stabilito dalla "Strategia Francese sulla Difesa e Sicurezza dei Sistemi Informativi" del 2011, la Francia mira a collocarsi tra le nazioni leader in materia di sicurezza cibernetica e ad acquisire le conoscenze specifiche e gli strumenti tecnici idonei ad assicurare "l'autonomia decisionale" della nazione, la sua integrità e sovranità, e a proteggere le sue infrastrutture critiche. Al fine di raggiungere tali obiettivi, la Francia intende promuovere iniziative rivolte a: favorire l'identificazione, la comprensione, la prevenzione e la risposta alle minacce cyber; acquisire soluzioni tecniche e risorse umane che consentano la difesa dello Stato e delle sue infrastrutture da tali minacce; definire un quadro legislativo idoneo a governare il cyber-spazio ed efficace nel perseguirne l'uso criminale; rafforzare la cooperazione con i principali attori internazionali; informare e sensibilizzare la popolazione circa i pericoli e le opportunità derivanti dall'uso dello spazio cibernetico. Gli obiettivi e le misure appena richiamati sono stati riconfermati ed elaborati oltre nel "Patto di Cyber Defence" che si articola e sviluppa in sei "assi" principali di intervento, o capisaldi, per ciascuno dei quali vengono previste specifiche azioni. Tali assi consistono ne:

1. il rafforzamento del livello di sicurezza dei sistemi informativi, in particolare di quelli in uso presso il Ministero della Difesa e amministrazioni o enti collegati;

2. la promozione di iniziative di ricerca e sviluppo a carattere multidisciplinare (tecnico ma anche strategico e di relazioni internazionali) in materia di cyber-defence orientate anche al fine di sostenere l'industria e le imprese nazionali;

3. il sostegno ad attività formative ed educative in materia di difesa cibernetica al fine di costituire e disporre di personale altamente preparato;

4. il sostegno alla costituzione di un centro di eccellenza in cyber-defence a vantaggio sia del Ministero della Difesa o, più in generale, della comunità nazionale di stake-holders della difesa cibernetica.

5. il rafforzamento della cooperazione internazionale con i principali attori attivi in Europa, in ambito Nato o nelle aree di interesse strategico per la Francia;

6. infine, la promozione della costituzione di una comunità nazionale di difesa cibernetica.

Sul piano organizzativo e a livello di direzione strategica, la responsabilità principale per la sicurezza e difesa del cyber-spazio viene attribuita al Primo Ministro che definisce le politiche, gli indirizzi e le linee di intervento in materia. Nello svolgere le sue funzioni, il Primo Ministro si avvale del supporto del Segretario Generale per la Difesa e la Sicurezza Nazionale alle cui dipendenze opera l'Agenzia Nazionale per la Sicurezza dei Sistemi Informativi [18]. L'Agenzia è un organismo centrale di coordinamento tra le differenti amministrazioni governative che ha competenza specifica in materia di sicurezza cibernetica e che si occupa di garantire la coerenza e l'efficacia delle misure adottate per salvaguardare la sicurezza dei sistemi informativi nazionali. L'Agenzia definisce gli standard di sicurezza per i sistemi informativi e di comunicazione di interesse governativo, monitora e vaglia il livello di sicurezza delle infrastrutture informative critiche, identifica e coordina la risposta ad attacchi o incidenti cyber, è responsabile per la cooperazione a livello internazionale, provvede alla formazione del personale in ruolo presso le amministrazioni dello Stato e offre consulenza e supporto ai Ministeri che ne avessero necessità. Per la sua aerea di competenza, l'Agenzia contribuisce inoltre alla definizione delle misure di prevenzione e risposta contenute nel piano nazionale anti-terrorismo (Vigipirate)[19]. Essa inoltre contribuisce alla definizione ed esecuzione delle misure previste nel piano settoriale di intervento per attacchi cyber su piattaforme informatiche e sistemi informativi (Piranet)([8] p. 14.). Nel definire la strategia e le politiche in materia di cyber-security e nel darvi attuazione, il Primo Ministro si avvale anche del Comitato Strategico sulla Sicurezza dei Sistemi Informativi[20], anche esso operante sotto la supervisione del Segretario Generale per la Difesa e la Sicurezza Nazionale.

A livello operativo, il Centro per la Sicurezza dei Sistemi Informativi presso l'Agenzia Nazionale è responsabile di identificare gli attacchi contro i sistemi informatici di infrastrutture critiche nazionali e di mitigarne gli effetti. Il Centro svolge anche la funzione di CERT nazionale (CERT-FR)[21] ovvero si occupa dell'analisi delle minacce e degli incidenti di natura cibernetica che posso interessare le infrastrutture critiche nazionali o altri enti governativi. Sempre a livello operativo, svolgono un ruolo rilevante il Centro Pianificazioni e Operazioni e il Centro Analisi per le Operazioni di Difesa Cibernetica istituiti presso il Ministero della Difesa francese. Il Centro Analisi si occupa di individuare, esaminare e rispondere ad attacchi cibernetici in collaborazione con Centro per la Sicurezza dei Sistemi Informativi. Qualora un attacco cyber sia in grado di

[18] `http://www.ssi.gouv.fr/`. L'Agenzia è stata istituita tramite Décret n. 2009-834 du 7 juillet 2009 disponibile su `http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212`.

[19] `http://www.ssi.gouv.fr/alertes/vigipirate/`

[20] `http://www.ssi.gouv.fr/agence/cybersecurite/comite-strategique/`.

[21] `http://www.cert.ssi.gouv.fr/`.

determinare una situazione di crisi tale da pregiudicare la sopravvivenza della nazione ovvero le sue capacità militari, il suo potenziale economico e la sua sicurezza, le agenzie e i servizi dello Stato, nei limiti del mandato assegnato loro dal Primo Ministro, sono autorizzati a condurre tutte le operazioni di natura tecnica necessarie a stabilire l'origine dell'attacco, attribuirne la responsabilità e a mitigarne gli effetti. Tale possibilità è prevista dal Codice della Difesa Militare come modificato dalla Legge n. 2013-1168[22].

Infine, occorre notare che in Francia è stata istituita la Riserva di Cyber-Defence[23]. Costituta da cittadini volontari con esperienza nel settore, la Riserva ha il mandato di contribuire alla sensibilizzazione della popolazione francese circa l'importanza della sicurezza del cyber ai fini della tutela dell'integrità e della sovranità della nazione. Posta sotto l'autorità dello Stato Maggiore della Difesa, la Riserva attualmente né svolge né partecipa a operazioni di cyber-defence, anche se è prevista la futura istituzione di una componente operativa della stessa.

A.3 La cyber security nei Paesi Bassi

La strategia, le priorità e l'organizzazione della cyber security dell'Olanda si comprendono considerando l'avanzato livello tecnologico e di democratizzazione del Paese, nonché l'alta competitività del mercato digitale nazionale. In particolare, due sono gli elementi portanti: un modello cooperativo stato-società civile in tutte le fasi di elaborazione e attuazione delle politiche di sicurezza cibernetica; una visione della cyber security più che come strumento finalizzato alla difesa dell'interesse nazionale in quanto tale, come fonte di benefici socio-

[22] V. Art. L. 2321-2. Codice Militare come modificato dall'Art. 21 della Legge n. 2013-1168: "Pour repondre a une attaque informatique qui vise les systémes d'information affectant le potentiel de guerre ou economique, la securité ou la capacité de survie de la Nation, les services de l'Etat peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires a la caractérisation de l'attaque et a la neutralisation de ses effets en accodant aux systémes d'information qui sont a l'origine de l'attaque". Il secondo paragrafo dell'articolo che prevede "Pour étre en mesure de répondre aux attaques mentionnées au premier alinea, les services de l'Etat determines par le Premier ministre peuvent détenir des équipements, des instruments, des programmes informatiques et toutes donnes susceptibles de permettre la réalisation d'une ou plusieurs des infractions provues aux articles 323-1 e 323-3 du code penal, en vue d'analyser leur conception et d'observer leur fonctionnemen" mira a ricondurre ad un quadro di legalità sia l'acquisizione che l'impiego da parte di autorità nazionali di tecniche e tecnologie di risposta di attacchi cyber altrimenti proibiti dal Codice Penale Francese.

[23] LOI n. 2013-1168, cit., Article Annexe (suite), par. 2.11.2.

economici allo stesso tempo per il Paese e per le attività private dei cittadini[24]. Tali elementi si ritrovano, con obiettivi diversi, nel contenuto di entrambi i documenti di strategia di cyber security pubblicati a oggi dal governo olandese. In effetti, nel primo, "Strategia di cyber-security nazionale: la forza attraverso la cooperazione"[25] (NCSS) del febbraio 2011, emergono l'estrema multipolarità, trasparenza e orizzontalità del sistema di cyber security nazionale; nel secondo, "Strategia di cyber-security nazionale: Dalla consapevolezza alla capacità"[26], (NCSS 2) dell'ottobre 2013, il collegamento tra difesa da minacce cibernetiche, innovazione tecnologica e sviluppo economico risulta centrale.

Con riguardo al NCSS del 2011, la presenza, fin dalla fine degli anni '90, di numerosi strumenti legislativi e di organi competenti in materia di tecnologie dell'informazione e comunicazione, spiega perché il documento si focalizzi sulla necessità innanzitutto di dare coerenza e organicità al sistema di cyber security esistente, rafforzando la cooperazione pubblico-privato e individuando con maggiore chiarezza le responsabilità dei diversi e molteplici attori coinvolti[27]. A tal fine, la NCSS ha previsto l'istituzione, a partire dal gennaio 2012, del Consiglio per la Cyber-security, come si dirà oltre, del coordinamento della strategia nazionale) e ha avviato la pubblicazione di analisi periodiche del rischio e delle minacce nazionali, i Cyber Security Assessments (CSAN).

Nel caso della NCSS 2, la consapevolezza di nuove e crescenti minacce cibernetiche internazionali è presentata come l'incentivo, prioritario, per rafforzare ed estendere, anche a livello transnazionale, alleanze e "coalizioni strategiche" tra i settori pubblico e privato, e per promuovere un elaborato risk-based approach per bilanciare continuamente la triade di interessi, spesso in conflitto, costituiti da 1) sicurezza nazionale e del business, 2) libertà individuali e del mercato digital, 3) benefici socio-economici[28]. Il Programma d'Azione 2014-2016, in appendice alla NCSS 2, individua poi più precisamente le azioni necessarie, nonché le corrispondenti figure governative e non governative responsabili, per il raggiungimento dei seguenti cinque obiettivi strategici del paese: 1)

[24] Sulla visione del governo olandese in materia di ICT si rimanda alla Digital Agenda del 2010 (Letter to Parliament, "Digital Agenda-nl", House of Representatives 2010-2011, 29 515, no. 331).

[25] Dutch National Cyber Security Centre, The National Cyber Security Strategy (NCSS): Strength Through Cooperation, Ministry of Security and Justice, The Hague, 2011.

[26] Dutch National Cyber Security Centre, National Cyber Security Strategy (NCSS) 2: From Awareness to Capability, Ministry of Security and Justice, The Hague, 2013.

[27] K. Kaska, National Cyber Security Organisation: the Netherlands, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, 2015, p. 7.

[28] Dutch National Cyber Security Centre, National Cyber Security Strategy (NCSS) 2, cit., p. 17.

la resilienza agli attacchi cyber e la protezione degli interessi vitali nella sfera digitale, 2) la capacità di risposta al *cyber crime*, 3) l'investimento nazionale in prodotti ICT sicuri e in servizi a protezione della privacy, 4) la creazione di alleanze per la libertà, la sicurezza e la pace nella sfera digitale, 5) le conoscenze e competenze sufficienti, in materia di cyber-security, a raggiungere gli obiettivi prefissati[29].

In tema di sicurezza e difesa, la cyber security è inclusa tra le questioni prioritarie nella "Strategia nazionale anti-terrorismo 2011-2015" del 2011[30], nella "International Security Strategy" del giugno 2013[31], e affrontata estesamente dal Ministero della Difesa nella "Strategia di Difesa Cyber", pubblicata nel giugno 2012[32]. La Strategia, basata in parte sulla NCSS del 2011, individua tre missioni principali di responsabilità del Ministero: proteggere l'integrità territoriale; promuovere la stabilità e il principio dello stato di diritto; dare supporto alle autorità civili responsabili dell'applicazione della legge. Per ognuna delle missioni le relazioni politico-costituzionali definiscono le procedure d'azione. In particolare, è previsto che lo spiegamento delle forze armate per missioni internazionali avvenga per mandato del Governo, mentre nel caso di iniziative nazionali a seguito di una richiesta di assistenza da parte delle autorità civili, generalmente il Ministero di Sicurezza e Giustizia[33].

Sul piano organizzativo, la NCSS 2 identifica più di venti attori con responsabilità individuali e collettive a livello governativo (Ministeri, agenzie governative, servizi di polizia, Procura, fiscal intelligence), nell'ambito della ricerca scientifica (l'Organizzazione per la Ricerca scientifica dell'Olanda) e nel settore privato (in particolare nel settore finanziario)[34]. Parallelamente, la NCSS ha promosso nel 2011 la creazione del Consiglio per la Cyber Security e del Centro Nazionale per la Cyber-Security Nazionale (NCSC).

Il Consiglio per la Cyber-Security è un organismo nazionale strategico, operativo dal 30 giugno 2011 e istituito formalmente dal Ministero di Sicurezza e Giustizia[35]. è co-diretto da rappresentanti del Governo e dell'industria nazionale, e più in generale da importanti rappresentanti dei settori privato, pubblico e scientifico, con l'obiettivo di garantire un bilanciamento degli interessi coin-

[29] Ibid., pp. 28-34.

[30] `https://english.nctv.nl/Images/nationale-ct-strategie-2011-2015-uk_tcm92-369807.pdf`.

[31] "A Secure Netherland in a Secure World", in inglese su `http://www.government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html`.

[32] The Defence Cyber Strategy. Defence Strategy for operating in Cyberspace, Ministry of Defence, 2012.

[33] Ibid., 4.

[34] K. Kaska, National Cyber Security Organisation: the Netherlands, cit., p. 10.

[35] `http://www.cyber-securityraad.nl`.

volti. Al Consiglio è attribuita la primaria responsabilità di coordinamento di tutti gli attori nazionali coinvolti sulla base di un'unica strategia cyber nazionale, insieme alle funzioni di consulenza al governo e agli attori privati sugli sviluppi nel settore della cyber-security, di contributo alla ricerca in coerenza con l'Agenda per la cyber security olandese e di coinvolgimento di membri del Consiglio durante gravi incidenti cyber[36].

Il Centro Nazionale per la Cyber-Security (NCSC) è inserito nel Dipartimento di Cyber Security, parte del Coordinatore nazionale per la sicurezza e l'antiterrorismo all'interno del Ministero di Sicurezza e Giustizia[37]. Sebbene subordinato formalmente al governo centrale, il NCSC è il risultato di una partnership pubblico-privata e le sue funzioni trascendono quelle governative: il board del NCSC include esperti indipendenti e rappresentanti del settore privato e il Centro, oltre ad incorporare il preesistente CERT governativo nazionale (`govCert.nl`), è finalizzato all'elaborazione di una Computer Network Defence tramite lo sviluppo di tre network e assi di ricerca e consulenza: un national detection network, un national response network (ICT Crisis) e un national expertise network [33]. Infine, il NCSC elabora e presenta i periodici Cyber Security Assessments Netherlands (CSAN, prima CSBN) di supporto al lavoro del Consiglio per la Cyber-Security[38].

A.4 La cyber security nella Federazione Russa

La Russia – oltre a essere uno tra i paesi da cui proviene il maggior numero di attacchi cyber del mondo[39] – ricopre, in materia di cyber security, un ruolo di grande rilievo a livello internazionale, da più punti di vista: per l'assoluta e ormai decennale priorità attribuita al tema nell'ambito della politica estera e di difesa nazionale; per lo stadio avanzato e in continua evoluzione delle tecnologie cyber (su impulso del Ministero della Difesa e del Governo); infine, per una posizione in sede ONU e in altre piattaforme internazionali nettamente a favore di una comune regolamentazione pubblica della sfera digitale, posizione che la avvicina alla Cina e che è invece in contrasto con l'orientamento liberale degli Stati Uniti e di altri paesi occidentali [4].

---

[36] Ibid.

[37] In inglese su `https://www.ncsc.nl/english/organisation`.

[38] Il documento più recente è il CSAN-4 - `https://english.nctv.nl/Images/cyber-securityassessmentnetherlands2014_tcm92-580598.pdf?cp=92&cs=65035`.

[39] Si vedano le dichiarazioni del Direttore dell'Intelligence Nazionale USA James Clapper: `http://blogs.wsj.com/washwire/2014/10/17/intel-chief-russia-tops-china-as-cyber-threat/`.

Nel suo complesso, la strategia di cyber security russa si fonda – soprattutto dall'avvio della Prima Presidenza Putin nel 2000 – su una visione tradizionale dell'interesse nazionale e del nemico, secondo cui i confini fisici territoriali delimitano tuttora la sfera interna da quella esterna e la sicurezza nazionale è prioritaria e autonoma rispetto alla cooperazione internazionale. Tale visione, incompatibile con l'intrinseca natura permeabile e transnazionale delle frontiere nella sfera digitale, porta la dirigenza russa a interpretare la progressiva digitalizzazione e l'esistenza di un mercato digitale a-nazionale come una minaccia all'integrità territoriale del Paese più che come un'opportunità e più precisamente come un'ingerenza veicolata da alcuni Stati (tra tutti, gli Stati Uniti) al fine di minare la sovranità statale del Paese. Conseguentemente, la strategia di cyber security nazionale, essenzialmente difensiva[40], si qualifica innanzitutto come sezione rilevante della politica di sicurezza e di difesa del Paese, ed è definita dal fondamentale "Concetto di Sicurezza Nazionale della Federazione Russa" del 2000[41], a cui hanno fatto seguito, nel 2011, il documento sulle "Visioni concettuali riguardanti le attività delle forze armate della Federazione Russa nella Sfera dell'Informazione"[42], e, nel 2013, il "Concetto di Politica Estera della Federazione Russa"[43]. Come si può notare, il concetto di cyber-security è, nel linguaggio ufficiale russo, sostanzialmente assimilato a quello di "sicurezza dell'informazione". In altri termini, l'idea di minaccia cibernetica è legata innanzitutto a quella di un flusso incontrollato (e da controllare a livello governativo) di informazione nella sfera digitale.

Dal punto di vista del contenuto, nel "Concetto di Sicurezza Nazionale della Federazione Russa" del 2000 si afferma che la volontà di un certo numero di Paesi di "dominare lo spazio dell'informazione globale ed espellere la Russia dal mercato nazionale e internazionale dell'informazione" rappresenta per la Russia una grave minaccia. Vengono poi individuati i principali obiettivi tesi a garantire la sicurezza dell'informazione in Russia: 1) il rispetto dei diritti e delle libertà costituzionali dei cittadini nelle attività relative all'informazione, 2) lo sviluppo di infrastrutture nazionali per l'informazione e l'integrazione della Russia nella sfera dell'informazione globale 3) la capacità di risposta alle minacce di antagonismo ("threats of rivalry") nella sfera dell'informazione[44].

Sulla base del Concetto di sicurezza nazionale, il successivo "Concetto di

[40] K. Giles, Russian Cyber Security: Concepts and Current Activity, REP Roundtable Summary, Chatham House, 6 settembre 2012, disponibile su http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Russia%20and%20Eurasia/060912summary.pdf

[41] http://www.mid.ru/bdomp/ns-osndoc.nsf/

[42] http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

[43] http://www.mid.ru/brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D.

[44] Concetto di Sicurezza nazionale della Federazione Russa', parte IV.

Politica Estera della Federazione Russa" del 12 febbraio 2013 afferma poi che il Paese si impegna 1) ad adottare le misure atte ad assicurare la sicurezza dell'informazione nazionale e internazionale e prevenire le minacce "politiche, economiche e sociali" alla sicurezza nazionale, incluse le azioni mirate a interferire negli affari interni nazionali e minacciose della pace internazionale, della sicurezza e della stabilità 2) a promuovere attivamente in sede ONU l'elaborazione di un codice internazionale di condotta per la sicurezza dell'informazione.

Con riguardo ai documenti specificamente relativi alla sicurezza dell'informazione, sono principalmente cinque quelli da tenere in considerazione: la "Dottrina della Sicurezza dell'Informazione" del settembre 2000[45]; la legge su "L'Informazione, le tecnologie informatiche e la protezione dell'informazione" del 2006[46]; la "Strategia di sviluppo della società dell'informazione" del febbraio 2008[47]; "I Principi base della politica statale della Federazione russa in materia di sicurezza internazionale dell'informazione" del 2013[48]; infine, il progetto legislativo sul "Concetto della strategia di cyber-security della Federazione Russa"[49].

La "Dottrina della Sicurezza dell'Informazione" espande il contenuto in materia di sicurezza dell'informazione già inserito nel Concetto di sicurezza nazionale sopra citato, e individua 4 elementi per la difesa dell'interesse nazionale nella sfera dell'informazione: 1) il diritto costituzionalmente previsto dei cittadini a ricevere e fare uso dell'informazione, contestualmente all'assicurazione di una "rinascita spirituale della Russia e di un rafforzamento dei valori morali della società" 2) il sostegno alle politiche governative da parte dei servizi di informazione tramite un rafforzamento dei mass media statali 3) la promozione di tecnologie moderne dell'informazione 4) La protezione delle fonti di informazione da accessi non autorizzati e la difesa dei sistemi di telecomunicazione esistenti.

Da ultimo il progetto sul "Concetto della strategia di cyber security della Federazione Russa" è stato presentato presso il Consiglio della Federazione (la Camera bassa del parlamento bicamerale) nel novembre 2013. Il testo, al febbraio 2015 ancora in fase di stallo, è importante nel suo contenuto per tre ragioni principali 1) è la prima volta che un documento strategico ufficiale della Federazione fa diretto riferimento al termine "cyber security" (in russo kiberbezopasnost') 2) sottolinea esplicitamente l'esigenza di un maggiore coordinamento degli

[45] In inglese su `http://www.mid.ru/bdomp/ns-osndoc.nsf/`

[46] In russo su `http://www.rg.ru/2006/07/29/informacia-dok.html`.

[47] In russo su `http://www.rg.ru/2008/02/16/informacia-strategia-dok.html`.

[48] In inglese su `https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf`.

[49] In russo su `http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf`

attori coinvolti nell'elaborazione e attuazione della strategia nazionale 3) individua e distingue, seppur genericamente, le responsabilità in capo allo Stato, al business e alla società civile.

I passaggi citati evidenziano come in Russia – contrariamente ad altri Paesi europei – l'attenzione sia maggiormente incentrata sulle minacce e sulla definizione di ampi obiettivi di difesa dell'interesse nazionale che non sulla trasparenza e l'attuazione pratica della strategia di cyber security elaborata.

Sul piano organizzativo, in effetti, i singoli e molteplici attori coinvolti mancano nella maggior parte dei casi di un coordinamento organico e di un'attribuzione di precise responsabilità per il raggiungimento degli obiettivi nazionali in materia di cyber security e i documenti legislativi relativi sono tradotti dal russo solo in rarissimi casi. Nel suo complesso, il sistema fa da ultimo capo al potere decisionale del Presidente della Federazione e si articola esclusivamente a livello statale e governativo, senza coinvolgere organicamente rappresentanti del settore privato. In particolare, il maggior numero di organismi a cui sono attribuite specifiche competenze in materia di sicurezza dell'informazione e cyber security si trovano all'interno del Ministero della Difesa, affiancati da uffici subordinati al Ministero degli Affari Interni, al Consiglio di Sicurezza, all'Organizzazione per la Sicurezza Federale e ai Servizi di Intelligence nazionale (FSB).

A.5 La cyber security negli Stati Uniti d'America

Il bilancio federale per il 2016 proposto dal presidente Obama prevede lo stanziamento di 14 miliardi di dollari in materia di cyber security, con un incremento del 10% rispetto all'anno precedente. L'aumento appare decisamente consistente soprattutto se confrontato con quanto accade negli altri capitoli della spesa pubblica statunitense; esso conferma che l'amministrazione americana ha inserito la *cyber security* nella agenda delle sue priorità strategiche sia sul versante della politica interna che della politica estera. Questa scelta era stata peraltro anticipata dal presidente Obama nel discorso dell'Unione del gennaio 2015[50] . La priorità assoluta di combattere con strumenti adeguati la minaccia cyber è stata successivamente ribadita nel rapporto "*Worldwide Threat Assessment*" presentato il 26 febbraio 2015 dal Director of National Intelligence James Clapper al Senato[51].

Rispetto alle previsioni complessive in materia di cyber security per il 2016, 5,5 miliardi di dollari sono destinati a una vasta gamma di iniziative che fanno

[50] `https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015`

[51] `http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-26-15.pdf`

capo al Pentagono. Non c'è qui spazio per descrivere dettagliatamente queste attività, ma basta dare uno sguardo alla Cyber Strategy del Department of Defense pubblicata nell'aprile 2015[52] per cogliere come alcune iniziative siano finalizzate alle esigenze specifiche delle forze armate, mentre altre vanno oltre l'ambito strettamente militare.

Per quanto riguarda le prime, il dato più rilevante è costituito dalla messa in sicurezza delle reti globali interforze (*securing DoD's systems, networks & data worldwide*)[53]. Esse prevedono, inoltre, l'incremento di spesa del 7% per il budget 2016 del Cyber Command (CYBERCOM)[54]. Questo aumento è soprattutto finalizzato alla creazione di una nuova forza (*Cyber Mission Force*) composta da circa 6200 operatori in grado di condurre *cyber operations* di carattere difensivo e offensivo. La *Cyber Mission Force* è articolata in 113 unità operative e dovrebbe essere pienamente operativa entro il 2018[55]. Il Pentagono intende attrarre i migliori talenti disponibili e a tale scopo la forza avrà al suo interno anche una significativa componente civile.

Il terzo blocco di obiettivi contenuti nella *Cyber Strategy* approvata dal Pentagono nell'aprile scorso travalica, invece, l'ambito della difesa e fa riferimento alla protezione cibernetica degli interessi nazionali degli Stati Uniti in un ampio spettro di settori strategici storicamente e/o potenzialmente oggetti di attacco informatico[56]. È soprattutto in questo ambito (sicurezza nazionale) che l'assetto istituzionale e organizzativo della cyber security negli Stati Uniti si interseca con il delicato rapporto tra Difesa e Intelligence (la cyber intelligence è parte integrante della cyber security).

Ci riferiamo specificatamente alla relazione "particolare" che lega il ruolo del Cyber Command (come abbiamo visto recentemente rafforzato) e le funzioni della NSA[57]. Al di là della stessa collocazione fisica di NSA e CYBERCOM a Fort Meade, il dato più importante è che la guida dei due organismi resta affidata alla stessa persona (dall'aprile del 2014 l'ammiraglio Michael Rogers). Ciò che risulta evidente è che – nonostante le polemiche collegate al cosiddetto"*Snowden effect*" – la concentrazione della responsabilità di comando nella stessa persona fisica è apparsa all'amministrazione americana come la formula più adatta per assicurare in modo pragmatico una efficace *interagency coordination* in ambi-

[52] `http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf`

[53] `http://www.c4isrnet.com/story/military-tech/disa/2015/05/13/disa-defends-dod-networks/27248881/`

[54] USCYBERCOM è stato creato nel 2010 e il suo peso all'interno del Pentagono è cresciuto notevolmente negli ultimi anni.

[55] `http://www.defense.gov/home/features/2015/0415_cyber-strategy/`

[56] Ibidem, pp

[57] `https://www.nsa.gov/public_info/press_room/2015/3rd_Science_of_security_competition.shtml`

to Cyber, condizione essenziale per far fronte alla maggiore sfida tecnologica e operativa che impegnerà la sicurezza degli Stati Uniti nei prossimi anni.

Non c'è qui spazio per approfondire le molteplici implicazioni giuridiche della responsabilità congiunta di organismi militari e di intelligence nell'ambito del diritto interno statunitense e in particolare il precario equilibrio tra il diritto dei cittadini alla privacy e il diritto dei cittadini alla sicurezza. Non possiamo tuttavia esimerci dal segnalare la sentenza del 7 maggio 2015 in cui la Second Circuit Court of Appeals di New York ha rovesciato il pronunciamento distrettuale di primo grado e contestato alla NSA di aver svolto attività di *surveillance* dei cittadini americani (raccolta di meta dati) che vanno oltre ciò che è consentito dal Patriot Act, legge peraltro in via di esaurimento[58]. Ad avviso della Corte non c'è stata un'esplicita violazione della Costituzione, ma spetta al Congresso rimettere le mani sulla materia riformulando i provvedimenti o semplicemente ordinando alla NSA l'interruzione della raccolta di meta dati.

A pochi giorni dalla sentenza, la Camera dei Rappresentanti ha approvato una nuova legge denominata"USA Freedom Act"[59], ma nelle settimane successive il Senato (anche sulla base di una dura campagna politica del senatore repubblicano del Kentucky Rand Paul) ha bocciato la nuova normativa. Proprio mentre scriviamo è in corso un braccio di ferro tra il Presidente Obama e il Senato su questa incandescente materia. Mentre al Congresso democratici e repubblicani avevano concordato una soluzione di compromesso, al Senato, invece, la nuova normativa è considerata ancora troppo invasiva della privacy dei cittadini americani.

È difficile prevedere l'esito finale di questo scontro, ma è probabile che nel prossimo futuro le strategie di cyber security degli Stati Uniti dovranno muoversi in un perimetro giuridico e operativo di maggiore prudenza nel caso in cui le attività operative coinvolgano direttamente o indirettamente cittadini americani. In altra sede abbiamo già avuto modo di sottolineare come non sia sempre facile conciliare i principi del diritto interno con gli imperativi di cyber security di una super potenza che opera su scala globale[60].

Oltre alla relazione CYBERCOM / NSA, un altro versante particolarmente complesso riguarda la protezione delle infrastrutture critiche. È noto che la grande maggioranza delle infrastrutture critiche statunitensi sono gestite da imprese private. Queste ultime in maggiore o minore misura si oppongono a un ruolo "intrusivo" di organismi governativi. È altrettanto noto come in questo campo le relazioni tra Pentagono, Department of Homeland Security e Depart-

[58] http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf

[59] http://www.theverge.com/2015/5/13/8601533/house-passes-usa\
-freedom-act-nsa

[60] https://www.academia.edu/4509736/La_politica_Internazionale_
nellEra_Digitale_bozza_da_non_citare_

ment of Commerce (NIST)[61] non siano facili, nonostante i ripetuti tentativi di definire e regolamentare i rispettivi ruoli.

È piuttosto chiara la distinzione nella protezione delle reti pubbliche: il `.mildomain` sotto la giurisdizione del DoD e il `.govdomain` sotto al DHS[62]. Tuttavia le infrastrutture critiche non appartengono né all'uno né all'altro dominio, ma il loro funzionamento è assolutamente vitale per entrambi. Ciò rende particolarmente complesso l'intervento pubblico e assai difficile una tempestiva capacità di information sharing su attacchi, rischi ed evoluzione tecnologica delle minacce [55]. Il più recente tentativo di affrontare questa materia risale al febbraio 2015. Il presidente Obama ha, infatti, emanato un executive order che punta a incentivare la collaborazione e la condivisione dei dati tra pubblico-privato in materia di cyber security[63]. La responsabilità del coordinamento degli interventi è affidata al Homeland Security Department, ma assai significativo è il ruolo affidato al Pentagono. In particolare, ad esso spetta formulare le prescrizioni operative di cyber security delle informazioni classificate riconducibili al National Industrial Security Program (le industrie più "sensibili")[64].

Al di là dei difficili meccanismi di coordinamento (tra le diverse agenzie governative e tra pubblico e privato), è importante segnalare che i nuovi stanziamenti rafforzano ulteriormente le capacità tecniche del binomio Cyber Command/NSA in materia di cyber security: già oggi – qualora l'intervento sia richiesto dal decisore politico – il Pentagono è in grado di garantire l'intervento più efficace.

Quanto affermato sin qui – a prescindere del variare delle norme giuridiche e degli assetti organizzativi formali – conferma la grande rilevanza della componente di estrazione militare nella concreta configurazione e implementazione della cyber security policy statunitense. Ma, al di là delle apparenze, queste evoluzioni recenti non indicano – a nostro avviso – una nuova tendenza alla "militarizzazione" della cyber security negli Stati Uniti. Certamente pesa la *historical legacy* (la tradizionale influenza degli apparati militari nelle politiche tecnologiche di Washington, nonché il ruolo storicamente conquistato da DARPA nella più avanzata ricerca tecnologica), ma ciò che più conta è il dato oggettivo: la profondità degli sconvolgimenti (e le grandi contraddizioni) indotte della rivoluzione digitale. Proprio l'ammiraglio Rogers ha recentemente sottolineato come essa abbia "travolto" gli assetti tradizionali e come una serie di distinzioni stiano rapidamente perdendo significato. L'era digitale ha innescato una com-

[61] `http://www.fiercegovernmentit.com/`

[62] `http://www.dhs.gov/topic/cybersecurity`

[63] `https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information\-shari`

[64] `http://www.dtic.mil/whs/directives/corres/pdf/522022_vol3t_2014.pdf`

plessa "catena di convergenze" che nella realtà statunitense saltano agli occhi con particolare evidenza: è sempre più arduo tracciare un nitido confine tra sfera civile e sfera militare, tra mondo virtuale e mondo reale, tra dimensione difensiva e dimensione offensiva, tra pubblica sicurezza e sicurezza nazionale.

L'accelerazione impressa negli ultimi mesi dall'amministrazione Obama in materia di cyber security non è peraltro limitata alle strutture militari e di intelligence, ma investe il governo federale a 360 gradi, ispirandosi a una visione strategica che il governo americano ha progressivamente reso sempre più esplicita negli ultimi cinque anni. Per quanto riguarda l'imperativo di superare la tradizionale rivalità tra le diverse amministrazioni, il presidente Obama ha, ad esempio, rilanciato e irrobustito la "*Comprehensive National Cybersecurity Initiative* (CNCI)[65] avviata da G. W. Bush sin dal gennaio 2008. La nuova versione della CNCI si articola in una serie di iniziative finalizzate a irrobustire le capacità di cyber security del governo federale nel suo insieme e coinvolge anche gli altri livelli istituzionali (Stati e autorità locali).

Per quanto riguarda le attività intraprese dal governo federale, è doveroso innanzitutto segnalare alcune rilevanti novità relative alla cyber security in politica estera. Da un lato l'amministrazione sta avviando una serie di accordi di cooperazione bilaterale in materia di cyber security con paesi amici e alleati. All'inizio del 2015 è stato raggiunto un importante accordo di cooperazione con il Regno Unito[66]. Mentre il passo più recente è quello con il Giappone ed è sancito dal *Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group* del 29 maggio 2015[67]. Tuttavia, mentre si sviluppano gli accordi bilaterali, si intensificano contemporaneamente le reazioni di natura offensiva e/o coercitiva: ad esempio con un Executive Order emanato il 1 aprile 2015, il Presidente Obama ha per la prima volta imposto una serie di pesanti sanzioni alle persone sospettate di condurre dall'estero cyber attacchi contro gli Stati Uniti[68].

Un notevole sforzo di carattere globale è anche compiuto dal Ministero del Tesoro che, attraverso il Financial Sector Cyber Intelligence Group (CIG)[69], svolge attività di analisi e di supporto con l'obiettivo di spingere le istituzioni finanziarie americane (oggetto di un numero impressionante di attacchi quotidiani) a dotarsi di strategie e di strumenti di cyber security sempre più aggiornati. In

[65] https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

[66] https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation

[67] http://www.defense.gov/releases/release.aspx?releaseid=17310

[68] https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging\-significant-m

[69] http://www.risk.net/operational-risk-and-regulation/news/2402102/us-treasurys-cyber-chief-lays-out-cyber-security-blueprint

questo ambito un ruolo sempre più importante è svolto dal Financial Services Information Sharing and Analysis Center (FS-ISAC)[70]. Il centro, promosso dalle stesse istituzioni finanziarie e nato nel lontano 1999, ha recentemente adottato il Critical Infrastructure Notification System (CINS) con l'obiettivo della condivisione in tempo reale delle informazioni disponibili sugli attacchi cyber, ma, come è noto, in questo delicato settore le resistenze del sistema bancario rendono particolarmente difficile gli sforzi di coordinamento.

Sul versante interno, infine, sono da segnalare le iniziative dei Ministeri dell'Energia e della Salute (attraverso la Food and Drug Administration) che hanno emanato direttive in materia di cyber security per i rispettivi settori industriali (aziende energetiche nel primo caso, forniture di attrezzature medicali ed ospedaliere nel secondo)[71].

Rilevante è inoltre quanto previsto dal Ministero della Giustizia che, nell'aprile 2015, ha definito una prima versione delle modalità di "Reporting of Cyber Incidents"[72].

Questo breve excursus – certamente non esaustivo – sulle più recenti iniziative intraprese dagli Stati Uniti in materia di cyber security non può non includere il tema cruciale della Cyber Security Awareness. Sotto gli auspici del Homeland Security Department si svolgono numerose iniziative della National Cyber Security Alliance dal 2008 diretta da Michael Kaiser e finanziata dai maggiori gruppi privati che operano nel settore. Le campagne di comunicazione promosse dalla NCSA sono assai vaste e articolate per singoli target (dal pubblico alle scuole, sino ai manager aziendali [73]) e si possono consultare nel sito `https://www.staysafeonline.org/`. Sempre in tema di Cyber Security Awareness possiamo segnalare, infine, la campagna promossa direttamente dal Homeland Security Department e denominata: Stop. Think. Connect[74] "*Stop: Before you use the Internet, take time to understand the risks and learn how to spot potential problems. Think: Take a moment to be certain the path ahead is clear. Consider how your actions online could impact your safety, or your family's. Connect: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer*".

---

[70] `https://www.fsisac.com/about`

[71] `http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf` and `http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/OtherMOUs/ucm412565.htm`

[72] `http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf`

[73] `https://www.staysafeonline.org/re-cyber/`

[74] `http://www.dhs.gov/stopthinkconnect`

Indice dei contributi

Affiliazioni degli autori

Luca Allodi	Università degli Studi di Trento
Alessandro Armando	Università degli Studi di Genova
Roberto Baldoni	Università degli Studi di Roma La Sapienza
Antonio Barili	Università degli Studi di Pavia
Sandro Bologna	Associazione Italiana Infrastrutture Critiche
Matteo E. Bonfanti	Scuola Superiore Sant'Anna di Pisa
Silvia Bonomi	Università degli Studi di Roma La Sapienza
Francesco Buccafurri	Università degli Studi Mediterranea di Reggio Calabria
Enrico Cambiaso	Università degli Studi di Genova
Costantina Caruso	Università degli Studi di Bari
Michele Colajanni	Università degli Studi di Modena e Reggio Emilia
Luigi Coppolino	Università degli Studi di Napoli Parthenope
Fabrizio d'Amore	Università degli Studi di Roma La Sapienza
Salvatore D'Antonio	Università degli Studi di Napoli Parthenope
Sabrina De Capitani di Vimercati	Università degli Studi di Milano
Rocco De Nicola	IMT Institute for Advanced Studies Lucca
Carolina De Stefano	Scuola Superiore Sant'Anna di Pisa
Tommaso De Zan	Istituto Affari Internazionali
Federica Di Camillo	Istituto Affari Internazionali
Giorgio Di Natale	CNRS, Francia

Andrea Di Nicola	Università degli Studi di Trento
Andrea Dimitri	Università degli Studi di Roma Tor Vergata
Gianluca Dini	Università degli Studi di Pisa
Riccardo Focardi	Università Ca' Foscari, Venezia
Giuseppe F. Italiano	Università degli Studi di Roma Tor Vergata
Giovanni Lagorio	Università degli Studi di Genova
Antonio Lioy	Politecnico di Torino
Michele Loreti	Università degli Studi di Firenze
Federico Maggi	Politecnico di Milano
Marco Mayer	Scuola Superiore Sant'Anna di Pisa
Alberto Marchetti Spaccamela	Università degli Studi di Roma La Sapienza
Luigi Martino	Università degli Studi di Firenze
Fabio Massacci	Università degli Studi di Trento
Massimo Mecella	Università degli Studi di Roma La Sapienza
Luca Montanari	Università degli Studi di Roma La Sapienza
Gian Domenico Mosco	Università LUISS *Guido Carli*
Ida Panetta	Università degli Studi di Roma La Sapienza
Vincenzo Piuri	Università degli Studi di Milano
Paolo Prinetto	Politecnico di Torino
Luigi Romano	Università degli Studi di Napoli Parthenope
Pierangela Samarati	Università degli Studi di Milano
Donatella Sciuto	Politecnico di Milano
Fabio Scotti	Università degli Studi di Milano
Stefano Silvestri	Istituto Affari Internazionali
Maurizio Talamo	Università degli Studi di Roma Tor Vergata
Alberto Trombetta	Università degli Studi Insubria
Fiamma Terenghi	Università degli Studi di Trento
Aaron Visaggio	Università degli Studi del Sannio
Stefano Zanero	Politecnico di Milano

Bibliografia

[1] M. Ambrosin, C. Busold, M. Conti, A.-R. Sadeghi, M. Schunter: Updaticator: Updating Billions of Devices by an Efficient, Scalable and Secure Software Update Distribution Over Untrusted Cache-enabled Networks Proceedings of the European Symposium on Research in Computer Security (ESORICS 2014), pages 76-93, 2014.

[2] M. Ambrosin, M. Conti, T. Dargahi: On the Feasibility of Attribute-Based Encryption on Smartphone Devices. Proceedings of the 1st International Workshop on IoT challenges in Mobile and Industrial System (MobiSys 2015 workshop: IoT-Sys, 2015.

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

[4] L. Arimatsu, A Treaty for governing cyber-weapons: Potential Benefits and Practical Limitations, in Cyber Conflict (CYCON), 2012 4th International Conference on (pp. 1-19). IEEE, 2012.

[5] R. Baldoni, G. Chockler: Collaborative Financial Infrastructure Protection - Tools, Abstractions, and Middleware. Springer 2012.

[6] R. Baldoni, F. d'Amore, M. Mecella, D. Ucci: A Software Architecture for Progressive Scanning of On-line Communities. ICDCS Workshops (pp. 207-212), 2014.

[7] R. Bardou, R. Focardi, Y. Kawamoto, L. Simionato, G. Steel and J.-K. Tsay: Efficient Padding Oracle Attacks on Cryptographic Hardware, 2012. In *32nd International Cryptology Conference* (CRYPTO 2012). Santa Barbara, USA, 2012.

[8] P. Brangetto: National Cyber Security Organisation: France - `https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015.pdf`, Tallin 2015.

[9] A. Bellissimo, J. Burgess, K. Fu: Secure Software Updates: Disappointments and New Challenges. In: 1st USENIX Workshop on Hot Topics in Security, pp. 37-43. USENIX Association, Berkeley, 2006.

[10] M. Bortolozzo, M. Centenaro, R. Focardi, G. Steel: Attacking and Fixing PKCS#11 Security Tokens. In proceedings of the *17th ACM Conference on Computer and Communications Security* (ACM CCS 2010), Chicago USA, 2010.

[11] A. R. Clarke, K.R. Knake: Cyberwar. The Next Threat to National Security and What to do About It, HarperCollins Pubblishers, New York, 2010.

[12] S. Checkoway et al.: Comprehensive Experimental Analyses of Automotive Attack Surfaces USENIX Security Symposium, 2011.

[13] N. Choucri: Cyberpolitics in International Relations, The MIT Press Cambridge, Massachusetts, 2012.

[14] J. Clulow: On the security of PKCS#11. In *5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'03)*, volume 2779 of *LNCS*, pages 411–425. Springer Verlag, 2003.

[15] A. L. Clunan and H. A. Trinkunas (editors): Ungoverned Spaces. Alternatives to State Authority in an Era of Softened Sovereignty. Stanford University Press, 2010.

[16] CIS Sapienza: Italian Cyber Security Report. Research Center of Cyber Intelligence and Information Security Università di Roma "La Sapienza", 2013.

[17] A. Dardanelli, F. Maggi, M. Tanelli, S. Zanero, S. M. Savaresi, R. Kochanek, T. Holz: A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth". IEEE Embedded Systems Letters 5(3): 34-37, 2013.

[18] S. De Capitani di Vimercati, S. Foresti, and P. Samarati:. Managing and accessing data in the cloud: Privacy risks and approaches. In Proc. of the 7th International Conference on Risks and Security of Internet and Systems (CRiSIS 2012), 2012.

[19] N. De Scalzi, I. Chiarugi, L. Martino, M. Mayer: La politica internazionale nell'era digitale. Dispersione o concentrazione del potere? in Intelligence e Interesse Nazionale (a cura di U. Gori e L. Martino), Aracne Editrice, Roma - https://www.academia.edu/14336129/International_Politics_in_the_Digital_Age, 2015.

[20] Department of Homeland Security, USA. Stop.Think.Connect. Industry Resources - http://www.dhs.gov/publication/stopthinkconnect-industry-resources.

[21] R. Donida Labati, V. Piuri, F. Scotti: Touchless Fingerprint Biometrics, CRC Press, Series in Security, Privacy and Trust, August, 2015.

[22] M. J. Fischer, N. A. Lynch, M. Paterson: Impossibility of Distributed Consensus with One Faulty Process. J. ACM 32(2): 374-382, 1985.

[23] C.B. Frey, M.A. Osborne: The Future of Employment - Oxford Martin School - http://www.oxfordmartin.ox.ac.uk/publications/view/1314, 2013.

[24] F. D. Garcia, G. de Koning Gans, R. Verdult, M. Meriac: Dismantling iClass and iClass Elite. In S. Foresti and M. Yung , editors, *17th European Symposium on Research in Computer Security* (ESORICS 2012). Lecture Notes in Computer Science, Vol. 7459, Springer Verlag, 2012.

[25] Gartner Research: Data center modernization and consolidation key initiative overview, Gartner research, 2014.

[26] A. Genovese, V. Piuri, F. Scotti:Touchless Palmprint Recognition Systems, Springer, Vol. 60, Advances in Information Security, 2014.

[27] C. Gentry: A Fully Homomorphic Encryption Scheme. Ph.D. Dissertation. Stanford University, CA, USA. Advisor Dan Boneh, 2009.

[28] S. Gilbert, N. A. Lynch: Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. SIGACT News 33(2): 51-59, 2002.

[29] World Economic Forum: Global Risks 2014, Insight Report Ninth Edition - http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, 2014.

[30] U. Gori, L. Martino (curatori): Intelligence e Interesse Nazionale, Aracne editrice, Roma, 2015.

[31] C. J. Hadnagy, J.O. Gorman, D. Shar, E. Maxwell: Security through education, Defcon19, 2011.

[32] M. Hasan, N. Prajapati, S. Vohara: Case Study on Social Engineering Techniques for Persuasion, International journal on applications of graph theory in wireless ad hoc networks and sensor networks Vol 2 (2), 2010.

[33] E.V.D. Heuvel, G.K. Baltink, Coordination and Cooperation in Cyber Network Defense: the Dutch Efforts to Prevent and Respond, Best Practices in Computer Network Defense: Incident Detection and Response, vol. 35, p. 121, 2014.

[34] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno: Experimental Security Analysis of a Modern Automobile," Security and Privacy (SP), 2010 IEEE Symposium on , vol., no., pp.447,462, doi: 10.1109/SP.2010.34, 2010.

[35] G.C. Kane, D. Palmer, A.N. Phillips, D. Kiron, N. Buckley: Strategy, not technology, drives digital transformation, MIT Sloan Management Review, 2015.

[36] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu Reverse Social Engineering Attacks in Online Social Networks, Proceedings of the 8th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA, 2011.

[37] ISO: La Serie ISO 27000 - `http://www.27000.org/iso-27001.htm`.

[38] L. Lamport, R. E. Shostak, M. C. Pease: The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4(3): 382-401, 1982.

[39] R. Langner: Stuxnet: Dissecting a Cyberwarfare Weapon, Security & Privacy, IEEE , vol.9, no.3, pp.49,51, 2011.

[40] C. M. Libicki: Conquest in Cyberspace. National Security and Information Warfare, RAND Corporation, Cambridge University Press, Cambridge (USA), 2007.

[41] C. M. Libicki: Cyberdeterrence and Cyberwar, RAND Corporation, Santa Monica, 2009.

[42] G. Lodi, L. Aniello, G. A. Di Luna, R. Baldoni: An event-based platform for collaborative threats detection and monitoring. Inf. Syst. 39: 175-195, 2014.

[43] P. S. Maan and M. Sharma: Social Engineering: A Partial Technical Attack International Journal of Computer Science Issues, Vol 9(3), 2012.

[44] M. Mayer, L. Martino: Cyber security and Cyber defence in the UK and Germany - `https://www.academia.edu/12345063/Cyber_security_and_Cyber_defence_in_the_UK_and_Germany`.

[45] M. Mayer, F. Rugge: Bridging the Cyber Security Governance Gap: A Realistic Agenda for Multi-Track Diplomacy. http://ecir.mit.edu/images/stories/Images/Conference2014/Folder/workshopreportFINAL3.pdf

[46] R. M. McDowell, The U.N. Threat to Internet Freedom Top-down, international regulation is antithetical to the Net, which has flourished under its current governance model, Wall Street Journal, 2012 - http://www.wsj.com/articles/SB10001424052970204792404577229074023195322, 2012.

[47] T. Minorik, National Cyber Security Organisation: Czech Republic, - https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZECH_REP_032015.pdf., Tallin, 2015.

[48] MIT: Cyber Security and the Governance Gap: Complexity, Contention, Cooperation 2014 - http://ecir.mit.edu/images/stories/Images/Conference2014/Folder/workshopreportFINAL3.pdf.

[49] NATO: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, 2010.

[50] NATO: 7000/TSC FCX 0010/TT-10770, Report on NATO Cyber Range Capability Requirements, 2014.

[51] National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure, Version 1.0, National Institute of Standards and Technology - http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, 2014.

[52] National Institute of Standards and Technology (NIST): Roadmap for Improving Critical Infrastructure Cybersecurity - http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf, 2014.

[53] National Institute of Standards and Technology (NIST): National Initiative for Cybersecurity Education (NICE) - http://csrc.nist.gov/nice/.

[54] National Institute of Standards and Technology (NIST): Cybersecurity Capability Maturity Model (C2M2) dell'Office of Electricity Delivery & Energy Reliability - Cybersecurity Capability Maturity Model (C2M2), 2014 - http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

[55] A. Nolan: Cyber security and Information Sharing: Legal Challenges and Solutions, Andrew Nolan Legislative Attorney CRS, 2015.

[56] Ponemon Institute: 2015 Cost of Cyber Crime: Global. Ponemon Institute, 2015.

[57] Presidenza degli Stati Uniti: Remarks on Securing Our Nation's Cyber Infrastructure, 2009 - https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[58] Presidenza del Consiglio dei Ministri: Quadro strategico nazionale per la sicurezza dello spazio cibernetico - http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf,2014

[59] Presidenza del Consiglio dei Ministri: Piano nazionale per la protezione cibernetica e la sicurezza informatica - http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf, 2014.

[60] Presidenza del Consiglio dei Ministri: Decreto del 24 gennaio 2013 - Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg, , 2013.

[61] P. Pritzker, U.S. Secretary of Commerce: Remarks at the Internet Corporation for Assigned Names and Numbers Meeting in Los Angeles - http://www.commerce.gov/news/secretary-speeches/2014/10/us-secretary-commerce-penny-pritzker-delivers-remarks-internet.

[62] R. Rajkumar, I. Lee, Lui Sha, J. Stankovic: Cyber-physical systems: the next computing revolution. In Proceedings of the 47th Design Automation Conference (DAC '10). ACM, New York, NY, USA, 731-736, 2010.

[63] Repubblica Ceca: Strategia in Materia di Sicurezza Nazionale della Repubblica Ceca - http://www.army.cz/images/id_8001_9000/8503/Czech_Security_Strategy_2011.pdf, 2011.

[64] Repubblica Ceca: Libro Bianco della Difesa della Repubblica Ceca - http://www.army.cz/assets/en/ministry-of-defence/whitepaperondefence2011_1.pdf, 2011.

[65] Repubblica Ceca: Strategia di Cyber Security della Repubblica Ceca - https://www.govcert.cz/download/nodeid-1190/, 2012.

[66] Repubblica Ceca: Strategia di Cyber Security della Repubblica Ceca per il periodo 2015-2020 - https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf, 2015.

[67] S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, pages 11-25, 2001.

[68] P. Samarati and S. De Capitani di Vimercati. Cloud security: Issues and concerns. In S. Murugesan and I. Bojanova, editors, Encyclopedia on Cloud Computing, Wiley, 2016.

[69] K. Sampigethaya et al. "Future e-enabled aircraft communications and security: The next 20 years and beyond." Proceedings of the IEEE 99.11: 2040-2055, 2011.

[70] K. Sampigethaya, P. Radha: Aviation cyber-physical systems: foundations for future aircraft and air transport. Proceedings of the IEEE 101.8: 1834-1855, 2013.

[71] S. Shackelford, S. Russell, A.Kuehn: Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors, Kelley School of Business Research Paper No. 15-64 - `http://dx.doi.org/10.2139/ssrn.2652446`, 2015.

[72] SysSec Consortium: SysSec Deliverable D3.5: Experiences with the Common Curriculum Implementation - `http://www.syssec-project.eu/publications/`, 2014 .

[73] E. Tikk, K. Kaska, K., L. Vihul: International Cyber Incidents: Legal Considerations. Tallinn: CCD COE Publications, - `https://ccdcoe.org/publications/books/legalconsiderations.pdf`, 2010

[74] A. Toffler: Lo choc del futuro, Rizzoli Editore, Milano, 1971; Id., The Politics of the Third Wave, Andrew and McMeel, Atlanta, 1995.

[75] A. Toffler: The Politics of the Third Wave, Andrew and McMeel, Atlanta, 1995.

[76] A. Toffler, War and Anti-War: Survival at the Dawn of the 21st Century, Little Brown and Company, Boston,1993.

[77] E. Tromer, D. A. Osvik, A. Shamir: Efficient Cache Attacks on AES, and Countermeasures. In *Journal of Cryptology* Volume 23 (1), pp 37-71, 2010.

[78] R. Verdult, F. D. Garcia and Josep Balasch: Gone in 360 Seconds: Hijacking with Hitag2. In *21st USENIX Security Symposium* (USENIX Security 2012). USENIX Association, pages 237-252, 2012.

[79] Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fratantonio, Y., Invernizzi, L., Kirat D., Shoshitaishvili, Y.: Ten Years of iCTF: The Good, The Bad, and The Ugly. University of California, Santa Barbara, 2014.