cini
Cybersecurity National Lab

Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici

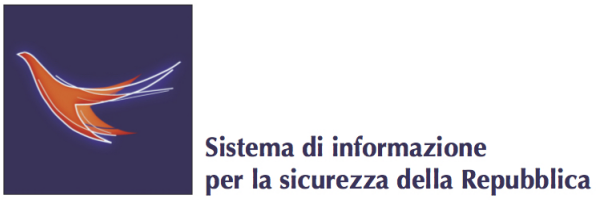
Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici

Laboratorio Nazionale di Cybersecurity
CINI - Consorzio Interuniversitario Nazionale per l'Informatica

A cura di:
Roberto Baldoni, Sapienza Università di Roma
Rocco De Nicola, IMT School for Advanced Studies, Lucca
Paolo Prinetto, Politecnico di Torino

Il volume è stato realizzato da:

Con il supporto di:



In collaborazione con:

ISBN 9788894137330

Titolo: Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici

Stampato in Italia, gennaio 2018

Ultima versione: 15 maggio 2018

Indice

Prefazione

Alla fine del 2015, il Laboratorio Nazionale di Cybersecurity del CINI ha realizzato un Libro Bianco [1] per raccontare le principali sfide di cybersecurity che il nostro Paese doveva affrontare nei cinque anni successivi. Il volume si concentrava soprattutto sui rischi derivanti dagli attacchi cyber e delineava alcune raccomandazioni anche organizzative.

Il presente volume nasce come continuazione del precedente, con l'obiettivo di delineare un insieme di *ambiti progettuali* e di *azioni* che la comunità nazionale della ricerca ritiene essenziali a complemento e a supporto di quelli previsti nel DPCM Gentiloni in materia di sicurezza cibernetica, pubblicato nel febbraio del 2017. La lettura non richiede particolari conoscenze tecniche; il testo è fruibile da chiunque utilizzi strumenti informatici o navighi in rete.

Nel volume vengono considerati molteplici aspetti della cybersecurity, che vanno dalla definizione di infrastrutture e centri necessari a organizzare la difesa alle azioni e alle tecnologie da sviluppare per essere protetti al meglio, dall'individuazione delle principali tecnologie da difendere alla proposta di un insieme di azioni orizzontali per la formazione, la sensibilizzazione e la gestione dei rischi.

Gli ambiti progettuali e le azioni, che noi speriamo possano svilupparsi nei prossimi anni in Italia, sono poi accompagnate da una serie di raccomandazioni agli organi preposti per affrontare al meglio, e da Paese consapevole, la sfida della trasformazione digitale. Le raccomandazioni non intendono essere esaustive, ma vanno a toccare dei punti che riteniamo essenziali per una corretta implementazione di una politica di sicurezza cibernetica a livello nazionale. Politica che, per sua natura, dovrà necessariamente essere dinamica e in continua evoluzione in base ai cambiamenti tecnologici, normativi, sociali e geopolitici.

All'interno del volume, sono riportati dei riquadri con sfondo violetto o grigio; i primi sono usati nel capitolo introduttivo e nelle conclusioni per mettere in evidenza alcuni concetti ritenuti importanti, i secondi sono usati negli altri capitoli per spiegare il significato di alcuni termini tecnici comunemente utilizzati dagli addetti ai lavori.

In conclusione, ringraziamo tutti i colleghi che hanno contribuito a questo volume: un gruppo di oltre 120 ricercatori, provenienti da circa 40 tra Enti di Ricerca e Università, unico per numerosità ed eccellenza, che rappresenta il meglio della ricerca in Italia nel settore della cybersecurity. Un grazie speciale va a Gabriella Caramagno e ad Angela Miola che hanno contribuito a tutte le fasi di produzione del libro. Tra i ringraziamenti ci fa piacere aggiungere il supporto ottenuto dai partecipanti al progetto FILIERASICURA.

In ultimo, precisiamo che il nostro lavoro editoriale ha comportato la significativa rielaborazione 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.

Roberto Baldoni
Rocco De Nicola
Paolo Prinetto

Roma, 15 gennaio 2018

CAPITOLO

1 Ruolo e impatto della cybersecurity

La cybersecurity è la seconda emergenza in Europa, dopo il cambiamento climatico e prima dell'immigrazione. Lo ha detto il presidente della Commissione Europea Jean-Claude Junker nel discorso sullo stato dell'Unione del 13 settembre 2017. In realtà da diversi anni le cancellerie di tutto il mondo mettono la cybersecurity ai primissimi posti delle loro agende. Blocco della operatività di aziende, controllo surrettizio di servizi di infrastrutture critiche, furto della proprietà intellettuale o di informazioni cruciali per la sopravvivenza di un'azienda sono esempi delle maggiori minacce che un paese deve affrontare. Le recenti campagne di malware *wannacry* e *notpetya* sono stati gli eventi visibili di una serie impressionante di attacchi in ogni angolo del pianeta.

*Il **cyberspace** è la cosa più complessa che l'uomo abbia mai costruito: da un lato unione di migliaia di reti che rendono difficile anche solo avere una fotografia istantanea di chi vi è connesso, dall'altro stratificazione di programmi software e protocolli sviluppati negli ultimi quaranta anni. Questa complessità è generatrice di vulnerabilità (errori software, errate configurazioni e debolezze nei protocolli) che vengono sfruttate dai cyber-criminali per sottrarre dati o arrecare danni.*

In un mondo sempre più digitalizzato, gli attacchi informatici suscitano allarme nella popolazione, causano danni ingenti all'economia e mettono in pericolo la stessa incolumità dei cittadini quando colpiscono reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti, vale a dire le infrastrutture critiche della società moderna. Immaginate cosa potrebbe succedere se si spegnessero all'improvviso tutti i semafori di una metropoli, si bloccassero gli ascensori, e le ambulanze non potessero più ricevere l'indirizzo giusto per recuperare i feriti. Inoltre, un attacco informatico di successo potrebbe anche rap-

presentare un momento di non ritorno per la credibilità di un'azienda, lo sviluppo del suo business e la capacità di vendere prodotti in un regime di sana concorrenza. Ugualmente, un attacco informatico riuscito potrebbe destabilizzare il mercato azionario facendo sprofondare interi paesi nel caos, oppure bloccare i rifornimenti di gas in inverno o il ciclo dei rifiuti urbani; il conseguente scenario politico sarebbe drammatico.

Molte volte i danni di attacchi informatici dipendono da un anello debole identificabile. L'anello debole della cybersecurity è il *fattore umano*. L'uomo ormai è parte integrante del cyberspace e quindi il fattore umano rappresenta la più importante e impredicibile vulnerabilità di questo macrosistema. Un click sbagliato può infatti distruggere qualsiasi linea di difesa tecnologica di un singolo apparato, di una organizzazione, di un paese. Sono le persone che si fanno "pescare" da una campagna di *phishing*, che usano come password il nome del gatto o del consorte, che usano lo stesso smartphone per farci giocare i figli e poi accedere alla rete aziendale. Queste persone sono le prime ad aprire le porte ai criminali verso i siti, le reti e i database della loro organizzazione, con effetti pericolosi e imprevedibili.

Prima dell'avvento del cyberspace, il mondo era basato su informazioni stampate su carta o immagazzinate su computer isolati e collocati in perimetri fisici ben delineati. Questo mondo aveva sviluppato dei modelli di minaccia molto precisi, permettendo la definizione di politiche nazionali, aziendali e individuali di sicurezza e di protezione sufficientemente chiare e dettagliate. Nel cyberspace le minacce sono invece in continua mutazione e molte rimangono sconosciute per mesi o anni prima di emergere. Ci troviamo, quindi, a dover definire delle politiche di sicurezza in un mondo dove è fortemente incompleta l'informazione sulla minaccia.

Quando si è immersi nel cyberspace guardare da un solo punto di vista significa non avere alcuna possibilità di affrontare la minaccia, poiché le vulnerabilità sono potenzialmente nascoste nell'hardware, nel firmware, nel software applicativo, ma anche nei processi organizzativi, nei contratti, nelle leggi.

> *Un paese che non metta la cybersecurity al centro delle proprie politiche di trasformazione digitale è un paese che mette a serio rischio la propria prosperità economica e la propria indipendenza.*

In Italia, interi settori di eccellenza, come la meccanica, la cantieristica, il made-in-Italy, il turismo, l'agroalimentare e i trasporti, potrebbero subire pesanti ridimensionamenti di fatturato a causa di attacchi perpetrati nel cyberspace da stati sovrani o da concorrenti.

Non solo l'industria, ma anche la democrazia è sotto attacco. Le *Fake news* sono l'evoluzione degli attacchi basati su *ingegneria sociale*: create e diffuse attraverso il cyberspace, le false informazioni tendono a confondere e desta-

bilizzare i cittadini di un paese immergendoli in uno spazio informativo non controllato, con un insieme pressoché infinito di sorgenti di notizie.

Dobbiamo dunque essere pronti a monitorare, come cittadini, imprese e Pubblica Amministrazione (PA), il nostro mondo digitale. Questo monitoraggio deve entrare nel nostro modo di vivere, esattamente come l'avvento delle automobili ha reso naturale guardare a destra e a sinistra prima di attraversare una strada trafficata. Tenere sotto controllo i nostri dispositivi, aggiornarne i software, conoscere le nostre eventuali vulnerabilità, sono tutte azioni che devono far parte di un processo di monitoraggio senza fine e di gestione continua del rischio informatico.

I processi di monitoraggio e controllo non possono essere scoordinati, né isolati tra loro: vanno raccordati e coordinati attraverso delle azioni multidimensionali che coinvolgano tutti gli attori in gioco: pubblico, privato, ricerca. Sensibilizzazione, formazione, comunicazione, *lingua cyber* comune, certificazione e impiego di *best practice* sono solo alcuni degli aspetti trasversali di questo complesso coordinamento.

In questo contesto, entra in gioco il *DPCM Gentiloni*[1] in materia di sicurezza cibernetica, pubblicato nel febbraio 2017. Il testo fornisce un riferimento nazionale strategico e operativo entro cui operare in modo coordinato tra pubblico e privato, militare e civile, dalle grandi organizzazioni ai cittadini.

Il coordinamento prevede anche lo sviluppo di progettualità che possano garantirci quelle capacità necessarie a migliorare la risposta e la resilienza del Paese ad attacchi informatici. Il DPCM Gentiloni propone un ventaglio articolato e multidimensionale di azioni, iniziative e centri all'avanguardia, quali il *Nucleo di Sicurezza Cibernetica* (NSC), il *Centro Nazionale di Ricerca e Sviluppo in Cybersecurity*, il *Laboratorio Nazionale di Crittografia*, il *Cyber Range Nazionale* e il *Centro di Valutazione e Certificazione*. Pezzi di un mosaico complesso che si deve comporre per supportare una *politica nazionale cyber*. È importante però che tutto questo si traduca al più presto in azioni concrete e si mettano a disposizione, in programmi pluriennali, le risorse necessarie che, come si vedrà nel cap. 8, altri paesi hanno già avviato da tempo.

Il nuovo libro bianco Il presente volume nasce con l'obiettivo di delineare un insieme di *ambiti progettuali* e di *azioni trasversali* che la comunità nazionale della ricerca ritiene essenziali a complemento e a supporto di quelli previsti nel DPCM Gentiloni.

Ambiti e azioni contengono tipicamente vari *progetti operativi* rivolti sia al settore pubblico sia a quello privato. Ciascuna presentazione include le motivazioni, un breve stato dell'arte, e un insieme di sfide da affrontare e di obiettivi

[1] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf`

da perseguire. Al riguardo, si ipotizza l'attivazione di un insieme di progetti che, nella loro globalità, mirino a fornire risposte adeguate e sostenibili a ciascuna delle sfide, per raggiungere gli obiettivi via via indicati.

I diversi ambiti progettuali sono stati raccolti in cinque aree operative:

- *Infrastrutture e Centri* — In quest'area vengono considerati gli strumenti e le azioni necessarie a mettere in sicurezza la rete Internet nazionale e i data center della PA; vengono inoltre presentate alcune tipologie di centri di competenza da attivare sul territorio nazionale per rafforzare le difese del sistema Paese.

- *Azioni abilitanti* — In quest'area vengono considerate le azioni necessarie a rendere più sicuro il ciclo di gestione della minaccia: dalla protezione di applicazioni critiche nazionali alla creazione di una banca nazionale delle minacce, dalla difesa da attacchi diversi (cibernetici, sociali, fisici) all'analisi forense, dalla gestione del rischio a livello sistemico alla protezione attiva.

- *Tecnologie abilitanti* — Gli ambiti progettuali in quest'area mirano a irrobustire alcune delle tecnologie di base da utilizzare per proteggere dati, limitare attacchi e loro effetti e, in generale, per aumentare la resilienza dei sistemi anche attraverso soluzioni mirate a *security by design*. In particolare vengono considerate architetture hardware che garantiscano livelli più alti di sicurezza, crittografia, blockchain, tecnologie biometriche e quantistiche.

- *Tecnologie da proteggere* — In quest'area vengono presentati gli strumenti e le azioni necessarie a proteggere alcune tecnologie chiave, quali comunicazioni wireless, servizi cloud, logiche funzionali dei sistemi e, anche nella prospettiva di *Impresa 4.0*, IoT, sistemi di controllo industriale e robot.

- *Azioni orizzontali* — Gli ambiti progettuali relativi a quest'area mirano a garantire la protezione dei dati personali, a innalzare il livello di conoscenza e competenza attraverso progetti di formazione, sensibilizzazione e certificazione e a migliorare la gestione del rischio a livello aziendale.

A valle della presentazione delle idee progettuali, il volume ne analizza l'impatto su alcuni degli assi portanti della trasformazione digitale, mettendo in evidenza come democrazia, finanza, industria, turismo e cultura possano trarre beneficio da una politica nazionale di sicurezza cyber.

Un capitolo del volume viene poi dedicato alla presentazione delle politiche e delle azioni intraprese da alcune nazioni chiave nello scenario europeo e internazionale.

Nel capitolo conclusivo vengono infine presentate alcune raccomandazioni che, se seguite, potranno permettere di rispondere in modo adeguato alla sfida della trasformazione digitale. Tali raccomandazioni, pur non essendo esaustive, toccano i punti ritenuti essenziali per una corretta implementazione di una politica di sicurezza cibernetica a livello nazionale.

Sinergie Necessarie La realizzazione dei progetti, data la diversità degli obiettivi e delle competenze necessarie, richiederà una particolare sinergia tra il mondo della ricerca, quello governativo e quello dell'industria, anche attraverso opportuni meccanismi di partnership pubblico-privato. In particolare:

- Il ruolo della ricerca in questo contesto è fondamentalmente legato allo studio di nuove soluzioni per le sfide di volta in volta evidenziate. In molti casi, oltre all'ottenimento di risultati teorici, è necessaria la realizzazione di sistemi prototipali mirati a una più rapida industrializzazione delle soluzioni.
- Le aziende avranno un ruolo fondamentale nella successiva prototipazione e industrializzazione all'interno di un sistema integrato di tutte le soluzioni proposte. Il rapporto tra ricerca e industria dovrà essere di tipo *circolare*, nel senso che i problemi affrontati dovranno essere definiti in modo condiviso; gli approcci innovativi, definiti sulla base di scenari e requisiti individuati in modo collaborativo; le soluzioni sviluppate, modificate e via via raffinate sulla base delle esperienze industriali *sul campo*. Tutto ciò permetterà di realizzare un trasferimento tecnologico tempestivo ed efficace.
- Dalla parte governativa ci aspettiamo la definizione dei necessari contesti normativi e la messa in atto di adeguati programmi di finanziamento.

1.1 Impatto degli attacchi cyber in Italia

I ministri delle finanze e i governatori delle banche centrali dei Paesi G7, al termine della riunione di Bari nel maggio 2017, hanno sottolineato la necessità di avere basi informative statisticamente valide e pubbliche sugli attacchi informatici: quanti sono, chi colpiscono, quali sono i costi che impongono alle vittime[2]:

> "Riconosciamo che gli incidenti *cyber* rappresentano una crescente minaccia per le nostre economie, e sono necessarie risposte

[2] `http://www.mef.gov.it/focus/g7/G7_FMxCBG_-_Bari_Communiqux.pdf`

> di *policy* che coinvolgano l'intero sistema produttivo … fondate su dati affidabili, imparziali, completi e largamente accessibili. … Le definizioni, le metodologie di raccolta e la condivisione dei dati stessi, laddove appropriato, dovrebbero essere coordinate e coerenti tra paesi e settori, in modo che i risultati siano confrontabili".

Nonostante sui *media* appaiano periodicamente, le stime di queste grandezze non sono quasi mai fondate su metodi di rilevazione scientifici. Esistono alcune eccezioni. Nel Regno Unito il governo conduce un'indagine campionaria che abbraccia l'intero settore privato: essa mostra che poco meno di metà delle imprese britanniche è stata vittima di almeno un tentativo di attacco nell'ultimo anno[3]. Nel nostro paese, la Banca d'Italia ha stimato che, tra settembre 2015 e settembre 2016, il 45% delle aziende nazionali è stata colpita da una qualche tipologia di attacco. I soggetti più a rischio sono le grandi imprese, gli esportatori e chi lavora in un settore ad alta intensità tecnologica. A questo proposito, la tab. 1.1, ripresa da [16], riporta le percentuali di imprese italiane dell'industria e dei servizi privati non finanziari, con almeno 20 addetti, colpite da uno o più attacchi cyber tra settembre 2015 e settembre 2016.

Nello stesso universo di riferimento, nel 2016 la spesa in sicurezza informatica era modesta: l'impresa mediana destinava alla prevenzione degli attacchi appena 4.530 euro, ovvero il 15% della retribuzione lorda annuale di un lavoratore rappresentativo [16]. Esistevano però importanti differenze tra settori: la cifra saliva a 19.080 euro tra le imprese ICT, per scendere a 3.420 tra quelle a bassa tecnologia. Quasi tutte le aziende dichiarano di usare almeno un software anti-virus e due terzi formano i dipendenti all'uso sicuro dei dispositivi informatici; risulta invece poco diffusa l'abitudine a cifrare i dati, adottata da meno di un terzo delle imprese non ICT.

Per quanto riguarda i danni provocati dagli attacchi, sia i dati britannici sia quelli nazionali mostrano che nella maggior parte dei casi l'impatto monetario diretto è limitato; in Italia i costi di ripristino dei sistemi colpiti e le perdite derivanti dall'interruzione di attività superano i 50.000 euro solo in un caso su cento. La distribuzione dei costi è però fortemente asimmetrica: da una parte la dimensione media del fenomeno è più contenuta rispetto a quanto riportato dalle fonti commerciali, dall'altra pochi grandi incidenti sembrano responsabili di una quota molto elevata dei danni economici complessivi. La misurazione dei fenomeni cosiddetti *di coda* pone sfide metodologiche; occorre sviluppare metodi di rilevazione e modelli di stima adeguati a quantificare con precisione il costo degli attacchi più gravi.

[3] `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf`

Tabella 1.1: Attacchi subiti da imprese italiane, settembre 2015–2016

Area geografica	
Nord Ovest	44.2
Nord Est	47,3
Centro	52,3
Sud e Isole	35,9
Numero di addetti	
20 – 49	42,7
50 – 199	48,4
200 – 499	56,0
500 e oltre	62,8
Intensità tecnologica	
Alta e medio-alta	48,8
Bassa e medio-bassa	43,8
Incidenza delle esportazioni sul fatturato	
Meno di 1/3	43,0
Tra 1/3 e 2/3	51,8
Più di 2/3	48,5
Percentuale sul totale delle aziende	**45,2**

È necessario, poi, tenere conto del fatto che l'impatto economico di un attacco spesso non è limitato al costo che impone alla vittima immediata. In alcuni casi, ad esempio quando viene colpita un'infrastruttura, questa dimensione è chiara anche al pubblico non specializzato. In altri casi, invece, la consapevolezza è limitata agli addetti ai lavori. In particolare, non appare ancora compreso da tutti quanto siano diffuse le tecniche di attacco indiretto, che fanno leva sulla vulnerabilità di un soggetto per colpirne un altro. Al riguardo, si vedano i due casi descritti di seguito.

1. *Attacchi indiretti che hanno coinvolto imprese italiane* [78] — Un'azienda cuneese che produce mangimi per animali, con clientela internazionale, ha subito il furto dell'elenco clienti e delle informazioni legate al rapporto di fornitura. I cyber-criminali hanno poi contattato i clienti per comunicare un cambiamento nell'IBAN della società piemontese; la verosimiglianza della comunicazione era legata al fatto che la mail riportava allegata la fattura con gli esatti importi previsti dal rapporto di fornitura esistente. Delle quattro imprese contattate, tutte asiatiche, tre hanno accreditato gli importi richiesti agli IBAN indicati per un totale di 200 mila dollari. Solo un'impresa, insospettita dal fatto che l'IBAN non fosse relativo a una banca italiana, ha condotto una verifica telefonica presso l'impresa cuneese, rendendola così consapevole dell'avvenuta truffa.

2. *Furto di identità*[4] — Un'azienda torinese nel 2013 ricevette una e-mail da parte di un suo (storico) fornitore cinese, che comunicava un cambio di banca di appoggio per i pagamenti. Senza effettuare ulteriori verifiche, l'azienda pagò al sedicente fornitore circa 60 mila dollari. Successive indagini individuarono il colpevole in un nigeriano, che era riuscito a rubare i dati dell'account mail dell'azienda cinese. I truffatori sono sfuggiti a ogni controllo riversando il maltolto su un conto tailandese, dal quale i soldi sono stati successivamente ritirati in contanti da un'ATM.

In molti paesi, compreso il nostro, non è chiaro quali siano le responsabilità in simili casi, al di fuori di fattispecie legate alla protezione dei dati personali, ai servizi di pagamento e ad alcune altre attività economiche. Gli eventuali risarcimenti dovuti dai soggetti vulnerabili ai terzi danneggiati si possono determinare solo al termine di iter giudiziali lunghi, complessi e costosi. Questo riduce gli incentivi a proteggersi da parte delle numerosissime imprese che non sono particolarmente appetibili per gli attaccanti e non lavorano in un settore regolamentato. La presenza di migliaia di anelli deboli nella catena del valore si ripercuote sulla sicurezza del cyberspace nel suo complesso e pone le condizioni per il proliferare di incidenti su larga scala, quasi sempre condotti con tecniche di attacco indiretto (*targeted attack*).

Vulnerabilità – Debolezza presente in un elemento software o hardware di un sistema che può essere sfruttato da un attaccante per condurre un attacco contro il sistema stesso.

Threat – Minacce agli asset di un'entità *target* che, basandosi su agenti software malevoli (*threat agent*) e sfruttando delle vulnerabilità, anche umane, del target stesso, sono in grado di penetrare nel suo sistema informatico e/o nella sua rete.

Targeted Attack – Attacco mirato e deliberato contro un target definito, sia esso un individuo, un'impresa o un sistema.

Sono particolarmente a rischio di divenire anelli deboli le imprese di piccola e media dimensione. Esse vedono con chiarezza i vantaggi economici della digitalizzazione, mentre sembrano non comprendere appieno i rischi che i nuovi strumenti implicano. Come evidenziato nelle sezioni 6.2 e 6.3, è particolarmente importante che in queste imprese si sviluppino adeguate prassi di *cyber-hygiene*, ovvero abitudini di condotta che, a un costo molto basso, possono vanificare i più comuni tentativi di attacco. È inoltre fondamentale che le stesse

[4] "Così ti rubo l'identità sul web", la Repubblica, 24/11/2014, (A. Longo).

acquisiscano almeno una minima consapevolezza delle proprie vulnerabilità e delle modalità operative tipiche degli attaccanti.

Analizzando gli incidenti segnalati nel 2016 è possibile fornire una tassonomia delle principali tendenze, riportata in fig. 1.1 (elaborazione propria di [5,6,7]); tale tassonomia risulta utile sia ai decisori politici sia alle potenziali vittime.

1.2 Scenario normativo europeo

Una raccomandazione, due comunicazioni, una proposta di regolamento e una proposta di direttiva: sono questi gli strumenti giuridici con cui la Commissione Europea, insieme all'Alto Rappresentante, ha aggiornato e rafforzato la propria strategia in tema di cybersecurity. Alcuni di questi strumenti sono immediatamente operativi, altri lo diventeranno non appena saranno adottati al termine della procedura legislativa avviata[8].

L'iniziativa, preannunciata dal Presidente Juncker nel discorso sullo "Stato dell'Unione", ha un obiettivo chiaro: aumentare la resilienza dell'Unione Europea (UE) nei confronti degli attacchi cyber e creare un'effettiva deterrenza per proteggere il nascente mercato unico della cybersecurity con interventi concreti, così da contribuire alla costruzione di un assetto istituzionale solido e coordinato a livello europeo e nazionale. Questo è basato su:

- un'Agenzia Europea già operante, la *European Union Agency for Network and Information Security* (ENISA)[9], il cui mandato viene reso permanente e a cui vengono attribuiti nuovi compiti e risorse per assumere un ruolo più direttamente operativo a supporto della Commissione Europea e degli Stati membri;
- un quadro di regole per una certificazione di sicurezza EU di prodotti ICT, sistemi e servizi, fondata su standard internazionali e su base volontaria;
- il *Blueprint*, vale a dire principi e meccanismi, in termini di obiettivi e modalità di cooperazione, per rispondere in modo coordinato a incidenti e crisi cyber su larga scala;
- la proposta di creare una rete europea e un centro di ricerca e competenza in tema di cybersecurity.

[5] https://www.enisa.europa.eu/publications/etl2015

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[7] https://www.enisa.europa.eu/publications/ce2016-after-action-report

[8] https://ec.europa.eu/commission/state-union-2017_it

[9] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014/

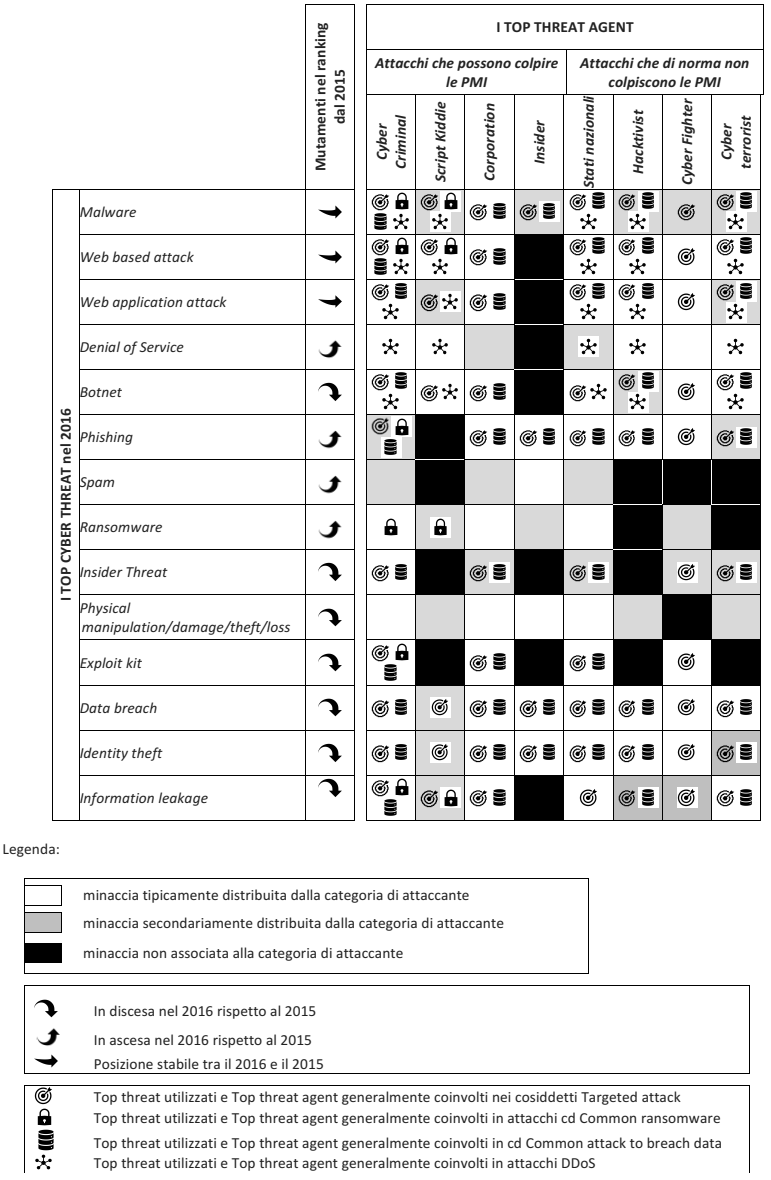


Figura 1.1: Threat Agent, Attack Vector e Threat: tendenze basate sugli incidenti rilevati nel 2016

A ciò si aggiunge una proposta di direttiva per combattere la frode e la contraffazione tramite gli strumenti di pagamento non in contanti (carte di credito e debito) per fornire una risposta più efficace, dal punto di vista dell'intervento repressivo e del diritto penale. Questa iniziativa è focalizzata sulla rilevazione, tracciabilità e repressione dei cyber criminali coinvolti in attività che per lo più hanno una dimensione transnazionale quali terrorismo, traffico di droga e di esseri umani. La proposta punta anche alla definizione di interventi per una risposta diplomatica congiunta UE alle attività cyber dannose e di misure volte a rafforzare la cooperazione internazionale in tema di cybersecurity.

L'ampia portata dell'iniziativa si coglie in particolare dai contenuti della comunicazione dedicata alla direttiva NIS (vedi sez. 1.2.1) e alla sua trasposizione, a cui è allegato un documento ricco di indicazioni operative. La preoccupazione della Commissione, già manifestata nella sua comunicazione del 2016, è evidente: poiché la direttiva NIS costituisce la pietra miliare della strategia europea in tema di cybersecurity, la sua attuazione da parte degli Stati membri deve avvenire sulla base di un approccio armonizzato, mirato a evitare disallineamenti e frammentazioni che possano compromettere gli sforzi finora dispiegati.

Di qui una serie di indicazioni concrete che costituiscono una sorta di manuale operativo per gli Stati membri in vista delle scadenze del 9 maggio e del 9 novembre 2018, rispettivamente per la trasposizione della direttiva e la designazione degli operatori dei servizi essenziali.

Innanzitutto è necessario che gli Stati membri dispongano di una strategia nazionale in tema di cybersecurity, mirata a definire obiettivi e azioni appropriate dal punto di vista politico e regolamentare, sulla base di un approccio olistico e coordinato.

Altro aspetto rilevante, al quale il documento della Commissione dedica una particolare attenzione, è l'individuazione dei soggetti a cui si applicano le regole della direttiva. Mentre gli Stati membri non debbono indicare i fornitori di servizi digitali, la designazione degli operatori dei servizi essenziali costituisce esercizio complesso e delicato. La direttiva, in merito, si limita a indicare i criteri da applicare a livello nazionale, con l'auspicio che ciò avvenga ovunque in modo coerente e che, laddove un operatore eroghi servizi in diversi Stati membri, intervenga un accordo fra gli stessi a regolare la loro individuazione ai sensi della direttiva. Occorre infatti evitare un approccio regolamentare diverso a seconda del Paese di riferimento. Gli Stati membri hanno peraltro la possibilità di estendere il raggio d'azione della direttiva e quindi applicare le sue regole (in termini di requisiti di sicurezza e obblighi di notifica) anche a settori non direttamente riguardati dalla direttiva, quali la PA (laddove questa eroghi servizi essenziali), il settore postale, quello alimentare, l'industria chimica e nucleare, il settore ambientale e la protezione civile.

1.2.1 Direttiva NIS

La direttiva NIS – *Network and Information Security*[10] sulla sicurezza delle reti e dei sistemi informativi è il primo insieme di regole relative alla sicurezza in ambito europeo approvata dall'UE. La direttiva, adottata il 6 luglio 2016 ed entrata in vigore nell'agosto 2016, si occupa soprattutto di tre aspetti essenziali: (i) rafforzare le capacità di gestione della cybersecurity in ogni Stato dell'UE; (ii) incrementare il livello di collaborazione tra gli Stati dell'UE; (iii) potenziare le strategie di gestione dei rischi e segnalazione di incidenti di cybersecurity.

L'obiettivo principale della direttiva è raggiungere un elevato livello comune di sicurezza delle reti e dell'informazione in tutti gli Stati membri dell'UE e di ottenere una maggiore cooperazione tra loro per facilitare la condivisione delle informazioni sui rischi, con particolare riferimento alla gestione degli incidenti di sicurezza informatica e ai relativi rischi. In particolare, essa si applica agli operatori di "servizi essenziali" operanti in "settori critici" e "ai fornitori di servizi digitali" e richiede agli operatori l'adozione di misure per la gestione dei rischi informatici e la segnalazione tempestiva, benché non temporalmente quantificata, degli incidenti di sicurezza.

La direttiva deve essere trasposta all'interno degli ordinamenti nazionali entro maggio 2018, mentre entro novembre 2018 ogni Stato membro dovrà identificare gli operatori di servizi essenziali.

Più specificamente, la direttiva NIS stabilisce una serie di requisiti di sicurezza delle reti e delle informazioni che si applicano agli operatori di servizi essenziali e ai fornitori di servizi digitali (DSP)[11]. Con l'obiettivo di affermare la cultura della sicurezza in settori vitali per l'economia dell'UE, tali soggetti dovranno adottare misure di sicurezza appropriate e comunicare gli incidenti gravi all'autorità nazionale competente. Gli operatori di servizi essenziali operano nei seguenti settori: energia, trasporti, banche e società finanziarie, salute, acqua e infrastrutture digitali. I fornitori di servizi digitali includono invece i mercati on-line, i servizi di cloud e i motori di ricerca[12].

Una delle caratteristiche essenziali della direttiva NIS è quella di costruire solide basi per formare un quadro europeo per la sicurezza delle reti e dell'informazione: essa nasce dalla necessità per ogni Stato membro di mettere in sicurezza le proprie infrastrutture e di garantirne il funzionamento secondo regole e requisiti comuni. Per ottenere tale obiettivo, ogni Paese deve quindi allineare i propri metodi, approcci e pratiche di sicurezza. Ciò impedirà alle im-

[10] http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&rid=1

[11] https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts

[12] http://europa.eu/rapid/press-release_IP-15-6270_it.htm

prese europee di operare in un ambiente frammentato e consentirà di facilitare e migliorare i loro sforzi di conformità alle predette regole.

Infine, la direttiva impone di designare a livello nazionale un'autorità competente per la sicurezza informatica e un *Computer Security Incident Response Team* (CSIRT) nazionale per la gestione dei rischi informatici e delle notifiche in caso di gravi incidenti che coinvolgono le infrastrutture critiche di ciascuno Stato membro[13]. I fornitori di servizi essenziali e digitali hanno l'obbligo di notificare questo tipo di eventi alle autorità competenti senza ritardi ingiustificati e tale notifica dovrà includere informazioni per consentire la determinazione del livello di gravità degli incidenti e il loro possibile impatto[14].

1.2.2 La normativa GDPR

Il 27 aprile 2016, la UE ha adottato il regolamento UE 2016/679 in tema di protezione dei dati, noto come *General Data Protection Regulation* (GDPR), applicabile dal 25 maggio 2018 e destinato a sostituire la direttiva sulla protezione dei dati del 1995. Il suo scopo principale è quello di riformare, aggiornare e modernizzare la legislazione europea in materia di protezione dei dati, così da renderla più solida e coerente. Direttamente applicabile senza necessità di alcuna norma di recepimento, essa avrà un impatto rilevante su ciascuno Stato membro e sulle regole vigenti a livello nazionale. Il GDPR viene illustrato in dettaglio nella sez. 6.1.1.

1.2.3 La cPPP in cybersecurity

All'interno della strategia per il mercato unico digitale, la Commissione Europea ha istituito una *contractual Public-Private Partnership* (cPPP) sulla cybersecurity, con l'obiettivo principale di rafforzare l'industria della sicurezza informatica dell'UE e stimolare il settore della sicurezza informatica europea. Questo scopo viene perseguito attraverso più azioni:

- riunire risorse industriali e pubbliche per migliorare la politica industriale europea sulla cybersecurity, focalizzando l'impegno sull'innovazione e seguendo una ricerca strategica congiuntamente concordata e un percorso innovativo;

- promuovere la fiducia tra gli Stati membri e gli attori industriali, favorendo la cooperazione bottom-up per la ricerca e l'innovazione;

[13] `https://clusit.it/wp-content/uploads/2017/02/direttiva_nis.pdf`

[14] `http://community.forumpa.it/system/files/file_upload/Direttiva%20NIS%20-%20allegato%201.pdf`

- contribuire a stimolare l'industria della cybersecurity allineando la domanda e l'offerta di prodotti e servizi, permettendo al settore di indirizzare in modo efficiente le esigenze future degli utenti finali;

- utilizzare i finanziamenti Horizon 2020 massimizzando l'impatto dei fondi di settore disponibili attraverso un migliore coordinamento e una migliore focalizzazione su alcune priorità tecniche;

- migliorare la visibilità dell'eccellenza europea in R&D in cybersecurity e della protezione dei dati personali digitali.

La parte pubblica della cPPP è rappresentata dalla Commissione Europea, mentre quella privata dall'associazione di diritto belga *European Cyber Security Organization* (ECSO)[15], che consta attualmente di circa 220 membri.

La costituzione della cPPP ha permesso una crescita del bilancio disponibile nella rimanente parte di Horizon 2020 da 200 a 450 milioni di euro. Un incremento analogo sembra essere possibile anche per il prossimo programma quadro.

La vastità e la complessità delle problematiche legate alla cybersecurity richiedono forme cooperative tra soggetti che, sia pure con ruoli distinti, operano in tale settore, strategico per la sicurezza e l'economia dell'UE e del nostro Paese. È indubbio che per una più efficace gestione dell'intera materia sia necessario sviluppare ogni possibile sinergia che faciliti tali integrazioni e in tale contesto ECSO rappresenta un elemento strategico della massima importanza.

1.3 Scenario normativo nazionale

L'entrata in vigore della direttiva NIS e del GDPR visti sopra, così come l'ormai sconfinata dimensione potenziale del danno che può causare un attacco cyber, hanno imposto, a livello italiano, una revisione del cosiddetto decreto Monti del 24 gennaio 2013 (nel seguito *DPCM Monti*)[16] che, insieme al *Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico* (QSN)[17] e al *Piano Nazionale per la protezione cibernetica e la sicurezza informatica* del 2015 (PN)[18], di fatto costituiva la strategia nazionale italiana per la cybersecurity.

[15] www.ecs-ppp.eu

[16] http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

[17] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

[18] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf

In questa sezione vengono esaminati sia il nuovo decreto del 17 febbraio 2017 (*DPCM Gentiloni*)[19], recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, che aggiorna, e di fatto sostituisce, il DPCM Monti, sia l'aggiornamento del *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*, pubblicato anch'esso nel 2017[20].

1.3.1 DPCM Gentiloni

Il DPCM Monti è stato estremamente importante nel panorama nazionale cyber soprattutto perché giunto in un momento in cui si stava facendo ancora molto poco e in modo destrutturato nei confronti della minaccia cyber. Il decreto induceva però una complessità nel numero e nell'interazione di una serie di attori che rendeva macchinosa la gestione della crisi, con tavoli diversi, operativi e gestionali, istituiti o da istituire al bisogno, all'interno di organi e palazzi diversi. Questa eterogeneità, che vedeva la partecipazione di vari dipartimenti della Presidenza del Consiglio dei Ministri, di diversi Ministeri e di AgID, difficilmente proni alla coordinazione in tempi rapidi, quali quelli richiesti da una crisi di ampio spettro, non poteva far altro che rendere alcuni soggetti dei meri osservatori, mal riponendo gli sforzi e ledendo la reattività. La revisione del decreto è stata quindi spinta, da un lato, dall'esigenza di riduzione della complessità e, dall'altro, dalla necessaria preparazione al recepimento della Direttiva NIS. Questa richiama a ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione delle situazioni di crisi, spingendo di conseguenza a individuare riferimenti unici all'interno dei Paesi membri. Richieste queste che mal si conciliano con l'eterogeneità del DPCM Monti.

Il DPCM Gentiloni mira principalmente ad alleggerire la gestione delle crisi e ad accentrare le responsabilità. Questo si ottiene tramite un rafforzamento del ruolo del *Dipartimento delle Informazioni per la Sicurezza* (DIS), il quale si sostituisce al Consigliere Militare nell'ospitare il *Nucleo Sicurezza Cibernetica* (NSC), coordinato da un vicedirettore del DIS appositamente nominato. Il DPCM definisce componenti e compiti dell'NSC, rendendo chiara la sua collocazione al centro dell'intera architettura, rafforzando quindi anche la posizione del DIS stesso, come riportato in fig. 1.3. Nell'ottica della semplificazione, vengono meno il NISP – Tavolo interministeriale di crisi cibernetica e l'osservatorio sicurezza previsto dal DPCM Monti in seno al Ministero dello Sviluppo Economico. Nello stesso Ministero viene però istituito un nuovo *Centro di Valutazione e Certificazione Nazionale*, con lo scopo di verificare la sicurezza nei prodotti e

[19] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf`

[20] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf`

dispositivi destinati alle infrastrutture critiche nazionali. Si conferma la presenza del *CERT Nazionale*, sempre al MISE, ma se ne prevede, come si vedrà nella sez. 1.3.2, un'integrazione con il *CERT-PA* in seno ad AgID. Immutati il ruolo del CNAIPIC, la composizione del CISR e il CISR Tecnico. Nuovo rispetto al passato, invece, l'incarico al Direttore Generale del DIS della definizione di linee di azione per la sicurezza cibernetica, per la realizzazione delle quali potrà ricorrere anche a professionalità provenienti dal mondo accademico. La fig. 1.2 riassume l'architettura definita dal DPCM Monti, mentre la fig. 1.3 riporta la nuova architettura.

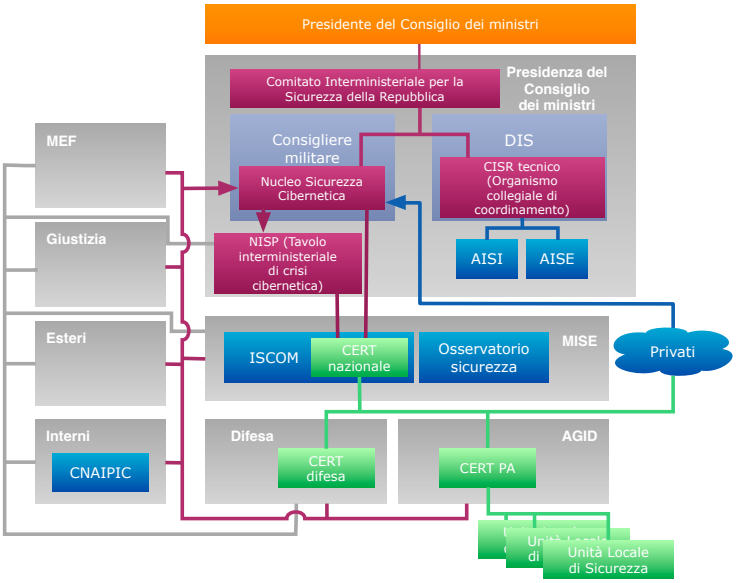


Figura 1.2: Architettura nazionale per la cybersecurity del DPCM Monti

1.3.2 Piano Nazionale per la protezione cibernetica e la sicurezza informatica

Il nuovo *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*[21] (nel seguito Piano Nazionale) recepisce il DPCM Gentiloni e mira ad aggiornare e alleggerire le modalità di gestione e di risposta alle crisi cibernetiche del Paese. A tal proposito, nello stesso Piano Nazionale è possibile leggere come

[21] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf`

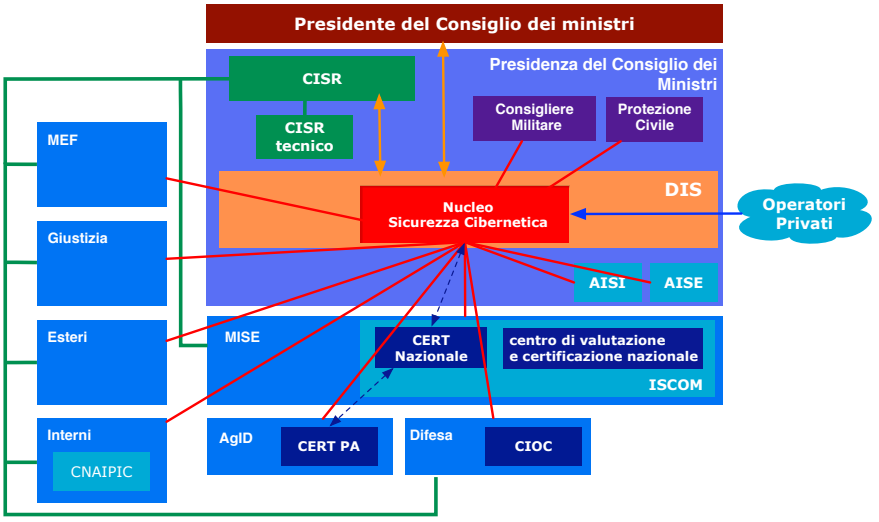


Figura 1.3: Architettura nazionale per la cybersecurity del DPCM Gentiloni

> "l'esigenza di consentire un rapido ed efficace salto di qualità dell'architettura nazionale cyber ha reso necessario individuare un nucleo essenziale di iniziative, cui attribuire carattere di priorità e urgenza, selezionate sulla base delle esigenze che hanno informato l'attività di revisione del QSN e del PN e a motivo dell'evoluzione del quadro normativo interno e internazionale".

Alla base del suddetto "nucleo essenziale di iniziative" vi è la consapevolezza che le minacce e i rischi provenienti dal domino cyber non possono essere affrontati attraverso un processo decisionale burocratico ed elefantiaco. Non a caso è stato formulato uno specifico *piano d'azione* (fig. 1.4) creato con lo scopo di rendere più efficace ed efficiente il framework operativo della cybersecurity nazionale. Tale piano di azione mira a snellire il processo decisionale in caso di crisi cibernetica e, allo stesso tempo, punta a rafforzare il contrasto delle minacce provenienti dal dominio cyber attraverso l'unificazione dei *Computer Emergency Response Team* (CERT), ritenuti non a caso gli organi operativi per eccellenza nelle loro funzioni di early warning, prevention, response e remediation in caso di attacco o incidente cyber, anche in vista del recepimento della Direttiva NIS.

CERT – Computer Emergency Response Team – Organismi ufficiali responsabili della fornitura di servizi di assistenza per la prevenzione dei rischi e per la risposta agli incidenti, i cui compiti prioritari sono:

- La centralizzazione delle richieste di assistenza a seguito d'incidenti di sicurezza (attacchi) sulle reti e sui sistemi informativi: ricezione delle richieste, analisi dei sintomi ed eventuale correlazione degli incidenti;
- Il trattamento delle allerte e le risposta agli attacchi informatici: analisi tecnica, scambio d'informazioni con altri CERT, contributo a studi tecnici;
- La creazione e la manutenzione di un database delle vulnerabilità;
- La prevenzione, grazie alla diffusione delle informazioni sulle precauzioni da adottare per minimizzare i rischi degli incidenti;
- La possibilità di coordinamento con altre entità: centri di competenze di rete, operatori e fornitori di accesso a Internet, CERT internazionali.

Figura 1.4: Il piano di azione del Piano Nazionale

In altre parole, il piano d'azione si pone l'ambizioso obiettivo di razionalizzare il processo decisionale in caso di crisi cibernetiche e nel contempo di sviluppare anche gli strumenti operativi di tipo tecnico e tecnologico per tale azione. Questi includono: la certificazione degli strumenti ICT, lo sviluppo di un partenariato pubblico-privato attraverso forme di venture capital, l'avvio di programmi scientifici e accademici attraverso l'istituzione di un *Centro Nazionale di Ricerca e Sviluppo in Cybersecurity* e la costituzione di un *Centro Nazionale di Crittografia* per proteggere la raccolta e lo scambio informativo dai rischi diffusi di esfiltrazione di dati.

Inoltre, il Piano Nazionale cerca di favorire un ulteriore salto di qualità sul versante della capacità di cooperazione tra gli organi della PA coinvolti nella cy-

bersecurity nazionale e il settore privato, il tutto ponendo l'accento sulla difesa dell'interesse nazionale e del sistema Paese. Tale obiettivo si evince nella fig. 1.5, che elenca gli undici indirizzi operativi del Piano Nazionale.

PIANO NAZIONALE (PN)

INDIRIZZI OPERATIVI

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività delle strutture nazionali di *incident prevention*, *response* e *remediation*
6. Interventi legislativi e *compliance* con obblighi internazionali
7. *Compliance* a *standard* e protocolli di sicurezza
8. Supporto allo sviluppo industriale e tecnologico
9. Comunicazione strategica e operativa
10. Risorse
11. Implementazione di un sistema di *cyber risk management* nazionale

Figura 1.5: Indirizzi operativi del Piano Nazionale

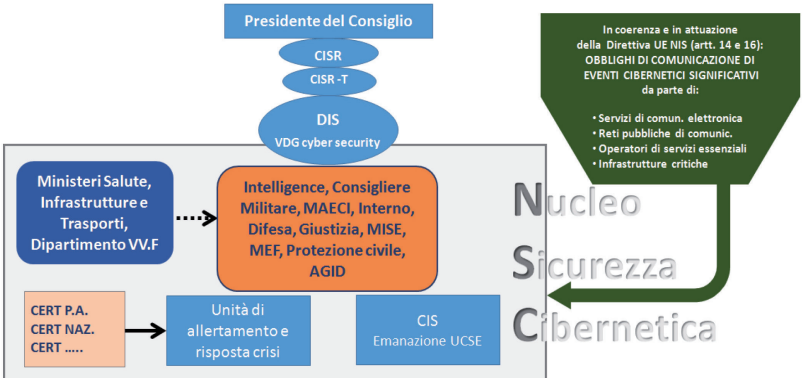


Figura 1.6: Modello di gestione delle crisi cibernetiche del Piano Nazionale

In conclusione quindi, se si analizza il risultato di breve periodo prodotto dal nuovo modello emergente dal DPCM Gentiloni, si riesce a comprendere come il Piano Nazionale sia allineato con le iniziative di aggiornamento introdotte rispetto alla precedente architettura istituzionale. In particolare, come specifica la fig. 1.6, il nuovo modello prevede un sistema di gestione delle crisi cyber e

di decision making così costituito: all'apice strategico della catena di comando e controllo vi è sempre il Presidente del Consiglio dei Ministri (coadiuvato dal *Comitato per la Sicurezza della Repubblica*) mentre sul piano operativo spicca il nuovo ruolo centrale riconosciuto al *Nucleo per la Sicurezza Cibernetica*, organo posizionato presso il DIS che avrà il compito di coordinare la gestione delle crisi cibernetiche e che sarà guidato dal Vice Direttore Generale dello stesso DIS.

1.4 Protezione degli asset del Paese

La minaccia cyber ha di fatto creato un collasso spazio temporale che ha fatto saltare i modelli di gestione della minaccia conosciuti fino a ora. Il tuo nemico può essere in ogni luogo, a non più di un centinaio di millisecondi da te e un singolo nemico, con una capacità cyber nella media, può effettuare nello stesso tempo attacchi verso migliaia di asset strategici di un Paese. Per questo occorre un nuovo modo di interpretare la sicurezza nazionale anche attraverso la protezione cibernetica del Paese tramite un piano operativo di coordinamento che sia flessibile, adattabile e con una catena di comando molto corta, ovvero veloce nella risposta. Pur essendo migliorabile sotto alcuni aspetti, le precedenti sono tutte qualità che il DPCM Gentiloni possiede.

La fig. 1.7 rappresenta il quadro d'insieme degli asset pubblici e privati del nostro Paese: dai Ministeri costituenti il *Comitato Interministeriale per la Sicurezza della Repubblica* (CISR) al *Nucleo per la Sicurezza Cibernetica* (NSC), dalle infrastrutture critiche al sistema industriale, fino ai cittadini. Innalzare il livello di sicurezza e di resilienza del Paese richiede necessariamente l'innalzamento del livello di sicurezza e di resilienza di ciascuna delle componenti del quadro d'insieme. Più vicini si è al centro del quadro d'insieme, più deve aumentare il coordinamento e la velocità nella risposta. Il settore con difese non adeguate diventa, infatti, l'anello debole dell'intero sistema Paese. Le modalità di innalzamento sono peculiari dello specifico asset: mentre, ad esempio, ai cittadini si richiede di mantenere un'adeguata forma di cyber-hygiene, al CISR è richiesto un livello di sicurezza estremamente più sofisticato, articolato e rapido nella risposta.

È opportuno evidenziare sin da subito come, al fine di minimizzare le conseguenze di un attacco, occorra attivare una sequenza di operazioni da svolgere nel minor tempo possibile da parte di soggetti diversi. Queste azioni includono, a titolo di esempio, il rilevamento, da parte dell'asset target, dell'attacco in corso, la notifica dell'attacco al CISR, la valutazione dell'entità della minaccia da parte del CISR attraverso l'NSC, l'identificazione degli asset potenzialmente oggetto di attacco e delle eventuali azioni da intraprendere, la loro comunicazione da parte dell'NSC agli asset coinvolti e l'applicazione delle opportune contromisure da parte di questi asset.

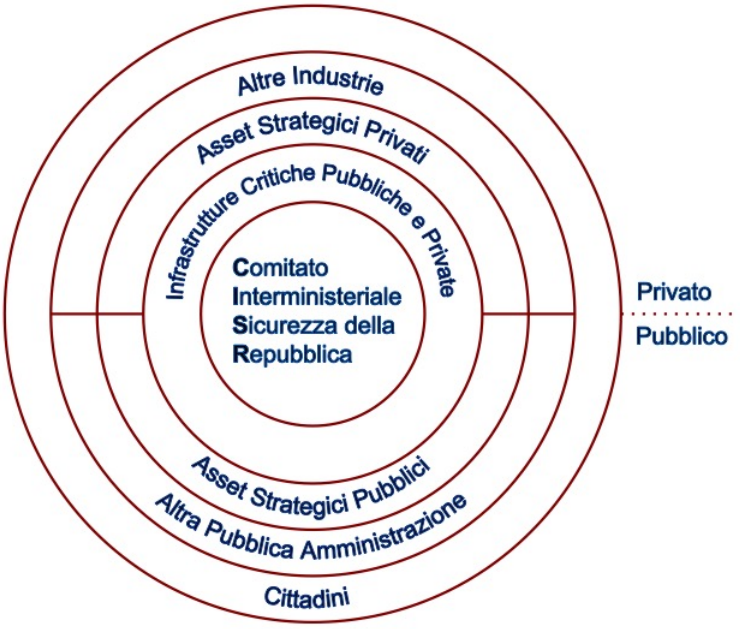


Figura 1.7: Quadro d'insieme degli asset pubblici e privati del paese

Per affrontare la minaccia dovuta al collasso spazio temporale del cyberspace occorre ridurre i tempi di transito delle informazioni rilevanti da un punto qualsiasi della fig. 1.7 verso il punto dove queste possono essere gestite in modo appropriato, portando verso il cuore dell'architettura solo quegli eventi che minacciano la sicurezza nazionale intesa come minaccia agli interessi economici, politici e scientifici del Paese. Una sorta di sistema nervoso della piattaforma Italia. Questi punti possono essere i *Centri di competenza* trattati nella sez. 2.3. In generale, i progetti operativi all'interno dei vari ambiti progettuali presentati in questo volume sono mirati, nella loro globalità, a innalzare il livello di sicurezza e/o di resilienza di uno o più asset del Paese.

1.5 Deterrenza nel cyberspace

La *deterrenza* ha un ruolo importante nella predisposizione di strumenti di cybersecurity. Essa mira a frenare un attaccante facendolo riflettere sul costo che il suo attacco potrebbe comportare ed è caratterizzata da due componenti: la

difesa e il *contro-attacco*[22]. La prima tende a elevare il livello di difesa di un sistema con l'obiettivo di aumentare a dismisura il costo dell'attacco, al fine di renderlo non profittevole. La seconda serve a "spaventare" l'attaccante che deve essere certo che un suo attacco scatenerà una risposta (rappresaglia) capace di infliggergli una punizione superiore a quella che lui stesso considera accettabile.

> **Deterrenza** – Prevenzione di una azione attraverso una minaccia credibile di rappresaglia con conseguenze di dimensioni non accettabili per l'attaccante e/o attraverso operazioni che portino alla convinzione che il costo dell'azione supera i benefici percepiti.

La componente del *contro-attacco* nel concetto di deterrenza ha funzionato bene nel contesto nucleare poiché la punizione che l'attaccante subirebbe potrebbe essere per lui catastrofica. Inoltre gli investimenti per creare armi nucleari sono tali che solo alcuni paesi sono in grado di possederle e l'attribuzione di un attacco diventa un questione relativamente semplice. Tutto ciò ha portato alla definizione di trattati internazionali di non proliferazione delle armi nucleari.

Il nucleare è però molto diverso dal cyberspace, dove armi cibernetiche possono essere in possesso potenzialmente di chiunque, e copiate e distribuite in modo capillare in ogni parte del pianeta in poche centinaia di millisecondi. In aggiunta, nel cyberspace, un singolo individuo può lanciare un numero enorme di attacchi e l'attribuzione delle responsabilità risulta essere un processo molto complesso e suscettibile di errori grazie alle possibilità di anonimato che la rete offre. Queste caratteristiche rendono difficile arrivare a trattati di non proliferazione di armi cibernetiche. Infine, qualora si riuscisse ad attribuire un attacco, il danno che si potrebbe infliggere con un contro-attacco cyber non sarebbe così catastrofico come un contro-attacco nucleare e l'attaccante potrebbe accettare di correre il rischio.

Di conseguenza, ad oggi, la *difesa* rappresenta nel mondo cyber l'unico possibile elemento di deterrenza. Gli ambiti progettuali e le azioni che vengono presentate nei capitoli successivi sono un modo per alzare il livello di cybersecurity (le difese) del Paese e quindi agire in modo implicito da deterrente rispetto a un cyberspace dove gli attacchi sono già un fattore endemico.

[22] `https://www.hsdl.org/?view&did=798700`

CAPITOLO

2 Infrastrutture e Centri

Per rendere il sistema Paese resiliente a campagne di attacchi cibernetici occorre sviluppare un cyberspace nazionale robusto, attraverso un rafforzamento dell'Internet nazionale e un consolidamento dei data center della PA al fine di diminuire la superficie d'attacco rispetto a dati e applicazioni di interesse nazionale. Inoltre, si deve sviluppare una capacità nazionale creando una rete di centri dedicati alla cybersecurity, distribuiti geograficamente sul territorio e, in alcuni casi, specializzati su singoli settori di mercato. I centri vanno da quelli di Ricerca e Sviluppo ai centri di competenza e supporto all'industria, ai centri per l'analisi delle informazioni, fino ai CERT. Questi centri devono essere dotati di un'adeguata massa critica in termini di risorse e di personale, con figure professionali adeguate. Infine, centri omologhi devono muoversi in modo coordinato ed essere interconnessi a rete per amplificare il loro effetto di resilienza sul sistema Paese.

2.1 Internet nazionale

Siamo ormai tutti così abituati ad avere a disposizione Internet che in assenza di connettività le nostre attività quotidiane sono in seria difficoltà. Questo rende Internet un asset indispensabile per la vita sociale e per buona parte delle attività strategiche del Paese, caratterizzandola come servizio indispensabile di pubblica utilità e quindi infrastruttura critica, al pari delle reti di distribuzione elettrica, idrica, etc.

Internet è una grande rete, anzi, una rete immensa e riuscire ad averne una mappa completa è molto difficile, se non impossibile, sia per la natura completamente decentralizzata e fortemente dinamica che ne caratterizza la crescita,

sia per la molteplicità ed eterogeneità delle soluzioni tecnologiche e degli attori coinvolti. Questo rende estremamente difficile definire un perimetro di sicurezza e, di conseguenza, individuare strategie di protezione e punti di intervento per implementarle.

Per capire il perché di questa affermazione e per valutarne le conseguenze è necessario comprendere come Internet sia costituita e come si sia evoluta nel tempo. Gli elementi che costituiscono la rete sono i cosiddetti *Internet Service Provider* (ad esempio TIM, France Telecom, Unidata, Deutsche Telekom, Fastweb, Interoute, Tiscali), nel seguito chiamati ISP. I collegamenti che costituiscono le maglie della rete sono i collegamenti tra ISP (ad esempio un collegamento potrebbe esserci tra Fastweb e Interoute o tra TIM e France Telecom). Per motivi economici, tecnici e logistici tali collegamenti cambiano continuamente nel tempo. Inoltre l'esistenza di ciascun collegamento è nota, in linea di principio, solo alle due parti che lo realizzano. Alcuni di questi collegamenti sono realizzati in luoghi pensati per essere punti di incontro (IXP - *Internet eXchange Point*) tra ISP. Altri, invece, sono realizzati in luoghi noti solo alle parti interessate.

La presenza della miriade di collegamenti realizzati con le modalità sopra descritte e utilizzando le più disparate tecnologie trasmissive (fibra ottica, ponti radio, satellite, etc.) fa in modo che Internet sia straordinariamente efficace nell'adattarsi ai guasti e alle caratteristiche geomorfologiche dei luoghi. D'altro canto, la natura completamente distribuita della rete e la mancanza di una visione globale della stessa espongono Internet ad attacchi, che, da una parte permettono di dirottare fraudolentemente il traffico in modo da poterlo analizzare senza necessità di accesso diretto agli apparati o linee terminali, con ovvi impatti sulla riservatezza e/o integrità del traffico stesso e, dall'altra, consentono di interrompere servizi cruciali per tempi significativi (*Denial of Service*). Il carattere asimmetrico della minaccia, la complessità delle infrastrutture coinvolte e la porosità del perimetro di sicurezza rendono indispensabile il potenziamento a livello sistemico delle capacità di difesa, contenimento e reazione.

2.1.1 Stato dell'arte

Il protocollo che viene utilizzato per il routing del traffico tra gli ISP di Internet è il *Border Gateway Protocol* (BGP)[1]. Nell'ambito delle metodologie di monitoraggio, il collezionamento delle rotte di traffico definite da BGP costituisce uno strumento fondamentale e abilitante per il miglioramento della conoscenza sulla struttura di Internet. Allo stato attuale, tra le poche fonti di dati BGP disponibili sulla connettività fra i circa 60.000 ISP componenti Internet vi sono il progetto *Route Views* dell'università dell'Oregon[2] e il progetto *Routing Informa-*

[1] https://tools.ietf.org/html/rfc4271

[2] http://www.routeviews.org/

tion Service (RIS) di RIPE-NCC[3]. I dati di routing resi pubblici da questi progetti sono tuttavia parziali (in quanto rappresentano soprattutto il punto di vista dei grandi ISP) e incompleti sia per quanto riguarda Internet nel suo complesso sia per quanto concerne le specificità dell'infrastruttura Internet italiana.

Considerazioni di questo tipo spingono varie organizzazioni internazionali a svolgere un monitoraggio continuo di Internet e a dotarsi di strumenti sempre più sofisticati di analisi anche predittiva. Ad esempio, negli USA l'organizzazione CAIDA (Center for Applied Internet Data Analysis)[4], ampiamente finanziata da DHS e NSF, effettua un monitoraggio continuo di Internet con strumenti che vanno dal controllo delle strade percorse dal traffico all'analisi di segnali sospetti captati dalla rete, con sistemi che ricordano la verifica di segnali radar. In Europa, il RIPE-NCC mette a disposizione della collettività un ampio insieme di servizi che vanno dai dati sulla raggiungibilità di alcuni punti della rete a dati sull'effettivo utilizzo degli indirizzi IP.

2.1.2 Sfide

Purtroppo mancano servizi che consentano, su scala nazionale, di svolgere almeno le seguenti azioni:

- Sorvegliare con continuità particolari porzioni di Internet considerate critiche (legate, a titolo d'esempio, a energia, trasporti, servizi finanziari, informazione) al fine di rilevare tempestivamente esperimenti preparatori di azioni malevole mirate o su vasta scala;
- Evidenziare le anomalie dell'instradamento del traffico in Internet che possano essere causate da operazioni che mirano a furti di informazioni;
- Verificare lo stato dei punti nevralgici della rete, quali ad esempio gli IXP o le *landing station* delle grandi direttrici intercontinentali di traffico;
- Rilevare, in tempo reale, azioni che mirano a impedire l'uso di Internet a larghe fasce di popolazione.

La realizzazione di servizi come quelli citati richiede di affrontare numerose sfide di ricerca di tipo sia metodologico sia tecnologico-applicativo.

Esiste innanzitutto un problema di scala, dovuto all'impossibilità, o comunque all'estrema difficoltà, di implementare controlli e politiche di ispezione e di filtraggio del traffico a livello centrale (e quindi su un numero limitato di punti strategici della rete), in ragione dei volumi di traffico coinvolti e dei limiti tecnologici degli attuali apparati di security enforcement (NG firewall, Intrusion

[3] https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris

[4] http://www.caida.org/home/

& anomaly detector, etc.) rispetto alle tecnologie trasmissive. In altre parole, se da un lato risulterebbe forse efficace (anche se per molti versi fortemente discutibile) introdurre dei punti di controllo sui collegamenti trans-frontalieri, contenendo le dimensioni del perimetro di intervento, le tecnologie utilizzate su tali collegamenti (allo stato dell'arte multipli di 100 Gbps, a breve collegamenti Tera-speed), deputati per propria natura a convogliare grandi volumi di traffico, rendono impraticabile sia l'ispezione "profonda" (a livello payload) in linea (e in modalità wire-speed) dei pacchetti trasmessi sia eventuali operazioni di blocco/filtraggio selettivo degli stessi. In pratica, allo stato dell'arte esiste almeno un'ordine di grandezza di differenza fra la capacità di elaborazione degli apparati di sicurezza e quella di inoltro degli apparati di trasmissione. Analogo discorso vale per gli IXP. Ciò comporta la necessità di spostare il focus della sicurezza, e quindi i punti di controllo e intervento, verso la periferia della rete, tipicamente sulla componente distribuzione, e quindi in maggiore prossimità delle risorse da proteggere. Questo introduce essenzialmente tre necessità:

- moltiplicare il numero di apparati deputati al monitoraggio e alla gestione della sicurezza, con una maggiore *polverizzazione* delle architetture risultanti;
- prevedere il coordinamento di tali apparati nell'ottica di implementare strategie e politiche di difesa e contenimento unitarie ed efficaci, imperniate su una scala sufficientemente larga;
- introdurre intelligenza algoritmica e capacità di analisi evolute nelle attività di monitoraggio, di individuazione delle anomalie e di contenimento delle minacce, in modo da superare gli attuali limiti tecnologici attraverso una migliore visione e comprensione dei fenomeni, in logica *situation awareness*.

Phishing – Truffa via Internet in cui l'aggressore cerca di ingannare la vittima inducendola a fornire informazioni personali, come ad esempio credenziali d'accesso, dettagli sul conto corrente bancario e sulle carte di credito. Si realizza tipicamente tramite l'invio, più o meno mirato, di e-mail che imitano nella grafica e nelle impostazioni siti bancari o postali con le quali si richiede di inviare dati personali.

2.1.3 Obiettivi

È importante sviluppare, a livello nazionale, un approccio di protezione dell'infrastruttura Internet che sia olistico, coordinato e multi-dimensionale. Esso deve inoltre essere caratterizzato dalla unitarietà di intenti fra gli attori coinvolti e

in grado, in modo almeno parzialmente automatico, di rilevare tempestivamente, contenere e, ove possibile, prevenire gli attacchi, consentendo inoltre di individuarne le reali origini, facilitando il tracciamento a ritroso e l'individuazione delle relative responsabilità.

Spear Phishing – Tipo particolare di phishing realizzato mediante l'invio di e-mail fraudolente a una specifica organizzazione o persona. Lo scopo di questi attacchi è tipicamente quello di ottenere accesso a informazioni riservate di tipo finanziario, a segreti industriali, di stato o militari.

Nel seguito si individuano e si descrivono tre grandi obiettivi progettuali, da realizzare nell'arco di tre-cinque anni:

- *Collezionamento delle rotte BGP degli ISP italiani* — Per eliminare i problemi di polarizzazione e mancanza delle informazioni di routing BGP è necessario aumentare il numero di punti di collezionamento delle rotte, coinvolgendo nel processo il più possibile i piccoli e medi ISP, che costituiscono i nodi foglia in Internet. Ciò al fine di delineare l'ecosistema di peering BGP realizzando una descrizione completa della rete Internet italiana dal punto di vista BGP. Raggiungere questo obiettivo significa, conseguentemente, disporre di dati attendibili a cui poter applicare algoritmi per la correlazione e l'estrazione di informazioni attendibili e utilizzabili in modo sicuro.

  Per centrare questo obiettivo si devono intraprendere alcune azioni in modo progressivo. In una prima fase, occorre mirare alla costituzione di un'architettura finalizzata espressamente al collezionamento delle rotte BGP degli ISP italiani. In una fase successiva, occorre costituire un sistema di collezionamento su base statistica del traffico scambiato tra gli ISP, al fine di rivelare, in modo certo, l'ecosistema BGP italiano, compreso il peering e quindi le strade effettivamente percorse dal traffico che interessa gli ISP italiani.

  Acquisito il dato che costituisce la conoscenza circa l'infrastruttura Internet Italiana e le strade percorse dal traffico che su di essa insiste, risulta ragionevole, in prima istanza, realizzare un sistema di monitoraggio e di allarmistica per gli obiettivi italiani considerati critici. Le segnalazioni generate da tali elementi devono essere raccolte, analizzate in tempo reale e correlate fra loro, in opportuni centri di controllo/monitoraggio del traffico in grado di individuare in maniera affidabile attacchi quali hijack e route flap e le direttrici di traffico ostile e, conseguentemente, di applicare strategie di mitigazione e contenimento delle minacce. Il protocollo BGP potrebbe essere ancora utilizzato per realizzare meccanismi di deviazione prevedendo il *blackholing* oppure la ripulitura e la re-iniezione in rete dei flussi di traffico interessati.

- *Monitoraggio del traffico che insiste sul DNS* — Al fine di migliorare la stabilità e la sicurezza dell'infrastruttura Internet italiana, con modalità correlate con quelle descritte al punto precedente, occorre monitorare e collezionare il traffico che insiste sul DNS, con l'intento di rilevare campagne di *phishing*, identificare il traffico riconducibile alle botnet e ad attacchi DDoS. In Italia un progetto simile è stato avviato dal Registro.it dell'Istituto di Informatica e Telematica del CNR di Pisa, mentre, al livello europeo, dal ccTLD olandese.
- *Correlazione di informazioni* — Occorre potenziare le metodologie e gli strumenti già oggi disponibili sul mercato e basati su tecniche di data mining e machine learning, per ricavare informazioni di vario tipo dalle numerose fonti dati disponibili, invi inclusi i dati sull'instradamento del traffico, i dati provenienti da reti di misura attive, i dati provenienti da rilevamenti passivi, i dati relativi al funzionamento del DNS e le attività di fondo su aree di indirizzi non usati (Internet radiation), dati relativi ai flussi di traffico. Le soluzioni proposte devono inoltre permettere di orientare la ricerca di anomalie su specifiche zone di Internet e/o su specifiche direttici di traffico. Tali approfondimenti potrebbero, ad esempio, prevedere misure attive mirate, da posizionare appositamente.

2.2 Rete nazionale di Data Center

Le amministrazioni pubbliche europee stanno investendo una grande quantità di risorse per migrare i loro processi e i servizi offerti verso un'organizzazione prettamente digitale. In tale ambito, si osserva come le sfide che queste si trovano a dover affrontare siano di natura disparata, a volte anche antitetiche. Le amministrazioni devono infatti investire una fetta significativa del denaro proveniente dalle tasse dei cittadini per consolidare e ampliare il portafoglio dei servizi, ma allo stesso tempo devono lavorare con budget sempre più ristretti. Per poter realmente conciliare questi aspetti, l'erogazione dei servizi deve necessariamente basarsi su nuove tecnologie da sfruttare in maniera efficace ed efficiente.

Data Center Consolidation – Utilizzo di tecnologie, metodologie e strategie al fine di consentire un efficientamento delle infrastrutture informatiche. In generale, l'obiettivo è quello di ridurre la superficie occupata da uno o più data center, razionalizzando l'utilizzo delle risorse hardware al fine di ridurre i costi operativi e le probabilità che attacchi informatici vadano a buon fine.

Molto spesso, però, questo non è in linea con la fotografia dell'attuale parco tecnologico impiegato. Infatti, molte PA hanno a disposizione infrastrutture

informatiche obsolescenti e spesso frammentate tra vari dipartimenti sul territorio. Questo scenario crea anche un fenomeno tale per cui il personale tecnico preposto alla gestione dell'infrastruttura manca di un giusto e doveroso aggiornamento che lo metta in grado di utilizzare tecnologie di ultima generazione e di intravedere progetti di sviluppo in linea con gli ultimi ritrovati sia tecnologici sia metodologici. In taluni casi diventa quindi difficile attuare politiche volte a uniformare i sistemi e le applicazioni utilizzate nei vari dipartimenti territoriali, spesso rendendo impossibile anche solo un reale censimento degli applicativi utilizzati o delle versioni/configurazioni in esercizio.

Un discorso analogo può essere fatto per i dati acquisiti, processati e conservati negli attuali sistemi informatici di molte PA. Si osserva, infatti, un livello di eterogeneità degli schemi di organizzazione e di gestione dei dati tale da rendere difficile, da un lato, l'interoperabilità tra applicazioni di amministrazioni diverse e tale da mettere a rischio, dall'altro, la confidenzialità e la sicurezza di dati critici da un punto di vista procedurale e legale.

Una grande sfida delle PA, a livello sia nazionale sia europeo, è quindi quella di intraprendere un processo di digitalizzazione orientato alla realizzazione di una rete nazionale di data center basata su tecnologie e metodologie informatiche d'avanguardia. Tale processo di *consolidamento* dell'infrastruttura consentirà, infatti, di realizzare servizi più omogenei, in cui sarà più facile attuare politiche di gestione/evoluzione e di sicurezza efficaci, grazie alla riduzione delle superfici e delle possibilità di attacco dall'esterno, consentendo, al contempo, di attuare processi di interoperabilità tra le PA che siano di reale beneficio per i cittadini. Il tutto, riducendo significativamente la spesa pubblica.

Il consolidamento è già riconosciuto essere un aspetto chiave per l'ammodernamento delle PA. Il *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017–2019*, realizzato da AgID e dal Team per la Trasformazione Digitale[5] [6], coordina un insieme di attività il cui investimento ammonta a circa 4,6 miliardi di euro. In questo piano, processi atti a consolidare l'infrastruttura hardware e software vengono visti come uno degli strumenti volti a ridurre, in previsione, di almeno il 50% la spesa annua legata all'infrastruttura ICT nella PA.

Si tratta però anche di una grande opportunità per innalzare i livelli della qualità dell'infrastruttura informatica nazionale e che può avere significative ricadute su molteplici fronti. Nell'ambito della sicurezza, ad esempio, spostare applicazioni in un ambiente confinato grazie al consolidamento può consentire l'attuazione di politiche efficaci di controllo degli accessi e la riduzione del numero di vettori d'attacco e dell'esposizione a vulnerabilità. Queste attività finalizzate all'aumento del livello della sicurezza devono però essere condotte in

[5] `https://pianotriennale-ict.italia.it/`

[6] `http://www.agid.gov.it/sites/default/files/documentazione/circolare_piano_triennale_24.6.2016._def.pdf`

maniera tale da far sì che gli utilizzatori delle applicazioni e dei relativi servizi non notino alcun cambiamento nella loro reattività.

2.2.1 Stato dell'arte

Gli strumenti tecnici come la virtualizzazione, che attualmente costituisce la base per il paradigma del *Cloud computing* e per progetti di consolidamento in campi applicativi disparati, sono disponibili già dagli anni '60 [41]. Essi consentono di mettere in esercizio, su una stessa macchina fisica, più "ambienti di esecuzione virtualizzati" in completo isolamento, dando l'impressione che ciascuna applicazione sia in esecuzione su un ambiente fisico dedicato. Si tratta di una pratica in rapida crescita, anche nel mondo della PA, al punto da poter stimare che a livello mondiale vi sarà, entro il 2020, un incremento di almeno il 16% di sistemi critici migrati verso ambienti Cloud, anche al fine di aumentare i livelli di sicurezza [55].

Tra le grandi organizzazioni che erogano servizi a vasti bacini di utenza, molte stanno concentrando la messa in esercizio delle rispettive applicazioni su non più di 3-4 data center, a loro volta espandibili. A livello europeo, alla fine del 2013, la Spagna e il Regno Unito avevano spostato più del 40% della propria infrastruttura per la PA su sistemi virtualizzati[7]. Secondo le stesse stime, nello stesso anno, la Francia aveva già avviato un processo di trasformazione tale da attestare la migrazione verso sistemi virtualizzati centralizzati a più del 30%, mentre l'Italia si attestava soltanto al 13%. Tuttavia, l'Italia può puntare alla riduzione da più di 4.000 data center a meno di 100 negli anni a venire.

Allo stesso tempo, attuare un progetto di consolidamento senza scendere nei dettagli di quali applicazioni debbano essere consolidate, e secondo quali logiche, è un processo destinato a fallire. Si stima che nel 2014 più del 30% dei progetti di consolidamento, a livello mondiale, non abbia infatti raggiunto gli obiettivi prefissati [27].

In Italia, AgID, nel quadro del Piano Triennale, ha posto obiettivi stringenti per l'anno 2018. In particolare, si prevede che entro la fine dell'anno si dovrà procedere all'individuazione dei requisiti minimi per le soluzioni SaaS per la PA da erogare su infrastruttura Cloud. Questa infrastruttura sarà soggetta, sempre nel corso dell'anno, a uno studio strategico per la definizione dei suoi requisiti tecnici e organizzativi. Allo stesso tempo, si procederà all'identificazione tra le PA di quelle in possesso di un'infrastruttura tale da potersi candidare a "Polo strategico nazionale", procedendo alla selezione di alcune con le quali avviare un progetto pilota per la sperimentazione dell'infrastruttura e della migrazione (o dell'adeguamento) dei data center.

[7] IDC: "Business Strategy: Western Europe Government Sector IT Cloud Computing Trends", 2012-2013, 2013.

2.2.2 Sfide

I progetti di consolidamento di applicazioni e sistemi di grandi dimensioni sono difficili, complessi, costosi e non scevri dalla possibilità di fallimento. Il loro successo scaturisce tipicamente da una pianificazione dettagliata e coordinata tra partecipanti chiave: gestori della rete, delle applicazioni, delle infrastrutture e anche delle risorse umane.

Tecnicamente, vi è un certo numero di false credenze che spesso inficiano il successo dei progetti di consolidamento. Un aspetto importante, infatti, è che consolidare verso un'infrastruttura che sia costituita dal minimo teorico di risorse computazionali non è necessariamente la soluzione ottimale. Spesso, infatti, agendo in questo modo non si lascia spazio per una crescita futura, oppure si potrebbe scoprire in seguito che l'ottimalità non è garantita ad esempio dal numero di licenze software necessarie a supportare il funzionamento dei servizi. Allo stesso tempo è fondamentale identificare le caratteristiche operative delle applicazioni ospitate, per poter determinare quante e quali di queste possano essere consolidate su uno stesso ambiente fisico garantendo comunque la non interferenza dei rispettivi indici prestazionali. Questa caratterizzazione deve essere svolta verticalmente, prendendo in considerazione le risorse computazionali, lo spazio di archiviazione, le disponibilità di banda a livello dell'infrastruttura di rete, l'hardware disponibile e le caratteristiche di tutti i componenti middleware che supportano l'esercizio di un moderno parco di applicazioni software.

Similmente, appare importante razionalizzare il parco degli applicativi software utilizzati dalle PA, al fine di supportare lo sviluppo di software certificati secondo standard definiti e integrati tra di loro. In questa direzione, Consip ha già provveduto[8] a rilasciare delle linee guida per l'adozione di applicativi forniti secondo il paradigma *Software as a Service* (SaaS) che prende in considerazione l'attuale situazione transitoria in cui le direttive tecnico/organizzative per un mercato unico per la PA sono ancora in fase di definizione.

Quando si parla di progetti di consolidamento massivi, è critico riuscire a inventariare in maniera completa ciò che è necessario migrare verso la nuova infrastruttura, documentare le metriche di utilizzo dei servizi e quelle prestazionali, e stimare le tendenze di crescita di utilizzo o di carico. È importante considerare soluzioni che limitino da principio una futura espansione della superficie dei data center, proprio perché questa porta con sé criticità importanti dal punto di vista della sicurezza. Il "consolidamento in avanti", ovverosia quello che prende in considerazione anche le eventualità future, permette infatti un grande risparmio e un alto indice di redditività del capitale investito, anche molti anni dopo la conclusione del piano di consolidamento.

[8] Consip: "Disposizioni per il Procurement dei Servizi "Software as a Services" per il Cloud della Pubblica Amministrazione," 10 ottobre 2017.

2.2.3 Obiettivi

Al fine di consentire un'efficace realizzazione di una rete di data center nazionali per la PA a più livelli, tenendo conto di tutte le possibilità strategiche e di metodo descritte in precedenza, occorre perseguire più obiettivi:

- Realizzare un censimento su larga scala delle infrastrutture fisiche in possesso delle PA e dei più comuni componenti middleware utilizzati per supportare l'esercizio dei servizi offerti[9]. A questo proposito, l'AgID chiarisce esplicitamente[10] la necessità di operare un censimento volto a produrre un quadro informativo/statistico sulle principali installazioni informatiche a livello nazionale, regionale e locale, a individuare l'insieme dei principali componenti hardware e software e a fornire dati/informazioni utili alla razionalizzazione delle infrastrutture. In questo modo sarà possibile delineare una strategia a medio termine per valorizzare e razionalizzare il patrimonio informativo delle PA e per ridurre drasticamente il costo associato all'esercizio delle infrastrutture, così da poter concentrare gli sforzi per la messa in sicurezza delle applicazioni su un ristretto numero di prodotti.

- Sviluppare nuove metodologie e tecniche per assistere gli esperti nella comprensione delle caratteristiche del carico di lavoro delle applicazioni che dovranno essere coinvolte in un processo di consolidamento, andando a considerare l'infrastruttura in maniera verticale, dall'hardware fisico a quello virtualizzato, fino alla singola applicazione, prendendo in considerazione anche i vari componenti middleware. Questo può essere fatto su più fronti, utilizzando tecniche di modellazione sia più tradizionali, quali quelle analitiche o simulative, sia basate su machine learning.

- Incentivare la formazione di nuove generazioni di sistemisti, anche realizzando percorsi di studio ad hoc, che siano in grado di comprendere il funzionamento di sistemi complessi in maniera verticale, conoscendo le caratteristiche dei sistemi reali (quelli fisici), dei supporti forniti dai Sistemi Operativi per l'esecuzione in ambienti virtualizzati, e degli stack software moderni che consentono di fornire servizi agli utenti delle PA. Questo percorso formativo consentirà alle PA di poter mettere a frutto le competenze delle nuove generazioni per manutenere un'infrastruttura complessa e allo stesso tempo critica come quella di una rete di data center nazionali, la cui realizzazione risulta essere imprescindibile per consentire significativi risparmi economici, fornire livelli di sicurezza sem-

[9] http://www.gazzettaufficiale.it/eli/id/2017/12/14/17A08400/sg

[10] https://www.censimentoict.italia.it/it/latest/docs/circolari/2017113005.html

pre crescenti, garantire reattività, alte prestazioni e scalabilità verso una crescita sempre maggiore.

2.3 Centri di competenza nazionali, territoriali e verticali

In questa sezione viene presentato l'insieme delle strutture ritenute necessarie per aumentare la resilienza del sistema Paese, delle aziende e delle PA, relativamente agli attacchi cyber. Attraverso queste strutture passerà il coordinamento necessario per alzare la protezione cibernetica del Paese. Nello specifico, si auspica la creazione di tre tipologie diverse di centri:

- *Centro Nazionale di Ricerca e Sviluppo in Cybersecurity* (CNRSC) — Ha come compito principale la ricerca avanzata, lo sviluppo di architetture, applicazioni e azioni di varia natura di respiro nazionale;
- *Centri Territoriali di Competenza in Cybersecurity* — Distribuiti sul territorio con valenza di città metropolitana, regionale o interregionale, si devono occupare soprattutto di innovazione in ambito cyber e curare il trasferimento tecnologico, la formazione, la consulenza e il supporto ad aziende locali, PA locali e cittadini;
- *Centri Verticali di Competenza in Cybersecurity* — Dedicati ciascuno a settori di mercato specifici, quali, ad esempio, energia, trasporti, mercati finanziari, etc.

Cyber Range – Poligoni virtuali dedicati all'addestramento dei professionisti del settore, costituiti da ambienti e sistemi controllati, tipicamente basati sulla virtualizzazione, che si prestano a un'ampia varietà di impieghi:

- formazione e aggiornamento individuale alla cybersecurity tramite lo svolgimento di esercizi pratici;
- addestramento e valutazione delle capacità di squadre di operatori mediante lo svolgimento di esercitazioni;
- progettazione, sviluppo e testing di nuove tattiche, tecniche e procedure di cybersecurity;
- valutazione delle capacità di difesa di un sistema.

Nei Centri Territoriali e in quelli Verticali possono trovare adeguata collocazione uno o più elementi quali: *CERT*, *Cyber Range* (istituzionali, accademici o specialistici), strutture dedicate al contrasto del cybercrime, *Information Sharing and Analysis Organization* (ISAO), Laboratori di certificazione, Laboratori

specialistici dedicati all'*Hardware Security and Trust* (analizzati nei dettagli nella sez. 4.1). Questo porterebbe alla creazione di reti specifiche di CERT, ISAO, strutture dedicate al contrasto al cybercrime e di laboratori dedicati e/o di certificazione che dovrebbero avere come centro stella l'organo preposto nazionale: la polizia postale nel caso del contrasto al cybercrime, l'intelligence nel caso degli ISAO, il MISE nel caso dei laboratori di certificazione, il CERT unificato nel caso della rete di CERT, il CNRSC per i Laboratori specialistici dedicati.

Oltre ai centri territoriali di supporto, sarebbe auspicabile che, seguendo l'esempio inglese, francese e tedesco (vedi cap. 8), venissero individuati e finanziati un certo numero di centri di eccellenza nel settore della ricerca distribuiti sul territorio nazionale il cui centro stella sia il Centro Nazionale di Ricerca e Sviluppo in Cybersecurity. Questi centri dovrebbero anche essere focalizzati sulle tecnologie di base essenziali per la cybersecurity, quali intelligenza artificiale, machine learning, data analytics, sistemi operativi, compilatori, ingegneria del software, sistemi distribuiti, architetture hardware, etc.

2.3.1 Centro Nazionale di Ricerca e Sviluppo

Come previsto dal DPCM Gentiloni, è inderogabile attivare un *Centro Nazionale di Ricerca e Sviluppo in Cybersecurity*: una struttura centralizzata, multidisciplinare, con adeguata massa critica, in parte governativa e in parte legata al mondo della ricerca, in grado di svolgere attività realizzabili solo da una struttura di questo tipo, per avviare il processo di implementazione del *Piano Nazionale per la protezione cibernetica e la sicurezza informatica* (illustrato nella sez. 1.3.2). Questo centro non dovrebbe avere alcun scopo commerciale e dovrebbe assistere il Governo in attività di Analisi, Ricerca scientifica, Scouting Tecnologico e System Engineering, seguendo l'esempio dei *Federally Funded Research and Development Center* (FFRDC) statunitensi. Una tale struttura dovrà attrarre ricercatori e investitori pubblici e privati (nazionali) per sviluppare ricerche di punta su tematiche di interesse strategico nazionale nel settore cyber.

Il CNRSC dovrà operare in stretta sinergia con il mondo universitario e della ricerca scientifica, cooperando con i centri di eccellenza sparsi sul territorio nazionale, al fine di valorizzare al meglio le loro competenze e di erogare servizi ad alto contenuto innovativo verso le organizzazioni governative, la PA e il sistema della ricerca, tenendo conto del panorama internazionale di riferimento e delle migliori pratiche.

Il CNRSC dovrà essere la punta di diamante nazionale e operare in stretta sinergia con i centri omologhi presenti in Inghilterra, Francia, Germania e Stati Uniti, ricoprendo anche, verso l'Europa, il ruolo di Centro di Eccellenza Nazionale all'interno dei programmi comunitari di cybersecurity, previsti,

ad esempio, nel *Cybersecurity package*[11] e nell'*EU cybersecurity certification framework*[12].

2.3.2 Centri Territoriali di Competenza

Per supportare adeguatamente l'innovazione digitale nelle imprese e nella PA e metterle in grado di fronteggiare le sfide che la cybersecurity pone, è necessario avviare efficaci meccanismi di trasferimento tecnologico, formazione, consulenza e supporto ad aziende locali, PA locali e cittadini. A tale scopo è necessario attivare una rete di *Centri Territoriali di Competenza in Cybersecurity* (CTCC) distribuiti sul territorio, a livello di città metropolitana, regionale o interregionale, in funzione delle necessità del territorio interessato.

Questi centri dovranno far leva su una stretta collaborazione a livello locale tra il sistema universitario, gli Enti Pubblici di Ricerca, le imprese private e la PA. Tale collaborazione è sicuramente un fattore chiave di successo, in quanto in grado non solo di ridurre i costi del processo di innovazione, ma anche di estendere la portata di progetti innovativi, sfruttando le complementarietà delle realtà coinvolte, attraverso opportune sinergie.

Per raggiungere questi obiettivi è necessario che ciascun CTCC disponga di un numero adeguato di ricercatori, operatori e tecnici in grado di garantire lo spettro di competenze multidisciplinari necessarie per affrontare e dominare la complessità dell'innovazione in ambito cyber. Ciascun centro dovrà avere un supporto finanziario iniziale garantito per almeno cinque anni per il personale e le infrastrutture. Tale supporto potrà poi andare a scalare, assumendo che, a partire almeno dal terzo anno, il centro abbia acquisito una capacità di cofinanziamento significativa grazie ai servizi verso le imprese e la PA e alle attività di trasferimento tecnologico.

I principali compiti di ciascun CTCC dovranno essere definiti in funzione delle specificità territoriali legate al tessuto produttivo e potrebbero includere:

- *Servizi e Consulenza* — (i) offerta di servizi e consulenza alle imprese per accompagnarle nel processo di innovazione e aiutarle sia a proteggerne il know how, gli asset fisici e virtuali e le proprietà intellettuali, sia a migliorarne offerta e competitività; (ii) gestione di osservatori locali sulla cybersecurity per condividere informazioni sugli attacchi tra i diversi enti, garantendo la dovuta riservatezza.
- *Supporto* — (i) supporto ai gestori/operatori di infrastrutture critiche, in funzione della criticità dei servizi offerti; (ii) supporto alle imprese e

[11] `https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en`

[12] `https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework`

alle PA locali nelle attività mirate a ottenere certificazioni di sicurezza di componenti hardware e software.

- *Progetti Strategici Territoriali* — (i) identificazione e gestione di progetti di ricerca e di trasferimento tecnologico di interesse strategico locale, realizzati anche attraverso consorzi tra enti di ricerca, università e industria; (ii) partecipazione, anche attraverso i consorzi di cui sopra, a iniziative e bandi nazionali e internazionali.

- *Formazione* — (i) organizzazione di corsi e seminari sul territorio e promozione di attività di formazione permanente, a diversi livelli di approfondimento, per le imprese e le PA locali; (ii) contributo allo sviluppo delle conoscenze a tutti i livelli, inclusa la consapevolezza dei cittadini sulle problematiche di cybersecurity; (iii) supporto alle imprese per attività fondamentali quali il potenziamento delle capacità di difesa, il testing e la valutazione degli strumenti di difesa, anche attraverso la realizzazione e la gestione di Cyber Range locali.

2.3.3 Centri Verticali di Competenza

I *Centri Verticali di Competenza in Cybersecurity* (CVCC) costituiscono la risposta alla necessità, espressa da alcuni settori specifici (energia, trasporti, sanità, finanza, etc.), di disporre di centri ad hoc per lo sviluppo di attività dedicate, quali CERT, ISAO, Cyber Range, Centri di ricerca, Laboratori di certificazione, contrasto al cybercrime, supporto alle imprese, etc.

A titolo di esempio, nel seguito sono riassunti i compiti legati allo sviluppo di un ISAO, mentra altre attività tra quelle sopra menzionate vengono trattate in altre parti del presente volume. La condivisione delle informazioni è alla base di qualunque strategia di cybersecurity: avere informazioni tempestive, complete e affidabili consente decisioni più consapevoli e accelera le azioni di protezione in tempo di regime, come pure le azioni di rilevamento, reazione, contenimento e ripristino in tempo di crisi. Per questo numerosi stati hanno istituito strutture per la collaborazione pubblico-privato al fine di creare tavoli di scambio e di analisi delle informazioni, focalizzati alla condivisione di informazioni sulla cybersecurity. Ne sono esempi gli *Information Sharing and Analysis Centre* (ISAC) istituiti in Olanda[13] e negli USA, le *Information Sharing and Analysis Organization* (ISAO) statunitensi[14] e i nodi del *Cyber Security Information Sharing Partnership* (CISP) program britannico[15].

[13] `https://www.ncsc.nl/english/Cooperation/isacs.html`
[14] `https://www.dhs.gov/isao`
[15] `https://www.ncsc.gov.uk/cisp`

ISAC statunitensi: principali settori coperti – Automotive, Aviation, Communication, Defense Industrial Base, Defense Security Information Exchange, Downstream Natural Gas, Electricity, Financial Services, Emergency Management & Response, Healthcare Ready, Information Technology, Maritime, Multi-State, National Health, Oil & Gas, Real Estate, Research & Education Network, Retail, Supply Chain, Transportation, Water.

Negli Stati Uniti sono nati prima gli ISAC come iniziativa dei privati riuniti per categoria per condividere informazioni di settore relative alle best practice e alla sicurezza in generale. Al di sopra degli ISAC è stato poi fondato il *National Council of ISACs* che garantisce la condivisione inter ISAC e la connessione con le Istituzioni. Obama ha poi fondato gli ISAO, anch'essi specifici per settore, ma coordinati dalle Istituzioni Federali.

ISAO statunitensi: informazioni di interesse – Key Factors Indicators, Vulnerability Information, Courses of Action, Incidents, Threat Actors, Tactics Techniques and Procedures, Campaings, Analytical Reports, Threat Intelligence Reports, Security Advisories and Alerts, Operational Practices.

In Italia, nel 2006 il Ministero delle Comunicazioni fondò, presso l'*Istituto Superiore delle Comunicazioni*, un ISAC delle Telecomunicazioni che fungeva da garante di parte terza e a cui partecipavano tutti gli operatori di TLC italiani. Questo ISAC funzionò per un anno sotto forma di "pilota", dopo di che si sarebbe dovuti passare alla regolamentazione ufficiale dell'esperimento. Le tecnologie dell'epoca non consentivano anonimizzazioni automatizzate: la condivisione e l'analisi venivano quindi realizzate "manualmente", grazie anche al fatto che la quantità di informazioni era esigua. Problematiche oggi ormai superate.

2.3.4 Obiettivi

Alzare il livello di protezione del cyberspace è un'operazione di lungo termine, nella quale è importante agire con gradualità, ma all'interno di una strategia chiara e ben definita. Evitare eccessive ridondanze è infatti uno dei primi obiettivi. Ad esempio, nel settore finanziario abbiamo registrato, in Italia, l'importante nascita di CERTFin[16]; questo tuttavia non preclude la nascita di specifici centri addizionali, nel settore finanziario, caratterizzati da uno o più elementi specifici, quali: ISAO, Cyber Range, centri di ricerca, laboratori di certificazione o strutture di supporto al cybercrime. Questi centri potrebbero essere sviluppati da stakeholder pubblici, privati o attraverso iniziative pubblico-privato, in un contesto territoriale; si pensi, al riguardo, alle filiere produttive localizzate o nazionali. In queste iniziative è fondamentale che vi sia chiarezza sugli obiettivi

[16] `https://www.certfin.it`

dello specifico centro, anche al fine di evitare sovrapposizioni e sprechi di risorse. Tutto ciò sottolinea l'importanza di una *politica nazionale di cybersecurity*, che verrà affrontata nelle conclusioni di questo volume (cap. 9).

CAPITOLO

3 Azioni abilitanti

Una volta realizzata l'infrastruttura basata su Centri per la cybersecurity, occorre sviluppare delle *azioni abilitanti* per innalzare il livello di sicurezza. Queste azioni mirano a irrobustire parti specifiche del ciclo di gestione di un attacco all'interno di un sistema complesso: dalla minimizzazione del tempo di scoperta dell'attacco alla protezione di dati e applicativi di interesse nazionale (che può essere attiva o preventiva), dalla creazione di una banca nazionale delle minacce, in grado di garantire una certa autonomia nel riconoscimento di malware ritrovati all'interno di organizzazioni nazionali, fino alla parte di analisi forense e di gestione delle prove.

Per quanto riguarda l'anticipo della risposta, il capitolo tratta tre tipi di situazioni: (i) l'anticipo della risposta ad attacchi cibernetici classici, quali le campagne di malware; (ii) l'anticipo della risposta nel caso di attacchi basati su ingegneria sociale, la cui evoluzione più importante ha portato al dispiegamento di campagne di fake news per accelerare la polarizzazione e il condizionamento delle opinioni dei cittadini; (iii) l'anticipo della risposta ad attacchi di tipo fisico, quali quelli terroristici, che sfruttano le potenzialità del cyberspace per portare a compimento le loro azioni.

Vengono infine presentate tre azioni abilitanti tra loro collegate. La prima concerne l'analisi forense e la sua esplosione, negli ultimi anni, dovuta all'aumento esponenziale di dati e di elementi fonte di prova a causa dell'incremento del numero di dispositivi IoT (analizzato nella sez. 5.4). La seconda riguarda la definizione di un processo di gestione del rischio sistemico attraverso nuovi strumenti per lo sviluppo di un quadro globale di governance pubblico-privato per il rischio cyber. La terza e ultima azione abilitante si focalizza sulle tecniche di difesa attiva, ovvero su come attaccare i propri sistemi per scoprirvi eventuali

falle di sicurezza e quindi porvi rimedio.

3.1 Analisi della sicurezza di applicazioni e servizi

Le applicazioni e i servizi in rete stanno rapidamente diventando il canale preferito dagli utenti per l'accesso ai servizi digitali erogati dalla PA e dalle aziende. Si pensi, ad esempio, ai servizi erogati dai portali dell'INPS e dall'Agenzia delle Entrate, al servizio di biglietteria digitale adottato da Trenitalia e all'inarrestabile ascesa dell'home banking offerto dagli istituti bancari. Tali applicazioni consentono di effettuare operazioni che presuppongono elevati standard di sicurezza, sia per la sensibilità dei dati trattati, come nel caso della dichiarazione dei redditi precompilata, sia per l'impatto economico o reputazionale che un abuso del servizio da parte di malintenzionati comporterebbe, come nel caso dell'home banking. Non a caso le certificazioni e valutazioni di sicurezza sono indicate tra le misure prioritarie nell'ambito del *Piano Nazionale per la protezione cibernetica e la sicurezza informatica* (illustrato nella sez. 1.3.2) e tra queste viene esplicitamente menzionata la

> "verifica delle misure di cyber defence applicate da gestori di servizi essenziali, incluse l'esecuzione di test periodici dei sistemi di protezione e la definizione di un sistema di verifica indipendente".

Coerentemente con questa impostazione, il *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017–2019*[1] prevede una serie di misure per aumentare il livello di sicurezza dei servizi digitali erogati quali l'*assessment* e il *test*, in cui ricadono le attività di verifica della corretta implementazione e della conformità agli standard delle funzionalità di sicurezza delle componenti di sistema o di servizio delle PA. Tra queste rivestono un'importanza particolare il *Servizio Pubblico d'Identità Digitale* – SPID[2], la *Carta d'Identità Elettronica* – CIE[3] e il servizio per i pagamenti elettronici – PagoPA[4] per la natura "abilitante" e la centralità che essi rivestono nel modello strategico di evoluzione del sistema informativo della PA.

Spesso servizi avanzati sono erogati combinando sistemi diversi che interagiscono, dando vista a dei veri e propri ecosistemi. Un ecosistema particolarmente rilevante sotto diversi punti di vista è quello sanitario, dove il cosiddetto

[1] `https://pianotriennale-ict.italia.it/`

[2] `http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid`

[3] `http://www.cartaidentita.interno.gov.it/elementi-di-sicurezza/`

[4] `http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/pagamenti-elettronici`

patient empowerment[5] promette di ridurre i costi e aumentare l'efficienza grazie anche al contributo di tecnologie ICT. Un tipico esempio è rappresentato dall'utilizzo (spesso combinato) dell'*Electronic Health Record* – EHR[6] (in Italia *Fascicolo Sanitario Elettronico*[7]) e del *Personal Health Record* – PHR[8]. Il primo veicola le informazioni generate dai professionisti del settore sanitario verso il paziente, mentre il secondo permette al paziente di condividere informazioni con medici e specialisti.

Poiché i dati presenti negli ecosistemi sono generati da applicativi interoperanti, di diversi livelli di sofisticazione, complessità e sicurezza, i rischi di una loro sottrazione sono amplificati. L'analisi di sicurezza di questi ecosistemi risulta pertanto particolarmente complessa, in quanto possono emergere problemi di sicurezza dovuti all'interazione tra componenti anche quando ciascuna di esse sia stata ben progettata, verificata e realizzata. Infatti, anche nel caso in cui tutte le componenti avessero un determinato *livello di sicurezza*, il sistema derivante dalla loro interazione potrebbe averne uno molto inferiore, a causa di interazioni anomale o malevoli tra le componenti stesse.

È pertanto importante disporre di metodologie, strumenti e ambienti per valutare, analizzare e misurare il livello di sicurezza delle singole componenti, dei sistemi ottenuti tramite la loro interazione e degli ecosistemi derivanti dalla composizione di altri sistemi.

3.1.1 Stato dell'arte

Per quanto concerne l'analisi della sicurezza di sistemi interoperabili, in Francia l'ANSSI[9] supporta un'iniziativa particolarmente rilevante: la *EIC (Environment for Cybersecurity Interoperability and Integration)*[10] gestita dall'Institute for Technological Research SystemX.

Per l'analisi della sicurezza di applicazioni e di sistemi interoperanti, sono stati proposti numerosi approcci; i principali sono:

- *Vulnerability Assessment and Penetration Testing* — Alla definizione di questi controlli contribuisce in modo determinante l'*Open Web Application Security Project* (OWASP)[11], mediante lo sviluppo e diffusione di

[5] https://joinup.ec.europa.eu/sites/default/files/document/2014-12/media2499.pdf

[6] https://ec.europa.eu/health/ehealth/projects/nationallaws_electronichealthrecords_en

[7] https://www.fascicolosanitario.gov.it

[8] http://europepmc.org/articles/pmc2605603;jsessionid=E16BF856642E785880C17373E53DA3CB?pdf=render

[9] https://www.ssi.gouv.fr/

[10] http://www.irt-systemx.fr/en/project/eic/

[11] https://www.owasp.org/index.php/OWASP_Testing_Project

metodologie e strumenti per la produzione di software sicuro da parte di una comunità di esperti e degli sviluppatori in generale. L'*OWASP Testing Guide* rappresenta lo standard de facto per la guida al "security and penetration testing" delle applicazioni web. Essa ha portato importanti benefici, ma le metodologie proposte sono ancora orientate all'esecuzione manuale da parte di analisti esperti. Per questo motivo esiste un forte interesse verso lo sviluppo di nuovi strumenti per l'identificazione automatica delle vulnerabilità.

VAPT – Vulnerability Assessment and Penetration Testing – Si basa sull'esecuzione sistematica di procedure e casi di test mirati a individuare la presenza di vulnerabilità conosciute. Interagendo solo con il perimetro (ingressi e uscite) del sistema bersaglio, comunemente la metodologia non richiede una particolare conoscenza del software in esecuzione (approccio a scatola nera). Le procedure possono essere parzialmente automatizzate sotto opportune condizioni, ma, in generale, richiedono la supervisione e spesso l'intervento diretto di un *penetration tester* esperto.

Analisi statica e dinamica delle applicazioni – Tecniche che analizzano il codice (sorgente o eseguibile) delle applicazioni al fine di verificare l'assenza di vulnerabilità e il corretto utilizzo delle informazioni da esse manipolate. L'analisi statica effettua queste verifiche prima di eseguire l'applicazione, mentre l'analisi dinamica si basa sull'osservazione dei comportamenti dell'applicazione durante la sua esecuzione. In principio, l'analisi statica permette di dimostrare la sicurezza del programma per ogni sua esecuzione futura, mentre l'analisi dinamica garantisce solo che le esecuzioni considerate non abbiamo violato i requisiti di sicurezza richiesti.

Verifica Formale – Unendo metodi e risultati teorici (provenienti dalla logica, dalla teoria dei grafi, degli automi, etc.) con soluzioni algoritmiche avanzate, i metodi formali permettono di individuare errori nella varie fasi del ciclo di vita delle applicazioni (progettazione, implementazione ed esecuzione) certificando l'assenza di vulnerabilità con un livello di affidabilità estremamente elevato. La comune base matematica garantisce la precisione e la completezza dei risultati di analisi. Tuttavia la loro applicazione a sistemi di grandi dimensioni risulta particolarmente onerosa a causa di dati condivisi, effetti collaterali, concorrenza, etc., che portano all'esplosione delle possibili situazioni da considerare.

Un'altra iniziativa di interesse è la *CBEST Intelligence-led testing guide*[12], redatta dal *Sector Cyber Team* (SCT) della *Bank of England*, che definisce linee guida e best practice per la valutazione della sicurezza dei servizi digitali, con particolare attenzione ai servizi di e-banking. La guida descrive un processo in più fasi, tra cui l'identificazione delle minacce e il penetration testing, ma non definisce i dettagli tecnici dei controlli da effettuare.

- *Analisi statica e dinamica delle applicazioni* — Le tecniche di analisi statica più usate per verificare la sicurezza delle applicazioni permettono il controllo del confinamento dell'informazione (*taint analysis*), la verifica della non interferenza fra dati riservati e pubblici (*information flow analysis*) e l'analisi delle sequenze di operazioni eseguite (*control flow analysis*). È già possibile applicare queste tecniche a linguaggi di programmazione *mainstream* come Java, come dimostrato nel caso dell'analisi di sicurezza del test OWASP [30]. Tuttavia esistono limiti teorici (per esempio in termini di complessità) che limitano l'applicabilità di queste tecniche. L'analisi dinamica può superare alcune di queste limitazioni e risulta applicabile nella maggior parte dei contesti. In ogni caso, le tecniche basate sull'esecuzione del software non possono coprire esaustivamente tutti i possibili comportamenti, fornendo pertanto solo garanzie parziali. Recenti sviluppi stanno anche investigando i benefici derivanti dall'impiego di tecniche ibride che combinano opportunamente fasi di analisi statica e dinamica.

- *Strumenti (semi)automatici* — L'analisi di sistemi, specialmente in considerazione del sempre maggiore utilizzo della concorrenza per applicazioni eseguite su architetture con più processori, anche diversi tra loro, è una sfida scientifica importante. Recenti sviluppi in tal senso, basati su tecniche e modelli avanzati, sono già utilizzati da grandi aziende informatiche quali Facebook, Google e Microsoft. Al fine di minimizzare i costi associati alla verifica, la comunità scientifica internazionale sta sviluppando e sperimentando tecniche di analisi e verifica automatica sempre più sofisticate ed efficaci. Ad esempio, strumenti software per l'analisi automatica di protocolli di autenticazione sono stati utilizzati con successo per la scoperta di gravi vulnerabilità dei servizi in rete [6, 69]. Strumenti per l'analisi automatica della sicurezza di applicazioni per dispositivi mobili sono già in fase di commercializzazione. In tutti i casi, questi strumenti utilizzano tecniche capaci di effettuare automaticamente un'analisi esaustiva dei comportamenti delle applicazioni quando queste sono eseguite su input malevoli e/o in ambienti di esecuzione ostili.

[12] `http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx`

3.1.2 Sfide

Tra le sfide scientifiche e tecnologiche più rilevanti da affrontare vanno ricordate:

- *Costi della verifica* — Le metodologie di verifica comportano necessariamente un costo in termini di tempo richiesto e di qualificazione del personale. Il costo è tanto maggiore quanto più alto è il livello di garanzia richiesto. Esso dipende inoltre dalla precisione delle tecniche impiegate: una tecnica che produce un alto numero di falsi allarmi (falsi positivi) richiede l'intervento manuale di operatori specializzati per identificare gli allarmi che necessitano attenzione. A titolo di esempio, l'applicazione di metodologie di analisi statica, oltre a risultare particolarmente onerosa da un punto di vista computazionale, può produrre falsi allarmi, richiedendo un supplemento di analisi da parte di un esperto.
- *Certificabilità e verificabilità delle analisi* — Alcune tecniche di verifica possono garantire formalmente l'assenza di certe vulnerabilità nelle applicazioni e nei servizi. Tuttavia, tali garanzie devono essere rese disponibili in modo da favorire l'integrazione di software e servizi in modo sicuro e verificabile. In tal senso è necessario investigare nuove metodologie per la certificazione delle proprietà di sicurezza del software allo scopo di favorire lo sviluppo di un ecosistema di applicazioni e servizi affidabili.
- *Limiti degli strumenti automatici* — Gli strumenti di analisi automatica devono essere in grado di analizzare applicazioni complesse in termini di dimensione, eterogeneità dei linguaggi impiegati e del flusso di dati e controllo. In particolare, le applicazioni web e quelle per i dispositivi mobili pongono nuove sfide legate alla programmazione a eventi, che rende difficile il tracciamento dei dati all'interno dell'applicazione stessa. L'utilizzo di linguaggi dinamici, in particolare in ambito di programmazione web, rende gli applicativi più vulnerabili all'inserzione di codice esterno malevolo e contemporaneamente ne rende più complessa l'analisi di sicurezza.
- *Ambienti per l'analisi della security di sistemi interoperanti* — Si registra una grande carenza di ambienti che permettano di:
  - integrare prodotti e soluzioni terze di cybersecurity con quelle esistenti, valutandone sperimentalmente il livello di sicurezza e la resilienza a possibili attacchi del sistema risultante;
  - analizzare componenti e sistemi sviluppati all'estero e/o da parti terze non fidate, al fine di accertare che questi non svolgano, oltre ai compiti previsti, anche operazioni indesiderate, illecite o fraudolente.

3.1.3 Obiettivi

Occorre perseguire i seguenti obiettivi:

- *Certificazione di applicazioni con dati sensibili* — Per le applicazioni che acquisiscono e trasmettono dati medico–sanitari sensibili tramite dispositivi personali, è necessario avviare un progetto che metta in atto tutte le misure necessarie per considerare tali dispositivi come veri e propri dispositivi medici, sottoponendoli, conseguentemente, agli opportuni regimi di certificazione prima del loro utilizzo.

- *Strumenti di analisi automatica* — Occorre sviluppare metodologie automatiche di analisi della sicurezza, configurazione, gestione e test, in grado di analizzare applicazioni reali, ovvero complesse per dimensione, eterogeneità dei linguaggi impiegati e del flusso di dati e controllo. I risultati dell'analisi devono essere di immediata comprensione (in modo tale da facilitare l'identificazione del rimedio o della contromisura più opportuna) e integrabili con le esistenti procedure di VAPT, fornendo, ove possibile, un'indicazione del rischio associato alle vulnerabilità identificate. Il progetto deve porsi l'obiettivo di includere i metodi formali nel processo di sviluppo e promuovere la definizione di controlli minimi sulla sicurezza di applicazioni e servizi in rete basati su metodi formali.

- *Ambienti per l'analisi della security di sistemi interoperanti* — È necessario: (i) sviluppare metodologie e strumenti per l'attestazione di integrità a livello sia di componenti (applicazioni, Sistemi Operativi, gestori di virtualizzazione, protezioni di sicurezza, sistemi embedded, etc.) sia di infrastruttura (reti fisiche e virtuali, cloud ed edge computing, etc.); (ii) sviluppare ambienti che permettano di integrare prodotti e soluzioni di cybersecurity, con particolare enfasi alla gestione automatica degli aspetti operativi, garantendo la protezione dei dati personali nell'interazione tra sistemi distribuiti quali quelli che gestiscono l'identità digitale federata con valore legale (SPID) e quelli commerciali usati, ad esempio, per le applicazioni di rete o di telefonia mobile.

- *Integrazione con i Cyber Range* — È auspicabile che gli ambienti di cui sopra siano collocabili all'interno di Cyber Range (si veda il box a pag. 35) opportunamente adattati. Questo al fine di permettere, tra l'altro: (i) la validazione congiunta delle capacità di difesa dei sistemi interoperanti; (ii) l'efficacia delle metodologie di analisi sviluppate di fronte a sistemi di complessità reale; (iii) l'addestramento dei nuovi esperti di sicurezza nell'uso di strumenti sempre allo stato dell'arte.

3.2 Analisi dei malware e banca dati nazionale delle minacce

I malware rappresentano una delle minacce primarie in ambito cybersecurity in quanto sono sia veicoli per accedere a un sistema remoto, per controllarlo e per comprometterlo (Botnet), sia strumenti per la sottrazione o distruzione di informazioni presenti in sistemi informatici selezionati su obiettivi specifici, come nel caso della compromissione delle caselle email del DNC (Democratic National Committee)[13] durante l'ultima campagna elettorale USA del 2016. Secondo il SANS Institute[14], le violazioni causate da malware rappresentano il 69% delle violazioni censite, con un incremento annuo del 10%. In particolare, secondo il Symantec Security Threat report 2017[15], nel 2015 si è registrato un incremento del 30% di nuovi malware non precedentemente censiti nel 2014, con una stima totale di oltre 350 milioni di nuovi malware trovati nel solo 2015 e altrettanti nel 2016.

Questi numeri suggeriscono che dietro la creazione e la distribuzione di nuovi malware vi sia un largo riutilizzo di codice. Analisi dettagliate hanno infatti evidenziato come molti malware trovati non siano altro che diversificazioni o parziali reingegnerizzazioni di malware preesistenti. Questo processo di trasformazione e diversificazione del codice fa sì che i sistemi di protezione tradizionali basati su *signature detection* non siano in grado di rilevare nuovi malware che, pur essendo in grado di produrre i medesimi effetti di quelli originali, hanno una forma diversa.

Malware – Qualsiasi programma usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata. Il principale modo di propagazione del malware è quello di generare frammenti di software parassiti (*code injection*, si veda il box a pag. 118) che si inseriscono all'interno di un codice eseguibile già esistente.

Botnet – Rete composta da dispositivi infettati da malware specializzati (*bot malevoli*, descritti nel box a pag. 61) e controllata da un cosiddetto *botmaster* il quale, da remoto, può lanciare attacchi di tipo *Distributed Denial of Service* (DDoS) contro altri sistemi o compiere operazioni illecite, anche su commissione di organizzazioni criminali.

[13] WikiLeaks' DNC Email Leak Reveals Off The Record Media Correspondence. SanFrancisco.cbslocal.com. July 22, 2016.

[14] SANS Institute: "Incident Response Capabilities in 2016". The 2016 SanFrancisco.cbslocal.com, SanFrancisco.cbslocal.com, June 2016.

[15] Symantec – 2017 Internet Security Threat Report, April 2017.

Uno dei problemi fondamentali in cybersecurity è il problema dell'*attribuzione di responsabilità*, vale a dire della determinazione della identità o del luogo da cui proviene un attacco o da dove provengono attacchi intermedi [75]. La possibilità di tracciare a ritroso (*traceback*) un attacco permette più accurate attribuzioni e quindi più sofisticate analisi forensi.

Esistono vari metodi per eludere un'analisi traceback a livello di rete, ad esempio mediante spoofing di pacchetti UDP e TCP, ovvero mascherandone l'identitá attraverso un'alterazione dei dati che la identificano, o mediante l'utilizzo di *laundering host*, ovvero di host compromessi ma non direttamente imputabili all'attaccante.

Le evidenze di rete sono quindi solo parzialmente rilevanti per attribuire la responsabilità in un attacco, soprattutto se questo è operato mediante malware. Maggiori evidenze sono acquisibili valutando la similarità con attacchi noti mediante riutilizzo di codice. In questa analisi è quindi fondamentale determinare in modo efficiente se due programmi sono simili dal punto di vista computazionale e se essi condividono strutture sintattiche. Un caso classico è la correlazione stabilita tra i malware *Stuxnet* e *Duqu* [12]. I due malware, pur avendo payload completamente diversi, con finalità completamente diverse (uno dedicato alla compromissione di sistemi industriali di controllo, l'altro all'accesso remoto a sistemi), condividono buona parte del codice e sono di fatto considerati attribuibili al medesimo autore.

Il fatto che una larghissima parte del codice malevolo distribuito in rete ogni anno derivi da codice malevolo già esistente rappresenta il tallone di Achille dei sistemi di attacco basati sul malware. Analizzando il codice è infatti possibile poter tracciare e correlare gli attori che operano attacchi informatici mediante malware. Così come nell'analisi del genoma umano la possibilità di ricondurre individui diversi a genomi simili permette di correlare gli individui e quindi correlare la possibilità che questi esprimano una stessa malattia, nel caso dell'analisi di malware, analizzando la similarità tra codice è possibile correlare attacchi diversi a codice simile, fornendo così un potente strumento sia di analisi forense sia di prevenzione di attacchi. Inoltre, così come la possibilità di ricondurre genomi diversi a fenotipi simili permette di classificare i genotipi, la possibilità di correlare malware differenti a medesimi attacchi permette di classificare le tecniche di offuscamento fornendo un potente strumento per individuare e prevenire attacchi.

3.2.1 Stato dell'arte

L'ingegnerizzazione del processo di analisi e prevenzione di attacchi mediante malware richiede, per sua natura, un approccio interdisciplinare che coinvolga tecniche di analisi del codice e tecniche di machine learning per la sua classificazione. Lo stato dell'arte nell'analisi di malware consiste principalmente

di tecniche di signature detection e behavioural analysis con il fine ultimo di classificare e prevenire infezioni dovute a nuovi malware.

Sul piano della classificazione, le metodologie maggiormente impegnate utilizzano machine learning (in particolare supervised machine learning) e tecniche di analisi statica e dinamica del codice isolato e posto in una sandbox. Poco è noto a livello di early threat detection, ovvero di prevenzione e monitoraggio delle tendenze del mercato dei malware attraverso predizione di nuovi modelli e metodi di attacco. Questo è uno dei fronti su cui lo stato dell'arte si trova carente sia sul piano delle tecnologie disponibili sia sulla loro effettiva messa in opera e sperimentazione. Le banche dati di malware esistenti permettono solo una interrogazione mediante hash (ovvero sulla struttura sintattica) dei malware senza fornire correlazioni sul piano semantico o di similarità in termini di comportamento e/o di stesura del codice. Questo è uno dei limiti fondamentali per quanto concerne le soluzioni disponibili sul mercato (e.g., *Virus Total*[16] di Google). Espandere gli strumenti di correlazione è una delle grandi sfide. Questi permetterebbero di aumentare il valore dei dati a disposizione e al tempo stesso aumentare la precisione in fase di analisi e comprensione di un malware.

3.2.2 Sfide

I malware evolvono continuamente, e le relative tecniche di analisi e rilevamento progrediscono di conseguenza, lasciando così intrinsecamente un margine di vantaggio all'efficacia dei nuovi software malevoli. Le principali sfide nel campo della ricerca e della innovazione riguardano la prevenzione (*early threat detection*) e la classificazione del codice malevolo. Questo può svolgersi a livello dipartimentale, aziendale, regionale o nazionale.

Sul piano della ricerca, considerando la continua evoluzione dei malware, spinta dalla necessità di adattarli per rendere vano il progredire delle tecniche di analisi e rilevamento che vengono continuamente elaborate, si rende necessario rompere tale paradigma per evitare di ritrovarsi sempre a "inseguire" le nuove varianti di malware. Questo necessita di strumenti flessibili e adattabili, in grado di identificare i comportamenti ostili, sia per quello che fanno sia per le modalità con le quali sono stati realizzati. Queste ultime, infatti, possono variare in modo non determinabile a priori, senza tuttavia alterare le finalità del codice. Siamo quindi di fronte alla possibilità di realizzare un numero illimitato di varianti dello stesso malware con poche strutture sintattiche comuni. Sapere riconoscere e isolare strutture simili permette di ricostruire la filogenesi dei malware e fornisce strumenti a supporto dell'attribuzione. Approcci basati su machine learning possono essere impiegati per estrarre in maniera semiautomatica i principali pattern usati per sviluppare nuovi malware, in modo da

[16] `https://www.virustotal.com/it/`

rendere più difficile per gli attaccanti realizzare malware in grado di bypassare le contromisure di sicurezza.

In questa direzione è fondamentale definire modelli aggiornati per la rappresentazione dei malware in grado di catturare in maniera fedele gli aspetti di interesse per le analisi da effettuare. A oggi, numerose rappresentazioni sono state proposte nella letteratura scientifica, suddivisibili in due grandi famiglie: rappresentazione per mezzo di grafi che rappresentano il funzionamento del malware, e rappresentazione per mezzo di parametri quantitativi che rappresentano la presenza o meno di alcuni contenuti o la loro consistenza numerica. Ciascuna rappresentazione coglie un aspetto diverso e ha diversa resistenza a tecniche di offuscamento del malware. Confrontare da un punto di vista metodologico le diverse soluzioni, proporre nuovi modelli di rappresentazione e modalità di integrazione delle diverse modalità di rappresentazione, consente di migliorare notevolmente le capacità di analisi automatica e di aumentare la difficoltà per gli attaccanti di evadere l'analisi con tecniche di offuscamento.

Per poter efficacemente difendersi dai malware, occorre inoltre essere in grado di individuare le attività che li hanno portati all'interno di un computer e, più in generale, di una rete aziendale, quali, a titolo di esempio, l'apertura di un allegato malevolo o la visita di un sito web contenente malware. Questo richiede il monitoraggio di reti aziendali, non solo in termini di traffico di rete, ma di attività dei singoli terminali (PC, tablet, smartphone) per correlare l'infezione alle azioni che ne hanno determinato l'installazione e l'attivazione.

Una seconda importante sfida riguarda le dimensioni del problema. L'evoluzione del mercato dei malware si configura come un caso di Big Code. Siamo infatti di fronte a una enorme quantità di codice immesso su rete, con caratteristiche di velocità, varietà e volume tipiche dei Big Data. Il volume di nuovi malware giornalieri rende impossibile un'analisi manuale dei singoli *sample*. Al riguardo, le soluzioni più efficaci oggi commercialmente disponibili adottano tecniche di analisi automatica basate su machine learning per raggruppare sample in famiglie e restringere l'analisi manuale ai soli casi che non sembrano appartenere a famiglie note.

In quest'ottica è importante realizzare una base di dati nazionale delle minacce, dove poter riversare le conoscenze acquisite nel tempo grazie alle analisi dei nuovi malware e da cui poter estrarre informazioni utili per supportare efficacemente queste stesse analisi.

Il codice, rispetto ad altri dati, presenta infatti caratteristiche proprie che pongono nuove sfide alla ricerca sia teorica sia applicata. Il codice (benevolo o malevolo che sia) ha un aspetto *estensionale*, che rappresenta la sua forma sintattica, e uno *intensionale* che ne rappresenta la funzionalità una volta in esecuzione. Entrambe queste caratteristiche devono essere considerate nella classificazione e nell'analisi su grandi quantità di malware. Gli aspetti estensionali permettono di comprendere come si attua una data minaccia in un dato

malware, mentre quelli intensionali permettono di comprendere e ricostruire la filogenesi, utile per l'attribuzione di responsabilità o la early threat detection.

È infine necessario integrare le attività di analisi dei malware all'interno dei processi di analisi di sicurezza. Questo comporta lo sviluppo di nuovi modelli organizzativi e di processo, con un'adeguata formazione e reclutamento di personale tecnico. Capire l'evoluzione dei malware, identificando quelli realmente nuovi è funzionale alla comprensione approfondita degli *Advanced Persistent Threat* (APT) (si veda il box a pag. 54).

Honeypot – Meccanismo di sicurezza impostato per rilevare, deviare o, in qualche modo, contrastare i tentativi di utilizzo non autorizzato dei sistemi o dati. Generalmente, appare come parte di un sito web con dati o risorse di interesse per eventuali attaccanti, ma in realtà è isolato e monitorato e usato come "esca" per capire le intenzioni o le strategie di eventuali attaccanti.

3.2.3 Obiettivi

Gli obiettivi principali da perseguire possono essere così riassunti:

- Creare una banca dati nazionale costruita a partire da un'infrastruttura che raccolga e permetta di coordinare le incident/response in caso di attacco via malware. È necessario migliorare e adeguare gli schemi esistenti di rappresentazione delle minacce; a titolo di esempio si vedano i progetti OpenIOC[17], CybOX[18] e STIX[19]. Nel nostro paese è necessario istituire una banca dati nazionale di codice malevolo ove le agenzie governative possono confrontare le minacce che coinvolgono il sistema Paese e attuare un adeguato reporting. Questo richiede strumenti di raccolta (*honeypot*) e strumenti di analisi automatica e classificazione del codice, nonché la realizzazione di meccanismi di consultazione/condivisione delle informazioni in accordo a opportune policy di sicurezza.
- Dotare le organizzazioni e i decision maker di strumenti per la classificazione e raggruppamento automatico dei malware in base a: (i) similarità e condivisione di codice, (ii) condivisione dei server remoti di comando e controllo, (iii) piattaforme obiettivo dell'attacco, (iv) mercato obiettivo dell'attacco, (v) finalità del malware, quali furto di dati e interruzione di servizio. Questi strumenti devono abilitare coloro che hanno la responsabilità di una rete ad azioni a breve termine, come l'individuazione tempestiva dei soggetti cui inviare segnalazione e la messa in opera delle contromisure più appropriate per evitare la diffusione su larga

[17] `https://www.fireeye.com/services/freeware.html`
[18] `https://cyboxproject.github.io/`
[19] `https://oasis-open.github.io/cti-documentation/`

scala di infezioni. Esse permettono, inoltre, di sviluppare azioni a medio termine, mirate all'individuazione di campagne di malware, attribuzione dell'origine e predisposizione di sistemi di difesa stabili.

- Dotare le organizzazioni e i decision maker di strumenti per l'individuazione di: (i) vulnerabilità (di processo, di sistema e software) sfruttate dal malware, al fine di permettere di programmare gli interventi correttivi e migliorare le capacità di prevenzione, rilevazione e difesa; (ii) finalità del malware, al fine di mettere a punto le opportune strategie di difesa, che devono coinvolgere non solo l'ambito strettamente tecnico, ma anche quello organizzativo e procedurale.
- Sviluppare un ecosistema di strumenti e metodologie per la sorveglianza automatica del cyberspace attraverso il monitoraggio e il raggruppamento dei malware in base ai canali di comunicazione utilizzati (ad esempio, condivisione di domini Internet o di algoritmi generatori di nomi di dominio) sia per attività di comando e controllo sia per l'esfiltrazione dei dati. Questi strumenti devono permettere l'individuazione preventiva di campagne di malware, di potenziali collegamenti fra malware di diversa tipologia, e lo sviluppo di tecniche di allerta tempestiva basate su analisi di traffico.
- Sviluppare strumenti e metodologie per la prevenzione da infezioni basate su: (i) sensibilizzazione e formazione delle persone che usano strumenti informatici (soprattutto non specialisti IT), (ii) sviluppo di sistemi di monitoraggio del traffico della rete aziendale (ad es., navigazione web) per individuare le modalità d'uso della rete che aumentano la probabilità di infezione da malware.

3.3 Anticipare la risposta ad attacchi cibernetici

Gli ultimi dieci anni sono stati caratterizzati da una enorme crescita del numero di incidenti legati alla sicurezza informatica di natura molto eterogenea: dal furto di identità al cyberspionaggio, dalle truffe finanziarie ai *ransomware*. Questo fenomeno è la conseguenza di un'evoluzione paradigmatica del mondo del cybercrime, che oggi agisce secondo un modello di *crime-as-a-service* in cui strumenti di hacking estremamente potenti e complessi diventano accessibili a prezzi contenuti e possono essere utilizzati senza richiedere competenze tecniche approfondite.

Ransomware – Malware che introduce limitazioni nell'uso di un dispositivo, ad esempio criptando i dati o impedendo l'accesso al dispositivo stesso.

APT – Advanced Persistent Threat – Minaccia, rappresentata da un hacker o, più spesso, da un gruppo di hacker, il cui obiettivo è colpire un sistema tramite una serie di attacchi mirati, caratterizzati da soluzioni avanzate, per acquisire e mantenere il controllo del sistema stesso per periodi di tempo anche molto lunghi.

Allo stesso tempo è cresciuta anche la complessità degli attacchi. Gli attacchi di cui sono state vittime giganti come Target[20] o Yahoo[21] hanno mostrato come i cyber-criminali siano in grado di infiltrarsi in organizzazioni complesse, prendere il completo controllo di sistemi di larga scala, e in tali sistemi persistere per anni, nascondendo efficacemente la loro presenza e le loro azioni. Questo tipo di attacchi particolarmente complessi e strutturati, tipicamente noti con il nome di *Advanced Persistent Threat* (APT), rappresenta oggi un problema fondamentale per tutte le grandi organizzazioni (pubbliche e private) che agiscono in un contesto globale. L'asimmetria tra chi attacca e chi si difende, infatti, continua a crescere: mentre il tempo necessario per penetrare un sistema si riduce grazie a strumenti di attacco sempre più efficaci, il tempo necessario per scoprire ed eradicare la presenza di una minaccia cyber cresce, lasciando quindi gli asset delle organizzazioni a rischio per lunghi periodi. Ridurre tale asimmetria è un obiettivo fondamentale per proteggere dagli attacchi di tipo APT i sistemi e le organizzazioni che li gestiscono.

Kill chain – Metodologia per la caratterizzazione di un attacco cyber attraverso le diverse fasi logiche che lo costituiscono: ricognizione, armamento, consegna, exploit, install e callback, movimenti laterali. In una fase iniziale l'attaccante studia la sua vittima (ricognizione) per definire una strategia di attacco e acquisire tutti gli strumenti necessari ad attuarla (armamento). In questa fase l'attacco non è ancora divenuto operativo e la vittima ne è completamente all'oscuro. L'attaccante ha quindi a disposizione tutto il tempo necessario per progettare l'attacco nel modo più efficace possibile.

I recenti attacchi di cui sono state vittima grandi società private e la PA hanno dimostrato come le ricadute spesso interessino la società a ogni livello. Dalla indisponibilità di servizi essenziali fino al furto delle identità, il cittadino è sempre più spesso l'ultimo anello di una lunga catena attraverso cui sono legate le vittime di un attacco.

[20] `https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219`

[21] `http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html`

Ogni attacco, complesso o meno, passa attraverso una serie di passi che l'attaccante sviluppa per arrivare fino al suo obiettivo finale (la cosiddetta *kill chain*). Per anticipare l'attacco è necessario fornire alle organizzazioni strumenti che possano aiutarle ad acquisire tutte le informazioni necessarie per tracciare l'attacco mentre questo è ancora nella fase di ricognizione e armamento. Le informazioni devono essere aggregate, correlate e analizzate con l'obiettivo di prevedere potenziali minacce. L'automazione di tale processo è fondamentale per anticipare la risposta agli attacchi e per aumentare il livello di consapevolezza delle organizzazioni rispetto alle minacce che su loro incombono.

Vista la crescente complessità degli attacchi, è necessario che la loro prevenzione sfrutti informazioni eterogenee e multi-livello. Non è più sufficiente basarsi esclusivamente sul, pur necessario, monitoraggio del traffico di rete e dei dispositivi connessi, alla ricerca di vulnerabilità note, ma occorre integrare tali approcci con informazioni ottenibili ad altri livelli. Per esempio, le informazioni relative alle interazioni tra utenti a livello applicativo (il loro cosiddetto *grafo social*[22]) possono far capire se determinati flussi di traffico tra dispositivi siano più o meno sospetti.

Infine, come evidenziato nella sez. 5.4, l'introduzione di scenari IoT, dove un gran numero di dispositivi mobili e pervasivi comunica in rete, apre scenari di attacco totalmente inediti, da considerare attentamente anche nel campo della prevenzione. Anche in questo caso, non è più sufficiente limitarsi a monitorare il traffico generato da tali dispositivi: questo deve, infatti, essere opportunamente "interpretato" anche sulla base degli specifici dispositivi coinvolti e dei loro possessori/utilizzatori.

Un'evoluzione dei sistemi di difesa volta ad anticipare la risposta agli attacchi per annullarne o ridurne l'impatto avrà ricadute positive sia dirette sia indirette: non solo permetterà di diminuire il numero e, soprattutto, l'entità degli incidenti, ma permetterà anche di incrementare la fiducia dei cittadini e delle imprese nell'adozione di strumenti e processi sempre più basati sull'uso intensivo di sistemi informatici e reti interconnesse. Tale fiducia, se declinata nel mondo dell'impresa, sarà fondamentale per realizzare pienamente la visione di *Impresa 4.0* e tutti i programmi di evoluzione tecnologica a essa legati.

3.3.1 Stato dell'arte

Molte delle soluzioni esistenti sono fortemente basate su team di specialisti in grado di estrarre dai dati informazioni utili a definire potenziali indicatori di compromissione da usare nei sistemi di difesa automatica. Tali team sono estre-

[22] `https://www.cbsnews.com/news/facebook-one-social-graph-to-rule-them-all/`

mamente costosi e difficilmente riescono a gestire un'enorme mole di informazioni, peraltro destinata a crescere di diversi ordini di grandezza nel prossimo futuro.

Oltre ai dati grezzi, anche l'analisi dei testi dei messaggi rappresenta un'inesauribile fonte di informazioni sugli attacchi in via di pianificazione e, più in generale, sulle potenziali vittime di attacco. Tale fonte richiede tuttavia una complessa elaborazione che spesso coinvolge quasi tutti i livelli di analisi linguistica, da quella morfologica a quella lessico-semantica e pragmatica.

Threat intelligence – Processo volto a identificare i contorni di una minaccia emergente, con particolare riferimento a contesto, indicatori, meccanismi, e implicazioni. Tale processo include la raccolta e analisi di tutte le informazioni che potrebbero rivelarsi utili nel processo decisionale di definizione della risposta alla minaccia.

A livello commerciale esistono offerte variegate di servizi di Threat intelligence che forniscono strumenti e dati sulle minacce emergenti. Molti di questi servizi hanno un target generale e offrono quindi informazioni non sempre contestualizzate. La contestualizzazione al caso applicativo viene offerta come servizio da ritagliare ad hoc sulla specifica realtà del cliente, ma in realtà essa rappresenta un aspetto che non può essere trascurato da chi intenda proteggersi da minacce mirate. L'integrazione del Natural Language Processing nei processi di Threat Intelligence è recente: un progetto è stato presentato recentemente da CrowdStrike[23] e altri progetti sono in corso di sviluppo. Tuttavia, con l'esclusione dell'estrazione di entità nominate, è ancora assente una vera componente di comprensione del linguaggio naturale multilingue a livello semantico.

Le soluzioni di Threat intelligence oggi disponibili offrono funzionalità dedicate e solo in rari casi sono integrate all'interno di suite in grado di supportare gli operatori in un processo completo che, partendo dalla selezione delle sorgenti di informazioni, arrivi alla messa in opera di contromisure. La mancanza di un supporto adeguato al processo integrato viene spesso sopperita dall'operatore umano, con le inefficienze che ne conseguono.

Infine, poche soluzioni utilizzano oggi in modo integrato fonti di dati eterogenee per individuare possibili vulnerabilità e valutare la pericolosità o meno di determinati fenomeni osservati in funzione del contesto dei dispositivi coinvolti e del loro dell'utilizzo da parte degli utenti.

3.3.2 Sfide

Lo sviluppo di un processo basato sulla Threat intelligence che offra le caratteristiche precedentemente illustrate passa necessariamente attraverso una serie

[23] `https://www.youtube.com/watch?v=VNuPmxGakw0`

di sfide che, a oggi, ne impediscono la completa realizzazione. Tra queste le principali sono:

Deep e Dark web – Parti del web contenenti dati non pubblicamente indicizzati o il cui accesso è protetto attraverso reti di anonimizzazione. Si ritiene che circa l'80% dei contenuti oggi presenti sul world wide web siano "nascosti" in queste parti.

- *Acquisizione dati da sorgenti protette* — Molte delle attività oggi legate allo sviluppo di nuovi attacchi richiedono una forte collaborazione tra attori criminali differenti. Tale collaborazione ha spesso luogo attraverso canali protetti e difficilmente penetrabili, per lo più rappresentati dal Deep e dark web o da chat room private. Le tecnologie usualmente adottate per l'acquisizione di informazioni dal web aperto si scontrano con complessi sistemi di "challenge" pensati per permettere l'accesso esclusivamente a esseri umani. L'integrazione di tali sorgenti all'interno di processi di intelligence automatizzati richiede lo studio di nuove soluzioni che permettano di superare tali barriere senza l'intervento dell'operatore umano.

- *Creazione e aggiornamento dinamico di basi di conoscenza sui cyber-criminali e le loro operazioni* — Queste devono includere informazioni linguistiche relative ai diversi nomi con cui, anche in lingue diverse, vengono espressi i concetti e le entità nominate, così da poter mettere in collegamento tali soggetti in un'analisi integrata con i dati non linguistici elaborati.

- *Analisi multilingua del testo* — Occorre disambiguarne il significato di testi e aggregare la semantica da essi estratta per argomenti e tematiche, così da ottenere un quadro complessivo del pensiero, delle intenzioni e degli obiettivi dei cyber-criminali, intersecando quindi le informazioni in modo indipendente dalla lingua, dalla sintassi e dal lessico con cui esse vengono espresse.

- *Profilazione lessico-semantica* — La profilazione degli autori dei testi e l'analisi semantica (non solo lessicale) permette di identificare e raggruppare testi del deep e dark web sulla base dello stile di scrittura anche a livello dei contenuti.

- *Distillazione automatizzata di indicatori di compromissione e regole per la rilevazione di attacchi* — La raccolta di informazioni relative a potenziali vettori di attacco, di per sé, non è sufficiente a rendere i sistemi più sicuri. Rendere tali informazioni azionabili richiede la distillazione di chiari indicatori di potenziale compromissione e relative regole per l'identificazione degli attacchi. L'automazione di tale processo è un pas-

so necessario per far fronte in modo adeguato al continuo aumento del numero di attacchi.

- *Contestualizzazione degli elementi di intelligence* — Uno dei maggiori limiti dei sistemi di Threat intelligence oggi disponibili sul mercato risiede nella loro incapacità di contestualizzare in modo automatico l'informazione raccolta alla specifica realtà di interesse. La definizione di appropriate metodologie per la contestualizzazione è fondamentale per ordinare correttamente le minacce in base alla loro priorità e, conseguentemente, migliorare l'efficienza dei sistemi di difesa, riducendone quindi i costi di gestione.

- *Caratterizzazione di vulnerabilità e scoperta di attacchi tramite informazioni complesse eterogenee* — Molti dei sistemi di monitoraggio per la prevenzione degli attacchi (es., monitoraggio del traffico) non tengono conto del tipo di utilizzo dei dispositivi da parte dei loro utenti, né del tipo di interazioni che questi tipicamente (o, ragionevolmente) svolgono tra di loro tramite i dispositivi stessi. È quindi necessario integrare informazioni multi-livello, che includano l'utilizzo delle applicazioni, la rete sociale degli utenti, i profili dei dispositivi che utilizzano, in modo da avere un quadro più chiaro di possibili vulnerabilità, migliorare la qualità della prevenzione e della scoperta, riducendo i falsi positivi e negativi.

- *Vulnerabilità e prevenzione in ambienti pervasivi* — Con la diffusione di tecnologie IoT, gli scenari di attacco si ampliano a dismisura, così come i possibili effetti negativi di attacchi sugli utenti finali, come ampiamente illustrato nella sez. 5.4.

- *Valutazione della qualità delle informazioni raccolte, dell'affidabilità delle sorgenti e dell'efficacia delle contromisure* — La mole di informazioni disponibili per i processi di intelligence rende necessario lo studio di opportuni metodi per valutarne la qualità, l'affidabilità e l'efficacia delle risposte che da esse deriva. Tali metodi giocheranno un ruolo fondamentale nel rendere il processo complessivo meno "rumoroso", aumentandone efficacia ed efficienza.

- *Processi integrati di intelligence, monitoraggio e protezione dei sistemi* — Le soluzioni alle sfide fin qui riportate non potranno fornire risultati soddisfacenti se non verranno inquadrate all'interno di processi integrati che, a partire dall'identificazione delle sorgenti informative per arrivare alla gestione degli incidenti, inneschino un ciclo di continuo miglioramento della sicurezza.

3.3.3 Obiettivi

I principali obiettivi da perseguire sono i seguenti:

- *Threat intelligence avanzata* — Sviluppo di una piattaforma di Threat intelligence che permetta l'acquisizione da fonti nascoste e protette, con la possibilità di superare in modo automatizzato possibili sistemi di evasione o di *challenge*, acquisire i dati raggiunti e arricchire gli stessi con contenuti semantici identificati in modo automatizzato. L'obiettivo finale è costruire una base di conoscenza relativa a gruppi cyber-criminali e ai vari attori legati a questo ecosistema.
- *Identificazione di vulnerabilità in ambienti complessi* — Sviluppo di un framework per il monitoraggio e l'analisi del comportamento di sistemi complessi per l'identificazione di vulnerabilità e possibili percorsi di attacco. Il framework dovrà avere come target specifico sistemi interconnessi, infrastrutture IT per la gestione di *Supply chain*, ecosistemi informatizzati complessi.
- *Automazione delle indagini forensi* — Sviluppo di una suite di strumenti finalizzati all'analisi automatizzata dei sistemi oggetto di attacco, al fine di estrarre e correlare in modo automatizzato informazioni legate alle attività dell'attaccante. Obiettivo di tali strumenti è supportare il lavoro dell'analista forense, automatizzando i processi di identificazione delle attività svolte dall'attaccante, con particolare riferimento ad attacchi multi-step.

3.4 Anticipare la risposta ad attacchi sociali

Proteggere i processi decisionali dalle attività di disinformazione e controinformazione è un'attività vitale per ogni Paese [54]. Storicamente si tratta di un compito affidato ai servizi di intelligence e la partita si è finora disputata in uno scenario in cui la diffusione di informazioni e conoscenze avveniva top-down, tramite le testate giornalistiche, gli organi di partito o le gerarchie accademiche.

Internet ha radicalmente cambiato il modo in cui si crea e si accede alla conoscenza [70], stravolgendo tutti i sistemi di mediazione a favore di un accesso diretto a una moltitudine senza precedenti di contenuti. La complessità dei fenomeni della realtà è apparentemente accessibile a tutti, ma non sempre in modo comprensibile: il nostro sistema cognitivo fatica ad adeguarsi a nuovi concetti come *incertezza*, *complessità*, *probabilità*, tendendo a favorire sintesi e narrazioni più semplici (o semplificate) e quindi rassicuranti. In questo contesto cambiato va affrontato il problema antico della diffusione delle notizie false e delle sue conseguenze.

Il processo della diffusione delle informazioni false passa per una serie di meccanismi cognitivi che ci porta (tutti, nessuno escluso) ad acquisire informazioni per coerenza con la nostra visione del mondo e a ignorare tesi a contrasto; tutti noi tendiamo poi a formare gruppi fortemente polarizzati su narrazioni condivise [59]. Questo rende feconda la diffusione di informazioni false a fini pretestuosi sia economici sia al servizio di altri interessi che possono avere un peso notevole nel dibattito pubblico. Il problema è serio e delicatissimo e la scienza in generale e l'informatica in particolare hanno un ruolo dirimente e fondamentale in questa sfida. È quindi necessario mettere in atto una serie di iniziative e sinergie su più piani per garantire una migliore comprensione del problema nel contesto attuale e mettere a punto risposte efficaci[24].

L'avvento dei social media ha radicalmente cambiato il processo di costruzione e di accesso alla conoscenza, permettendo una produzione e un consumo non mediato alle informazioni. Nei prossimi anni, visto il crescente affacciarsi dei processi di impatto della scienza sulla società (automazione del lavoro, biotech, etc.), si prevede un aumento significativo delle problematiche da affrontare per soddisfare il fabbisogno informativo delle persone in maniera mirata e puntuale, onde evitare il proliferare di narrazioni fuorvianti e potenzialmente lesive del processo democratico.

Le narrazioni percepite come lesive rispetto a un'agenzia, entità o persona vengono spesso definite *Fake News* dalla stampa e sono diventate un tema di rilevanza centrale sia politica sia istituzionale[25].

A livello europeo, le comunità accademiche e istituzionali riconoscono il problema della misinformation, delle fake news e della information warfare come tema altamente prioritario: sin dal 2013 il World Economic Forum segnalava la diffusione massiva di informazioni fuorvianti e non accurate attraverso internet come uno delle più serie minacce globali e le riferiva come *Digital Wildfire*[26].

La presidente Boldrini, convocando esperti di tutti i settori collegati al problema per un'indagine conoscitiva, ha sottolineato l'importanza dell'educazione digitale e la centralità del ruolo dell'informazione nei processi democratici. La stessa Autorità garante per le comunicazioni riconosce il problema nell'articolazione e modulazione dell'informazione in un ambiente completamente nuovo e favorisce e patrocina un'iniziativa per la costituzione di un osservatorio sulle dinamiche della disinformazione sui social media.

La sola soluzione tecnologica infatti non è sufficiente per via della complessità del fenomeno. L'approccio nella costruzione di soluzioni deve essere necessariamente fortemente interdisciplinare e deve puntare alla creazione di siner-

[24] `https://www.weforum.org/reports/the-global-risks-report-2017`

[25] `https://www.weforum.org/reports/the-global-risks-report-2017`

[26] `http://reports.weforum.org/global-risks-2013/risk-case-1/digital-wildfires-in-a-hyperconnected-world/#read`

gie tra i vari attori del sistema informativo. In questo scenario, la costituzione di un osservatorio sui flussi informativi nei social media potrebbe rappresentare un ponte di connessione tra i vari stakeholder che, su base quantitativa, possano disegnare insieme soluzioni mirate e strategie condivise.

Non intercettare la natura interdisciplinare del problema significherebbe escludere l'Italia dal dibattito internazionale sul tema, mentre con la costituzione di un tale osservatorio avremo un ruolo di prima fila su un'iniziativa pilota che potrà poi essere replicata su scala europea.

3.4.1 Stato dell'arte

Al momento, la strategia di contrasto auspicata dai *debunker* si avvale massimamente di siti on-line dove vengono segnalate le notizie palesemente false. Mentre tale attività è di sicura utilità per coloro che hanno bisogno di controllare rapidamente la veridicità di una notizia, è stato dimostrato che, nella lotta alla disinformazione, i siti di debunking possono essere addirittura controproducenti, inducendo chi crede a notizie false a rafforzare le proprie credenze e ad aumentare l'impegno nel diffonderle [80].

Debunker – Persona che analizza le notizie on-line per porne in evidenza discrepanze, inesattezze e infondatezze.

Bot – Applicazione software, chiamata anche *robot Web*, che esegue attività automatizzate. Esempi di uso corretto dei bot sono la trasmissione di informazioni utili, la generazione automatica di contenuti e le risposte automatiche. Esempi di uso improprio sono la sottrazione di dati personali, lo spamming e diffusione di messaggi impropri.

Un approccio alternativo è stato di tipo algoritmico, con tentativi di soluzioni automatizzate finalizzate a neutralizzare la vasta mole di informazioni presenti on-line ritenute false. Mentre tale approccio può aiutare a individuare bot [31] e profili falsi – aiutando ad esempio a costruire ambienti "trusted" in cui le identità on-line siano associate con maggiore probabilità a identità reali [19] – esso trova i suoi limiti nell'impossibilità algoritmica di decidere sulla falsità di un'affermazione, a meno di non ridurre brutalmente le capacità espressive di un linguaggio [60]. Non a caso, i recenti tentativi di introdurre filtri automatizzati sui social media hanno messo in evidenza sia il problema dei falsi positivi (legati spesso a un uso ironico o sarcastico del linguaggio) sia quello dei falsi negativi (legati a cambi nell'uso del linguaggio da parte di chi desidera nascondere le proprie comunicazioni). Ma il maggior pericolo di un approccio algoritmico "puro", in cui il processo di classificazione e di risposta alle fake news

venga totalmente automatizzato, è il rischio di evocare scenari censori, aumentando le polarizzazioni già presenti e inasprendo i conflitti fra i gruppi sociali appartenenti a *echo-chamber* diverse.

> **Echo-chamber** – Luogo digitale dove si finisce per parlare solo all'interno di gruppi che hanno idee omogenee, con meccanismi che si autoalimentano. La comunicazione all'interno di tale gruppo tende a rinforzare gli elementi comuni e ad attenuare, se non a eliminare, quelli dissonanti.

Da quanto detto, è evidente come la strada di una bruta risposta algoritmica al problema non sia percorribile: promettere software che sia in grado di distinguere il vero dal falso appartiene al dominio delle fake news. Quindi, per quel che concerne il *fact-checking* e la verifica delle fonti con conseguente etichettatura dell'informazione, si può al massimo ottenere una classificazione di tipo statistico in cui comunque un insieme esemplare di elementi considerati veritieri e/o affidabili venga individuato a priori. Non per questo bisogna demonizzare gli strumenti di classificazione "parziale": essi sono ad esempio utili per filtrare le enormi moli di dati presenti in Internet prima di poterli trattare con metodi tradizionali, ovvero con persone fisiche che decidano il da farsi. Al momento questa è appunto la strategia adottata su alcuni social media, anche se con risultati non esattamente soddisfacenti, probabilmente anche a causa della non adeguata specializzazione dei team di analisti impiegati.

> **Polarizzazione** – Tendenza a separarsi in echo-chamber distinte e basate su sistemi di credenze contrapposti e contrastanti; tali echo-chamber tendono a rigettare a priori informazioni esterne.

3.4.2 Sfide

L'utente continuerà comunque a scegliersi le proprie fonti di informazione in base alla loro coerenza con la sua visione del mondo. La sfida principe consiste quindi nell'evitare che le echo-chamber legate alle diverse visioni del mondo si "polarizzino" sino al punto in cui venga a morire il dibattito necessario all'essere in atto di una democrazia compiuta. Dobbiamo pertanto creare sinergie per progettare e implementare strumenti ad hoc per il monitoraggio e il sensing dell'opinione pubblica on-line che permettano di capire gli argomenti polarizzanti del momento, al fine di poter intervenire in maniera tempestiva o ancor meglio preventiva prima che il dibattito degeneri in uno scontro fra due fazioni senza contatti. Da questo punto di vista, l'informatica si trova ad avere un ruolo centrale rispetto ad altre discipline; allo stesso tempo, la necessità di abbassare le barriere disciplinari indica la *complexity science* come un possibile framework interdisciplinare per aggregare dati e modelli, mantenendo una componente fortemente quantitativa che eviti l'eccesso di speculazioni.

Complexity science – Disciplina sviluppatasi dai successi della fisica statistica nell'interpretazione dei fenomeni collettivi della materia; grazie alla possibilità di analizzare grandi quantità di dati, ha permesso di rivedere sotto nuova luce e reinterpretare fenomeni delle scienze sociali, economiche, biologiche, fino ad aprire nuove prospettive sulla comprensione del comportamento di sistemi tecnologici complessi come le infrastrutture di rete.

L'attività scientifica, da sola, rischia però di non avere effetto se non si instaurano sinergie con gli operatori dell'informazione, i quali vanno costantemente aggiornati sulle dinamiche osservate, permettendo loro di comprendere meglio gli effetti delle loro azioni nella infosfera. Vanno quindi realizzati percorsi formativi e momenti di incontro, rivolti al sistema dei media, volti a favorire la reciprocità e il perseguimento di obiettivi comuni sia in ambito generale sia su temi specifici come la salute pubblica.

Infine, saranno importantissime le attività di formazione e aggiornamento delle forze deputate a proteggere e a regolare l'intersezione fra l'infosfera e il cyberspace affinché i loro operatori acquisiscano una visuale di come i processi e i flussi informativi evolvano in questi nuovi spazi, di come ci si debba muovere per intervenire in maniera efficace e tempestiva e di quali possano essere i metodi efficaci per introdurre forme di regolamentazione in tali spazi virtuali e non più geografici. Allo stesso tempo, bisogna far capire che qualsiasi intervento deve fortemente tutelare la diversità delle opinioni, in quanto anche non tenendo conto di ovvie implicazioni etiche, diminuire la ricchezza di un sistema significa diminuirne le capacità di reazione e di adattamento.

A tal scopo, la grande sfida è non solo quella di produrre modelli coerenti con le osservazioni dei dati sperimentali, ma anche semplificare e comunicare tali modelli affinché diventino utili strumenti nelle mani di chi ha il compito di proteggere la nostra società.

3.4.3 Obiettivi

Al fine di comprendere e verificare le dinamiche delle informazioni sui social media bisogna poter osservare e analizzare con continuità i grandi flussi scambiati fra i loro utenti. L'analisi non può essere né puramente algoritmica (per i problemi precedentemente ricordati), né puramente antropica, non fosse altro per i volumi in gioco. In base allo stato dell'arte e al livello di conoscenze presente attualmente in Italia, si deve aspirare a raggiungere in tempi relativamente brevi (primi risultati presumibilmente da sei mesi a un anno dall'inizio dell'attività) i seguenti obbiettivi:

- *Monitoraggio e sensing dello spazio informativo sui social media* — Occorre effettuare un continuo monitoraggio dei social media per identifi-

care i temi di interesse e le loro tendenze in modo da capire il fabbisogno informativo degli utenti. Il monitoraggio sarà utile per individuare e seguire la dinamica (nascita–vita–morte) delle echo-chamber. In base ai dati raccolti sarà possibile espletare diverse valutazioni basate su metriche e/o algoritmi di machine learning.

- *Grado di polarizzazione* — La polarizzazione separa le echo-chamber, diminuendo la diversità e inficiando i processi democratici. È necessario sviluppare, come già avvenuto in altri ambiti per l'analisi della competitività e delle potenzialità di sviluppo delle nazioni [20], metriche e ranking di provata efficacia. Poter definire un *polarization rank* permetterebbe di avere un'indicazione quantitativa per le testate giornalistiche su scala locale, regionale, nazionale ed europea sulle loro prestazioni sui social, tenendo conto dell'accuratezza e dell'effetto polarizzante (o meno) della presentazione delle notizie.

- *Early Warning dei potenziali argomenti che possano essere veicolo di informazioni false-fuorvianti-strumentali* — L'approccio dovrà essere di tipo statistico, in cui un classificatore basato su machine learning userà caratteristiche sintattiche, semantiche, nonché la rete dei flussi di informazione, per fare previsioni accurate sui possibili argomenti suscettibili di veicolare o diventare essi stessi fake news.

- *Benchmarking* — Analizzando e confrontando fra di loro le caratteristiche delle cascate di informazione legate a determinate notizie, occorre misurare l'efficacia di penetrazione di vari tipi di comunicazione su temi specifici come l'immigrazione, le vaccinazioni, la salute, il cibo, la geopolitica.

Una volta raggiunti tali obbiettivi, si potrà integrare i mezzi e le tecniche sviluppate per mirare a un obbiettivo di ordine superiore, ovvero alla tutela della *biodiversità degli ecosistemi dell'informazione on-line*, dove per biodiversità si intende la coesistenza in uno stesso ecosistema di diverse specie animali e vegetali che raggiunge un equilibrio grazie alle loro reciproche relazioni [52]. L'analisi delle echo-chamber e delle loro interazioni permetterà di valutare la robustezza e la biodiversità degli ecosistemi informativi a vari livelli, da quello locale a quello mondiale.

3.5 Anticipare la risposta ad attacchi fisici

Le immagini e i video che vengono postati sul web, o ricavati da telecamere di sorveglianza, stanno assumendo un'importanza crescente per supportare le agenzie nazionali e internazionali di controllo del territorio nella loro attività

di contrasto a organizzazioni terroristiche e alla criminalità organizzata. Le apparecchiature adibite alla videosorveglianza, pubbliche o private, costituiscono sempre di più uno strumento investigativo fondamentale per le indagini delle forze dell'ordine.

A livello di sistema Paese, tuttavia, manca ancora uno sforzo coordinato e continuato finalizzato al monitoraggio del territorio tramite i video acquisiti dalle telecamere di sorveglianza disseminate sul territorio, all'elaborazione e all'analisi dei dati raccolti e all'uso rapido ed efficace di tali informazioni da parte delle autorità competenti.

Una situazione analoga si sta verificando nell'ambito del monitoraggio automatico di immagini e video condivisi da utenti tramite i loro profili social. Nonostante sempre più spesso l'acquisizione e l'analisi di tali contenuti multimediali costituiscano un elemento prezioso per le forze dell'ordine, tale analisi è tipicamente condotta manualmente, senza il supporto di strumenti automatici di raccolta e analisi.

3.5.1 Stato dell'arte

La quantità di dati video prodotti da telecamere di videosorveglianza, particolarmente quelle ad alta definizione, sta crescendo in modo impressionante. Basti considerare che una singola telecamera HD può generare approssimativamente 0,7 TB di dati video compressi al mese, e che quelle installate sono decine di milioni: uno studio della IHS[27] riporta la media di una telecamera, non necessariamente HD, ogni 29 abitanti del pianeta. Si può quindi ragionevolmente sostenere che i dati video generati dalle telecamere stanno diventando il "più grande" Big Data [43]. Non è però solo una questione di volumi: vi sono anche i problemi posti dall'elevatissima velocità di raccolta in tempo reale e dall'analisi e comprensione del contenuto di tali video in tempi rapidi. Tutto questo porta a nuove sfide tecnologiche che vanno dalla compressione, memorizzazione e trasmissione di video, all'analisi automatica dei loro contenuti, fino allo sviluppo di strumenti di analisi e sintesi di metadati in grado di rendere fruibili a utenti specializzati il risultato di tali analisi.

Le agenzie di finanziamento internazionali hanno colto queste esigenze e numerosi progetti internazionali sono stati finanziati, sia in Europa nell'ambito di Horizon 2020, sia negli USA nell'ambito delle attività supportate dal DARPA. Sebbene la ricerca nel settore sia in un momento di grande espansione, con forte interesse e supporto economico anche delle grandi multinazionali come IBM, nVIDIA, Google, Facebook e Microsoft, manca ancora, nel panorama italiano, un piano specifico di investimenti di ampio respiro e su larga scala temporale, in grado di coinvolgere le energie migliori del sistema Italia in ambito accademico e industriale per affrontare in maniera convincente tali problematiche.

[27] `https://www.ihs.com/info/0615/video-surveillance-methodology.html`

Un circolo virtuoso tra università, impresa e Stato ha portato, in paesi come la Germania e la Svezia [63, 51], allo sviluppo di una economia della conoscenza di avanguardia, competitiva a livello mondiale.

3.5.2 Sfide

Le sfide principali riguardano:

- *Intelligenza visuale collaborativa a livello urbano* — Lo sviluppo di sistemi di intelligenza visuale finalizzati a supportare il controllo del territorio da parte delle forze dell'ordine necessita innanzitutto di sistemi integrati di acquisizione e trattamento di video, provenienti tendenzialmente da: telecamere di videosorveglianza, telecamere aeree da sistemi di remote sensing (dai satelliti ai droni), telecamere mobili sulle auto e sui mezzi di trasporto pubblico che sempre di più saranno collegate in modalità vehicle-to-vehicle e vehicle-to-infrastructure, telecamere egocentriche (solidali con le persone che le indossano), e da smartphone in possesso a cittadini e/o forze dell'ordine. Questo richiederà la realizzazione di sistemi e servizi integrati, basati sulla collaborazione tra la competenza umana e l'Intelligenza Artificiale, tendenzialmente tramite architetture neurali allo stato dell'arte, per elaborare in tempo reale i big data visuali. L'obiettivo è fornire: (i) risultati comprensivi di analisi visiva, (ii) classificazione e rilevamento di eventi di interesse, (iii) correlazione automatica tra viste diverse provenienti da sensori diversi, (iv) identificazione e ri-identificazione di individui, (v) rilevazione e predizione automatica di comportamenti e/o intenzioni di gruppi di persone.

- *Monitoraggio automatico di contenuti visivi provenienti dal web* — Lo sviluppo di sistemi in grado di analizzare automaticamente immagini e video condivisi sui social media riveste un'estrema importanza al fine di contrastare la minaccia terroristica. La grande sfida in questo ambito è quella di identificare e segnalare alle forze dell'ordine contenuti di probabile matrice criminale. In particolare, un problema aperto è l'analisi automatica di immagini/video al fine di identificare simboli culturali e religiosi per rilevare contenuti di potenziale matrice terroristica, quali i video utilizzati per reclutare adepti. Un aspetto più sottile, ma altrettanto rilevante, è capire automaticamente l'impatto che questi contenuti visuali sono destinati ad avere sugli utenti dei social media. I contenuti multimediali condivisi nei social media per la propaganda sono tipicamente scelti per attirare l'interesse del maggior numero di utenti (cioè per diventare virali) e per evocare sentimenti forti negli osservatori. Pertanto, una sfida fondamentale per comprendere la strategia dei terroristi e ostacolare i loro sforzi è quella di analizzare la relazione tra contenuti vi-

suali e viralità, nonché fornire strumenti in grado di inferire il contenuto emozionale evocato da immagini e video.

- *Gestire, visualizzare e analizzare contenuti visivi su larga scala* — La cardinalità e la complessità dei dati visivi di interesse rendono necessario l'utilizzo di soluzioni basate su *visual analytics* che, combinando tecniche di visualizzazione avanzate con analisi automatica, siamo in grado di estrarre informazioni dai dati analizzati e presentarle tempestivamente e in modo efficace agli operatori che devono prendere decisioni relative alla sicurezza nazionale. Risulta essenziale, a tal fine, rendere disponibili all'operatore informazioni aggregate e filtrate contestualizzate ad aspetti geografici, temporali e sociali. L'analisi automatica permette di evidenziare comportamenti ripetitivi o simili (per esempio evidenziare persone sospette che sono state fisicamente nello stesso luogo in un certo intervallo temporale o che hanno effettuato spostamenti simili); tale analisi deve essere guidata dall'utente che, sulla base delle sue attività esplorative, fornisce all'algoritmo i parametri necessari al suo funzionamento, e.g., le località su cui effettuare l'analisi, il periodo temporale, gli individui da osservare, e così via. Un'altra sfida, ortogonale alla visualizzazione, consiste nello sviluppo di tecniche di riduzione dei dati oggetto di analisi, riducendone la complessità e la cardinalità, mantenendone la ricchezza informativa, per permetterne una più efficace esplorazione visuale.

3.5.3 Obiettivi

I progressi degli ultimi anni nel campo dell'intelligenza artificiale applicata alla visione computerizzata, con particolare riferimento all'impatto legato all'utilizzo di tecniche di deep learning, rendono maturi i tempi per la realizzazione di progetti a lungo termine e su scala nazionale per:

- l'acquisizione e l'analisi automatica dei video da telecamere di sorveglianza su tutto il territorio nazionale, finalizzata all'individuazione di comportamenti e individui sospetti, anche su scale temporali di svariati mesi, robusti alle variazioni dell'illuminazione, delle condizioni meteorologiche e dell'abbigliamento delle persone di interesse;

- l'analisi automatica di immagini e video postati dalle persone di interesse sui loro profili social, in grado di (i) riconoscere il luogo di acquisizione di immagini senza ricorrere a metadati non sempre disponibili, (ii) descrivere il contenuto emotivo di video e/o foto postate e/o condivise con altri utenti;

- lo sviluppo di tecniche di visualizzazione avanzata per la fruizione efficace delle analisi effettuate da algoritmi sui dati visivi, in modo da poter

rendere tempestivamente utilizzabili tali dati dagli operatori che devono prendere decisioni relative alla sicurezza nazionale, per aspetti legati sia ad attacchi terroristici sia a emergenze naturali.

In particolare i progetti devono perseguire lo sviluppo di:

- sistemi di ricostruzione automatica di viste integrate da telecamere fisse, mobili ed egocentriche;
- sistemi per il rilevamento di persone e target "in the wild"; loro possibile (ri)-identificazione su vasta scala sia spaziale sia temporale;
- sistemi di tracking predittivo di target in movimento, con modelli comportamentali sociali per l'analisi del comportamento delle folle in caso di eventi critici e modelli comportamentali specifici per l'analisi delle relazioni tra persone;
- tecnologie per identificare elementi simbolici ricorrenti in immagini e video, e metodi di analisi per valutare il contenuto emozionale di dati visuali al fine di riconoscere immagini dal forte impatto emozionale e di predire automaticamente attributi percettivi come il "potenziale" di viralità e popolarità di specifici dati visuali;
- sistemi per la visualizzazione geografica e temporale di dati e metadati relativi a persone, eventi catastrofici e/o informazioni legate a social media, con meccanismi visuali per parametrizzare algoritmi di analisi automatica;
- modelli di architetture per la realizzazione di una nuova generazione di sistemi di video sorveglianza per la sicurezza pubblica.

3.6 Analisi forense e conservazione delle prove

L'informatica forense ha vissuto negli ultimi 20 anni un periodo di straordinaria fortuna, guadagnandosi frequentemente il prime time nei notiziari e nei talk show televisivi. Questo è in gran parte legato al fatto che per lungo tempo le principali fonti di prova sono rimaste *tecnologicamente stabili* e hanno pertanto consentito di sviluppare e affinare metodologie e strumenti di indagine forense straordinariamente efficaci. Le fonti di prova digitale non assimilabili ad artefatti dei Sistemi Operativi sono rimaste a lungo limitate a fonti documentali (digitali) come basi dati (es. a fini contabili), documentazione del traffico telefonico e registri cronologici variamente denominati, rispetto alle quali sono stati sviluppati efficaci approcci investigativi.

3.6.1 Stato dell'arte

La situazione era ed è tuttavia destinata a mutare: già nel 2010 Garfinkel [36] preconizzava la fine della *golden age* dell'informatica forense di fronte all'incremento esponenziale di capacità dei dispositivi di memorizzazione, al diversificarsi delle fonti di prova digitale e alla diffusione del cloud computing e della crittografia.

Nel lavoro di Karie et. al. del 2015 [47] vengono riassunte, in una tassonomia che comprende quasi trenta voci, le principali sfide con le quali l'informatica forense si dovrà confrontare, distinguendo tra sfide tecnologiche, giuridiche, relative al personale e operative. Fra esse si ritrovano le problematiche già evidenziate da Garfinkel e altre legate sia alla difficile interoperabilità tra diversi strumenti utilizzati nelle indagini, sia alla carenza di personale adeguatamente addestrato a svolgere indagini forensi digitali.

Vale la pena di sottolineare che alcune sfide sono state nel frattempo aggravate dall'ulteriore incremento della capacità dei dispositivi di memorizzazione e da una marcata diversificazione delle fonti di prova. Tutto ciò richiede un profondo ripensamento del modello tradizionale di uso degli accertamenti informatici, essenzialmente basato sull'esecuzione di una copia immagine (bitstream) dei supporti rinvenuti e la successiva analisi in laboratorio.

A oggi non è più (in generale) possibile seguire tale modello, vuoi per il tempo necessario ad acquisire copia dei supporti (con conseguente blocco delle attività del soggetto indagato), vuoi per l'impossibilità tecnica di eseguire copie immagine di alcuni tipi di dispositivi, quali quelli mobili di ultima generazione, i sistemi embedded e i dispositivi IoT, per i quali si deve o ricorrere giocoforza alla cosiddetta *acquisizione logica* del contenuto, ove possibile, oppure rinunciare a una possibile preziosa fonte di prova.

Nell'ottica illustrata diventa quindi di fondamentale importanza sviluppare nuove tecniche di acquisizione e analisi forense che, abbinate a un'adeguata riflessione giurisprudenziale, consentano di evitare o superare il momento di impasse, riportando la disciplina ai fasti della *golden age*.

3.6.2 Sfide

Le principali sfide riguardano pertanto:

- *Incremento esponenziale del volume dei dati* — Il contenimento del tempo necessario per la generazione delle copie può essere affrontato anche implementando il cosiddetto *triage forense*. Sebbene siano stati proposti diversi approcci della selezione preventiva delle fonti, il problema rimane aperto soprattutto perché ogni eventuale soluzione deve bilanciare interessi differenti. Inoltre la selezione preventiva della fonte:

  - viola in apparenza il principio di completezza della prova, talché un ipotetico difensore potrebbe argomentare che il ragionamento investigativo e probatorio è viziato dalla stessa selezione operata a monte e quindi che la difesa sarebbe privata della possibilità di effettuare ulteriori indagini difensive);
  - è intrinsecamente esposta ad azioni di *antiforensic*, in quanto un ipotetico attaccante sarebbe inevitabilmente a conoscenza degli artefatti oggetto di prima indagine e potrebbe alterarli o distruggerli. Difatti, recentemente sono comparsi alcuni tipi di attacchi informatici intesi a introdurre dolosamente delle *fake evidence* allo scopo di sviare le indagini.

- *Diversificazione delle fonti di prova* — Già a una prima riflessione risulta evidente che non è possibile immaginare un modello di acquisizione generalizzato senza la fattiva collaborazione dei produttori dei dispositivi. Infatti, nell'impossibilità di accedere direttamente alle informazioni memorizzate, diventa necessario fidarsi di quelle volontariamente comunicate dal dispositivo stesso.

  Va inoltre tenuto conto che, a causa delle limitazione delle risorse hardware o per esigenze di riservatezza, spesso i dispositivi di piccole dimensioni non consentono alcun accesso alle informazioni memorizzate internamente, se non con mezzi eccezionali. Nel caso poi dei dispositivi di telefonia mobile è noto come i produttori tendano a incrementare le misure di sicurezza verso accessi esterni non autorizzati dal possessore del dispositivo stesso. La strategia è certamente condivisibile nell'ottica della tutela della riservatezza, dato che un indebolimento delle protezioni si risolverebbe in un indubbio vantaggio sia per le investigazioni lecite sia per le intrusioni abusive, ma rappresenta un grave ostacolo per le prime.

  Peraltro, l'argomento della riservatezza non è altrettanto spendibile nel caso di quei dispositivi (es. dispositivi medici e diagnostici, centraline embedded per il controllo di veicoli, sistemi di controllo degli impianti industriali, sistemi "intelligenti") per i quali è interesse non solo del possessore, ma dell'intera collettività, poter acquisire le informazioni che ne provano il corretto funzionamento o – per contro – che consentano di rivelare eventuali abusi (si pensi al recente caso delle centraline di alcune case automobilistiche "programmate" per falsificare i risultati dei test delle emissioni).

- *Volatilità delle fonti ed estensione della* window of opportunity *per l'acquisizione* — Una sfida a parte che deve necessariamente essere considerata riguarda la cosiddetta *window of opportunity* per l'acquisizione della fonte di prova. Le informazioni contenute nei supporti informatici non sono infatti soggette a un degrado naturale come i reperti biologici,

ma sono soggette a tempi di conservazione programmati esplicitamente o implicitamente in fase di progetto. In alcuni casi, quali i documenti contabili e la documentazione del traffico telefonico, la legge stabilisce un *retention time*, ovvero il termine entro il quale l'informazione deve essere conservata e oltre il quale può o – in qualche caso – deve essere distrutta.

Vi sono tuttavia casi di registrazioni cronologiche (log) il cui *retention time* è legato alle motivazioni per cui sono state raccolte (cioè per la diagnosi di malfunzionamenti del dispositivo/sistema) e non a scopo investigativo. Si pone dunque il problema di definire e – possibilmente – regolamentare quali informazioni devono essere raccolte obbligatoriamente e le loro modalità di acquisizione rispettando allo stesso tempo le legittime aspettative di privacy e le esigenze di repressione del crimine (spesso nell'interesse dello stesso soggetto possessore del dispositivo da esaminare).

Un aspetto particolare che rientra comunque in questo punto riguarda la definizione delle corrette modalità di generazione e conservazione dei log, relativamente alle quali regna oggi la più competa anarchia. Se è vero che i log di sistema vengono generalmente generati e conservati correttamente dagli operatori delle infrastrutture informatiche, che ne sono anche i principali utenti, a scopo diagnostico o di ottimizzazione delle prestazioni, è altrettanto vero che – come può testimoniare chiunque abbia una minima pratica forense – i log applicativi, nei casi in cui sono presenti, raramente consentono di rispondere anche alla più elementare delle domande investigative e spesso non sono neppure documentati. Peraltro anche per le fonti di prova più tradizionali, quale la documentazione del traffico telefonico, si pone spesso il problema di rendere semanticamente omogenee le informazioni ottenute dai diversi gestori e di arricchirle di quelle annotazioni che permettano di interpretarle correttamente a distanza di tempo, anche a fronte della continua evoluzione tecnologica.

3.6.3 Obiettivi

Gli obiettivi del progetto sono identificabili in tre linee di azione, ciascuna correlabile a una precisa sfida:

- *Incremento esponenziale del volume dei dati* — Sviluppo di metodologie e strumenti di triage forense, idonei a contenere il tempo di acquisizione e quello di successiva analisi, senza tuttavia compromettere la qualità e l'affidabilità del mezzo di prova;

- *Diversificazione delle fonti di prova* — Analisi delle nuove fonti di prova e sviluppo di metodologie di analisi più flessibili, ma altrettanto efficaci, della copia bitstream;
- *Volatilità delle fonti ed estensione della* window of opportunity *per l'acquisizione* — Sviluppo di linee guida relativamente alla corretta modalità di generazione e conservazione delle registrazioni cronologiche e definizione di periodi minimi di conservazione che tengano conto anche delle esigenze di analisi forense dei dati generati.

3.7 Gestione del rischio a livello sistemico

La gestione dei rischi è una disciplina ben consolidata nei settori degli investimenti finanziari, delle attività aziendali e della gestione dei progetti. Le metodologie tradizionali di gestione del rischio non possono tuttavia essere applicate nel campo della sicurezza informatica. In particolare, la natura dinamica del rischio cyber (minacce, agenti, vulnerabilità, incidenti e impatti) non è correttamente rappresentata nei metodi statici e iterativi degli attuali modelli e standard di gestione dei rischi.

È necessario un approccio che miri alla creazione di un *framework dinamico di gestione dei rischi cyber* (Dynamic Cyber Risk Management – DCRM) in grado di considerare correttamente le vulnerabilità ICT in evoluzione in un'intera organizzazione e di mitigare le relative minacce e rischi, che richieda una nuova dimensione rispetto alla gestione tradizionale del rischio: la necessità di essere dinamici e adattarsi continuamente.

3.7.1 Stato dell'arte

Molti sforzi sono stati intrapresi dal mondo della ricerca e dall'industria per sviluppare una disciplina solida e coerente applicabile al cyberspace. Negli ultimi anni sono stati elaborati quadri di riferimento differenti e standard specifici, tra cui ISO/IEC 27005[28], NIST 800 30[29], IT Risk (ISACA)[30], COSO[31], ITIL[32] e OCTAVE[33]. Tuttavia, tutti questi framework sono costituiti da un approccio statico e

[28] https://www.iso.org/standard/56742.html

[29] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[30] https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

[31] https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[32] https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[33] https://www.cert.org/resilience/products-services/octave/

non possono essere applicati per gestire il rischio cyber dinamico. Inoltre, questi modelli sono parzialmente discutibili quando introducono e valutano i rischi basandosi sulla probabilità degli eventi: in particolare, nelle grandi organizzazioni questo processo di valutazione può essere complicato e richiedere molto, troppo tempo: a causa delle vulnerabilità e delle minacce in costante evoluzione, i risultati di una valutazione dei rischi possono diventare rapidamente obsoleti.

La protezione delle infrastrutture critiche sta diventando una delle pietre miliari della sicurezza nazionale. La Commissione Europea richiede già agli Stati membri di aumentare la loro consapevolezza e di migliorare la loro reciproca cooperazione. La Direttiva NIS (illustrata nella sez. 1.2.1) incentiva in particolare lo sviluppo di relazioni di fiducia tra soggetti pubblici e privati e la valorizzazione di una cultura condivisa e cooperativa di gestione dei rischi.

3.7.2 Sfide

Occorre definire gli strumenti per sviluppare un quadro globale di governance pubblico-privato per il rischio cyber, introducendo strumenti innovativi di intelligence e metodologie specifiche. Una delle principali sfide riguarda il rafforzamento delle politiche e delle procedure di notifica e di condivisione delle informazioni tra le entità nazionali e in particolare nel settore privato, al fine di mantenere una visione complessiva del panorama delle minacce e migliorare le capacità di preparazione e di risposta agli incidenti.

È pertanto importante definire dei framework che definiscano approcci metodologici, politiche, processi e tecnologie abilitanti da adottare in enti e aziende per affrontare specifici requisiti di gestione dei rischi cyber e dalle organizzazioni governative per la condivisione delle informazioni sulle principali minacce, vulnerabilità, impatti e incidenti che si verificano nel cyberspace.

Questi framework consentiranno a tutte le istituzioni coinvolte nella gestione del rischio di costruire un contesto più ricco di consapevolezza situazionale (*situational awareness*) a livello nazionale, permettendo loro di: (i) comprendere l'attuale posizione di sicurezza di tutti i soggetti interessati alle infrastrutture critiche; (ii) valutare ed eventualmente sostenere i progressi verso il corretto posizionamento; (iii) comunicare il rischio cyber con gli interlocutori interni; (iv) coordinare le autorità competenti pubbliche per reagire agli incidenti e adottare adeguate misure di attenuazione; (v) determinare il processo decisionale dei responsabili politici sulle priorità strategiche.

3.7.3 Obiettivi

Due sono i principali framework dei quali si rileva l'esigenza:

- *Dynamic Cyber Risk Management – DCRM* — Le componenti del DCRM devono essere progettate, sviluppate, implementate e convalidate in contesti reali tenendo conto dei seguenti importanti principi:

  - definizione chiara della politica di gestione dei rischi cyber e dei criteri correlati per la valutazione e la gestione del rischio (attitudine al rischio dell'organizzazione, criteri di gestione dei rischi e livello di tolleranza, articolazione dei ruoli e della responsabilità);
  - focalizzazione sulla valutazione della *gestione dinamica* dei rischi: le criticità delle operazioni e dei servizi critici, le vulnerabilitá, la presenza di minacce dinamiche, la probabilità di un evento/incidente, l'impatto di un evento in atto;
  - applicabilità alle diverse società e infrastrutture critiche;
  - flessibilità nel comprendere legislazioni diverse e nuove;
  - processi e attività chiare per supportare l'individuazione precoce (identificazione dei rischi) e la risposta rapida agli incidenti (mitigazione dei rischi), consentendo iniziative immediate e operative, fornendo feedback ai processi di governance e di gestione del rischio aziendale; questo include anche la dinamicità nella rilevazione, valutazione e gestione di nuove minacce e vulnerabilità;
  - possibilità di condivisione di informazioni su rischi cyber dinamici e incidenti all'interno di un quadro di condivisione sicura delle informazioni con gli organismi pubblici (vedi il PPIS);
  - utilizzo di indicatori e metriche chiari per sostenere sia il miglioramento continuo del quadro DCRM, sia la revisione del modello di garanzia della sicurezza, i controlli relativi e i quadri di riferimento.

- *Public–Private Cyber Risk Information Sharing – PPIS* — Le componenti del PPIS devono essere progettate, sviluppate, implementate e testate in organizzazioni governative istituzionali, tenendo conto dei seguenti principi fondamentali:

  - allineamento con la strategia dell'UE per la sicurezza cyber, la legislazione specifica nazionale e requisiti specifici di settore (ad es., energetico, telecomunicazioni, idrico, etc.);
  - chiarezza dei ruoli e delle responsabilità sulla condivisione delle informazioni e sulla collaborazione tra le organizzazioni pubbliche e private coinvolte;

- concentrazione sulla “necessità di conoscere e di condividere” e su requisiti specifici di sicurezza di tutti i partecipanti e degli stakeholder per la condivisione di informazioni, collaborazione e fiducia reciproca;
- utilizzo di indicatori e metriche chiare per valutare e monitorare le tendenze del rischio a livello nazionale e settoriale;
- focalizzazione sull’attivazione del rilevamento precoce e la rapida risposta agli incidenti.

3.8 Difesa attiva

Il raffinamento delle tecniche di attacco informatico porta spesso le vittime ad accorgersi troppo tardi di un attacco in corso. La correzione di una vulnerabilità può impedire che venga sfruttata nuovamente, ma non può fare nulla nei confronti dell’attacco che l’ha portata alla luce. È necessario quindi un approccio proattivo di cosiddetta *difesa attiva*.

Difesa Attiva – Impiego di tecniche di hacking e di penetration testing (si veda il box a pag. 44) mirate all’individuazione di vulnerabilità di sistemi prima che queste possano essere sfruttate per attacchi; impiego di tecniche di contrattacco e di generazione di malware, per identificare e fermare attacchi in corso.

In generale, il concetto di difesa attiva è destinato a ricoprire un ruolo sempre più centrale nella protezione delle infrastrutture strategiche nazionali.

Disponendo di tecnologie avanzate e strumenti automatici per il rafforzamento delle proprie difese, le aziende coinvolte potranno garantire una maggior tutela dei propri asset strategici. Conseguentemente, anche la delicata gestione dei dati sensibili dei cittadini e delle infrastrutture critiche verrà irrobustita, innalzando le difese dell’intero Paese verso attacchi informatici.

È quanto mai urgente avviare adeguate campagne di formazione mirate a incrementare le capacità di difesa attiva. La comprensione delle tecniche di attacco e delle loro applicazioni pratiche si rivela infatti utile non solo per la formazione di personale qualificato, ma anche per chi intende intraprendere percorsi professionali diversi, quali il programmatore di sistemi.

3.8.1 Stato dell’arte

Tra le iniziative di formazione alla difesa attiva più popolari vi sono le competizioni in stile *Capture-The-Flag* (CTF), utilizzate da un numero crescente di aziende e agenzie governative, seguendo l’esempio di realtà come Google, Facebook e GCHQ.

CTF – Capture-The-Flag – Gara con simulazione di scenari realistici in cui i partecipanti svolgono attività di difesa attiva di complessi sistemi informatici, di attacco di applicazioni, di sviluppo e di analisi (*reverse engineering*) di malware.

Bug Bounty – Programma di ricompensa mirati al rilevamento di vulnerabilità di sistemi o servizi informatici (fase di *bug hunting*) e alla loro immediata segnalazione confidenziale ai titolari dei sistemi target, con chiare tutele legali per tutte le parti in causa.

A livello internazionale, negli USA sono da sottolineare le iniziative intraprese da DARPA che, oltre ad aver avviato un programma specifico di difesa attiva, ha recentemente organizzato la prima competizione CTF fra sistemi autonomi, denominata *Cyber Grand Challenge* (CGC)[34]. I team partecipanti hanno combinato le più innovative tecniche di difesa attiva e intelligenza artificiale per sviluppare sistemi in grado di identificare vulnerabilità presenti nel software fornito, generare patch di sicurezza e attaccare i sistemi avversari senza alcun supporto da parte di analisti.

In ambito italiano va segnalato il progetto *CyberChallenge.IT* del Laboratorio Nazionale di Cybersecurity del CINI, illustrato nella sez. 6.2.1.

Altri progetti vedono coinvolti il Team per la Trasformazione Digitale, il CERT Nazionale e il CERT-PA per definire politiche di "responsible disclosure" nazionale al fine di agevolare la rapida risoluzione dei problemi di sicurezza della PA e minimizzare i rischi per la cittadinanza. Tale iniziativa si allinea a progetti europei quali l'*EU Free and Open Source Software Auditing* (EU-FOSSA) [35] che prevede l'identificazione di vulnerabilità in software critici anche tramite iniziative di *Bug Bounty*.

3.8.2 Sfide

In tema di difesa attiva occorre definire nuove metodologie per la prevenzione e la mitigazione degli attacchi. Esse devono superare il tradizionale concetto di difesa passiva allo scopo di identificare e reagire prontamente alle minacce emergenti, quali le vulnerabilità *zero-day*. Infatti, a causa della natura eterogenea e altamente dinamica dei moderni sistemi ibridi, diventa necessario anticipare le azioni ostili, mettendo in pratica le stesse operazioni di un potenziale attaccante. Scopo principale di questa attività è l'individuazione di possibili falle nella sicurezza di un sistema, al fine di potenziarne le difese là dove più necessario o conveniente. In aggiunta, le azioni devono essere sviluppate in

[34] `https://www.darpa.mil/program/cyber-grand-challenge`

[35] https://joinup.ec.europa.eu/collection/eu-fossa

un ambito multidisciplinare che tenga conto dello specifico contesto operativo, coinvolgendo gli esperti dei vari domini applicativi.

> **Zero-day** – Vulnerabilità del software non nota ai gestori di un sistema interessati a difenderlo da attacchi, ma nota a eventuali attaccanti. Fino a quando la vulnerabilità non viene resa nota, gli attaccanti possono sfruttarla per compromettere il sistema stesso o altri sistemi. Un attacco che sfrutta una vulnerabilità zero-day è chiamato *exploit zero-day*.

Tali metodologie devono portare allo sviluppo di prodotti innovativi per l'analisi e la protezione dei servizi e delle infrastrutture. Questo processo dovrà avvenire sia coinvolgendo le principali industrie nazionali attive nel settore della cybersecurity, sia attraverso la creazione di start-up innovative con forti competenze verticali.

Inoltre, per garantire l'efficacia di queste iniziative, il legislatore dovrà definire e regolamentare i protocolli di sicurezza per i gestori delle infrastrutture critiche. Sarà necessario definire regole di comportamento e di ingaggio per permettere operazioni di difesa attiva, come il penetration testing (si veda il box a pag. 44), in condizioni compatibili con la sicurezza delle infrastrutture stesse.

Infine, dovranno essere definite procedure per la prevenzione, mitigazione e segnalazione delle minacce. Queste procedure dovranno fare capo a opportuni CERT (si veda il box a pag. 20) dedicati alla protezione di specifiche infrastrutture di interesse, quali ad esempio trasporti, energia e telecomunicazioni.

3.8.3 Obiettivi

Tra i principali obiettivi vanno annoverati:

- *Pratiche di difesa attiva* — Al riguardo è opportuno "istituzionalizzare" iniziative quali il progetto *CyberChallenge.IT* del Laboratorio Nazionale di Cybersecurity del CINI (illustrato nella sez. 6.2.1), estendendole a tutti gli studenti potenzialmente interessati, di ogni fascia d'età.

- *Programmi di Bug Bounty* — Con il duplice scopo di formazione e di miglioramento della sicurezza informatica nazionale, occorre incentivare la crescita dei programmi di *Bug Bounty* (si veda il box a pag. 76). Alle università spetta la formazione, pratica ed etica; alle aziende, l'aumento dell'utilizzo di tali strumenti, visti ancora con diffidenza. Iniziative comuni possono consistere nella pratica del "bug hunting" da parte di studenti universitari come parte di laboratori di cybersecurity, in stretta collaborazione con aziende partner, garantendo piena confidenzialità delle debolezze riscontrate.

- *Legislazione in tema di "white-hacking"* — Al legislatore spetta la riflessione riguardo le implicazioni legali di tali pratiche, fornendo tutele ai *white-hat hacker* che agiscono nell'ambito di campagne di penetration testing e bug hunting. È necessaria una comprensione del fenomeno e l'introduzione di chiare distinzioni legali tra chi sfrutta vulnerabilità e chi invece le comunica tempestivamente ai gestori dei sistemi/servizi analizzati. Strumenti quali la *responsible disclosure* dovrebbero diventare parte di iniziative di legge concrete, volte alla tutela, da un lato, delle aziende e delle PA e dei loro interessi, dall'altro degli scopritori di vulnerabilità che si impegnano alla confidenzialità e non dovrebbero quindi poter essere bersaglio di azioni legali.
- *Incident Response* — Un importante passo verso la difesa degli interessi nazionali e di infrastrutture e industrie strategiche è la creazione di CERT "verticali" dedicati ognuno a un aspetto specifico (come ad esempio distribuzione di energia, trasporti, mercati finanziari), con partner statali, industriali e accademici. Ulteriore responsabilità di tali consorzi dovrebbe essere la definizione dei confini del contrattacco digitale, (tema sempre più attuale, come evidenziato dalla proposta di legge USA *Active Cyber Defense Certainty Act*[36]), pratica volta alla difesa attiva contro attacchi in corso e all'identificazione dei responsabili.

White Hacking – Attività di esperti informatici, chiamati anche *hacker etici* o *white hat*, che si oppongono all'uso criminale dei sistemi informatici. Questi esperti sono specializzati nel *penetration testing* e in tutte le metodologie per testare la sicurezza dei sistemi, essi si differenziano dai *black hat* per le loro finalità positive e altruistiche.

[36] `https://www.congress.gov/bill/115th-congress/house-bill/4036/text`

CAPITOLO

4 Tecnologie abilitanti

Le tecnologie abilitanti aumentano il livello di cybersecurity di un sistema complesso.

Vengono dapprima analizzate le sfide poste dalle architetture hardware, che purtroppo, come Paese, abbiamo abbandonato da tempo, ma che giovano tuttavia un ruolo fondamentale nell'ottica della cosiddetta tecnologia nazionale.

Seguono alcuni sistemi verticali, quali la crittografia (in particolare la crittografia post-quantum), i sistemi biometrici e le tecnologie quantistiche, individuate come capisaldi tecnologici nei quali l'Italia ha una grande tradizione scientifica e industriale, che dovrebbe essere tramutata in vantaggio competitivo a livello internazionale.

Successivamente il capitolo presenta una tecnologia abilitante nelle quale l'Italia dovrebbe investire per costruire un ulteriore vantaggio competitivo: la costruzione di una blockchain nazionale.

Da notare che, in questo capitolo, non vengono considerate "abilitanti" tecnologie quali machine learning, big data, data analytics o intelligenza artificiale in quanto, di fatto, trasversali a tanti sistemi di sicurezza e da questi largamente impiegati. Sotto questa luce, gli algoritmi che ne sono alla base vanno invece protetti e vengono esaminati nel cap. 5.

4.1 Architetture Hardware

Analogamente a quanto avviene per il software, i dati e le infrastrutture di comunicazione, anche l'hardware deve essere progettato, costruito, collaudato, usato e manutenuto tenendo conto dei possibili attacchi cyber e delle loro conseguen-

ze. Le principali problematiche di security derivanti dalle componenti hardware presenti all'interno dei dispostivi *IoT* e degli *Industrial Control System* saranno analizzate rispettivamente nelle sezioni 5.4 e 5.5. In questa sezione vengono invece considerati i sistemi hardware nella loro complessità, con particolare attenzione al loro impatto sulla cosiddetta *Tecnologia Nazionale*.

Baco di progetto (Design Bug) – Errore principalmente ascrivibile al fatto che, nella fase di progettazione, è stata messa l'attenzione sugli aspetti funzionali ma non su quelli di sicurezza, per cui il dispositivo, pur "funzionando" correttamente, presenta delle vulnerabilità.

Hardware Trojan – Componente addizionale o componente modificato rispetto a quelli inizialmente previsti, mirato a introdurre vulnerabilità di vario tipo. Le modifiche possono essere apportate sia durante la progettazione del circuito da fornitori non attendibili di blocchi funzionali (IP-core) reperiti sul mercato o da progettisti malevoli, sia durante il processo di fabbricazione da fabbricanti non fidati.

Side-Channel Effect – Possibile vulnerabilità di un circuito o di un sistema derivante dalla possibilità di misurare (dall'esterno) e analizzare i valori di alcune grandezze fisiche dell'hardware, quali temporizzazioni, tensioni, correnti, campi elettromagnetici indotti, temperature, consumi di energia, etc. Questi valori possono essere correlati con i dati trattati dal software al fine di esfiltrare informazioni segrete in modo fraudolento.

Dispositivo contraffatto (Counterfeited hardware device) – Dispositivo che, ricuperato da apparati dismessi (ad esempio dissaldandoli dalle piastre), viene illegalmente riciclato e ri-immesso in modo fraudolento sul mercato, eventualmente dopo averne opportunamente contraffatto il package. Al di là del danno economico, l'uso di componenti "riciclati" può avere gravi conseguenze sulla safety dei sistemi nei quali vengono utilizzati (a causa del loro alto tasso di guasto) e grande impatto sulla security.

L'hardware esegue il software e costituisce, di fatto, l'ultima linea di difesa: se l'hardware è corrotto, tutti i meccanismi introdotti per rendere sicuro il software (a qualsiasi livello) possono rivelarsi inutili. Un hardware non opportunamente protetto può costituire l'anello debole della catena, diventando una facile porta di accesso al sistema, alle sue funzionalità e ai dati trattati.

Attacco fisico – Interazione fisica con un dispositivo hardware per accedere a suoi elementi interni (ad esempio, tramite *probing*) oppure per iniettare guasti durante l'esecuzione di un algoritmo di sicurezza. I guasti iniettati possono permettere, a titolo di esempio, di: (i) forzare il valore di un registro di un processore al fine di modificare il flusso di esecuzione di un programma, così forzandolo a saltare le funzioni di controllo della sicurezza; (ii) alterare la qualità di un generatore di numeri casuali; (iii) scoprire il valore della chiave segreta usata in un algoritmo crittografico. I guasti possono essere iniettati tramite impulsi laser, impulsi elettromagnetici, valori anomali sulle tensioni di alimentazione e/o sui segnali di temporizzazione, variazioni di temperatura di funzionamento.

Come per il software, le *vulnerabilità dell'hardware* possono derivare da bachi di progetto (*Design Bug*) o da dispositivi malevoli inseriti intenzionalmente all'interno di dispositivi (*Hardware Trojans*). Inoltre, a differenza del software, l'hardware può essere osservato e controllato (e quindi anche fisicamente attaccato) *dall'esterno*, tramite delle grandezze fisiche e/o le sue interazioni fisiche con il mondo reale (*Side-Channel effect*). Inoltre, nel caso dell'hardware, oltre agli attacchi tipici anche del software e mirati alla sottrazione indebita di dati e all'interruzione del servizio, si registrano anche (i) attacchi mirati al furto della proprietà intellettuale intrinseca nelle soluzioni tecnologiche impiegate e (ii) contraffazioni, tramite la ri-immissione fraudolenta sul mercato di dispositivi dismessi e quindi tipicamente usurati (*Hardware Counterfeiting*).

4.1.1 Stato dell'arte

Si trovano in letteratura numerosi articoli e testi che contengono analisi dettagliate dello stato dell'arte sul tema cui si rimanda per eventuali approfondimenti, si vedano ad esempio [66, 61, 46].

Sono note da anni [28] le criticità derivanti da un uso non accorto (dal punto di vista della security) di soluzioni di *Design for Testability*, quali le *catene di scan*, introdotte per permettere il collaudo dei dispositivi sia a fine produzione sia sul campo. In aggiunta a queste, agli inizi del 2018 hanno trovato ampia risonanza, anche sui mezzi di comunicazione di massa, due attacchi, noti come *Meltdown*[1] e *Spectre*[2], che sfruttano bachi nella progettazione hardware di processori avanzati. Questi bachi fanno sì che sia possibile sfruttare degli effetti collaterali della esecuzione *out-of-order* di istruzioni macchina (caricamento in cache di dati non autorizzati) per leggere il contenuto di locazioni di memoria alle quali non si dovrebbe avere accesso. I dati esfiltrati possono includere, a titolo di esempio, password, chiavi segrete, dati sensibili, autorizzazioni ad accedere ad altri servizi, e così via.

[1] `https://meltdownattack.com/meltdown.pdf`
[2] `https://spectreattack.com/spectre.pdf`

L'attacco Meltdown (noto come CVE-2017-5754[3]) crea un'eccezione software (trap) che fa abortire le istruzioni eseguite in anticipo e successivamente esegue una *privilege escalation* (vedi box a pag. 118) specifica dei processori Intel. L'attacco Spectre, invece, (CVE-2017-5753[4] e CVE-2017-5715[5]) si basa sulla tecnica classica della *branch-prediction* e, per la sua generalità, può essere effettuato con successo su processori Intel, AMD e ARM.

In entrambi i casi si tratta di "errori" nella progettazione che non impattano in alcun modo sulle funzionalità dei processori coinvolti, ma che introducono vulnerabilità dal punto di vista della sicurezza. In alcune condizioni, è infatti possibile, per un utente (processo) "normale", quindi senza particolari privilegi, accedere in modo fraudolento a informazioni che dovrebbero invece essere accessibili solo a utenti "privilegiati". Benché sviluppare attacchi come Spectre o Meltdown sia estremamente complesso (è quindi poco probabile che siano stati effettuati in pratica), essi rappresentano un'ulteriore dimostrazione di come corrompendo l'hardware o sfruttandone le vulnerabilità, tutti i meccanismi introdotti per rendere sicuro il software (a qualsiasi livello) possono rivelarsi inutili. Al riguardo, l'impatto di Meltdown e di Spectre sul Cloud viene analizzato nella sez. 5.2.

In conclusione, è importante sottolineare l'assoluta necessità di considerare in modo integrato gli aspetti di sicurezza e le varie vulnerabilità dell'hardware e del software. In alcuni casi, come quella sfruttata da Meltdown e di Spectre, la vulnerabilità hardware è eliminabile solo modificando il progetto delle prossime versioni dei processori, per cui l'unico modo per rimediare ("metterci una pezza", "sviluppare una patch") sui processori esistenti, che rimarranno "bacati" per sempre, consiste nell'agire a livello software ovvero modificare tutti i Sistemi Operativi esistenti che li usano. In altri casi è invece l'hardware a "venire in soccorso" delle possibili vulnerabilità del software, effettuando direttamente in hardware, anziché in software, una serie di verifiche e di operazioni in modo più sicuro e meno attaccabile.

4.1.2 Sfide

Tra le principali sfide da affrontare in questo ambito vanno annoverate le seguenti:

- *Hardware Security* — Nell'analisi dei problemi connessi con la sicurezza dell'hardware (*Hardware Security*) occorre tener conto di aspetti diversi, quali: (i) la tecnologia realizzativa impiegata; (ii) il livello gerarchico di astrazione considerato (blocchi logici, IP-core, chip, piastre, sistemi,

[3] `https://access.redhat.com/security/cve/cve-2017-5754`
[4] `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753`
[5] `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715`

etc.); (iii) le varie tipologie di componenti impiegati (processori, memorie, dispositivi di ingresso/uscita, sensori, attuatori, reti di interconnessione, dispostivi custom, dispositivi dotati di capacità di riconfigurazione, etc.); (iv) il dominio applicativo (automotive, industrial, consumer, etc.), (v) la complessità del sistema (sistemi embedded, mobile, personal, server, cluster, HPC, etc.).

- *Hardware Trust* — Gli aspetti di sicurezza vanno considerati in tutte le fasi del ciclo di vita di un dispositivo hardware (*Hardware Trust*): dalla progettazione alla fabbricazione, dal collaudo (sia a fine produzione sia sul campo) alla dismissione.

- *Lunghezza del ciclo di vita di dispositivi hardware* — 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 è tipicamente molto maggiore di quella del software, il quale può essere periodicamente aggiornato, anche con interventi da remoto. L'hardware, inoltre, può porre problemi di security al di là del termine la sua vita operativa, in quanto i componenti e dispositivi dismessi possono essere attaccati per esfiltrarvi i dati memorizzati o essere usati come dispositivi contraffatti. Mentre nel primo caso si hanno ovvi problemi di protezione dei dati, nel secondo, oltre ai già citati problemi di safety, si possono avere problemi di security derivanti, ad esempio, dall'impiego di un dispositivo, presunto di ultima generazione, ma in realtà di una generazione precedente che era nota contenere delle vulnerabilità, eliminate invece nelle ultime release della stessa famiglia.

- *Tolleranza alle vulnerabilità* — Come sopra evidenziato, le vulnerabilità derivanti dall'hardware, indipendentemente dalla loro natura, si possono correggere solo modificando il progetto e sono quindi di fatto destinate a rimanere presenti per sempre all'interno dei dispositivi. Per poter utilizzare in modo sicuro dispositivi vulnerabili occorre pertanto sviluppare delle soluzioni architetturali in grado di *tollerare* le vulnerabilità hardware impedendone lo sfruttamento da parte di attaccanti malevoli.

  Le soluzioni proposte possono essere di varia natura, a seconda della tipologia della vulnerabilità e del livello di criticità del sistema che utilizza i dispositivi. A mero titolo di esempio, si citano: (i) soluzioni basate esclusivamente sul software e mirate a impedire ad attaccanti malevoli di sfruttare vulnerabilità note; è questa la soluzione adottata da molti Sistemi Operativi nel caso di Meltdown e Spectre, modificati in modo tale da non permettere lo sfruttamento di alcune funzionalità; (ii) soluzioni basate sul *confinamento* nelle quali, in modo concettualmente analogo a quanto avviene nel caso delle Smart Card, i dispositivi interessati vengono "confinati" in zone *protette* (trusted) ed è permesso loro di eseguire

solo codice "sicuro", sviluppato e caricato in ambienti protetti e garantiti, essendo di fatto impossibile iniettarvi all'interno del codice malevolo tramite il quale sferrare attacchi di qualsiasi natura; (iii) soluzioni basate sull'interazione di opportune combinazioni di componenti diversi, quali processori, FPGA, Smart Card, dispositivi hardware dedicati; (iv) soluzioni mirate a tollerare comportamenti *bizantini* [48] nel caso di sistemi complessi con numerosi dispositivi interagenti.

- *Tecnologia nazionale* — La necessità dello sviluppo di una tecnologia nazionale verrà discussa nelle conclusioni di questo volume (cap. 9). È comunque opportuno considerare che nell'allestimento di una produzione "nazionale" di dispositivi hardware è necessario rendere trusted (e quindi sviluppata in ambienti protetti) l'intera filiera, che va dalla progettazione (persone coinvolte, gli strumenti di ausilio alla progettazione, fornitori di IP-core) al processo di produzione, al collaudo, alla installazione e alla manutenzione. Un'accorta programmazione e gestione garantirebbe la realizzabilità del progetto a costi non eccessivi e compatibili con le disponibilità del Paese.

- *Certificazioni* — Nel caso dell'hardware occorre evidenziare come, rispetto alle vulnerabilità analizzate sopra, le certificazioni vadano applicate e considerate avendone ben chiari i limiti derivanti dalla difficoltà (in molti casi dalla impossibilità) di misurare il livello di resilienza di un dispositivo verso un determinato tipo di attacco.

  Per quanto riguarda gli errori di progettazione, come quelli che rendono possibili attacchi quali Meltdown e Spectre, questi sono estremamente difficili da identificare e nessuna certificazione relativa al livello di sicurezza dei processori sarebbe in grado di certificarne l'assenza.

  Per quanto riguarda gli Hardware Trojan, è teoricamente possibile, con sforzi e costi non marginali, rilevare la presenza di un Trojan "noto", ma questo non darebbe in ogni caso alcuna garanzia sull'assenza di altri, ancora non noti.

  Per quanto riguarda i Side Channel effect è possibile misurare il livello di resilienza di un dispositivo rispetto a un attacco che sfrutti uno (o più) di questi effetti, avendo definito a priori l'ammontare della quantità e qualità delle risorse da impiegare nell'attacco stesso.

  Per quanto riguarda gli attacchi fisici, occorre preliminarmente definire modelli accurati del comportamento della tecnologia target rispetto a un insieme di mezzi di attacco, quali iniezione di corrente, luce, laser, sorgenti elettromagnetiche, etc. I modelli dovranno essere sviluppati a diversi livelli gerarchici di astrazione (elettrico, logico, RT, sistema), al fine da poterli integrare in simulatori in grado di valutare la resilienza dei di-

spositivi e l'efficacia delle eventuali contromisure contro questo tipo di attacco.

- *Root cause analysis di una vulnerabilità* — Nel caso della scoperta di un attacco portato avanti con successo, il capire se la vulnerabilità che l'ha reso possibile sia, in ultima analisi, ascrivibile all'hardware può essere molto complesso e ancora più complesso il risalire alla causa ultima. Emblematico, al riguardo, la difficoltà nell'identificare gli errori di progettazione che hanno reso possibili Meltdown e Spectre.

4.1.3 Obiettivi

In riferimento alle sfide da affrontare, e sopra riassunte, è necessario attivare un insieme di azioni mirate al raggiungimento dei seguenti obiettivi:

- *Sensibilizzazione e formazione* — (i) Incrementare nei policy maker e negli stakeholder la consapevolezza della gravità della minaccia e della rilevanza, anche economica, dei problemi connessi con la sicurezza dell'hardware; (ii) Sensibilizzare attivamente quanti, a livello nazionale, sono a vario titolo coinvolti nella progettazione, nella produzione e nel collaudo di sistemi hardware, attraverso le varie azioni e l'insieme dei progetti ampiamente illustrati nelle sezioni 6.2 e 6.3. Al riguardo occorre evidenziare come sia necessario agire, da un lato, a livello universitario, all'interno dei percorsi mirati alla formazione dei progettisti hardware: gli aspetti di *Hardware Security and Trust* sono oggi di fatto quasi completamente assenti nel panorama universitario italiano. Dall'altro, è necessario avviare percorsi di aggiornamento sia per i progettisti operanti nei *Design Center* attivi sul territorio nazionale, sia per quanti, a vario titolo, utilizzano componenti di tipo FPGA nelle architetture e nelle applicazioni più disparate.
- *Laboratori specialistici all'interno dei Centri di competenza* — In modo del tutto analogo a quanto già avviene in numerosi altri Paesi, è necessario prevedere, all'interno dei costituendi Centri di competenza in cybersecurity (analizzati nella sez. 2.3), l'attivazione di sezioni dedicate all'*Hardware Security and Trust*. In particolare è necessario prevedere l'attivazione, all'interno del *Centro Nazionale di Ricerca e Sviluppo in Cybersecurity*, di laboratori specialistici dedicati alla ricerca, allo sviluppo e al trasferimento tecnologico, in grado di fornire agli stakeholder nazionali, sia pubblici sia privati:
  - analisi, valutazioni qualitative e quantitative, misure della resilienza ad attacchi fisici di sistemi hardware, a tutti i livelli gerarchici di astrazione, per i vari tipi di componenti, e per le variegate complessità dei sistemi;

  - analisi dell'impatto sulla security di tecnologie diverse, da quelle cosiddette "emergenti" a quelle microelettroniche consolidate e a quelle del packaging;
  - supporto al *Centro di Valutazione e Certificazione Nazionale* nelle varie fasi e per le diverse tipologie di certificazioni discusse nella sez. 6.5;
  - supporto ai policy maker nella redazione di norme relative alle problematiche di security derivanti dalla dismissione di apparecchiature hardware;
  - consulenza sulle problematiche di security nella gestione di tutte le fasi del ciclo di vita (definizione dei requisiti, procurement, progettazione, produzione, test, analisi, ...) di infrastrutture hardware.

- *Supporto alla rete di CERT* — Avviare una stretta collaborazione con la rete di CERT nazionali per fornire loro supporto in tutte le fasi di *Root cause analysis* di vulnerabilità.
- *Sviluppo di architetture "nazionali" tolleranti le vulnerabilità* — Sviluppare architetture "nazionali" in grado di garantire livelli di security predefiniti, anche in presenza di dispositivi hardware contenenti vulnerabilità di diversa natura, note e/o non ancora rivelate. Le soluzioni proposte devono essere adattabili in funzione della criticità dei sistemi target.
- *Supporto alle produzioni "nazionali"* — A seguito della definizione, da parte dei policy maker, delle produzioni "nazionali" ritenute strategiche per la sicurezza nazionale e di quelle da reperire, invece, sul mercato estero, i Laboratori di cui sopra dovranno fornire il supporto necessario alla messa in atto delle relative politiche di sicurezza.

4.2 Crittografia

Nell'ambito della sicurezza nelle comunicazioni, la crittografia rappresenta la tecnica di base per garantire informazioni sicure dal punto di vista della indecifrabilità dei messaggi. Essa è uno dei meccanismi fondamentali per la protezione dei dati e per l'identificazione, ormai utilizzato in modo pervasivo, ad esempio, quando ci colleghiamo alla nostra banca via Web, disabilitiamo il dispositivo per immobilizzare la nostra automobile o utilizziamo bancomat, carte di credito, smartphone e addirittura chiavette per le macchinette dei caffe. Anche le nuove tecnologie *blockchain* (illustrate nella sez. 4.4) si basano su tecniche crittografiche per garantire l'integrità e la sicurezza delle transazioni.

È noto che negli ultimi anni il numero di vulnerabilità di sistemi crittografici è aumentato considerevolmente [15, 67, 7]. Gli attacchi basati sulla crittografia, un tempo considerati possibili solo da agenzie governative, fanno infatti ormai parte degli skill standard di hacker, come dimostrato dalla presenza di svariate sessioni di addestramento e presentazioni tecniche su attacchi crittografici nelle ultime edizioni di Black Hat[6,7,8] e DEFCON[9,10].

La sicurezza di un sistema crittografico non dipende solo da come i diversi algoritmi vengono combinati e implementati, ma è fortemente legata alla sicurezza degli algoritmi stessi. Sistemi ritenuti inviolabili fino a qualche anno fa sono oggi considerati insicuri: basti pensare a funzioni hash crittografiche quali MD5 e SHA1 per i quali è stato dimostrato che è possibile computare collisioni e, conseguentemente, falsificare eventuali firme digitali basate su tali funzioni [67, 68]. L'avvento di computer quantistici metterà in crisi sistemi di cifratura standard come RSA ed è quindi di fondamentale importanza studiare algoritmi *post-quantum* che siano robusti rispetto a tecnologie che, verosimilmente, saranno disponibili tra pochi anni.

Occorre infine evidenziare come l'hardware che esegue gli algoritmi crittografici costituisca, 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, 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.

I sistemi crittografici devono, quindi, essere realizzati in modo corretto e robusto per quanto riguarda sia gli algoritmi sia la loro implementazione in software e in hardware; in questa sezione vengono evidenziate le principali sfide e le linee di ricerca in tale ambito.

4.2.1 Stato dell'arte

Gli ultimi anni hanno evidenziato un approccio "fantasioso" delle aziende alla crittografia, con lo sviluppo di sistemi proprietari che sono stati, uno dopo l'altro, violati: si pensi, a titolo di esempio, ai sistemi di protezione automotive (e.g.

[6] https://www.blackhat.com/us-16/training/crypto-uses-and-misuses-how-to-use-cryptography-properly-and-attack-those-that-dont.html

[7] https://www.blackhat.com/us-17/training/schedule/index.html#beyond-the-beast-a-broad-survey-of-crypto-vulnerabilities-57601483747943

[8] https://www.blackhat.com/eu-17/training/crypto-attacks-and-defenses.html

[9] https://www.youtube.com/watch?v=lTngMxmymX4

[10] https://www.defcon.org/html/defcon-25/dc-25-workshops.html

[35, 73]). Questo ha creato una svolta e un'adozione sempre maggiore di sistemi crittografici standard ma, come abbiamo evidenziato, in molti dei casi non è semplice scegliere e configurare i meccanismi crittografici in modo da fornire le garanzie desiderate. La ricerca sulla crittografia ha prodotto risultati eccellenti a partire dagli anni '70, ma la crescente pervasività della crittografia impone di affrontare nuovi problemi per far sì che la sicurezza teorica degli algoritmi crittografici sia preservata dalle implementazioni e rimanga sicura negli anni anche a fronte di tecnologie rivoluzionarie, come i calcolatori quantistici.

Sicurezza dei sistemi crittografici Raccomandazioni sull'uso corretto dei sistemi crittografici vengono regolarmente emanate da importanti enti quali *National Institute of Standards and Technology* (NIST)[11], *European Union Agency for Network and Information Security* (ENISA)[12], *PCI Security Standards Council* [13], *Agence nationale de la sécurité des systemes d'information* (ANSSI)[14], *Bundesamt für Sicherheit in der Informationstechnik* (BSI)[15]. Ciononostante, non è sempre immediato tradurre le raccomandazioni in configurazioni e implementazioni sicure. Iniziative pubbliche e private come Better Crypto[16] e Cryptosense[17] cercano di colmare il gap tra le raccomandazioni "teoriche" e le loro implementazioni "pratiche".

Crittografia post-quantum Lo *European Telecommunications Standards Institute* (ETSI) ha istituito un gruppo di lavoro[18] e pubblicato un Libro Bianco[19] sul possibile impatto delle tecnologie quantistiche sulle attuali soluzioni di sicurezza IT. Nel 2013, la Commissione Europea ha finanziato, su queste tematiche, il progetto PQCRYPTO (*Post-quantum cryptography for long-term security)*[20]. Il NIST ha recentemente emanato un bando internazionale[21] per incentivare la progettazione e lo sviluppo di sistemi crittografici asimmetrici che risultino resistenti ad attacchi crittoanalitici eseguiti con computer sia quantistici sia classici e che, allo stesso tempo, possano interagire con i protocolli e le

[11] http://csrc.nist.gov/groups/ST/toolkit/key_management.html

[12] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014/

[13] https://www.pcisecuritystandards.org/document_library

[14] http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

[15] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

[16] https://bettercrypto.org/

[17] https://cryptosense.com

[18] http://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography

[19] http://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography

[20] http://cordis.europa.eu/project/rcn/194347_en.htm

[21] http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents.html

reti di comunicazione esistenti. In Italia la ricerca sui sistemi crittografici post-quantum ha visto una particolare enfasi sulle soluzioni che fanno uso di codici per la correzione d'errore [50, 8, 53].

4.2.2 Sfide

L'aumento esponenziale di attacchi effettuati su sistemi che adottano soluzioni crittografiche ha fatto emergere la necessità di un'analisi sistematica della crittografia applicata, ovvero di come un sistema crittografico venga realizzato e configurato. Esiste una vasta letteratura sull'analisi di protocolli crittografici, a livello *logico* di scambio di messaggi (e.g. [5, 17, 29]) e sono state analizzate specifiche implementazioni di protocolli (e.g. [14, 13]), ma è necessario studiare soluzioni sistematiche e ripetibili al problema di realizzare e configurare sistemi crittografici sicuri.

- *Sicurezza di librerie crittografiche esistenti* — Occorre analizzare la sicurezza di librerie e API crittografiche esistenti, per comprendere il livello di sicurezza fornito alle applicazioni. Infatti, in molti casi non è possibile per uno sviluppatore capire se l'utilizzo di un determinato meccanismo crittografico sia in grado di fornire le garanzie di sicurezza richieste dall'applicazione. Allo stesso modo, non è possibile per l'utente finale capire il livello di sicurezza crittografica di un'applicazione. Si pensi, ad esempio, alle app per l'home banking: l'utente deve fidarsi degli sviluppatori e non ha alcuna visibilità sul livello di protezione effettivo. È quindi fondamentale un'analisi sistematica delle librerie standard e lo sviluppo di strumenti e tecniche che permettano di valutare il livello di sicurezza crittografica delle applicazioni. Occorre poi effettuare un monitoraggio accurato degli errori crittografici "tipici", in modo da prevenire futuri attacchi. Questo permetterà di andare verso una certificazione di qualità dei sistemi crittografici rispetto alle raccomandazioni degli enti internazionali precedentemente menzionati.
- *Sicurezza di un algoritmo crittografico come parte di un sistema hardware/software* — Gli algoritmi crittografici sono tipicamente realizzati in complessi ecosistemi che, se mal configurati o implementati, potrebbero comprometterne la sicurezza teorica. Attacchi recenti hanno dimostrato che è molto importante porre attenzione al sistema nella sua interezza: l'attacco KRACK [72] su WPA2 mostra come un errore del protocollo possa compromettere completamente la sicurezza dei parametri dati in input agli algoritmi crittografici; in [32] vengono presentate alcune vulnerabilità dei *Java keystore*[22] che permettono di estrarre chiavi e certificati

[22] CVE-2017-10345 and CVE-2017-10356 `http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html`

crittografici utilizzati dalle applicazioni scritte nel linguaggio Java; in [56] è stata individuata un'implementazione insicura della generazione delle chiavi per il cifrario RSA che permette, per alcuni dispositivi in commercio, di determinare i fattori primi e quindi di rompere completamente lo schema crittografico. Per quanto riguarda la crittografia tradizionale, è quindi di fondamentale importanza investigare la sicurezza dei sistemi crittografici nella loro interezza, piuttosto che investire nella ricerca di nuovi algoritmi crittografici.

- *Sistemi di crittografia post-quantum* — I principali sistemi crittografici asimmetrici attualmente impiegati per cifrare e firmare digitalmente dati e comunicazioni basano la loro robustezza sulla difficoltà di risolvere, in modo computazionalmente efficiente, i problemi della fattorizzazione di numeri interi e dell'estrazione di logaritmi discreti. Questi sistemi sono però sempre più a rischio di decifrazione a causa della crescente potenza di calcolo a disposizione. Nel 1994, P. Shor [64] introdusse un algoritmo, progettato specificamente per essere eseguito da un computer quantistico, in grado risolvere i problemi della fattorizzazione di interi e dell'estrazione di logaritmi discreti in modo molto più efficiente rispetto agli equivalenti algoritmi progettati per computer classici. Nel momento in cui saranno disponibili i primi calcolatori quantistici, la loro capacità di fattorizzare i numeri interi in numeri primi, in modo estremamente più rapido rispetto ai calcolatori tradizionali, renderà vulnerabile (e quindi praticamente non più utilizzabile) qualunque sistema di cifratura attuale che utilizzi chiavi di dimensioni praticabili [57]. Considerando il crescente sviluppo di tecnologie quantistiche per sistemi elettromeccanici e ottici, è facile prevedere, entro pochi anni, l'introduzione di macchine quantistiche con potenza di calcolo in linea con le previsioni teoriche. Una recente relazione del Global Risk Institute[23], riporta

  > "una possibilità su sette che gli strumenti fondamentali della crittografia a chiave pubblica diventino obsoleti entro il 2026 e un 50% di possibilità che ciò avvenga entro il 2031".

  Risulta dunque di straordinaria importanza la definizione di schemi alternativi *post-quantum*, in grado di garantire un adeguato margine di sicurezza anche in presenta di elaboratori quantistici.

- *Sistemi crittografici quantistici* — A differenza dei sistemi crittografici post-quantum, i sistemi crittografici quantistici realizzano primitive crittografiche basandosi su proprietà della meccanica quantistica. La crittografia quantistica rappresenta un'importante area di ricerca sviluppata

[23] `http://globalriskinstitute.org/download/a-quantum-of-prevention-for-our-cybersecurity-1-pdf/`

a partire da un lavoro pionieristico di S. Wiesner [74]. Una delle principali sfide di questa disciplina è indubbiamente la sua realizzabilità pratica. Tuttavia, l'interesse per questa tecnologia è sempre crescente ed esistono oggi svariate aziende che producono e commercializzano sistemi crittografici basati su crittografia quantistica, tra cui ID Quantique (Ginevra, Svizzera),[24] MagiQ Technologies Inc. (Boston, MA, USA),[25] QuintessenceLabs (Canberra, Australia).[26]

- *Sistemi crittografici omomorfici* — La sfida più complessa resta quella di utilizzare o analizzare dati cifrati direttamente sul cloud: nelle soluzioni attuali è necessario decifrarli o spostarli all'interno dei propri sistemi, senza quindi sfruttare appieno le capacità offerte dal cloud. Esistono nuovi approcci che risolverebbero questo problema, come ad esempio la *cifratura omomorfica* di C. Gentry [37], che consente di operare su dati cifrati, ottenendo gli stessi risultati delle medesime operazioni svolte sui dati in chiaro. Utilizzando tali tecniche, si potrebbero eseguire applicazioni su dati memorizzati nel cloud senza doverli mai decifrare. Sfortunatamente, tali tecniche sono molto complesse a livello computazionale e rimangono quindi 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.

4.2.3 Obiettivi

I principali obiettivi da perseguire sono:

- Sviluppare strumenti e tecniche che permettano di: (i) valutare il livello di sicurezza crittografica di applicazioni, librerie e API crittografiche; (ii) monitorare gli errori crittografici "tipici" in modo da prevenire futuri attacchi; (iii) investigare tecniche di "crittoanalisi applicata" in grado di aggirare le garanzie di sicurezza degli algoritmi crittografici. Il tutto al fine di predisporre nuove certificazioni di qualità dei sistemi crittografici.

- Far avanzare lo stato attuale della crittoanalisi dei sistemi basati su problemi matematici diversi dalla fattorizzazione di interi e dall'estrazione del logaritmo discreto. Progettare nuovi crittosistemi il cui livello di sicurezza sia quantificabile con precisione, rispetto a calcolatori sia quantistici sia classici. Investigare l'attuabilità dei crittosistemi post-quantum su dispositivi di calcolo di uso generale e/o dedicato.

[24] `https://www.idquantique.com/`
[25] `http://www.magiqtech.com/`
[26] `https://www.quintessencelabs.com/`

A livello nazionale l'obiettivo principale di questo ambito rimane la costituzione di un *Laboratorio Nazionale di Crittografia*, come previsto dal DPCM Gentiloni. Questo laboratorio dovrà affrontare la sfida fondamentale di capire dove il nostro Paese dovrà investire in ambito crittografico, lanciando successivamente progetti di rilevanza nazionale. Le questioni importanti su cui riteniamo dovrà interrogarsi sono: (i) i rischi e opportunità dello sviluppo di algoritmi di *crittografia nazionale* e (ii) come affrontare l'emergenza legata all'arrivo dei computer quantistici.

4.3 Biometria

La verifica dell'identità digitale è elemento essenziale per la sicurezza di un sistema non solo informatico. L'importanza delle identità digitali è resa evidente dal fatto che il loro furto è uno dei crimini digitali più diffusi. Spesso, inoltre, il furto dell'identità digitale di un utilizzatore legittimo di un sistema è il primo passo utilizzato da hacker e criminali per portare attacchi molto complessi.

I metodi tradizionali per il riconoscimento degli individui sono basati su chiavi, token, documenti di identità e password. Questi approcci, seppur ancora validi, stanno però mostrando tutti i loro limiti in termini di sicurezza e soprattutto di usabilità. Infatti, sono sempre più diffusi dispositivi dotati di touchscreen o, più in generale, di interfacce non basate sull'uso delle tradizionali tastiere.

Per questo motivo, in aggiunta agli strumenti di autenticazione precedentemente menzionati, stanno velocemente diffondendosi tecnologie di riconoscimento biometrico che valutano tratti fisici o comportamentali della persona, quali l'impronta digitale o la faccia. Attraverso sensori di acquisizione sempre più diffusi e accurati, i sistemi biometrici digitalizzano il tratto biometrico dell'utente e ne producono una rappresentazione, chiamata *template*, che sintetizza le caratteristiche univoche e costanti del tratto analizzato rispetto all'individuo che lo possiede.

Il template è appositamente progettato per essere efficace ed efficiente nelle successive comparazioni. In una prima fase di registrazione, detta *enrollment*, il template viene memorizzato su un documento o in un archivio. Durante le successive fasi di riconoscimento, il template acquisito da una persona sottoposta a verifica viene confrontato con i template memorizzati. Il sistema biometrico decide se il riconoscimento è avvenuto o meno utilizzando una misura di similarità o di distanza fra il template acquisito e quelli presenti in archivio.

I tratti biometrici non possono essere smarriti, sono difficili da condividere, poco soggetti a furti e permettono ottimi risultati di accuratezza del riconoscimento. Queste caratteristiche stanno portando a un sempre più vasto utilizzo dei sistemi biometrici in diversi contesti operativi, quali il controllo di accessi

fisici e logici a dati, applicazioni e strumenti (ivi compresi computer e cellulari) e il controllo intelligente degli ambienti.

Le prestazioni di un sistema biometrico possono variare notevolmente in base al tratto biometrico impiegato e al livello di cooperazione richiesto agli utenti. La scelta del tratto biometrico da usare per applicazioni specifiche avviene sulla base di un'accurata analisi dei requisiti operazionali e di sicurezza, tenendo ovviamente in considerazione le leggi sulla protezione dei dati personali.

4.3.1 Stato dell'arte

La tecnologia biometrica, automatizzando il processo di screening dei passaporti tramite chioschi automatici, contribuisce a rendere più agevole il compito delle forze dell'ordine nella fase di identificazione dei passeggeri. In ambito bancario vengono utilizzate modalità biometriche quali impronte digitali, iride, voce, viso, pattern delle vene palmari, comportamento, da sole o in modo combinato, per bloccare conti e reprimere frodi. Applicazioni della biometria sono inoltre presenti in ambito giudiziario e molte importanti innovazioni nella gestione delle identità sono nate in questo ambito. Oggi, la biometria delle forze dell'ordine è veramente multimodale: le impronte digitali, il riconoscimento facciale e vocale ricoprono un ruolo fondamentale per migliorare la sicurezza pubblica e per rintracciare le persone ricercate.

Inoltre, partendo dal presupposto che "l'identificazione fornisce una base per altri diritti e dà voce a chi non ha voce", il *World Bank Group* ha avviato progetti e iniziative per utilizzare la biometria per garantire servizi e assistenza (cure mediche, istruzione, ...) mirati nei paesi in via di sviluppo.

La biometria è stata già oggetto di molti progetti europei nei vari Programmi Quadro che si sono susseguiti negli anni, fino all'attuale H2020. Alcuni esempi sono: il progetto *Tabula Rasa*[27], che ha coinvolto ben dodici partner concentrati sulle vulnerabilità dei sistemi biometrici; il progetto BEAT[28], mirante a uniformare i protocolli sperimentali correnti per garantire la ripetibilità scientifica degli esperimenti, sui quali l'avanzamento scientifico-tecnologico fa affidamento in tutte le discipline relative alla biometria; il progetto PROTECT[29,30], orientato alla ricerca su possibili biometrie emergenti; l'azione IDENTITY[31] orientata all'interscambio di ricercatori sul tema.

[27] https://ec.europa.eu/programmes/horizon2020/en/news/eu-funded-project-take-biometric-security-systems-next-level

[28] https://www.beat-eu.org/

[29] http://cordis.europa.eu/project/rcn/202685_en.html

[30] http://projectprotect.eu/(BES)

[31] http://www2.warwick.ac.uk/fac/sci/dcs/research/df/projects/identity/.

4.3.2 Sfide

Le principali sfide riguardano, in particolare, i seguenti aspetti:

- *Biometria comportamentale* — Le cosiddette *biometrie comportamentali* sono sempre esistite, ma sono state scarsamente considerate per le loro limitate attitudini identificative e gli alti costi implementativi. Le innovazioni hardware degli ultimi anni hanno reso possibile la costruzione di sensori molto sofisticati a basso costo e la loro installazione nei dispositivi più disparati.
- *Miglioramento dell'accettabilità e dell'usabilità* — Le tecnologie biometriche vengono spesso percepite come eccessivamente invasive, difficilmente utilizzabili o pericolose per la privacy, per esempio a causa del rischio di furto dei template.
- *Interoperabilità* — Gli attuali sistemi biometrici utilizzano differenti sensori di acquisizione e algoritmi di riconoscimento. La realizzazione e il mantenimento di banche biometriche e di sistemi informativi complessi richiede quindi l'adozione di tecniche per la gestione dell'interoperabilità. Questo tema diventa di particolare rilevanza con lo sviluppo di nuove forme di autenticazione.
- *Protezione dei dati personali* — Occorre garantire la protezione dei template, anche ricorrendo alle biometrie cancellabili e all'uso congiunto di crittografia e biometria.
- *Classificatori omomorfi* — Occorre realizzare classificatori omomorfi, in grado quindi di funzionare direttamente su template cifrati, mutuando le necessarie tecnologie dalla crittografia omomorfica.

4.3.3 Obiettivi

Tra i principali obiettivi del progetto vanno annoverati:

- Costruire e mettere a disposizione dataset adeguati per tutte le biometrie ritenute "mature" per renderle adattabili su larga scala e utilizzabili come riferimenti comuni per validazioni di sicurezza.
- Mettere a punto metriche che permettano di validare i sistemi biometrici rispetto a criteri fondamentali quali l'usabilità, la resistenza ad attacchi sofisticati miranti a replicare le biometrie e i comportamenti di un individuo, l'interoperabilità, i costi e le prestazioni.
- Avviare sperimentazioni sulla definizione di tratti comportamentali da impiegare nelle biometrie comportamentali che siano allo stesso tempo biometrici e sicuri, in quanto non replicabili.

- Sviluppare tecnologie "usabili" al fine di incrementare la diffusione dei sistemi biometrici in ambito commerciale e privato, con particolare riferimento a tecniche di acquisizione senza contatto e a maggiore distanza.
- Sviluppare tecniche per permettere l'accesso a diverse banche dati e di sfruttare altri metodi di comparazione, gestendo in modo flessibile metodi di fusione multimodale in funzione delle biometrie disponibili.

4.4 Blockchain e Distributed Ledger

Bitcoin e altre criptovalute occupano le pagine dei giornali quotidianamente. Alla base di tali sistemi vi è la tecnologia del cosiddetto *registro distribuito* (*Distributed Ledger Technology* – DLT), chiamata anche *blockchain*, della quale le criptovalute rappresentano solo una delle possibili applicazioni.

Obiettivo di questo capitolo è analizzare le opportunità, i rischi e le sfide dell'adozione di un'infrastruttura nazionale che offra al sistema Paese la tecnologia per un uso consapevole e controllato delle DLT.

DLT – Distributed Ledger Technology – Tecnologia basata su un database distribuito chiamato *blockchain*, che contiene blocchi di transazioni. Grazie a crittografia a chiave pubblica e algoritmi di consenso, è in grado di garantire la sua irreversibilità e integrità (nel tempo).
L'approccio è naturalmente decentralizzato e non necessita di intermediari che convalidino o autentichino le transazioni. Ogni nodo nella rete mantiene la propria copia di tutte le transazioni e i nodi lavorano per verificare la validità di una nuova transazione attraverso un processo chiamato *consenso*. Ognuna di queste transazioni viene inviata a tutti i nodi della rete per essere verificata e raggruppata in blocchi di transazioni marcati con un timestamp.
Vi sono due categorie principali di piattaforme DLT: *unpermissioned* (aperta) e *permissioned* (regolata). La prima è mantenuta da nodi pubblici ed è accessibile a chiunque (Bitcoin ne e il più noto esempio). La seconda (per esempio, la piattaforma Corda), coinvolge solo nodi autorizzati e quindi facilita transazioni più veloci, più sicure e più convenienti.

4.4.1 Stato dell'arte

Il report *The future of financial infrastructure* pubblicato dal World Economic Forum nel 2016[32] ha previsto che l'80% delle banche inizierà progetti basati sul-

[32] `www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf`

le DLT entro il 2017. Più di 24 paesi e più di 90 banche centrali stanno investendo sulla DLT o discutendo sulla sua adozione. Solo negli ultimi 3 anni sono stati depositati più di 2.500 brevetti sulla DLT e investiti oltre 1,4 miliardi di dollari. Vari Stati e organizzazioni nazionali e internazionali stanno analizzando l'opportunità di supportare lo sviluppo di DLT come base di applicazioni in ambito pubblico e privato. Tra questi spiccano l'Autorità Monetaria di Singapore (MAS)[33], l'Hong Kong Monetary Authority (HKMA)[34], la Bank of England (UK)[35] [36]. Il Parlamento Europeo [37] e la Banca Centrale Europea [38] hanno riconosciuto le numerose sfide regolamentari e le opportunità presentate dalla DLT.

In Italia, secondo Assinform (l'associazione di Confindustria che riunisce le aziende dell'ICT), nel 2017 è prevista una crescita di +2.3% nell'intero mercato ICT, spinta dalle componenti più legate a idee innovative, DLT in primis[39]. Stime conservative prevedono inoltre che gli investimenti in progetti basati su DLT supereranno i due miliardi di euro nel 2017.

Oltre a questo, è palese l'interesse in varie comunità scientifiche e tecniche (W3C - Blockchain Community Group, OASIS - ISITC Europe, ITU-T, comitato tecnico ISO/TC 307)[40].

4.4.2 Sfide

Una DLT nazionale (aperta o regolata) apre sfide di ricerca, di innovazione e di progresso in vari campi: dal controllo in campo monetario, al *digital rights management* e alla protezione dei brevetti; da innovazioni possibili nell'e-voting, agli smart contract, al supporto per un tracciamento delle Supply chain, oltre che a introdurre altri scenari volti alla realizzazione di servizi pubblici innovativi. Tra le sfide più rilevanti vanno ricordate le seguenti:

[33] http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf

[34] http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf

[35] http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx

[36] http://www.bankofengland.co.uk/research/Documents/onebank/cbdc.pdf

[37] http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

[38] https://www.ecb.europa.eu/paym/initiatives/shared/docs/dlt_task_force_mandate.pdf

[39] https://www.confindustria.ud.it/upload/pagine/Industria%2040/la%20posizione%20del%20sistema%20confindustria/Confindustria%20Digitale%20-%20Assinform%20-%20%20Lug%202016.pdf

[40] https://www.iso.org/committee/6266604.html?view=participation

- *Estensione del DLT al di là delle applicazioni finanziarie* — L'uso originario e a oggi predominante della blockchain è legato alle crittomonete. Poiché le applicazioni valutarie dominano le discussioni sulle DLT e rappresentano le applicazioni più mature e ben note, esse influenzano lo sviluppo delle tecnologie alla base di applicazioni innovative. Tuttavia, la disponibilità di DLT con bassi costi di gestione rispetto al valore delle transazioni e la disponibilità di un registro capace di immagazinare informazioni in modo permanente e sicuro, amplierebbe le possibilità d'utilizzo di questa tecnologia oltre i confini delle applicazioni finanziarie. La sfida in questo ambito non è creare una moneta digitale nazionale a corso legale, ma la gestione e il controllo di una DLT nazionale (potenzialmente permissioned) per supportare applicazioni non finanziarie e forme di "quasi moneta" (es. monete locali, titoli di credito) a basso costo e alta accessibilità e usabilità. Perché questo sia possibile è importante che si individuino forme di certificazione che richiedano minori capacità computazionali e di memorizzazione e permettano quindi di limitare il consumo energetico, che nel caso di bitcoin sta diventando troppo oneroso.

- *Analisi e protezione da transazioni illecite* — Oltre a fornire nuove possibilità e sfide, le DLT introducono nuovi problemi di sicurezza. Le transazioni sono di per sé semi-anonime (specie nelle DLT unpermissioned) e questo ha introdotto mercati illeciti di ampia portata, che vivono nel deep/dark web (si veda il box a pag. 20). Inoltre, la mancanza di autenticazione (sia forte sia debole) ha introdotto frodi finanziarie di grandi dimensioni (oltre alla chiusura dei siti di exchange, false lotterie, false vendite on line, etc.)

  La sfida in questo campo include quindi attività di analisi del traffico (che a tutti gli effetti si può classificare come Big Data) e di riconoscimento della parte nascosta e illecita, sia con strumenti di forensic e machine learning, sia di studio tecnico economico del mercato finanziario che si appoggia alle DLT unpermissioned.

- *Modellazione, analisi e verifica degli Smart contract* — Gli *Smart contract* sono programmi eseguiti in modo automatico dalla rete di nodi che controlla una criptovaluta. Il meccanismo di consenso usato per garantire la consistenza della blockchain garantisce anche che l'esecuzione di questi programmi sia corretta (proprietà cruciale dato che tipicamente gli smart contract servono per trasferire valuta). Una delle principali sfide di ricerca sugli smart contract riguarda la loro modellazione, analisi e verifica. Questo tipo di ricerca è particolarmente innovativa e urgente: l'inadeguatezza degli strumenti (sia pratici sia teorici) attualmente disponibili mina, infatti, la sicurezza dell'intero ecosistema degli smart con-

tract, come testimoniato dai molti attacchi[41,42] portati a termine contro Ethereum, la più diffusa piattaforma che li supporta.

- *Aspetti normativi e di processo* — Un altro aspetto è la vigilanza sulla corretta applicazione delle regole. La magistratura e le forze dell'ordine devono poter agire in caso di comportamento anomalo della DLT a causa di errori tecnici o di uso improprio per errore umano o dolo. Vi sono poi altre sfide relative all'integrazione con gli altri sistemi dell'amministrazione, alla standardizzazione, al progetto delle procedure con cui privati e imprese possono accedere alla DLT, e alla realizzazione e governance dell'infrastruttura fisica per la DLT che dovrebbe essere considerata una infrastruttura critica del Paese.

- *Avvento dei computer quantistici* — Un'ultima sfida riguarda lo studio accurato dell'impatto che i computer quantistici avranno sulla DLT. Questa si basano infatti su crittografia classica e l'avvento dei computer quantistici potrebbe, se non corrompere, almeno violare la confidenzialitè delle informazione contenute nel ledger.

4.4.3 Obiettivi

Le attività legate allo sviluppo di una DLT nazionale perseguono cinque obiettivi, diversi sia come ambito sia come ricadute.

- *DLT come infrastruttura per erogare servizi pubblici* — La realizzazione di una DLT permissioned per il sistema Paese con supporto per smart contract, dove poter migrare tutti quei servizi pubblici che necessitano di un controllo normativo e di elevate garanzie in termini di integrità di protezione di dati/funzioni, come ad esempio tutte le applicazioni in ambito amministrativo che richiedono registrazione di tipo legale di documenti, quali registri di atti notarili, registri di imprese, catasto e protocollo. Le ricadute previste includono il miglioramento di tali servizi in termini di affidabilità, sicurezza, trasparenza e accessibilità, nonché una riduzione dei costi rispetto ai metodi tradizionali di memorizzazione e di elaborazione delle informazioni.

- *Voto Elettronico* — Sperimentazione dell'organizzazione di elezioni interne tramite blockchain, purché nel rispetto della normativa GDPR (sez. 6.1.1). La legislazione europea non specifica precise modalità per le elezioni politiche negli Stati membri, ma si registra un interesse all'uso del voto elettronico nel rispetto dei principi costituzionali della legge

[41] `http://blockchain.unica.it/projects/ethereum-survey/attacks.html`
[42] `https://www.coindesk.com/understanding-dao-hack-journalists/`

elettorale (universale, eguale, libero, segreto e diritto di voto diretto). L'obiettivo è sperimentare sistemi di voto elettronico basati su tecnologie blockchain e smart contract, caratterizzati da costi relativamente bassi e con elevati livelli di trasparenza e sicurezza, al fine di valutarne la possibilità di impiego in ambienti reali.

- *Digital Right Management* — La blockchain può essere utilizzata per registrare vendite, prestiti, donazioni e altri trasferimenti. Tutte le transazioni vengono testimoniate e concordate da tutti gli utenti senza necessità di una terza parte fidata. Inoltre, i manufatti non possono essere trasferiti a meno che non siano legittimamente posseduti.

  Identificare le opere protette da copyright o da brevetto, e risolvere le relative dispute, è un'attività di estrema importanza in ambito legale. Lo sviluppo di blockchain in questo settore può consentire politiche di licenza multi-territoriale e aumentare la certezza del diritto per i creatori e gli acquirenti, fornendo efficaci meccanismi di risoluzione delle controversie, ad esempio per quanto riguarda tariffe, condizioni di licenza, concessione/revoca dei diritti di gestione. Gli acquirenti potrebbero quindi, ad esempio, verificare di acquistare copie legittime di brani musicali o di video.

- *Supply Chain* — Le Supply chain sono alla base degli odierni processi di produzione e distribuzione su scala globale e riguardano lo svolgimento di svariate attività, tra le quali: gestione dei contratti, pagamenti ed emissione fatture, etichettatura e impacchettamento, logistica e trasporto. Al riguardo occorre sviluppare soluzioni che permettano l'impiego di DLT per un tracciamento efficiente, affidabile e trasparente delle interazioni che avvengono in una supply chain, con l'obiettivo di ridurre notevolmente i costi dovuti a prestazioni scadenti ed errori degli attuali processi di gestione, spesso affidati parzialmente a operatori umani. Le soluzioni proposte rappresenteranno inoltre un importante deterrente per attività illecite, essendo, a quel punto, relativamente semplice usare le transazioni riportate nel ledger per verifiche anti-frode e anti-contraffazione. Di conseguenza, l'intera supply chain diventerà più efficiente e sicura, con importanti ricadute sui costi di gestione, sulle garanzie di autenticità dei prodotti finali e sulla possibilità di ricostruire in maniera affidabile l'intera storia di qualsiasi prodotto, dalla sua origine fino alla sua distribuzione al dettaglio.

- *Analisi di criptovalute per controllo di attività illegali* — Il monitoraggio e l'analisi delle transazioni nelle DLT unpermissioned esistenti può consentire di individuare frodi e comportamenti illeciti. In particolare, l'obiettivo è fornire all'autorità governativa degli strumenti in grado di rilevare attività illegali come il riciclaggio di denaro, l'evasione fiscale, i

traffici illeciti (per esempio, droga, armi, esseri umani) e i pagamenti per ransomware. Inoltre, occorre controllare il livello di affidabilità dei *nodi miner*, in modo da stimare l'eventualità di situazioni pericolose per l'integrità della DLT stessa.

4.5 Tecnologie quantistiche

Lo sviluppo, negli ultimi due decenni, delle *Quantum Technologies* (Tecnologie Quantistiche) ha posto le premesse per una nuova rivoluzione scientifica e industriale. In particolare, l'applicazione delle tecnologie quantistiche rappresenterà un *game-changer* in settori strategici quali le comunicazioni sicure e i nuovi paradigmi di calcolo (*quantum computing*).

Sviluppi fondamentali per creare nuovi sistemi di comunicazione intrinsecamente sicura sono in corso utilizzando la crittografia quantistica, e in particolare la distribuzione quantistica di chiavi crittografiche (*Quantum Key Distribution*, QKD), che, utilizzando le proprietà della luce a livello quantistico, permette di rivelare in tempo reale la presenza di attacchi e violazioni del canale di comunicazione, garantendo quindi la sicurezza della trasmissione. La QKD consiste nella generazione di chiavi crittografiche, condivise unicamente tra il trasmettitore e il ricevitore e sicure (ovvero ignote a terze parti), mediante la trasmissione di singoli fotoni attraverso canali di comunicazione convenzionali e non protetti (ad esempio fibre ottiche o in "free-space"). Le chiavi crittografiche, la cui sicurezza è garantita dalle leggi della fisica, potranno poi essere utilizzate per cifrare messaggi tra due utenti, o per altri protocolli crittografici, si vedano [38, 62] e il White Paper dell'ETSI[43].

Le tecnologie quantistiche sono una tecnologia strategica per il Paese ed è quindi fondamentale che l'Italia potenzi le proprie capacità scientifiche e tecnologiche in questo settore al fine di limitare, se non eliminare, la propria dipendenza da paesi e aziende straniere in un campo così strategico. Nel breve-medio termine è poco probabile, a causa dei costi elevati, che la QKD sarà utilizzata dai privati cittadini, mentre utilizzatori attesi sono: il governo, la diplomazia, la sicurezza, la difesa, la sanità, gli istituti finanziari, le banche e le imprese multinazionali. Molti di questi potenziali utenti agiscono a livello globale e, quindi, il loro interesse per questa tecnologia crescerà proporzionalmente allo sviluppo della QKD su scala globale.

Al riguardo occorre sviluppare e testare sul campo le nuove tecnologie, intrinsecamente sicure, per la protezione delle comunicazioni, basate sui principi

[43] "Quantum Safe Cryptography and Security: an introduction, benefits, enablers and challenges", ISBN 979-10-92620-03-0 – `https://docbox.etsi.org/workshop/2014/201410_crypto/quantum_safe_whitepaper_1_0_0.pdf`, 2014.

della meccanica quantistica e di raccordarle con le più avanzate tecniche classiche di sicurezza e protezione dei dati. Il progetto è molto ambizioso e non privo di rischi, ma offre la possibilità di svolgere una ricerca che potrà avere un rilevante impatto, sia tecnologico sia economico, nel prossimo futuro. L'obiettivo è quello di realizzare uno sforzo che valorizzi le specifiche competenze e i risultati di frontiera italiani, promuovendo il passaggio *dalla scienza quantistica all'ingegneria quantistica* con lo sviluppo della tecnologia quantistica necessaria a supporto del Paese.

4.5.1 Stato dell'arte

Reti QKD in fibra ottica dimostrative sono state realizzate in varie aree metropolitane, nei diversi continenti: a Vienna[44], a Tokyo[45], e in Cina. Di particolare rilievo è l'attuale progetto cinese[46] per la realizzazione di un collegamento QKD di 2.000 km, da Shangai a Pechino, coadiuvato da una trasmissione QKD terra-satellite per raggiungere zone estremamente distanti. I collegamenti QKD su fibra ottica hanno già trovato applicazione durante le elezioni Svizzere[47], per la trasmissione sicura delle informazioni sui votanti, durante la Coppa del Mondo di calcio del 2010[48] e in Australia[49] per comunicazioni governative. L'applicabilità di sistemi QKD a reti in fibra ottica già esistenti è stata dimostrata in [24], e recentemente sono stati anche realizzati collegamenti QKD *point-to-multipoint*, il tutto sempre su fibra ottica. Oggi sono disponibili prodotti commerciali o prototipi industriali per la realizzazione di sistemi QKD in fibra ottica *point-to-point*, prodotti sia da piccole e medie imprese sia da grandi aziende quali, ad esempio, ID Quantique SA (Svizzera), QuantumTech (Cina), Toshiba Research Europe (UK) e QuintessenceLabs (Australia).

Molti paesi europei hanno avviato ambiziosi programmi di ricerca per trasformare i prototipi di laboratorio in prodotti commerciali. Nel Regno Unito[50] il governo ha investito 270 milioni di sterline per un programma di cinque anni, con l'obiettivo di arrivare a un miliardo di sterline su lungo periodo, per l'ulteriore sviluppo di tecnologie quantistiche e il loro trasferimento all'industria. Programmi sono stati lanciati anche nei Paesi Bassi[51] (135 milioni di euro per

[44] http://www.secoqc.net/html/technology/network.html
[45] http://www.uqcc.org/QKDnetwork/index.html
[46] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7607012
[47] https://www.newscientist.com/article/dn12786
[48] https://phys.org/news/2010-06-world-cup-physics-thwart-hackers.html
[49] https://www.computerworld.com.au/article/278658/
[50] http://uknqt.epsrc.ac.uk/
[51] https://qutech.nl/investmentquantumtechnology/

un programma decennale), in Germania[52] e fuori dall'Europa, prima di tutto, in Cina e negli Stati Uniti.

In Italia, la ricerca in questo contesto ha una posizione di rilievo internazionalmente riconosciuta. In particolare, si segnalano la collaborazione fra INRIM e CNR per la realizzazione di una dorsale di comunicazione quantistica lungo il Paese (progetto Q-SecGroundSpace, in corso di realizzazione) e la collaborazione fra l'Università di Padova e ASI che ha portato alla prima comunicazione quantistica satellitare [76, 71].

Sotto l'impulso dell'iniziativa Europea *Quantum Flagship*, è in corso di sviluppo un piano nazionale volto a favorire il passaggio dalla scienza all'ingegneria quantistica.

4.5.2 Sfide

Le sfide riguardano la progettazione, la realizzazione e la sperimentazione di un'infrastruttura di comunicazione che sfrutti la QKD su scala globale per supportare servizi critici, quali le transazioni finanziarie, la telemedicina, i sistemi di controllo industriale e i sistemi per il controllo energetico (*smart grid*).

I collegamenti QKD *point-to-point* in fibra, anche con il previsto miglioramento dei dispositivi a singolo fotone, saranno comunque limitati a distanze massime di collegamento di alcune centinaia di chilometri. Per trasmissione su scala più lunga, sarà necessaria la realizzazione di ripetitori quantistici[53] (*quantum repeater*), strumenti al momento allo stadio di prototipi da laboratorio. A oggi, lo scenario più immediato per una rete QKD su scala globale prevede lo scambio di chiavi crittografiche su distanze relativamente piccole (da qualche centinaio a qualche migliaio di chilometri) tramite fibra ottica, sfruttando dei "nodi sicuri" (*trusted node*) per passare da un collegamento *point-to-point* a un altro, accompagnato da scambi di chiavi su distanze intercontinentali attraverso collegamenti QKD in "free-space" via satellite.

Le sfide riguardano, quindi, lo sviluppo di piattaforme QKD in fibra, di piattaforme spaziali e della loro connessione per garantire operatività intermodale sicura su scala globale. Inoltre, come notato nel White Paper dell'ETSI, è fondamentale un'interazione tra le tecniche quantistiche e quelle classiche della cybersecurity per poter garantire la continuità dei livelli di protezione.

Per quanto riguarda i collegamenti QKD *point-to-point* in fibra, significativi sviluppi tecnologici sono già avvenuti ed esistono le prime soluzioni commerciali ma, per poter pensare a un utilizzo diffuso di questa tecnica di protezione delle comunicazioni, è necessario validare l'affidabilità della tecnologia "sul campo" e mettere a punto una strumentazione precisa e affidabile in

[52] http://www.qutega.de/en/home/

[53] http://quantumrepeaters.eu/quantumrepeaters.eu/index/

grado di poter essere integrata e utilizzata da operatori delle compagnie di telecomunicazioni e non solamente nei laboratori di ricerca.

Gli attuali sistemi QKD commerciali sfruttano dispositivi a singolo fotone (sorgenti e rivelatori) migliorabili sia dal punto di vista delle prestazioni sia da quello dei protocolli quantistici utilizzati. Ad esempio, nuove tecnologie attualmente in sviluppo nei laboratori sono i rivelatori a singolo fotone, basati sulle tecnologie dei semiconduttori o dei superconduttori, con elevata risoluzione temporale e basso rumore di fondo, che appaiono fondamentali per assicurare un alto *bit rate* (efficace) su lunghe distanze.

I sistemi di QKD via satellite sono, attualmente, in fase di studio e argomento di ricerca avanzata ed è necessario un importante sforzo scientifico e tecnologico per renderli commercialmente utilizzabili. Occorre primariamente verificare la fattibilità sperimentale, sviluppare le tecnologie e le infrastrutture di misura necessarie per i collegamenti QKD satellite-terra e investigare il problema dei collegamenti QKD satellite-satellite. Allo stesso tempo, andrà sviluppato un *intermodal trusted node* per mettere in comunicazione il collegamento QKD *free-space* al sistema QKD in fibra ottica e per dimostrare l'interoperabilità dei due tipi di collegamento per QKD.

In parallelo, al fine di rispondere a una esigenza primaria della nascente industria delle comunicazioni quantistiche, occorre anche sviluppare criteri di standardizzazione e tecniche di controllo per garantire la riferibilità delle misure a singolo fotone e la sicurezza dei relativi protocolli.

Infine, sia per la comunicazione quantistica terrestre sia per i collegamenti da e verso sistemi satellitari, sarà fondamentale individuare il miglior tipo di codifica dell'informazione che permetta la massima efficienza e sicurezza. Negli ultimi anni, agli schemi standard basati su singoli fotoni e a una codifica binaria dell'informazione quantistica (generalmente nella polarizzazione del fotone), si sono affiancate nuove proposte e realizzazioni, basate su impulsi di luce classici e variabili continue [45] e sulla codifica su gradi di libertà spettrali e temporali [58]. Tali schemi alternativi presentano grandi vantaggi legati all'alta efficienza e selettività della rivelazione (tramite schemi tipo omodina). Essi offrono, inoltre, la possibilità di manipolare l'informazione in modo deterministico in protocolli avanzati quali il teletrasporto, l'*entanglement swapping* e i ripetitori quantistici [33], di cui il progetto studierà possibili schemi di implementazione. È quindi essenziale affiancare a quelli esistenti nuove sorgenti e rivelatori che permettano di sfruttare la miglior codifica dell'informazione nelle varie sezioni di un sistema di comunicazione quantistica globale e sviluppare schemi efficienti per interfacciare tali sezioni.

4.5.3 Obiettivi

Il progetto prevede il raggiungimento dei seguenti obiettivi e sotto-obiettivi:

- Sviluppo di una piattaforma sperimentale italiana di QKD su scala globale basata su sistemi QKD in fibra ottica e in “free-space”:
  - Progettazione, messa in opera e sperimentazione di un sistema QKD in fibra ottica;
  - Realizzazione del prototipo di trasmettitore e ricevitore per QKD su satellite;
  - Studio di codifiche a variabili discrete e continue in configurazione adattiva, sulla base delle caratteristiche del canale;
  - Integrazione dei componenti in piattaforme di circuiti fotonici;
  - Progettazione, sviluppo e sperimentazione di un *trusted node* per lo scambio di chiavi crittografiche sicure tra collegamenti QKD in fibra ottica e quelli in “free-space”;
  - Realizzazione dell’infrastruttura metrologica per la caratterizzazione dei dispositivi a singolo fotone dei sistemi QKD.
- Integrazione e interazione tra le tecniche di sicurezza classica e quantistica.
- Sviluppo di nuovi schemi e tecnologie per QKD di prossima generazione:
  - Realizzazione e test di sorgenti e rivelatori innovativi a singolo fotone;
  - Studio e sviluppo di schemi di codifica dell’informazione quantistica che permettano la massima efficienza e sicurezza;
  - Progettazione e implementazione di protocolli di comunicazione quantistica avanzati quali il teletrasporto quantistico, i *quantum repeaters* e l’*entanglement swapping*.

CAPITOLO

5 Tecnologie da proteggere

In questo capitolo vengono analizzate le *tecnologie da proteggere,* quali le comunicazioni wireless, il Cloud, l'IoT, i sistemi di controllo industriali (ICS), i robot, che stanno avendo un ruolo fondamentale nel processo di trasformazione digitale nelle PA e nel settore industriale, diventando sempre più pervasive.

La loro protezione e l'incremento della loro resilienza ad attacchi cibernetici è quindi prioritaria e va perseguita agendo in due direzioni: da un lato inserendo adeguate misure di sicurezza all'interno dei sistemi legacy che impiegano tecnologie obsolete e, dall'altro, lavorando per arrivare al concetto di *Security by design* in quelle di nuova generazione. Progettare e sviluppare queste tecnologie con il concetto di sicurezza cibernetica al centro dello sviluppo può trasformarsi in un vantaggio competitivo per le aziende del Paese.

Il capitolo si occupa, in chiusura, del problema della protezione degli algoritmi, veri motori di tutte le tecnologie digitali: l'avvelenamento delle *ground truth* degli algoritmi di machine learning o l'alterazione del codice di algoritmi per la gestione di dati replicati su server diversi sono esempi di minacce che devono essere gestiti in un cyberspace resiliente.

5.1 Comunicazioni wireless e sistemi 5G

La natura wireless e mobile delle comunicazioni nei sistemi cellulari ha implicato storicamente la necessità di proteggere i dati in transito. Tale attività è stata debitamente affrontata nel corso delle precedenti generazioni di sistemi cellulari, con soluzioni che, seppur gradualmente e tramite varie evoluzioni, hanno oggi raggiunto un livello di protezione considerato soddisfacente (non è un caso che nell'ultima decina di anni non vi siano state significative evoluzioni in

questo settore).
Però, la rete 5G include non solo la rete cellulare ma anche la rete fissa, fornendo servizi organizzati da estremo a estremo e con parametri prestazionali migliori anche di diversi ordini di grandezza rispetto alle soluzioni attuali; ha un più vasto ecosistema, che include più attori e più complesse relazioni e opportunità commerciali; pone nuovi requisiti (e.g., relativi al mondo IoT e ad applicazioni ad alta affidabilità e bassa latenza); ha caratteristiche di maggiore eterogeneità e dinamicità; è caratterizzata da soluzioni tecniche radicalmente nuove, tra cui la "softwarizzazione" delle funzioni di rete e la suddivisione della rete in "slice". Softwarizzazione significa realizzare in software funzioni di rete, anche complesse e critiche, oggi realizzate almeno in parte in hardware, anche virtualizzando odierni dispositivi fisici. Una rete realizzata in software può poi essere suddivisa in fette (slice), ognuna delle quali fornisce a un sottoinsieme degli utenti una rete virtuale autonoma da estremo a estremo, capace di soddisfare specifiche esigenze di uno specifico scenario/caso d'uso, in un quadro complessivo che vede la convivenza all'interno della rete di diverse organizzazioni (multi-tenancy).
L'insieme di queste caratteristiche muta profondamente le problematiche di sicurezza della rete.

5.1.1 Stato dell'arte

I sistemi di prima generazione non specificavano alcuna soluzione per la protezione delle comunicazioni, ma già il GSM (seconda generazione) ha iniziato a introdurre esplicitamente soluzioni per l'autenticazione degli utenti e la crittografia a livello di interfaccia radio. Le soluzioni di sicurezza GSM sono però risultate estremamente preliminari e insufficienti per numerosi motivi, a partire dalla totale inadeguatezza delle tecniche crittografiche adottate. L'algoritmo COMP128, peraltro inizialmente non reso noto alla comunità scientifica, seguendo un modello di *security by obscurity* risultato nefasto, è stato infatti "rotto" nel 1998 in brevissimo tempo dopo la sua (presumibilmente involontaria) divulgazione. In aggiunta, il GSM non aveva previsto autenticazione mutua, ovvero non limitata alla sola autenticazione del terminale utente nei confronti della rete, ma anche atta a permettere all'utente di verificare l'autenticità della stazione radio base e ciò ha portato ad attacchi basati su *rogue base station*, ovvero stazioni radio base fittizie, controllate da attaccanti in grado pertanto di intercettare le comunicazioni. Infine, nel GSM non era stata standardizzata alcuna soluzione di sicurezza nella parte di rete core.

La successiva terza generazione, UMTS, è stata probabilmente la generazione in cui sono stati fatti i maggiori passi avanti relativamente alla sicurezza, sia in termini di qualità delle soluzioni adottate, sia in termini di interventi nei molteplici sottosistemi coinvolti. In primo luogo, i sistemi 3G hanno adottato

algoritmi crittografici nella famiglia AES (Advanced Encryption Standard), decisamente più sicuri e ancora oggi stato dell'arte. L'applicazione delle tecniche crittografiche è stata altresì significativamente migliorata, sia mediante esplicita differenziazione delle chiavi (e delle tecniche) di cifratura da quelle di integrità dei dati, sia mediante l'introduzione di funzionalità di privacy e di protezione per gli utenti da attacchi atti a riconoscere e tracciare la posizione (location privacy). I sistemi 3G hanno inoltre ovviato al problema delle rogue base stations, prevedendo una tecnica estremamente efficace di autenticazione mutua. Infine, hanno definito soluzioni di sicurezza anche a livello di core network e relativa segnalazione.

In linea con i progressi fatti nei sistemi 3G, la quarta generazione, 4G, ha apportato svariate migliorie e ha, soprattutto, esplicitamente adottato il tema della *security by design*, ovvero ha considerato gli aspetti di sicurezza sin dall'inizio della fase di specifica architetturale, organizzando l'architettura complessiva in cinque espliciti domini (e proponendo, ove necessario, algoritmi specifici per fornire i relativi servizi di protezione):

- *Network access security* — Protezione a livello di interfaccia radio;
- *Network domain security* — Protezione a livello di scambio dell'informazione e della segnalazione tra i componenti di rete;
- *User domain security* — Protezione a livello di terminale mobile e interfacciamento tra USIM e dispositivo;
- *Application domain security* — Protezione a livello di servizi applicativi;
- *Visibility and configuration of security*: — Modalità per permettere di verificare se (e quali) aspetti di sicurezza siano attivi.

5.1.2 Sfide

A fronte dei numerosi passi avanti fatti nelle scorse generazioni, relativamente alla sicurezza delle reti cellulari, e sopra brevemente riassunti, è lecito chiedersi se il problema della sicurezza debba avere un ruolo importante anche nelle reti 5G, oppure se il grosso del lavoro sia già stato fatto. La risposta è che, nonostante i significativi miglioramenti apportati alle reti cellulari nel corso delle precedenti generazioni, i nuovi requisiti emergenti nei sistemi 5G e, soprattutto, il radicale cambio di prospettiva che caratterizza la rete 5G (che include non solo la rete cellulare ma anche la rete fissa), porta alla necessità di affrontare nuovi problemi. Se, infatti, i precedenti sistemi 2/3/4G erano ben definiti a priori e i loro requisiti ben delimitati, omogenei e relativamente stabili, così come le relative soluzioni di sicurezza e protezione dei dati, gli emergenti sistemi 5G sono fortemente incentrati sull'integrazione tra tecnologie eterogenee, sul partizionamento (slicing) e virtualizzazione delle infrastrutture di rete, e sul supporto

di servizi estremamente diversificati e non più esclusivamente dedicati a utenti umani.

Riteniamo quindi che l'architettura di sicurezza dei sistemi 5G debba essere estesa al fine di comprendere (almeno) i seguenti aspetti:

- *IoT e Terminali eterogenei* — Una tra le più significative differenze tra i sistemi cellulari tradizionali e la nuova generazione 5G consiste nella disponibilità di servizi non più necessariamente riservati a terminali gestiti da esseri umani, ma estesi anche a *Machine-Type-Communication* (MTC). Ciò porterà alla diffusione di terminali con caratteristiche (in termini di costo, consumo energetico e complessità implementativa) estremamente disparate, per cui un modello di sicurezza "unico per tutto e tutti" (one-size-fits-all), che aveva caratterizzato le soluzioni di sicurezza nelle generazioni precedenti, potrebbe non essere più adeguato. Per esempio, meccanismi di sicurezza pensati per servizi "mission critical" potrebbero non essere per nulla applicabili in un contesto di dispositivi IoT, in cui i sensori di rete sono dotati di scarsissime risorse computazionali ed energetiche e in cui la trasmissione dei dati è sporadica. I sistemi 5G saranno pertanto non solo chiamati a supportare tecniche crittografiche (per autenticazione o cifratura dei dati) estremamente variabili in termini di robustezza e livello di protezione, ma, soprattutto, sarà necessario pensare a nuovi modelli per la gestione di tali soluzioni eterogenee di sicurezza e a nuovi modelli di trust.

- *Traffico di segnalazione* — Oltre alla necessità di identificare soluzioni di sicurezza differenziate per i servizi offerti e più flessibili rispetto alla soluzione "unica" attualmente offerta nei sistemi 4G, un ulteriore aspetto importante relativo ai servizi di tipo MTC è che il traffico di segnalazione potrebbe risultare addirittura dominante rispetto al traffico dati. Da ciò segue ad esempio la necessità di sviluppare soluzioni in grado di riconoscere (e difendersi da) attacchi volti a saturare le risorse di rete dedicate al traffico di segnalazione; un ben noto collo di bottiglia in caso di servizi MTC consiste nell'accesso al RACH (Random Access Channel) che potrebbe diventare critico, in caso di attivazione simultanea e malevola da parte di una botnet (si veda il box a pag. 48) IoT.

- *Virtualizzazione e softwarizzazione delle funzioni di rete* — Una caratteristica fondamentale della rete 5G è la migrazione verso sistemi virtualizzati, in cui le funzioni di rete non sono più fornite da dispositivi fisici specifici, ma realizzate in software ed eseguite su macchine virtuali o container, in ambienti Cloud. Queste funzioni sono instanziate o spostate dinamicamente dove necessario e anche rilocate verso il bordo della rete, in modo da soddisfare i requisiti di bassa latenza richiesti da applicazioni 5G critiche. Questo nuovo paradigma di virtualizzazione delle funzioni

di rete implica numerose nuove sfide in termini di sicurezza. Da un lato, la separazione fisica di tali funzioni in dispositivi distinti non è più applicabile come misura di sicurezza ed è necessario individuare soluzioni di separazione e isolamento delle funzioni in un contesto virtualizzato. È infatti necessario pensare a soluzioni per la sicurezza dell'ambiente in cui le funzioni di rete verranno eseguite, e che siano indipendenti per ogni "slice" in cui la rete verrà suddivisa. Dall'altro lato, la possibilità di eseguire funzioni di rete su macchine virtuali porta alla necessità di identificare (eventualmente adattandole dal mondo IT) soluzioni di autorizzazione, gestione e migrazione sicura di immagini software, che implementino tali funzioni di rete virtualizzate. Infine, naturalmente, la virtualizzazione non comporta esclusivamente "problemi", ma offre anche nuove opportunità, ad esempio per sviluppare funzioni di rete virtuali dedicate alla sicurezza stessa, ovvero offre la possibilità di ripensare le funzioni di sicurezza in un'ottica di *SEcurity-as-a-Service* (SEaaS) e di automazione delle funzionalità di protezione della rete.

- *Sicurezza "flessibile"* — La rete 5G sarà caratterizzata dalla necessità di disporre di soluzioni per la sicurezza di tipo estremamente flessibile e adattabile agli specifici (differenti) scenari considerati. Ad esempio, servizi con caratteristiche di bassissima latenza richiederanno soluzioni di sicurezza a loro volta a bassissima latenza e quindi (in ultima analisi) flessibilità nella capacità della rete di attivare le soluzioni di sicurezza più adeguate a un determinato scenario. Inoltre, il problema della flessibilità di gestione della sicurezza deve andare di pari passo con strumenti atti a semplificare la gestione della sicurezza stessa nella rete, consentendo un veloce adattamento a nuovi servizi ed esigenze, non solo dell'operatività della rete, ma anche delle soluzioni di sicurezza preposte.

5.1.3 Obiettivi

Relativamente ai contesti sopra illustrati vanno perseguiti i seguenti obiettivi:

- *Realizzazione e gestione sicura di reti virtualizzate e segmentate logicamente* — Tale obiettivo comprende attività specifiche quali:
  - tecniche sicure di virtualizzazione e, soprattutto, di isolamento per le "slice" che compongono la rete e per le funzioni preposte a tale segmentazione, includendo hardening delle funzioni di rete, gestione dell'autenticazione e dell'integrità delle stesse, e così via;
  - necessità di "mettere in sicurezza" le emergenti piattaforme, architetture, soluzioni tecniche e linguaggi (es. P4) per la programmazione software delle funzioni di rete. La ricerca si è finora con-

centrata soprattutto sull'identificazione e sullo sviluppo di soluzioni estremamente flessibili, con purtroppo modesta attenzione alle significative problematiche di sicurezza che questi nuovi approcci comportano;

  - integrazione della sicurezza nei servizi di gestione e orchestrazione delle funzioni di rete, con particolare attenzione alla programmabilità di soluzioni di sicurezza eterogenee per servizi eterogenei e alla verifica dello stato di sicurezza della rete mediante apposite tecniche di visualizzazione;
  - sviluppo di moduli virtualizzati, e relativo controllo, atti a implementare funzionalità di sicurezza della rete, quali firewall, deep packet inspection e analisi dei flussi di traffico, tecniche di mitigation e di isolamento delle minacce basate sul paradigma *Software-defined networking*, sonde di rete programmabili e rilocabili per rilevamento di moderne intrusioni sofisticate, quali Advanced Persistent Threats - APT (si veda il box a pag. 54), che fanno uso di movimenti laterali, etc;

- *Sicurezza di scenari di rete 5G dedicati al supporto di servizi IoT* — Occorre garantire la sicurezza di scenari di rete 5G per supporto di servizi IoT, sviluppando e sperimentando:

  - soluzioni crittografiche di tipo lightweight, pensate per dispositivi sensori e attuatori a bassissimo costo e bassissimo consumo energetico, e loro integrazione nei protocolli di comunicazione IoT emergenti in contesti cellulari (NB-IoT, LTE-M), in contesti Low Power WAN unlicensed (ad esempio LoRaWan) e in contesti short range (RFID, NFC, BLE, etc.);
  - soluzioni di controllo di accesso per scenari IoT a larga scala, basate su una gestione flessibile di attributi di autorizzazione e in grado di operare in contesti multi-tenant;
  - algoritmi di analisi scalabile dei dati generati dai sensori, e atti a identificare anomalie e pattern di traffico riconducibili ad attacchi a larga scala coordinati, ad esempio guidati da botnet tipo Mirai.

- *Protezione dei dati nell'ambito di nuove tecnologie e nuovi contesti di comunicazione e "wireless sensing"* — Occorre focalizzare la ricerca relativa alla sicurezza e alla protezione dei dati relativamente a tecnologie e contesti di comunicazione e *wireless sensing* emergenti, includendo:

  - analisi degli aspetti di sicurezza (inclusa la protezione da Jamming e da attacchi di tipo Denial of Service) in contesti di rete "densa",

e per tecnologie di beamforming, massive MIMO, mmWave, e integrazione o miglioramento delle soluzioni di sicurezza nei protocolli e tecnologie 3GPP e IEEE 802 – in quest'ultimo caso in quanto sicuramente parte integrante delle future reti 5G (e.g., 802.11ax/ay, etc.);

- studio di nuove tecniche di crittografia a livello fisico (includendo anche tecniche quantistiche), in grado di sfruttare le caratteristiche uniche del canale radio, la loro integrazione nell'architettura 5G e la sperimentazione in sistemi reali;
- uso di tecnologie (e forme d'onda) wireless non solo per la comunicazione, ma anche per la sicurezza personale e ambientale, mediante sviluppo e sperimentazione di soluzioni basate su segnali radio per il riconoscimento di pattern e la protezione degli ambienti da intrusioni fisiche.

5.2 Cloud

Il paradigma del Cloud offre indubbiamente grandi benefici economici e grande flessibilità nell'utilizzo delle risorse; tuttavia, il problema della sicurezza in ambienti Cloud rappresenta una delle maggiori preoccupazioni per le aziende e le organizzazioni pubbliche che vogliono spostare i propri servizi, applicazioni e dati sensibili nel Cloud, come evidenziato da numerose analisi quali, ad esempio, i rapporti Gartner[1,2] e IDC[3].

Un sistema informatico è considerato sicuro in base alla correttezza della sua *politica di sicurezza* (*security policy*), ossia l'insieme delle regole atte a garantire un opportuno livello di protezione, e alla sua capacità di applicare tale politica correttamente. Il paradigma Cloud è basato sul principio della delega a una terza parte di ogni tipo di servizio (infrastrutture, mantenimento dei dati e delle applicazioni); dal punto di vista di un esperto di sicurezza, tale delega rende inaccessibile parte del sistema e quindi impossibile non solo verificare la corretta applicazione delle politiche previste, ma, in alcuni casi, anche semplicemente specificare con la dovuta precisione la politica da adottare.

I *Cloud Service Provider* (CSP) possono anche adottare avanzate procedure e meccanismi di sicurezza, ma dal punto di vista dell'utilizzatore (*Cloud Service Customer* – CSC), non è normalmente possibile conoscere il dettaglio delle policy implementate in questi sistemi. In sostanza, le *security policy* dei CSP risultano inaccessibili per gli utenti e soprattutto non monitorabili. In tale contesto,

[1] `https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/`

[2] `https://www.gartner.com/doc/3328818/survey-analysis-cloud-adoption-trends`

[3] `http://www.oracle.com/assets/cloud-inhibitors-3257526.pdf`

anche la garanzia che i vincoli normativi locali siano rispettati può diventare un problema insormontabile.

5.2.1 Stato dell'arte

A livello europeo, ENISA ha giocato un importante ruolo negli ultimi anni, fornendo ai Cloud stakeholder una panoramica dettagliata dei benefici e dei rischi di sicurezza legati alla migrazione delle loro applicazioni e dei dati nel Cloud[4].

A livello comunitario si moltiplicano i riferimenti alla *Cloud security* nei documenti strategici e nei principali programmi quadro di ricerca 2016 e 2020[5]. A tal riguardo, il *Data Protection, Security and Privacy (DPSP) European cluster* ha come obbiettivo massimizzare la ricaduta dei risultati dei progetti di ricerca europei nell'area della *Cloud security*[6]. A ciò si aggiunge l'azione specifica della Commissione Europea espressamente mirata a utilizzare al meglio il potenziale del Cloud Computing: *Pre-commercial Procurement Cloud for Europe*[7].

A livello nazionale, tale azione si traduce nel *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017–2019* realizzato da AgID [8], il cui obiettivo è una razionalizzazione coordinata di tutta la PA e in cui è previsto lo sviluppo di un modello strategico evolutivo del Cloud della PA[9]. In particolare, tale piano prevede: (i) l'individuazione di un insieme di infrastrutture fisiche della PA che diventino *Poli Strategici Nazionali* (PSN); (ii) la definizione di un percorso delle PA verso il Cloud, anche tramite le risorse messe a disposizione dai PSN e dal *Sistema Pubblico di Connettività* (SPC); (iii) la definizione di un processo di qualificazione dei PSN e di altri CSP. A tale piano strategico vanno affiancate opportune strategie per la fornitura dei servizi di sicurezza e professionali[10].

In questa direzione, il progetto SPC *Security Cloud*[11] ha come obiettivo l'erogazione di servizi *SECurity as-a-Service* (SECaaS) secondo il paradigma del

[4] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

[5] http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-179-EN-F1-1.PDF

[6] https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

[7] http://www.agid.gov.it/agenda-digitale/innovazione-del-mercato/gara-pre-commerciale

[8] https://pianotriennale-ict.italia.it/

[9] https://www.agendadigitale.eu/infrastrutture/come-cambia-il-cloud-della-pa-dopo-il-piano-nazionale-e-delle-regioni/

[10] http://www.agid.gov.it/notizie/2017/04/05/workshop-agid-csa-italy-spc-cloud-sicurezza-del-sistema-cloud-computing-nazionale

[11] https://www.ictsecuritymagazine.com/articoli/spc-cloud-le-best-practice-cloud-security-sistema-cloud-computing-italiano/

Cloud Computing, tra cui la gestione delle identità digitali, la firma digitale remota, i servizi atti a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi. Attualmente solo un numero limitato di CSP offre SECaaS[12].

Un altro aspetto fondamentale riguarda come mettere in comunicazione Cloud diverse in maniera sicura per consentire l'integrazione di servizi offerti da soggetti distinti, al fine di realizzare delle *federazioni di Cloud* (*Cloud federation*) in grado di fornire nuove e più ricche funzionalità. Il progetto *SUNFISH*[13] affronta questa tematica, proponendo un'architettura e le relative tecnologie abilitanti per creare Cloud federation che siano *secure by design* e amministrabili in maniera democratica. Uno dei principali casi d'uso dove SUNFISH ha mostrato la sua efficacia riguarda l'integrazione sicura delle Cloud private del Ministero dell'Economia e delle Finanze e del Ministero degli Interni per la gestione affidabile e confidenziale delle buste paga del personale delle Forze Armate.

Infine, a livello internazionale, la *Cloud Security Alliance* (CSA) è un'organizzazione dedicata alla difesa e alla diffusione di *best practice* che possano rafforzare la sicurezza degli ambienti Cloud[14]. Dal 2010, la CSA ha promosso il primo programma di certificazione professionale per l'acquisizione di competenze nell'ambito della sicurezza Cloud.

5.2.2 Sfide

La sfida principale, per la corretta adozione del Cloud, passa per la costruzione di metodologie e tecniche che permettano di definire e verificare il livello di sicurezza di un sistema informatico che utilizzi e integri al suo interno servizi Cloud.

È importante mettere in evidenza come attraverso le informazioni fornite dai CSP (raccolte in repository pubbliche, quali cloud28[15] e CSA STAR[16]) è possibile ottenere dati utili a costruire una policy di sicurezza per Cloud, come mostrato dai risultati dei recenti progetti di ricerca europei dedicati al tema, quali SPECS[17], MUSA[18], SLA-Ready[19] e SLALOM[20].

[12] http://www.crn.com/slide-shows/security/300083542/the-20-coolest-cloud-security-vendors-of-the-2017-cloud-100.ht

[13] http://www.sunfishproject.eu/

[14] https://cloudsecurityalliance.org/

[15] https://www.cloud28plus.com/

[16] https://cloudsecurityalliance.org/star/

[17] http://www.specs-project.eu

[18] http://www.musa-project.eu

[19] http://www.sla-ready.eu/

[20] http://slalom-project.eu/

È essenziale che i CSC siano messi nelle condizioni di poter scegliere tra i servizi offerti dai diversi CSP in modo inequivocabile e con la consapevolezza di dove i dati sensibili siano materialmente memorizzati, al fine di garantire il rispetto delle leggi in materia. A titolo di esempio, occorre permettere a chi gestisce dati sensibili o partecipa ad appalti pubblici, di poter scegliere tra diverse offerte, attraverso una valutazione chiara e quantitativa dei servizi e delle garanzie di sicurezza e protezione dei dati personali offerte. Poter confrontare le procedure e le policy di sicurezza implementate dai CSP, o ancora di più, i servizi offerti da una terza parte che utilizza a sua volta servizi Cloud, diventa quindi un fattore abilitante chiave per l'adozione del paradigma Cloud. Pertanto, lo sviluppo di *metriche di sicurezza* che permettano di valutare quantitativamente un'offerta di servizi Cloud, eventualmente arricchita da procedure di *security benchmarking*, che permettano di valutare lo stato di sicurezza complessiva di un servizio Cloud da parte dei CSC, rappresenta una delle sfide più sentite dal punto di vista degli utenti.

Allo stesso modo, esiste una domanda crescente da parte del CSP, relativamente alla necessità di stipulare assicurazioni contro gli attacchi informatici. Domanda difficile da soddisfare, a causa di un mercato di *cyber insurance* ancora immaturo a causa delle difficoltà nel valutare sia il *rischio residuo*, ovvero quello che non può essere mitigato con delle opportune misure di sicurezza, sia il danno subito a fronte di un attacco[21].

L'attenzione sulla possibilità di attacchi informatici verso CSP è cresciuta recentemente a seguito della scoperta di due gravi vulnerabilità dei moderni processori messe in luce dagli attacchi *Meltdown* e *Spectre* (analizzati nella sez. 4.1). Questi attacchi consentono a un processo di leggere la memoria privata di un altro processo. Ciò ha un impatto rilevante per la confidenzialità dei dati su Cloud; infatti, all'interno dell'infrastruttura gestita da un CSP, i dati sensibili di un CSC potrebbero essere letti da un altro processo, gestito da un CSC diverso, con conseguente perdita della confidenzialità di tali dati. Data la frequenza della scoperta di nuove vulnerabilità del genere, si rende necessario lavorare su soluzioni che possano garantire confidenzialità anche a seguito della compromissione dell'infrastruttura Cloud. Un esempio di queste soluzioni è stato investigato nell'ambito del progetto SUNFISH[22], dove viene impiegata la *Secure Multi-party Computation* [23, 39] per distribuire i dati sensibili su Cloud diverse all'interno di una Cloud federation, in modo che attaccare una singola Cloud non sia sufficiente per esfiltrare dati.

[21] `https://www.dimt.it/index.php/it/mercatoconcorrenzaregolazione/10466-9la-responsabilita-contrattuale-nella-gestione-dei-dati-nel-cloud-computing`

[22] `http://www.sunfishproject.eu/`

MPC – Secure Multy-Party Computation – Classe di protocolli per gestire lo scambio di messaggi tra n processi ognuno dei quali fornisce dati, sconosciuti agli altri, per calcolare una funzione $F(i_1, i_2 \dots i_n)$. Alcuni dei processi possono essere malevoli e collaborare tra loro per esfiltrare dati inviati dagli altri. Un protocollo MCP ha l'obiettivo di calcolare correttamente F facendo in modo che i processi malevoli non riescano a venire a conoscenza dei dati forniti dai processi corretti. Molti protocolli distribuiti crittografici (*voting*, *on-line auction*, etc.) possono essere considerati casi particolari di MPC.

A livello nazionale, la principale sfida consisterà nello sviluppo di un modello di *community Cloud*, che consenta l'interoperabilità tra servizi sviluppati per la PA a livello nazionale (come SPID, fatturazione elettronica, etc.) e quelli già presenti a livello locale in strutture Cloud regionali, opportunamente affiancati da appositi servizi di sicurezza erogati secondo un modello SECaaS. Una community di questo tipo richiede un'infrastruttura per integrare in maniera sicura servizi offerti da Cloud diverse. Una sfida collegata riguarda quindi lo sviluppo ulteriore di soluzioni per Cloud federation sulla falsariga degli obiettivi perseguiti dal progetto SUNFISH.

Un ulteriore punto da sviluppare è un rapporto strutturato con i soggetti privati al fine di garantire che anche le loro soluzioni (opportunamente testate e certificate) siano integrabili nel Cloud nazionale. Pertanto, è necessario un lavoro di concerto tra le attività di *service brokering* nazionali e regionali, sui diversi fornitori, con un processo strutturato di validazione e integrazione di servizi e soluzioni di sicurezza nell'ambiente del Cloud nazionale.

In definitiva, la sfida che l'adozione del paradigma Cloud pone in termini di sicurezza, soprattutto tenendo conto del contesto italiano, consiste nel fornire ai CSC, pubblici e privati, strumenti che permettano, da un lato, di acquisire la consapevolezza dei rischi che il Cloud introduce e, dall'altro, di avere garanzie, servizi di sicurezza e contromisure commisurate all'effetto prodotto dalle minacce introdotte da tale paradigma.

5.2.3 Obiettivi

In riferimento alle sfide da affrontare e sopra riassunte, nel seguito sono indicati i principali obiettivi da perseguire.

- Progettare e sviluppare strumenti che permettano ai CSC di valutare e confrontare i servizi e le policy di sicurezza implementate dai CSP, rispetto ai propri requisiti di sicurezza e alle normative vigenti sulla protezione e località dei dati, attraverso l'utilizzo di apposite metriche di sicurezza e di *security benchmarking*.

- Definire modelli e strumenti utili alla stesura di polizze assicurative per i CSP, capaci di stimare il *rischio residuo* e valutare il danno subito a fronte di un attacco informatico, tenendo conto del differente impatto che il mancato rispetto di un vincolo normativo o di uno specifico requisito di sicurezza ha nella PA rispetto al privato.
- Definire modelli e strumenti per Cloud federation sicure, che possano consentire di integrare in maniera affidabile servizi offerti da Cloud diverse.
- Sviluppare soluzioni per garantire la confidenzialità dei dati su Cloud anche a fronte della compromissione di parte dell'infrastruttura Cloud stessa.
- Sviluppare *security service* open-source che possano essere, attraverso il riuso, adottati e specializzati da enti pubblici, e soprattutto dalle PMI italiane, permettendo loro di rispettare vincoli normativi, come quelli presenti nel GDPR (si veda al riguardo la sez. 6.1), che possono avere costi esorbitanti se applicati in piccolo all'utilizzo di servizi in Cloud.
- Sulla base di specifici casi d'uso applicabili alla PA, realizzare dei dimostratori delle soluzioni individuate per superare le sfide sopra citate e, in particolare, dimostrare come queste possano migliorare la posizione, in termini di competitività, del Cloud italiano, facilitando in questo modo lo sviluppo di business innovativi.

5.3 Algoritmi

Un algoritmo è un procedimento definito da una serie finita di passi elementari per la risoluzione di un problema. Il concetto di algoritmo è un concetto fondamentale per lo sviluppo di un software: dato un problema che si vuole automatizzare, la programmazione rappresenta essenzialmente la traduzione o codifica di un algoritmo in un programma (che ne rappresenta la logica di elaborazione) attraverso un linguaggio che può essere interpretato ed eseguito da un calcolatore. Se ne può quindi dedurre che gli algoritmi rappresentano la base su cui poggiano l'automazione e le facilitazioni che caratterizzano la nostra vita quotidiana.

Diretta conseguenza del ruolo centrale degli algoritmi è il fatto che sono anch'essi un bene di elevato valore che deve essere protetto da attacchi di tipo cibernetico, alla stessa stregua dell'infrastruttura di calcolo e dei dati. Il problema è ancora più evidente se si considera l'incidenza che gli algoritmi di apprendimento automatico stanno rivestendo nella vita quotidiana.

Contrariamente a quanto si possa pensare, gli algoritmi non sono immuni da minacce. Un algoritmo non è altro che una funzione che riceve un insieme

di valori (dati) in input e ne genera altri in output (chiamato *soluzione*) attraverso l'esecuzione di un numero finito di passi intermedi. Un attaccante può quindi cercare di compromettere un algoritmo alterando i dati di input e/o la sequenza di operazioni da svolgere su tali dati. Nel seguito sono riportati alcuni esempi di scenari applicativi per i quali un attacco a un algoritmo può avere gravi conseguenze.

La maggior parte delle applicazioni web che tutti noi utilizziamo comunemente (e.g., gestione di conti correnti, gestione di utenze domestiche, etc.) è implementata in maniera distribuita e replicata. La replicazione è, infatti, la tecnica principalmente utilizzata per garantire la disponibilità di un servizio a fronte delle variazioni del carico (dovute al mutare delle richieste) e della eventuale presenza di guasti che porterebbero altrimenti a un degrado della qualità del servizio e conseguentemente del livello di soddisfazione degli utenti.

Nel paradigma della replicazione, il servizio viene offerto da molteplici copie dello stesso servizio e il requisito fondamentale è che tale distribuzione sia del tutto trasparente all'utente finale. A tal fine, un cliente interagisce con una replica tramite operazioni di lettura (es. l'accesso al saldo di un conto corrente) e/o operazioni di scrittura che aggiornano lo stato della replica (es. depositi o prelievi da un conto corrente).

Un attaccante, in questo caso, può aver interesse a compromettere la disponibilità del servizio (potrebbe, ad esempio, voler rendere il sevizio non accessibile) o l'integrità delle informazioni gestite (potrebbe, ad esempio, alterare i risultati delle operazioni di lettura e scrittura). Tutto questo può avvenire attraverso la compromissione, da parte dell'attaccante, di una o più istruzioni contenute nel frammento di codice che gestisce le operazioni, facendo deviare il comportamento del servizio rispetto alle specifiche e alle attese. Questo tipo di attacco è facilmente realizzabile una volta che l'attaccante ha preso il controllo di una replica. In letteratura esistono alcune soluzioni per la definizione di algoritmi di replicazione tolleranti alla presenza di attaccanti che prendono il controllo di alcune repliche (i cosiddetti algoritmi tolleranti ad agenti Bizantini o maliziosi [48]).

Un altro contesto applicativo dove gli algoritmi rappresentano un punto debole è quello degli algoritmi basati su *machine learning*, che sono alla base di tantissime applicazioni che noi tutti utilizziamo quotidianamente e in cui spesso riponiamo notevole fiducia. Ad esempio, Facebook utilizza il machine learning per il riconoscimento dei volti nelle immagini; Amazon e Netflix analizzano i gusti dei clienti (ultime cose viste o acquistate) per suggerire prodotti; Google utilizza algoritmi di machine learning nell'ambito delle traduzioni e degli spostamenti, suggerendoci una strada meno trafficata in base alle nostre abitudini e al posto dove siamo soliti andare in un dato giorno della settimana; Apple e Microsoft utilizzano il machine learning per fornirci un assistente vocale che possa aiutarci a utilizzare un telefono o un tablet con il solo uso della nostra vo-

ce, magari quando siamo alla guida. Altre aziende al momento perfezionano, tramite metodi di intelligenza artificiale, la guida automatica. Recentemente, gli algoritmi di machine learning sono anche largamente impiegati in ambito sanitario per lo studio dei dati dei pazienti e dell loro cartelle cliniche, per identificare, ad esempio, le persone più a rischio di contrarre determinate patologie, come il diabete, oppure di andare incontro a problemi cardiaci.

In tutti questi esempi, l'algoritmo impara un determinato comportamento che deve ripetere sulla base dei dati di input che gli vengono forniti. È evidente quindi come la correttezza di tutte queste applicazioni dipenda fortemente dalla correttezza dei dati su cui l'algoritmo viene addestrato. Un attaccante potrebbe quindi mirare a compromettere i dati dai quali l'applicazione impara per indurre un comportamento non corretto; ad esempio una guida impropria nel caso di guida autonoma o una diagnosi volutamente non corretta nel caso di predizione applicata al contesto sanitario.

5.3.1 Sfide

Ground truth – Insieme di dati utilizzati per addestrare gli algoritmi di machine learning, che sono oggi alla base di molteplici applicazioni quali, ad esempio, il riconoscimento e la classificazione di mail come spam o il riconoscimento delle abitudini di un utente per pre-calcolare e suggerire itinerari ottimizzati o acquisti mirati.

Code injection – Tecnica che permette di trarre vantaggio da una vulnerabilità del codice basata sul dare in input ad un programma dati diversi da quelli attesi per indurlo ad eseguire specifico codice fornito ("iniettato") da un attaccante per modificarne il comportamento.

Priviledge escalation – Tecnica di sfruttamento delle vulnerabilità del codice basata sullo sfruttamento di errori di programmazione e/o di configurazione che consentono a un attaccante di guadagnare privilegi di amministratore partendo da un normale account utente. Con i privilegi di accesso di amministratore, un attaccante può prendere il controllo dell'intero sistema, e, ad esempio, alterare i dati memorizzati, modificare le procedure e le regole di accesso a parti del sistema, arrestare o modificare i parametri delle applicazioni in esecuzione.

Tra le principali sfide da risolvere dal punto di vista della protezione degli algoritmi, possiamo sicuramente citare:

- *Avvelenamento delle ground truth* — I dati delle ground truth vengono collezionati sia in maniera automatica (ad esempio memorizzando le informazioni sui percorsi di un utente in modo a lui del tutto trasparente) sia manuale (ad esempio richiedendo all'utente di indicare le mail ritenute spam). In entrambi i casi, tali dati vengono memorizzati e un attaccante può provare a comprometterne l'integrità durante il processo di memorizzazione. In aggiunta, nel caso di raccolta automatica dei dati, questi possono essere alterati dalla compromissione della sensoristica preposta alla rilevazione.

- *Sfruttamento di Vulnerabilità* — Ogni algoritmo deve essere codificato in un linguaggio di programmazione per poter essere interpretato ed eseguito da un sistema di elaborazione. Il processo di codifica di un algoritmo non è immune da errori e spesso porta all'introduzione di vulnerabilità (si veda il box a pag. 10) che può diventare una porta d'accesso per un attaccante. Dal punto di vista della protezione degli algoritmi, due tipi di sfruttamento di vulnerabilità sono particolarmente rilevanti e devono essere tenuti in considerazione: (i) l'iniezione di codice e (ii) la scalata dei privilegi.

- *Virus e Malware* — I malware (si veda il box a pag. 48), inserendosi in codice eseguibile esistente, agiscono modificando un algoritmo già in esecuzione oppure le informazioni utilizzati dall'algoritmo, non modificando quest'ultimo per nascondere le evidenze di compromissione e non insospettire l'attaccato.

5.3.2 Obiettivi

Di seguito riportiamo una serie di possibili progetti che coinvolgono sia una componente di ricerca sia una di innovazione.

- *Nuovi approcci al rilevamento di code injection* — Rilevare la presenza di software non voluto è un compito molto difficile perché le tecniche di intrusione ed i programmi stessi sono in continua evoluzione e, a oggi, non esiste una valida metodologia generale. Nuovi approcci devono quindi essere investigati in modo tale da fondere insieme i risultati provenienti da più contesti come ad esempio quelli dell'anomaly detection, del secure coding o dell'analisi statica o dinamica del codice, in un unico framework che garantisca flessibilità e accuratezza nella rilevazione.

- *Nuovi approcci per rendere gli algoritmi di learning più robusti* — La maggior parte di algoritmi di machine learning utilizzati attualmente come supporto all'automazione non è stato pensato per essere resistente ad attacchi. Diventa quindi necessario pensare a una loro evoluzione che ne

preservi le caratteristiche ma che li renda più sicuri. Questo può essere declinato sia nella definizione di nuove logiche su cui essi si poggiano, sia nella modifica strutturale degli algoritmi stessi.

- *Nuovi approcci al vulnerability assessment* — L'obiettivo di questa linea progettuale è lo sviluppo di nuovi approcci anche attraverso l'integrazione di tecnologie esistenti che tengano conto che le minacce alla sicurezza infomatica possono provenire non solo da intrusioni nel perimetro aziendale ma anche attraverso la manipolazione delle logiche funzionali dei sistemi "esperti" attraverso la compromissione degli algoritmi che rappresentano il *core* delle applicazioni.

5.4 IoT

I dispositivi IoT trovano ormai impiego nelle situazioni più disparate che includono, tra l'altro: dispositivi mobili (smartphone e tablet), casa e applicazioni domotiche, sensori e attuatori in ambito industriale (Industrial IoT – IIoT), trasporti (dall'automotive al ferroviario, dalla cantieristica all'aeronautica e ai droni), infrastrutture critiche e Cyber Physical System (sistemi di monitoraggio e controllo). Le stime più recenti parlano di circa 6 miliardi di dispositivi connessi a Internet nel 2017, con una previsione di crescita a 21 miliardi nel 2020.

IoT – Internet of Things – Espressione che fa riferimento alla moltitudine di "cose", o "oggetti" che, connessi in rete e identificati in modo univoco, sono in grado di comunicare tra di loro, o con altri sistemi, senza richiedere l'intervento umano. Gli "oggetti" possono essere dispositivi, apparecchiature, impianti e sistemi, macchine e attrezzature, nei campi più disparati della nostra vita quotidiana.

IIoT – Industrial IoT – Dispositivo IoT utilizzato in ambito industriale che ha assunto particolare rilevanza a seguito delle iniziative di digitalizzazione facilitate dai vari piani di sviluppo all'interno di *Impresa 4.0*.

In generale, l'impiego di dispositivi IoT permette sia di migliorare la qualità dei servizi offerti dalle apparecchiature in cui sono inseriti, sia di crearne ulteriori, completamente nuovi.

Come per tutti i sistemi connessi in rete, anche per i dispositivi IoT occorre affrontare il problema della cybersecurity. In questo caso, però, questa presenta aspetti del tutto peculiari dovuti, principalmente alla specifica *natura* dei dispositivi coinvolti e alle loro modalità di impiego. I dispositivi IoT hanno, infatti, un insieme di caratteristiche "fisiche" che li rende peculiari sia nel panorama dell'ICT sia nei confronti delle architetture hardware analizzate nella sez. 4.1. Tra

queste caratteristiche vanno certamente annoverate: bassi costi, bassi margini operativi, necessità di ridotti consumi energetici, limitata capacità elaborativa in termini sia di potenza di calcolo sia di capacità di memorizzazione, limitata connettività in termini di protocolli e di banda. Inoltre, i dispositivi utilizzati per la connessione di sensori e attuatori remoti, essendo installati sul campo dove vengono lasciati anche per lunghi periodi di tempo, sono più facilmente soggetti ad attacchi fisici o sferrati sfruttandone i Side-Channel Effect (si vedano i box a pag. 81).

La diffusione di dispositivi IoT e dei nuovi servizi da loro resi disponibili ha accresciuto a dismisura la cosiddetta *superficie di attacco*, introducendo di fatto nuove vulnerabilità. Molte applicazioni, infatti, abilitate dagli scenari IoT, aprono la porta a vulnerabilità totalmente nuove e largamente inesplorate, che possono esporre gli utenti a effetti particolarmente seri, se non prevenuti e trattati in modo specifico, come è stato recentemente dimostrato dagli attacchi portati avanti con successo sfruttando, ad esempio, dispositivi IoT presenti in giocattoli, in distributori automatici di bevande e in interruttori intelligenti per la domotica [77, 79]. Questo fenomeno è oggi particolarmente sentito anche in ambito industriale dove, grazie anche agli incentivi resi disponibili dai vari piani di sviluppo di *Impresa 4.0*, la diffusione di dispositivi IIoT ha raggiunto livelli molto significativi, come illustrato nella sez. 5.5.

Occorre poi evidenziare come la scoperta e la pubblicizzazione di una vulnerabilità in un dispositivo IoT si traduca, immediatamente e contemporaneamente, in una vulnerabilità per *tutte* le apparecchiature e *tutti* i sistemi in cui quel dispositivo è impiegato.

Inoltre, nel caso dell'impiego di più dispositivi IoT di uno stesso tipo all'interno di un sistema, un attacco portato avanti con successo a quel tipo di dispositivi si può tradurre in un comportamento *bizantino* [48] del sistema stesso, con ripercussioni potenzialmente devastanti nel caso in cui quel sistema sia impiegato in applicazioni critiche dal punto di vista della safety.

Un altro aspetto non marginale è l'impiego di numerosi sistemi che adottano dispositivi IoT e che, pur essendo impiegati in infrastrutture critiche che richiedono particolari condizioni di sicurezza, non sono stati progettati considerando in modo adeguato le vulnerabilità introdotte dai dispositivi IoT impiegati. Purtroppo, a oggi, mancano ancora appropriate metodologie di progetto per sistemi che, impiegando dispositivi IoT, siano in grado di garantire livelli di sicurezza adeguati sia alle tipologie dei sistemi stessi sia alla criticità del loro impiego.

Occorre poi rilevare la crescente interazione di servizi assicurativi con dispositivi e sensori mobili IoT, che presenta due aspetti fondamentali: (i) la messa a punto di prodotti assicurativi specifici rivolti a chi impiega dispositivi IoT rispetto ai danni potenzialmente apportati a terzi: si pensi, a titolo di esempio, a droni o veicoli a guida autonoma equipaggiati con dispositivi IoT; (ii) l'erogazio-

ne di assicurazioni tradizionali ma con tariffa "a consumo" con premi e modalità legate a grandezze misurabili sul campo dai dispositivi IoT (ad esempio, il chilometraggio effettivamente percorso in automobile, o altri aspetti legati agli stili di vita individuali). In Italia, l'integrazione attualmente in corso dei servizi assicurativi con la tecnologia IoT permetterà alle assicurazioni di venire incontro alla crescente domanda di prodotti assicurativi altamente personalizzati; tuttavia, quest'integrazione pone evidenti problemi in termini di protezione dei dati personali.

5.4.1 Stato dell'arte

L'analisi dello stato dell'arte verrà affrontata considerando dapprima le principali azioni intraprese in ambito governativo e successivamente i principali progetti di ricerca in corso.

Negli Stati Uniti il NIST ha definito il programma per la cybersecurity nell'IoT (*NIST Cybersecurity for IoT Program*)[23] che supporta lo sviluppo e l'applicazione di standard, linee guida e relativi strumenti per migliorare la cybersecurity dei dispositivi connessi e degli ambienti in cui vengono impiegati.

Inoltre, il Department of Homeland Security ha pubblicato nel novembre 2016 la guida *Strategic Principles for Securing the Internet of Things*[24] che specifica un insieme di principi per migliorare la sicurezza nelle fasi di progettazione, produzione e installazione di dispositivi IoT.

Infine, il Dipartimento di Tecnologia e Innovazione della Città di New York ha coordinato un progetto di ricerca in collaborazione con organizzazioni pubbliche e private, università ed enti di standardizzazione per la produzione di linee guida riguardanti la realizzazione di sistemi IoT, il cui uso abbia un potenziale impatto su spazi o beni pubblici[25].

In Europa, ENISA ha attivato un programma per lo sviluppo di linee guida in materia di sicurezza di infrastrutture critiche basate su tecnologie dell'IoT nei settori delle auto, case e città intelligenti.

Il Governo del Regno Unito ha promosso il programma IoTUK[26] mirato a favorire l'adozione di tecnologie e servizi IoT di elevata qualità nel campo dei servizi sanitari, delle applicazioni industriali e delle città intelligenti. Il programma pone particolare attenzione ai temi della sicurezza dei servizi e dei sistemi, della loro affidabilità e dell'interoperabilità dei dati, e mira a promuovere iniziative di cooperazione tra università, aziende, centri di ricerca e start-up.

[23] `https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program`

[24] `https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf`

[25] `https://www.diffchecker.com/diff`

[26] `https://iotuk.org.uk/`

In Asia, il Governo di Singapore ha lanciato l'iniziativa *Smart Nation*[27] con l'obiettivo di migliorare la qualità della vita in un contesto urbano grazie all'utilizzo di tecnologie dell'IoT. Contestualmente, è stato attivato il programma *Singapore Cybersecurity Strategy*[28] riconoscendo al tema della sicurezza un ruolo chiave per un'ampia ed efficace implementazione del progetto Smart Nation.

In termini di progetti di ricerca, tra quelli finanziati dalla Commissione Europea, di particolare rilevanza sono il progetto USEIT[29] mirato a sviluppare nuovi algoritmi di crittografia, linguaggi di policy e strumenti di sicurezza che garantiscano agli utenti dei dispositivi IoT un accesso sicuro e riservato, e il progetto ANASTACIA[30] che si propone di creare un framework di sviluppo trustworthy-by-design a supporto a tutte le fasi di progettazione e di monitoraggio intelligente e dinamico della sicurezza.

5.4.2 Sfide

Tra le principali sfide da affrontare in questo ambito vanno annoverate le seguenti:

- *Modellizzazione* — Nei domini ormai consolidati dell'affidabilità (dependability) e sicurezza (safety) di sistemi esiste da anni un'accurata modellizzazione dei principali possibili tipi di guasti, errori e conseguenti malfunzionamenti. Questi modelli, riconosciuti e accettati a livello internazionale, in alcuni domini applicativi hanno anche trovato adeguati riconoscimenti in termini di standard de iure e de facto. Nel caso di dispositivi IoT una modellizzazione consolidata e accettata dei possibili tipi di attacco e delle loro potenziali conseguenze non è ancora purtroppo disponibile.
- *Correttezza delle grandezze fisiche* — Nel caso dell'impiego sul campo di dispositivi IoT è molto importante poterne misurare un vasto insieme di grandezze e caratteristiche "fisiche", quali, ad esempio, consumo, temperatura, tensione di alimentazione, carico di lavoro, posizione geografica georefenziata. Sono al riguardo disponibili, e ampiamente adottate in sistemi IT complessi, soluzioni architetturali basate su opportuni mix di hardware e software trusted, che, per ragioni di complessità e costo, non sono applicabili ai dispositivi IoT. In generale, infatti, la spinta a ridurre il costo dei dispositivi finali fa anche sì che le protezioni a livello di singolo dispositivo siano piuttosto scarse.

[27] `https://www.smartnation.sg`

[28] `https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy`

[29] `http://www.chistera.eu/projects/useit`

[30] `http://www.anastacia-h2020.eu`

- *Comportamenti anomali* — Nel caso di architetture e di sistemi basati su IoT per applicazioni industriali, comportamenti "anomali", indotti da attacchi malevoli, non manifestandosi come conseguenza di "guasti" fisici, potrebbero non essere rilevati dai normali sistemi di monitoraggio degli impianti. Più in generale, è necessario studiare approcci e soluzioni per interpretare correttamente le interazioni tra dispositivi IoT, i loro utenti e gli altri dispositivi in rete, sulla base di dati eterogenei e complessi, in modo da sviluppare soluzioni efficienti di monitoraggio e anticipo di attacchi.

- *Soluzioni olistiche* — Purtroppo non sono a oggi disponibili soluzioni architetturali olistiche di cybersecurity compatibili con la "natura" dei dispositivi IoT e con il livello di criticità dei sistemi in cui sono impiegati.

- *Aggiornamenti del Software* — Tipicamente, quando viene resa nota una vulnerabilità di una applicazione software, entro breve tempo vengono resi disponibili gli *aggiornamenti* per quella applicazione, che contengono le modifiche (*patch*) apportate per eliminare tale vulnerabilità. La mancata installazione degli aggiornamenti mette a grave rischio il sistema, in quanto la sua vulnerabilità, prima latente e/o nota solo agli addetti ai lavori, è ora di pubblico dominio e può essere sfruttata da chiunque per accedervi in modo malevolo. È pertanto evidente come, nel caso in cui l'applicazione software in questione sia parte integrante di una linea di sviluppo industriale, il suo mancato aggiornamento possa avere conseguenze catastrofiche nel caso di attacchi cyber.

- *Integrità dell'Hardware e del Software* — Nel caso di sistemi che impiegano dispositivi IoT dotati di capacità di aggiornamento da remoto del software e/o di riconfigurazione parziale o totale dell'hardware (resa possibile, ad esempio, dall'ormai consolidato impiego di dispositivi di tipo FPGA) è necessario essere in grado di garantire l'integrità degli aggiornamenti software, dell'hardware riconfigurato e dei relativi file di riconfigurazione.

- *Protezione dei dati personali e confidentiality* — Molte delle soluzioni IoT presenti o previste per l'immediato futuro includono la condivisione di informazioni tra utenti. Questo implica uno scambio di dati che può essere lesivo per la protezione dei dati personali in quanto attuato senza la completa consapevolezza dell'utente sui dati scambiati e sulla loro rilevanza.

- *Integrazione e tradeoff tra safety e security* — L'impiego di dispositivi IoT in sistemi di controllo industriale e, più in generale, di sistemi *safety critical* pone nuove sfide derivanti dalla necessità di garantire, al tem-

po stesso, adeguati livelli di safety e di security, come evidenziato nella sez. 5.5.

- *IoT in ambito 5G* — Le reti 5G renderanno disponibili servizi non più necessariamente riservati a terminali gestiti da esseri umani, ma estesi anche a terminali con dispositivi IoT, in cui i sensori di rete saranno dotati di scarsissime risorse computazionali ed energetiche e in cui la trasmissione dei dati sarà tipicamente sporadica. Come analizzato in dettaglio nella sez. 5.1, i sistemi 5G, per poter gestire in sicurezza dispositivi IoT dovranno pertanto supportare non solo tecniche crittografiche estremamente variabili in termini di robustezza e livello di protezione, ma anche implementare nuovi modelli per la gestione di soluzioni eterogenee di sicurezza e nuovi modelli di trust.
- *Valutazione del rischio assicurativo* — Per quanto riguarda specificamente il settore assicurativo, un elemento di rischio importante consiste nella difficoltà di garantire la sicurezza dei dispositivi IoT integrati nei nuovi servizi assicurativi. Il calcolo dei modelli di rischio assicurativi è reso difficile non solo dai possibili errori sulle stime di probabilità in tempo reale, per le quali servono dati affidabili per tradurre le stime in polizze e premi coerenti, ma anche per le valutazione della severità stessa degli eventi oggetto delle polizze assicurative cyber. Ad esempio, è difficile quantificare le perdite economiche o le lesioni personali che i nuovi dispositivi come i droni o i veicoli a guida autonoma potrebbero causare in presenza di compromissioni fisiche dei dispositivi IoT impiegati a bordo.

5.4.3 Obiettivi

In riferimento alle sfide da affrontare e sopra riassunte, è necessario attivare un insieme di progetti che, nella loro globalità, mirino a fornire risposte adeguate e sostenibili a ciascuna delle sfide e, in particolare, al raggiungimento degli obiettivi indicati nel seguito.

- *Modellizzazione* — Occorre sviluppare adeguati modelli in grado di descrivere i possibili attacchi a sistemi che impiegano dispostivi IoT. Questi vanno analizzati e descritti sia a livello *fisico* (o *strutturale*), dove le conseguenze sono, tipicamente, errati valori di grandezze fisiche rilevati da sensori e trasmessi al sistema di controllo, sia a livello *funzionale* (o *applicativo*), dove si manifestano funzionalità anomale del sistema conseguenza dei valori errati di cui sopra.
- *Correttezza delle grandezze fisiche* — Occorre definire soluzioni efficienti in termini di usabilità e costi per la misura e la verifica della correttezza di grandezze e caratteristiche “fisiche” di dispositivi IoT. In particolare, si devono sviluppare soluzioni architetturali nelle quali sia possibile

una distribuzione gerarchica della catena di trust, demandando, a titolo di esempio, a un PC o a uno smartphone “certificati” (e quindi ritenuti “sicuri”) il controllo della sicurezza di un insieme di dispositivi IoT a essi connessi.

- *Comportamenti anomali* — Occorre sviluppare piattaforme e sistemi di monitoraggio in grado di identificare comportamenti anomali in dispositivi IoT impiegati nel controllo di sensori e attuatori. In particolare, le soluzioni proposte devono essere in grado di:

  – estendere le prestazioni degli attuali sistemi SIEM (Security Information & Event Management), ampiamente utilizzati per la difesa di sistemi IT, sviluppando lato IoT (veri end-point, in questo caso) architetture hardware in grado di svolgere pre-elaborazioni intelligenti degli eventi (dati, comunicazioni, comandi, controlli, etc), da inviare successivamente al SIEM;

  – eseguire localmente, sull’end-point, parte del SIEM stesso. A livello pratico questo richiederà, da un lato, considerare come eventi i valori dei segnali scambiati con i sensori e gli attuatori e, dall’altro, adottare efficaci ed efficienti tecniche di machine learning per l’individuazione tempestiva dei comportamenti anomali;

  – eseguire il monitoraggio, il tracciamento degli attacchi e l’anticipazione delle mosse dell’attaccante per sistemi IoT, attraverso approcci integrati comprendenti monitoraggio del traffico di rete, utilizzo dei dispositivi utenti, interazioni tra utenti, e tra utenti e dispositivi specifici, reti sociali tra utenti e tra dispositivi;

  – permettere analisi scalabili dei dati generati dai sensori, atte a identificare anomalie e pattern di traffico riconducibili ad attacchi a larga scala coordinati, ad esempio guidati da botnet tipo Mirai.

- *Soluzioni olistiche* — Occorre definire sia metodologie e strumenti per la progettazione e lo sviluppo di applicazioni basate su dispositivi IoT sicure, distribuite ed eterogenee, sia piattaforme per l’installazione, la gestione e l’operatività sicura e usabile di sistemi IoT eterogenei e dinamici. Le soluzioni proposte devono essere in grado di:

  – garantire i requisiti di confidenzialità, protezione e autenticità, consentire interazioni sicure sia human-to-machine sia machine-to-machine, assicurando, laddove richiesto, anche i requisiti di usabilità, efficienza, scalabilità, affidabilità e user-awareness;

  – garantire livelli misurabili di protezione dei dati e delle informazioni “at rest”, “in motion” e “at use”, in grado di assicurare sia la

confidenzialità e l'autenticità dei dati end-to-end sia l'integrità e la disponibilità delle infrastrutture di interconnessione;

  - prevedere lo sviluppo, lato IoT, di adeguate architetture hardware sicure, garantendo la compatibilità con gli standard di comunicazione e memorizzazione maggiormente in uso;
  - prevedere adeguati schemi e servizi di gestione delle chiavi di crittografia che coprano sia tutti i passi del ciclo di vita di una chiave sia tutte le figure professionali coinvolte nella realizzazione e nella gestione del sistema;
  - essere usabili anche da tecnici non esperti di cybersecurity;
  - essere applicabili, a seguito dei necessari adattamenti, a tutte le applicazioni e a tutti i sistemi che impiegano dispositivi IoT.

- *Integrità dell'hardware e del software* — Occorre adattare le soluzioni già ampiamente adottate in altri ambiti IT alle caratteristiche peculiari dei dispositivi IoT remoti.
- *Certificazione e revisione* — Occorre definire adeguate procedure, da adottare a livello nazionale, per la certificazione e la revisione periodica da richiedere o imporre ai dispositivi IoT in base alla loro criticità all'interno dei sistemi in cui sono impiegati.
- *Protezione dei dati personali e confidentiality* — Occorre definire architetture che rispettino la protezione dei dati personali dell'utente e lo proteggano da potenziali accessi malevoli ai dati sfruttando dispositivi IoT. Inoltre, i dispositivi IoT impiegati devono garantire compatibilità con le prescrizioni del GDPR, introdotto nella sez. 6.1.1.

In aggiunta, si ritiene strategico per il Paese pervenire, nell'arco dei prossimi 3 anni, allo sviluppo di una soluzione olistica applicabile ad almeno due soluzioni "verticali" e i cui livelli di sicurezza possano essere predefiniti e successivamente validati tramite gli approcci più avanzati dello stato dell'arte.

5.5 Industrial Control System

Nel recente passato gli operatori delle infrastrutture critiche hanno sostenuto, con ferma convinzione, la tesi secondo la quale i sistemi di controllo industriali (*Industrial Control System – ICS*), che includono i sistemi *SCADA (Supervisory Control And Data Acquisition)*, i sistemi di controllo distribuiti (*Distributed Control System – DCS*) e altri sistemi, quali i controllori a logica programmabile (*Programmable Logic Controller – PLC*), fossero intrinsecamente sicuri, in quanto scollegati da reti pubbliche e quindi protetti dall'*air gap* esistente tra gli stessi

sistemi di controllo e la rete aziendale. Di conseguenza, secondo loro, non era necessario mettere in atto alcun meccanismo di sicurezza.

Oggigiorno lo scenario è radicalmente mutato a causa dell'elevato livello di integrazione raggiunto tra l'*Information Technology* (IT) e l'*Operational Technology* (OT), per cui il mito della sicurezza intrinseca è stato in parte, se non del tutto, smentito. L'introduzione, infatti, delle tecnologie dell'informazione nei sistemi di controllo fisici, motivata dalla riduzione dei costi e dal miglioramento delle prestazioni di questi ultimi, ha senza dubbio favorito la nascita di una serie di tecnologie intelligenti, dalle smart grid allo smart transportation, sino allo smart manufacturing. Tale processo evolutivo, portatore di nuove funzionalità e servizi, ha, tuttavia, fatto emergere, al contempo, la necessità di incrementare la sicurezza e la resilienza dei sistemi ICS.

Tra gli aspetti di cui tener conto nella progettazione e nello sviluppo di soluzioni per la sicurezza dei sistemi di controllo industriali, una particolare attenzione va posta alla differenza tra il tempo di vita di un sistema ICS e quello di un sistema IT. Tipicamente, infatti, mentre il tempo di vita di un sistema ICS, basato su tecnologie progettate e sviluppate per uno specifico dominio, è dell'ordine di 10–15 anni, quello di un componente IT è molto inferiore, mediamente dell'ordine di 3–5 anni. Questa differenza rappresenta un fattore estremamente critico nel momento in cui si pianificano attività di aggiornamento e manutenzione dei sistemi ICS, a causa dei requisiti stringenti di disponibilità e affidabilità posti da tali sistemi. Lo scenario presentato evidenzia, quindi, la necessità di affrontare le problematiche di sicurezza e affidabilità dei sistemi di controllo industriali combinando competenze *cross-functional*, che consentano di comprendere appieno le possibili implicazioni derivanti dall'installazione e dall'uso di tecnologie IT sull'operatività dei sistemi ICS.

5.5.1 Stato dell'arte

Tra le iniziative riguardanti la sicurezza dei sistemi ICS, va senza dubbio menzionata la pubblicazione da parte del NIST del documento 800-82 *Guide to Industrial Control Systems (ICS) Security*[31], che fornisce un'analisi accurata delle topologie tipiche di tali sistemi, identifica le possibili minacce di sicurezza e presenta le contromisure da adottare per mitigare i rischi connessi.

Un'altra importante iniziativa è stata la creazione, da parte del governo americano, di un CERT dedicato: l'ICS-CERT[32], avente il compito di coordinare gli sforzi e le iniziative delle istituzioni governative e dell'industria per il miglioramento del livello di sicurezza dei sistemi di controllo industriali utilizzati per il monitoraggio e la gestione delle infrastrutture critiche.

[31] `https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final`
[32] `https://ics-cert.us-cert.gov/`

In Europa, ENISA ha pubblicato diversi studi sulla sicurezza dei sistemi di controllo industriali, affrontando temi, quali: l'analisi delle vulnerabilità e della finestra di esposizione di sistemi SCADA a minacce informatiche[33]; il testing del livello di sicurezza dei sistemi ICS[34]; la certificazione delle competenze, in materia di sicurezza, delle figure professionali operanti nel settore dei sistemi ICS/SCADA[35]; l'analisi del livello di maturità, dal punto di vista della sicurezza, dei sistemi ICS/SCADA impiegati nelle infrastrutture critiche[36]; l'identificazione degli insegnamenti ricavabili dalla valutazione degli incidenti di sicurezza concernenti sistemi SCADA[37]. Il documento più recente prodotto da ENISA sulla sicurezza dei sistemi ICS è stato pubblicato a febbraio 2017 ed è un report sull'analisi delle dipendenze dei sistemi ICS/SCADA dalle reti di comunicazione[38].

Altra iniziativa nel panorama europeo è stata la istituzione di uno specifico gruppo di lavoro su Industry 4.0 e sistemi ICS da parte di ECSO (European Cyber Security Organisation)[39].

5.5.2 Sfide

Tra le principali sfide da affrontare nel settore dei sistemi ICS sono da annoverare le seguenti:

- *Messa in sicurezza di sistemi legacy* — Come detto in precedenza, negli attuali sistemi di controllo industriali coesistono tecnologie che hanno un tempo di vita estremamente lungo (alcune installate prima che le reti OT si interconnettessero con le reti IT) e tecnologie soggette a una rapida obsolescenza. L'integrazione dei due domini tecnologici ha generato nuove vulnerabilità e introdotto nuovi percorsi sfruttabili per mettere in atto strategie di attacco: è pertanto necessario lo sviluppo di specifiche misure di sicurezza.
- *Sicurezza e disponibilità (availability) dei processi industriali* — Un importante requisito dei sistemi ICS è garantire la più ampia disponibilità

[33] https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems

[34] https://www.enisa.europa.eu/publications/good-practices-for-an-eu-ics-testing-coordination-capability

[35] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals

[36] https://www.enisa.europa.eu/publications/maturity-levels

[37] https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents

[38] https://www.enisa.europa.eu/publications/ics-scada-dependencies

[39] https://www.ecs-org.eu/

possibile dei processi industriali. Il soddisfacimento di questo requisito rende complesse le procedure di gestione e aggiornamento degli strumenti e dei meccanismi per la sicurezza dei componenti dei sistemi ICS, basati sulle tecnologie dell'informazione. Di conseguenza, occorre sviluppare tecniche e metodi che consentano di assicurare la sicurezza del sistema senza minarne la continuità della disponibilità.

- *Analisi delle relazioni tra safety e security nei sistemi ICS* — Date le peculiari funzionalità dei sistemi di controllo industriali, sono di rilevante importanza l'analisi e la modellazione delle dipendenze tra le proprietà inerenti la safety e quelle inerenti la security, al fine di una corretta ed efficace gestione del sistema durante l'intero suo ciclo di vita.

- *Impatto dell'IIoT sui sistemi ICS* — La crescita dell'IIoT implica un potenziale aumento del numero delle sorgenti di attacco, introducendo un'ampia varietà di sensori distribuiti e altri dispositivi che non sempre sono stati progettati in conformità con gli standard di sicurezza industriale. In questo senso gli enti di standardizzazione devono definire normative e requisiti per ridurre l'impatto, in termini di sicurezza, dell'uso di dispositivi IIoT sui sistemi di controllo industriali. Particolare attenzione va anche dedicata allo sviluppo di strumenti per la definizione, organizzazione e realizzazione di adeguati *assurance case* mirati a dimostrare congiuntamente l'adeguatezza del sistema agli standard di Safety e Security.

5.5.3 Obiettivi

In relazione alle sfide poste dalla sicurezza dei sistemi ICS, occorre attivare iniziative progettuali finalizzate al raggiungimento dei seguenti obiettivi:

- *Analisi delle vulnerabilità dei sistemi ICS/SCADA* — Definizione di tecniche specifiche per l'analisi delle vulnerabilità dei sistemi ICS/SCADA, motivate delle peculiarità di tali sistemi, derivate anche dalla coesistenza e integrazione di tecnologie IT e OT. Al riguardo occorre: (i) proporre una tassonomia dei sistemi; (ii) sviluppare metodologie per l'identificazione delle vulnerabilità e l'analisi delle minacce; (iii) identificare contromisure e best practice per il trattamento del rischio.

- *Framework per l'analisi delle proprietà di safety e security di sistemi ICS/SCADA* — Definire un framework per l'analisi delle proprietà di safety e security di questi sistemi, l'individuazione e la modellazione delle loro interdipendenze e dei loro requisiti (che possono anche essere tra loro conflittuali) e la valutazione automatica dell'impatto di problematiche di security sugli aspetti di safety. In particolare, occorre: (i) realizzare

strumenti e processi per la simulazione e il monitoraggio di effetti a cascata causati da attacchi informatici; (ii) progettare soluzioni che consentano di mitigare tali effetti, aumentando la resilienza dei sistemi coinvolti; (iii) sviluppare strumenti per la definizione, organizzazione e realizzazione di adeguati *assurance case* mirati a dimostrare congiuntamente l'adeguatezza del sistema agli standard di safety e security.

- *Programmi di formazione* — Occorre definire e attuare programmi di formazione mirati per i profili professionali operanti nel settore dei sistemi di controllo industriali, come illustrato nella sez. 6.2.

5.6 Robot

In questa sezione si analizzano, con riferimento agli aspetti di cybersecurity, gli scenari in cui un dispositivo (*robot*), in grado di compiere direttamente azioni meccaniche nel mondo fisico, possa operare in modo completamente (o parzialmente) autonomo e senza un diretto e continuo controllo da parte di un operatore umano. Con questa caratterizzazione, un frigorifero, ad esempio, non rientra nell'ambito considerato in quanto tipicamente non si muove nell'ambiente (anche se potrebbe aprire automaticamente il proprio sportello), mentre vi rientra un aspirapolvere in grado di spostarsi autonomamente all'interno dell'appartamento.

La robotica sta oggi rompendo le proprie delimitazioni classiche e, da sistema automatico utilizzato principalmente nel mondo industriale e dell'automazione, si sta ibridando con tecnologie quali il Cloud Computing, l'Intelligenza Artificiale e l'IoT. Essa gioca inoltre un ruolo centrale nel contesto di *Impresa 4.0*, nel quale si possono identificare alcune significative linee di tendenza:

- *L'informatizzazione del settore industriale* — Il Cloud Computing e l'Intelligenza Artificiale entrano nei processi produttivi industriali (e delle catene di montaggio automatiche) e ne cambiano sensibilmente i canoni. Dalla produzione in serie si sta passando alla produzione personalizzata in cui una stessa catena di montaggio, grazie all'impiego di robot sempre più sofisticati, è in grado di produrre oggetti diversi tra loro sulla base di richieste specifiche fornite direttamente dal cliente finale. Questo scenario è già realtà in numerosi contesti, quali, ad esempio, la verniciatura personalizzata di alcuni tipi di automobili.

- *La robotizzazione del mondo consumer* — La robotica entra e trasforma la quotidianità della vita e del lavoro, nell'ottica della massimizzazione dell'efficienza e della sicurezza dei servizi, non solo nei settori della produzione industriale, ma in maniera pervasiva in moltissimi altri ambiti della società. In questo contesto, stiamo assistendo a una forte trasformazione

degli oggetti della nostra vita quotidiana, che, da semplici strumenti sotto il controllo dell'essere umano, stanno diventando strumenti autonomi e in grado di prendere decisioni. Esempi tipici vanno dall'aspirapolvere all'automobile.

- *La distribuzione dell'intelligenza* — Mentre negli anni '80 l'*intelligenza* dei robot era localizzata all'interno degli stessi robot, si registra oggi la tendenza a delocalizzare parte di questa intelligenza in Cloud (tecnologia identificata con il nome di *Cloud Robotic*), in modo da avere robot più economici, leggeri e intelligenti. Se da un lato tale approccio ha notevoli vantaggi nella realizzazione di robot sempre più autonomi e connessi, dall'altra il connettere un robot a internet e delocalizzarne l'intelligenza (e quindi la capacità di prendere decisioni) apre le porte ad attacchi informatici verso questi dispositivi.

Per quanto concerne gli aspetti di cybersecurity, oltre alle problematiche di sicurezza derivanti dalle azioni fisiche del robot, un ulteriore aspetto da considerare riguarda il fatto che la capacità di movimento "autonomo" può essere strumentale anche all'acquisizione di dati e informazioni tramite sensori mobili, con potenziali rischi per la protezione delle informazioni e dei dati personali.

Senza voler essere esaustivi, si elencano nel seguito una serie di dispositivi la cui sicurezza risulta critica in relazione ad azioni che essi possono svolgere nel mondo fisico. L'automobile rappresenta un caso già molto studiato nel quale un attacco cibernetico può causare conseguenze significative. Le criticità in questo ambito sono già uscite dal contesto accademico e ne sono state date dimostrazioni che hanno richiesto l'intervento delle case automobilistiche: ad esempio, nel 2015, Chrysler effettuò il richiamo di vari modelli di automobili[40] a seguito della dimostrazione di gravi vulnerabilità sfruttabili per ottenere il controllo remoto del veicolo. In generale, la crescita degli ausili alla guida, fino ad arrivare a veicoli a guida autonoma, aumenta il numero e la criticità delle decisioni demandate a sistemi informatici ed elettronici (i.e., ECU) interconnessi tra loro, invece che al guidatore. Se, da un lato, questo aumenta la sicurezza nell'uso quotidiano del veicolo, d'altra parte fa sì che segnali critici, con un effetto rilevante nel mondo fisico (e.g., i freni) siano controllati da sistemi che potrebbero essere compromessi da un attacco cibernetico.

Le capacità di guida autonoma si estendono anche ad altre classi di veicoli *unmanned*, cioè in grado di operare senza il controllo diretto dell'operatore, il cui utilizzo si sta diffondendo rapidamente in ambito militare, negli scenari di emergenza, in campo agricolo, nelle miniere e in numerosi altri contesti "all'a-

[40] `https://www.theguardian.com/business/2015/jul/24/fiat-chrysler-recall-jeep-hacking`

perto". In questi contesti è infatti sempre più diffuso l'impiego di droni e microdroni, tramite i quali è possibile non solo acquisire dati per il monitoraggio, ma anche eseguire operazioni quali il rilascio di prodotti fitosanitari. Non è difficile immaginare conseguenze derivanti da intrusioni in questo tipo di sistemi.

Anche in ambito domestico i robot sono già una realtà diffusa, non solo per quanto riguarda l'aspirapolvere che si costruisce la mappa della casa per poterla pulire in modo sistematico, ma anche per quanto riguarda, ad esempio, i dispositivi di telepresenza che, sebbene per lo più teleguidati, consentono di vedere cosa fanno i bambini a casa o di interagire con i nonni lontani. A titolo di esempio, attraverso il canale audio sono stati attaccati dispositivi in grado di interagire in linguaggio naturale con l'operatore (e.g., Siri[41], Alexa[42]). L'utilizzo di comandi vocali è una funzionalità che si diffonderà rapidamente anche su dispositivi robotici mobili. Appare evidente come la presenza di sistemi mobili all'interno di un'abitazione rappresenti una criticità importante dal punto di vista della sicurezza. La loro presenza offre, infatti, un punto di osservazione mobile, che pone non solo delle questioni di protezione dei dati personali ma anche la possibilità di acquisizione indebita di informazioni per usi impropri.

La categoria dei sistemi robotici cosiddetti di servizio, si estende ad ambienti, quali l'ufficio, il ristorante, il centro commerciale, l'ospedale dove l'introduzione di sistemi autonomi per il trasporto o l'interazione con l'utente, sebbene non ancora molto diffusa, è prevista in forte espansione nei prossimi anni. Anche in questi contesti, l'attacco cibernetico al dispositivo può avere conseguenze molto rilevanti.

Una delle più interessanti applicazioni in campo medico è la *chirurgia robotica*, che consente di eseguire interventi chirurgici manovrando, attraverso una console, un robot non completamente autonomo, ma capace di eseguire manovre comandate. La tecnologia consente oggi di manovrare il robot a distanza (*teleoperated surgical robot*) utilizzando anche le "normali" reti di telecomunicazione. Questo apre ovviamente la strada ad attacchi informatici che possono alterare il comportamento del robot, con conseguenze sulla sicurezza del paziente. Recentemente, un robot chirurgico (Raven II), che utilizza lo standard *Interoperable Telesurgery Protocol* sulla rete Internet per le comunicazioni fra la console e il robot, è stato sottoposto con successo a vari tipi di attacchi cibernetici, con lo scopo di analizzare i possibili rischi per il paziente (anche un semplice attacco di tipo "denial of service", se avviene in momenti particolari dell'intervento, può portare alla morte del paziente) [18]. Questi robot devono essere progettati in modo da essere resilienti a possibili attacchi cibernetici, prima di poter essere usati in pratica.

In generale, esistono tre tipologie di possibili attacchi che possono alterare il funzionamento di un sistema robotico, compromettendone l'interazione fisica:

[41] `https://www.apple.com/it/ios/siri/`

[42] `www.amazon.it/alexa?`

- Il primo, più banale e catastrofico, è un attacco diretto al robot, in cui l'attaccante riesce a prendere direttamente il controllo completo dei sistemi di locomozione del robot stesso, trovandosi nella condizione di poterlo quindi controllare direttamente, al fine di arrecare danni fisici.

- La seconda tipologia è un attacco diretto al sistema decisionale del robot, che in ambito *Cloud Robotics* è delocalizzato in un sistema Cloud. In questo caso, il robot si comporta come dovrebbe, ma i dati di controllo e movimentazione possono essere alterati o indebitamente esfiltrati. In questo caso i sistemi di safety locali (come ad esempio l'obstacle avoidance) dovrebbero comunque essere in grado di evitare danni fisici diretti.

- La terza tipologia di attacco rientra nel contesto degli attacchi *spoofing*. In questo caso, non viene attaccata direttamente l'intelligenza, ma vengono alterati i dati in base ai quali l'intelligenza stessa elabora le proprie decisioni, in modo da far sì che il robot esegua le operazioni volute dall'attaccante. Un interessante esempio di tale applicazioni è il cosiddetto *GPS spoofing*[43], grazie al quale è stato possibile dirottare una nave militare alterando i dati GPS ricevuti da questa.

5.6.1 Stato dell'arte

Nell'ottobre 2016 il Dipartimento delle politiche per i diritti dei cittadini e per gli affari costituzionali dell'UE ha approvato un documento di studio sulle regole giuridiche civili europee in materia di robotica, commissionato dalla Commissione affari legali del Parlamento Europeo per analizzare la prospettiva di un futuro quadro normativo di regole civili per la robotica[44]. Il risultato ha prodotto un quadro generale di principi etici tesi a proteggere l'umanità dai robot, ponendo a direttiva la previsione: (i) del dovere per i robot di non causare offese agli individui umani; (ii) dell'obbligo del rispetto delle regole di cautela e attenzione rispetto all'uomo; (iii) del principio di responsabilità civile oggettiva per i danni causati dai robot, secondo il modello della responsabilità "vicaria" (responsabilità per fatto altrui): la macchina artificiale, difatti, manca di una sua autonomia psico-fisica su cui poter fondare una responsabilità giuridica "individuale".

Il documento conclude col ritenere inappropriata la creazione di una categoria giuridica ad hoc per i prodotti dell'IA.

[43] https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

[44] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf

Viene fatta così propria la convinzione etica, sociale, giuridica, per cui solo una persona fisica può essere ritenuta responsabile attraverso diversificati meccanismi di imputazione.

Il problema della cybersecurity nei dispositivi robotici medici è stato affrontato da enti regolatori quali la Food & Drug Administration (FDA) Statunitense che ha promosso varie iniziative per proteggere la sanità pubblica da vulnerabilità relative alla cybersecurity. In particolare nel 2016 ha emesso delle linee guida che raccomandano ai produttori di affrontare la cybersecurity durante il progetto e lo sviluppo di dispositivi medici, cosa che può portare a una mitigazione più efficace dei rischi dei pazienti[45,46]. Inoltre, è richiesta la protezione dei dati nei sistemi robotici che memorizzano informazioni mediche dei pazienti [65].

Tra gli scenari delineati nella sezione precedente, quello dell'automobile non solo ha suscitato l'interesse di agenzie governative di vare nazioni, tra le quali gli USA[47], ma ha già richiesto l'intervento del legislatore. È recente l'approvazione di una legge al riguardo negli USA, dove la sperimentazione su strada è già pratica comune; altri stati seguiranno a breve.

5.6.2 Sfide

Senza voler ripetere le sfide che derivano dalle tecnologie che si intersecano con la robotica, quali Cloud e IoT, già analizzate nelle sezioni precedenti, si vogliono qui analizzare quelle sfide di natura interdisciplinare che stanno nascendo con l'evoluzione della robotica e che investono, oltre alla sfera scientifica e tecnologica, anche quella sociologica e quella giuridica.

- Per quanto riguarda l'ambito sociologico e giuridico, l'Italia (e molti altri paesi) sono ancora sprovvisti di norme che regolino l'utilizzo di robot e dispositivi autonomi all'interno della società. Ad esempio, attualmente è illegale il volo di droni autonomi in modo non supervisionato. In generale, manca ancora una comprensione approfondita dei profili di criticità introdotti da possibili attacchi cyber in ambiti diversi, quali:
  - la gestione/manipolazione dei dati personali dell'individuo acquisiti dal robot nei contatti sociali;
  - la possibile manipolazione delle emozioni umane dei soggetti deboli in contatto quotidiano con macchine artificiali sociali (robot

[45] `https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf`

[46] `https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf`

[47] United States Government Accountability Office: VEHICLE CYBERSECURITY - DOT and industry have efforts under way, but DOT needs to define its role in responding to a real world attack, 2016 – `http://www.gao.gov/assets/680/676064.pdf`

in ambienti domestici o paradomestici, in particolare vicini ad anziani, bambini, malati);

  - la vulnerabilità fisica di chi usa apparecchi meccanici sanitari per integrare/sostituire proprie disfunzionalità organiche, anche come protesi;

  - la circolazione di veicoli e mezzi di trasporto automatizzati o autonomi.

- Sotto il profilo più strettamente scientifico e tecnologico, le problematiche di interesse si possono ricondurre essenzialmente a due categorie.

  - Studiare come, sotto il profilo architetturale, si declinano le strategie di attacco e, conseguentemente, di difesa, nell'ambito di sistemi robotici sui quali tipicamente sono presenti tanto sistemi embedded quanto sistemi di elaborazione convenzionali, quali PC, tablet, telefoni cellulari etc. [25].

  - Monitoraggio e sicurezza (nel senso di "safety" di questi dispositivi). Infatti, nel caso dei dispositivi considerati in questo ambito, lo studio delle anomalie di comportamento ha una connotazione specifica che si incentra sull'interazione con l'ambiente, e, in particolare, con l'uomo. La caratterizzazione dei comportamenti anomali dei dispositivi autonomi rappresenta una sfida della ricerca nel prossimo futuro.

5.6.3 Obiettivi

Il progetto si pone come obiettivo primario quello di individuare e consolidare le basi metodologiche per lo sviluppo della ricerca e dell'innovazione nel campo della cybersecurity per le categorie di sistemi autonomi qui considerate.

Sotto il profilo strettamente tecnico, sono state individuate le seguenti linee di intervento:

- specializzazione delle tecnologie di cybersecurity per i sistemi robotici autonomi, sviluppando protocolli e soluzioni di sicurezza che garantiscano non sono le informazioni ma anche la sicurezza fisica di questi sistemi e siano quindi in grado di coniugare opportunamente safety e security;

- normare, dal punto di vista giuridico, gli aspetti legati all'introduzione dei sistemi autonomi nella società e il sistema di imputazione della responsabilità per danni;

- definire degli obiettivi a lungo termine sul piano sociale ed educativo per preparare adeguatamente i cittadini alla diffusione dei robot nella vita di tutti i giorni, in modo che ne diventino non solo fruitori passivi, ma partecipanti attivi al cambiamento in corso e sensibili ai rischi indotti in termini di protezione dei dati personali, di safety e di security.

CAPITOLO

6 Azioni orizzontali

In questo capitolo vengono presentate alcune *azioni orizzontali*, trasversali rispetto alle tecnologie abilitanti e a quelle da proteggere analizzate nei due capitoli precedenti.

Vengono dapprima analizzati gli aspetti connessi con la difesa della protezione dei dati personali, anche in relazione con la prossima entrata in vigore della normativa GDPR.

Successivamente vengono presentate le azioni necessarie nei settori dell'educazione, della formazione e della sensibilizzazione. È diventata una esigenza strategica 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. Per rispondere ai problemi posti dal crescente utilizzo del cyberspace e dalle criticità in termini di protezione dei sistemi informatici, è necessario promuovere la cultura della sicurezza e rendere consapevoli i cittadini e i lavoratori che la mancanza di attenzione a questi aspetti può mettere a rischio un'intera comunità. Per raggiungere tale obiettivo è necessario potenziare l'educazione specialistica, innalzando la sicurezza a obiettivo strategico e considerando l'educazione di base, la formazione universitaria e la formazione professionale.

Il capitolo si chiude analizzando le azioni necessarie per un'accurata gestione del rischio cyber per le imprese e per l'attivazione, anche in Italia, di un sistema di certificazioni sostenibili e compatibili con la realtà del nostro Paese.

6.1 Protezione dei dati personali e normativa GDPR

In un mondo dove le agenzie di sicurezza degli stati e i giganti globali dell'Internet economy raccolgono e collezionano i dati dei nostri comportamenti, la protezione di tali dati impatta direttamente con i diritti dei cittadini. Soprattutto perché la gestione usuale dei dati personali e sensibili limita sempre di più il diritto alla protezione dei dati personali e alla libertà d'espressione, producendo talvolta reazioni di paura in chi non ne comprende la portata e di conformismo in chi ne conosce le dinamiche.

La cybersecurity non è soltanto protezione degli asset nazionali, ma riguarda anche i diritti fondamentali dei cittadini. È pertanto necessaria una riflessione globale su cosa significhi sicurezza digitale in un contesto in cui i poteri di sorveglianza statuali vengono ampliati, l'anonimato e le tecnologie per la protezione dei dati personali limitate, messe fuorilegge, o addirittura i loro utilizzatori sorvegliati, mentre i sistemi di garanzia sono indeboliti e delle *backdoor* vengono installate nei software più popolari con la compiacenza di aziende spregiudicate.

> **Backdoor** – Metodo per aggirare la normale autenticazione in un sistema informatico e accedervi in remoto per prenderne il completo o parziale controllo.
> Backdoor possono essere nascoste all'interno di programmi di sistema, di applicazioni software o di componenti hardware e possono essere introdotte da un programmatore, da un progettista o da un compilatore.
> Una backdoor può essere anche di tipo matematico all'interno di sistemi crittografici per poter decifrare flussi di dati.
> Tipicamente chi scopre una backdoor è in grado di sfruttarla, mentre una backdoor matematica può essere utilizzata esclusivamente solo da chi l'ha introdotta.

Se la sicurezza di dati e informazioni viene meno, a risentirne è la nostra privacy, che è la precondizione per esercitare il diritto d'opinione, d'espressione, di cronaca, d'associazione, di movimento, d'impresa, fino al diritto alla proprietà. Per questo, tutelare i nostri dati e le informazioni che qualificano noi e le nostre azioni diventa un'esigenza fondamentale: la conoscenza delle nostre più intime convinzioni e dei nostri comportamenti può consentire ad altri di manipolarci, intimidirci, perfino ricattarci.

Le grandi organizzazioni sono coscienti che la prima linea di difesa è data da un'adeguata gestione del rischio e dall'osservazione delle procedure di sicurezza, ma spesso aziende ed enti non hanno un recovery plan in caso di attacchi cyber e i manager e i decisori pubblici hanno scarsa consapevolezza del rischio reale che si corre quando un solo anello della catena della sicurezza viene spezzato.

Nel seguito di questa sezione vengono affrontare le principali problematiche connesse con la protezione dei dati personali derivanti dalla normativa

General Data Protection Regulation (GDPR) o *Regolamento generale sulla protezione dei dati* che è stata introdotta nel regolamento UE 2016/679[1] del 27 aprile 2016 e che abroga la precedente direttiva 95/46/CE.

6.1.1 La normativa

Lo scopo principale della normativa GDPR, applicabile dal 25 maggio 2018, è quello di riformare, aggiornare e uniformare la legislazione in materia di protezione e libera circolazione dei dati personali, così da renderla più solida e coerente tra i vari Paesi UE.

La direttiva 95/46/CE e la normativa GDPR sono profondamente diverse: la prima prevedeva una serie di prescrizioni, assimilabili a una check list, mentre la seconda indica gli obiettivi da raggiungere, lasciando alla discrezionalità degli operatori la scelta degli strumenti più opportuni in relazione al contesto, ma impone al contempo l'obbligo di documentare le ragioni che hanno motivato tali scelte.

Premesso che per *dati personali* si intendono tutte le informazioni relative a un individuo e alla sua figura professionale e pubblica[2], il concetto di protezione dei dati che caratterizza il GDPR comprende anche gli obblighi relativi alla loro gestione, che riguardano sia la sicurezza sia ambiti ulteriori come la conservazione, la riservatezza, l'anonimizzazione e la cancellazione a richiesta del soggetto interessato.

Il GDPR distingue tra il *titolare del trattamento* (ovvero il *controller* della versione inglese), il *responsabile del trattamento* (in inglese il *processor*) e il *soggetto interessato*, vale a dire il soggetto a cui i dati si riferiscono.

Il GDPR impone alle aziende di rivedere i sistemi di gestione dei dati all'interno delle proprie strutture organizzative per prevenire la perdita o l'errata condivisione degli stessi. Il nuovo regolamento rivede il concetto di *accountability* (responsabilizzazione)[3]: la responsabilità del trattamento è in capo al titolare del trattamento e non al responsabile del trattamento (che è il processor). Le aziende devono poi prevedere la figura del *Data Protection Officer* (DPO) che ha il compito di supervisionare i processi organizzativi interni ed è esperto in materia di diritto e tecniche di protezione dei dati[4].

---

[1] `http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4964718`

[2] `http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT`

[3] `http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati`

[4] `http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento`

Le problematiche relative al trattamento dei dati non sono circoscritte al perimetro aziendale, ma coinvolgono sub-fornitori, distributori, agenti, outsourcer, partner industriali e commerciali, cloud provider, etc., a protezione dell'intera filiera dei servizi per l'azienda. Tutti i partner aziendali sono coinvolti in questo processo e devono attuare strategie condivise ed efficienti.

Il GDPR impone, inoltre, l'applicazione del principio della *data protection by design* che richiede di considerare la protezione dei dati fin dalla fase di ideazione e progettazione di un sistema per il trattamento o la gestione di dati personali, coinvolgendo quanti si occupano dello sviluppo di servizi, prodotti, applicazioni che fanno uso di dati personali.

Evidenziamo, in chiusura, alcuni principi di base del trattamento che incidono sulla sicurezza. Poiché nessuna banca dati è sicura in Internet, alcuni dei principi fondamentali del GDPR sono proprio volti a limitare il campo di esposizione ai rischi:

- *minimizzazione dei dati* — raccolgo solo i dati necessari e non altri;
- *limitazione delle finalità* — non posso decidere di fare ciò che voglio dei dati, ma solo perseguire la finalità per cui li ho raccolti;
- *limitazione della conservazione* — sono chiamato a eliminare i dati appena finisce lo scopo per cui li ho raccolti.

6.1.2 Impatto della normativa

Il GDPR avrà un impatto diretto su ciascuno Stato membro, che a sua volta sarà tenuto a rispettare le norme applicate uniformemente all'interno dell'UE. Per questo motivo la sua attuazione da un lato richiederà alle aziende e agli enti pubblici una profonda revisione dei propri sistemi di gestione dei dati e, dall'altro, incrementerà nella società la consapevolezza dei problemi relativi alla protezione dei dati personali.

Le aziende che non si adeguano alle previsioni del GDPR entro la scadenza sono soggette a sanzioni fino a 20 milioni di euro, o fino al 4% del volume d'affari globale registrato nell'anno precedente. È inoltre previsto il diritto all'azione risarcitoria da parte di chiunque subisca un danno materiale o immateriale causato dalla violazione della normativa.

La protezione dei dati personali costituisce già una priorità per molti soggetti, ma il periodo di transizione che precede la data di applicazione di questo regolamento è fondamentale per molti individui, organizzazioni, imprese e servizi che operano nell'UE. Infatti, queste categorie dovranno analizzare il loro approccio alla protezione dei dati al fine di individuare eventuali discrepanze tra i metodi applicati e i requisiti imposti dal GDPR. A tal fine, le aziende dovranno porre la protezione dei dati personali al centro dei loro processi interni

e potenziare la comunicazione aziendale tramite programmi di formazione specifici che garantiscano un'adeguata preparazione per coloro che hanno accesso ai dati personali degli utenti[5].

La severità delle sanzioni rende evidente l'importanza di sensibilizzare tutti gli operatori sulla necessità di adeguarsi al GDPR. Oltre alle conseguenze pecuniarie, la compromissione della sicurezza dei dati e la violazione della normativa sul trattamento dei dati riservati possono avere conseguenze non solo pecuniarie, ma anche sulla perdita di immagine, la svalutazione del marchio e la perdita di avviamento dell'impresa.

Data breach – Evento che mette a rischio, rendendoli accessibili o pubblici, i dati personali di un individuo, quali, ad esempio, dati anagrafici, informazioni medico/sanitarie o finanziarie, copie di documenti di identità, dati relativi alle carte di credito, etc. Le cause principali di un Data breach sono tipicamente ascrivibili ad attacchi cyber, a vulnerabilità presenti nei sistemi e/o a errori umani.

Infine, non è da sottovalutare il rischio che, attraverso azioni collettive risarcitorie riservate a chiunque subisca un danno, materiale o immateriale, per una violazione della normativa dall'art. 82, si possano subire condanne per importi ingenti, anche a fronte di danni individuali esigui, in ragione del numero di vittime coinvolte nei *data breach*, spesso dell'ordine di decine di migliaia o di decine di milioni di persone.

L'attuazione del nuovo regolamento rappresenta quindi un passaggio chiave per le normative sul trattamento dati e permetterà un maggior controllo sull'utilizzo dei dati personali. Vi è, però, il reale rischio che gli strumenti normativi previsti dal GDPR non vengano pienamente utilizzati dai cittadini per via di una scarsa consapevolezza dei rischi di protezione dei dati personali a cui essi sono soggetti ogni volta che compiono una qualsiasi azione mediata da Internet: dall'accesso a servizi web-based o mobile (email, e-banking, e-commerce, etc.) all'utilizzo di dispositivi sempre più smart (smartwatch, fitness tracker, etc.). Questi rischi sono ulteriormente ampliati se si considera la mole di dati personali e sensibili che ogni giorno vengono inseriti nelle piattaforme social, quali Facebook e Twitter. Occorre quindi, da un lato, come illustrato nei dettagli nella sez. 6.3, aumentare la consapevolezza dei rischi di protezione dei dati personali sui social media e, dall'altro, prevedere adeguate regolamentazioni delle modalità di informazione dei diritti degli utenti da parte dei provider di servizi.

[5] `http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili`

6.1.3 Attuazione della normativa

Il 13 dicembre 2016 il Gruppo dei Garanti UE (WP 29) ha rilasciato tre documenti con indicazione e raccomandazioni in vista della prossima applicazione da parte degli Stati membri del GDPR. Le Linee Guida[6] sono state approvate nel testo definitivo in data 5 aprile 2017.

Per l'Italia, si rileva quindi la necessità di procedere rapidamente nell'adozione del regolamento GDPR per quanto riguarda sia gli aspetti normativi sia di consapevolezza delle aziende.

Per quanto riguarda gli aspetti normativi, al momento in cui si scrive, l'Autorità Garante per la Protezione dei dati personali non ha diffuso informazioni riguardo i codici di condotta destinati a integrare il GDPR con disposizioni specifiche e di dettaglio. Queste disposizioni hanno un ruolo fondamentale in quanto il rispetto delle prescrizioni di dettaglio previste determinerà la presunzione di conformità in caso di procedimento di infrazione.

Per quanto riguarda la predisposizione di codici di comportamento e strumenti tecnologici volti a fornire supporto alle imprese per l'attuazione delle norme previste nel GDPR si segnalano alcune iniziative presenti nel panorama europeo che possono rappresentare un'utile base di riferimento. In particolare, il codice adottato da CISPE.cloud[7] fornisce un valido esempio per tutti quegli operatori che offrono servizi di cloud computing; la Confindustria danese ha inoltre approvato delle Linee Guida[8] per l'attuazione della GDPR a livello imprenditoriale che intendono offrire alle imprese danesi indicazioni sui controlli che supportano l'implementazione dei requisiti della normativa.

Occorre infine evidenziare come l'adozione congiunta delle due normative GDPR e NIS (vedi sez. 1.2.1) introduca obblighi di comunicazione degli incidenti di sicurezza, da un lato per tutelare i titolari di dati personali oggetto di attacco (GDPR), dall'altro per la "protezione sistemica" delle infrastrutture critiche nazionali ed europee (NIS). Lo sviluppo o la trasformazione di queste funzioni non sono dunque ulteriormente procrastinabili (scadenza maggio 2018). In particolare, si sta delineando un'evoluzione verso il cosiddetto *Next Generation SOC*, nel quale un ruolo determinante è svolto da strumenti di *soft law* e fonti di autoregolamentazione di categoria, attraverso regole di correlazione che includono metodi e tecniche di analisi business oriented e, soprattutto, sono integrabili con strumenti di monitoraggio predisposti per i Big Data.

[6] `http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3815707`

[7] `https://cispe.cloud/code-of-conduct/`

[8] `https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen_engelsk.pdf`

Security Operations Center (SOC) – Centro per la fornitura di servizi finalizzati alla sicurezza dei sistemi informativi interni a un'azienda o di clienti esterni. Le tipologie di servizi offerti tipicamente includono: (i) gestione delle funzionalità di sicurezza legate all'infrastruttura IT (rete, sistemi e applicazioni); (ii) monitoraggio dell'infrastruttura IT per individuare tempestivamente tentativi di intrusione o uso improprio dei sistemi; (iii) controllo per migliorare il livello di protezione attraverso *security assessment* ed *early warning*. Pur avendo ruoli e finalità tra loro diversi, in alcuni casi i SOC fungono anche da CERT (si veda il box a pag. 20).

6.1.4 Obiettivi

In un contesto aziendale, l'adeguamento delle procedure di trattamento di dati personali e di informazioni sensibili alle regolamentazioni indicate nel GDPR può nei fatti realizzarsi in due modi: la personalizzazione di tecnologie esistenti che hanno già in sé sviluppata una parte della logica di business oppure la realizzazione ex-novo di algoritmi innovativi. Gli obiettivi implementativi da perseguire sono i seguenti:

- Identificare strumenti e tecnologie di *data discovery* in grado di riconoscere, sulla base di regole euristiche, le basi dati all'interno dell'intero sistema informativo in cui sono presenti le informazioni in perimetro GDPR a cui applicare i requisiti della normativa.
- Sviluppare strumenti e tecnologie che, analizzando i processi di ciclo di vita del dato e dell'informazione, siano in grado di segnalare e rintracciare procedure che abbassino i livelli di protezione in termini di sicurezza o che rendano possibili violazioni delle politiche di protezione dei dati personali. Questo strumento deve, dunque, poter valutare quanto l'implementazione di una procedura di trattamento dei dati esponga l'impresa a un rischio di violazione del GDPR.
- Sviluppare metodologie e strumenti integrati con le best practice in cybersecurity. In particolare integrare framework di gestione del rischio cyber, come il *Framework Nazionale di Cybersecurity* [10], con le metodologie imposte dalla GDPR. Molte delle best practice del Framework corrispondono infatti a pratiche di attuazione di GDPR. Una visione unificata delle politiche di cybersecurity e di protezione dei dati personali fornisce una vista integrata sia nel processo di valutazione del rischio sia nelle iniziative di adeguamento e remediation, contribuendo a sviluppare sinergie progettuali e a migliorare l'efficienza degli investimenti.
- Realizzare una regolamentazione (*recommender*) con semplici regole che siano di supporto alle imprese nel disegno di procedure di accesso e gestione dell'informazione che rispettino i requisiti del GDPR. Il recommender deve avere la capacità di astrarsi dalle specifiche tecnologie e

procedure utilizzate e guidare l'utente nella definizione di un adeguato trattamento del dato in relazione sia alle sorgenti del dato/informazione, sia alle applicazioni che dovranno averne accesso o gestiranno il suo ciclo di vita.

6.2 Formazione

Una delle ragioni principali del successo degli attacchi informatici in vari ambiti, ormai quotidianamente riportati anche dalla stampa non specialistica, è la mancanza di forza lavoro adeguatamente qualificata nel settore della cybersecurity. La scarsità di professionisti con capacità adeguate rende vulnerabili aziende, PA e intere nazioni ed esaspera le difficoltà di gestione degli incidenti. Vari organismi specializzati prevedono una carenza di più di un milione e mezzo di unità di forza lavoro entro il 2020[9], evidenziando una domanda costantemente in crescita[10].

Anche l'Italia sconta la carenza di professionisti nell'area della cybersecurity, esacerbata dalla fuga di giovani, formati nelle nostre università, ma attratti all'estero da stipendi più appetibili. In assenza delle professionalità appropriate, il programma *Impresa 4.0* può diventare un boomerang per settori chiave della nostra economia: estendere al mondo manifatturiero il principio del "tutto connesso, sempre" porterà infatti a un significativo aumento del rischio che attacchi informatici riescano a sottrarre informazioni sensibili alle aziende e a comprometterne l'operatività.

Per ridurre tali rischi sono necessari significativi investimenti per formare esperti di sicurezza con solide competenze tecniche in grado di: (i) definire politiche, strategie e programmi di protezione e controllo per garantire la sicurezza dei dati, delle reti e dei sistemi; (ii) gestire situazioni, eventi e persone in presenza di attacchi cyber; (iii) contribuire a creare una cultura della sicurezza informatica nelle aziende e nella società.

Data la pervasività degli aspetti della cybersecurity in ambito professionale, educativo, accademico fino al contesto più ampio, cioè quello sociale, gli aspetti legati alla formazione sul tema devono pertanto essere affrontati lungo sei direttrici complementari:

[9] http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[10] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

1. *Alta formazione* — Finalizzata a fornire gli strumenti tecnici e metodologici fondamentali della cybersecurity mediante corsi di laurea, master universitari e programmi di dottorato offerti dai vari atenei;
2. *Educazione di base* — Finalizzata a fornire i *fondamentali* della cybersecurity a partire almeno dalle scuole medie di secondo grado, indipendentemente dall'indirizzo specifico del percorso scolastico, con l'obiettivo di porre le basi per una migliore comprensione della tematica e per stimolare lo sviluppo formativo verso corsi universitari di specializzazione;
3. *Formazione professionale* — Finalizzata alla formazione continua per tutte le professioni che sempre più dovranno confrontarsi con problematiche di cybersecurity;
4. *Ricerca di talenti* — Finalizzata alla ricerca di giovani talenti da indirizzare verso una carriera in cybersecurity, catalizzandone l'interesse mediante sfide informatiche, simulazioni in ambienti virtuali protetti e, in generale, attraverso iniziative che consentano di sperimentare un possibile contesto operativo e valutare le opportunità di crescita professionale;
5. *Addestramento* — Finalizzato a consolidare, migliorare e valutare le capacità operative degli operatori e delle procedure preposte al contrasto e alla gestione degli incidenti informatici all'interno delle organizzazioni;
6. *Formazione e sensibilizzazione dei cittadini* — Finalizzata a fornire ai cittadini le nozioni elementari di cybersecurity e i concetti base di quella che viene ormai comunemente chiamata *igiene-cyber* (*cyber-hygiene*).

Delle sei direttrici, le prime cinque vengono analizzate in questa sezione, mentre la sesta sarà affrontata in quella successiva.

6.2.1 Stato dell'arte

Alta Formazione Numerose prestigiose università straniere, fra cui MIT, Harvard, Cambridge, Carnegie Mellon, Georgia Institute of Technology, Imperial College, Eindhoven, ETH Zurigo e molte altre[11] offrono programmi di alta formazione in cybersecurity.

In Italia non siamo all'anno zero. Presso l'Università di Milano sono attive da anni una laurea Magistrale e una Triennale in Sicurezza Informatica. L'Università di Trento fa parte da alcuni anni di un consorzio all'interno dello European Institute of Innovation and Technology (EIT) che offre una laurea Magistrale in Security e Privacy. Dall'anno accademico 2017-2018, anche Sapienza

[11] `https://digitalguardian.com/blog/cybersecurity-higher-education-top-cybersecurity-colleges-and-degrees`

Università di Roma offre una Laurea Magistrale in Sicurezza Informatica. All'interno di vari corsi di Laurea Magistrali in Informatica o Ingegneria Informatica sono previsti o in corso di attivazione curriculum in cybersecurity. Queste iniziative sono accompagnate da numerosi master di primo e di secondo livello, accessibili rispettivamente dopo il conseguimento di una laurea triennale o magistrale o da corsi di perfezionamento come quello della Cyber Academy[12] dell'Università di Modena e Reggio Emilia. Per un quadro completo si rimanda alla indagine[13] svolta congiuntamente dal *Laboratorio Nazionale Competenze Digitali, Formazione e Certificazione* del CINI e dal *Laboratorio Nazionale di Cybersecurity* sempre del CINI. Questo secondo Laboratorio, inoltre, sta guidando varie iniziative di formazione e sensibilizzazione[14], declinando in ambito italiano quanto fatto dall'Association for Computing Machinery (ACM), che ha istituito una commissione per stilare orientamenti curriculari basati su una visione completa della cybersecurity, che tengano conto delle specifiche esigenze disciplinari per una formazione aperta e critica e del rapporto tra curriculum e tipologia della forza lavoro richiesta[15].

Educazione di base Numerosi paesi dedicano particolare attenzione a questi aspetti; ad esempio in Gran Bretagna sono stati investiti più di 20 milioni di euro nel *Cyber Schools Programme*[16] destinato ai giovani tra i 14 e i 18 anni, per incoraggiarli a occuparsi di queste tematiche e a sviluppare abilità che saranno sempre più importanti per difendere gli assi portanti dell'economia.

In Italia, al momento, nelle scuole superiori viene dato poco spazio alle problematiche di cybersecurity e tra le 34 azioni considerate nel Piano Nazionale per *La buona Scuola digitale*[17] non figura alcuna azione dedicata alla cybersecurity.

Ricerca di talenti Vi sono numerose iniziative internazionali per promuovere la diffusione di una cultura della cybersecurity facendo leva sulla competizione come stimolo per attrarre giovani talenti. Ad esempio, in Gran Bretagna, sotto il brand *CyberFirst*[18], il governo supporta la crescita della prossima gene-

[12] http://cyber.unimore.it/

[13] https://www.consorzio-cini.it/index.php/it/lab-cfc/59-italiano/laboratori/lab-cfc/notizie-in-evidenza/1183-il-laboratorio-cfc-e-l-osservatorio-delle-competenze-digitali-2017

[14] https://www.consorzio-cini.it/index.php/it/labcs-home/formazione-in-cyber-security-in-italia

[15] https://www.csec2017.org

[16] https://www.gov.uk/guidance/cyber-schools-programme

[17] http://www.istruzione.it/scuola_digitale/allegati/Materiali/pnsd-layout-30.10-WEB.pdf

[18] https://www.ncsc.gov.uk/new-talent

razione di esperti di cybersecurity attraverso uno schema di corsi, apprendistati e gare per giovani dagli 11 ai 17 anni.

Tra le iniziative di formazione più popolari vi sono certamente le competizioni in stile *Capture-The-Flag* (CTF) (si veda il box a pag. 76). Paesi come USA, Australia, UK, Austria, Germania, Svizzera, Spagna, Romania organizzano da alcuni anni competizioni che selezionano i migliori candidati per formare le squadre nazionali.

ENISA organizza annualmente la *European Cybersecurity Challenge* (ECSC), una competizione dedicata alle squadre nazionali europee alla quale, dal 2017, partecipa anche l'Italia sotto l'egida del CINI e del MISE.

CyberChallenge.IT[19] è il primo programma italiano di ricerca di giovani talenti in cybersecurity promosso dal Laboratorio Nazionale di Cybersecurity del CINI. Il progetto punta a far emergere le eccellenze in materia di cybersecurity fra gli studenti delle scuole superiori o dei primi anni universitari. L'edizione 2017 ha visto 700 domande di partecipazione provenienti da tutta Italia, mentre l'evento del 2018 proporrà corsi di addestramento presso 8 sedi universitarie italiane e culminerà nel primo campionato italiano in cybersecurity. Parallelamente, l'iniziativa punta a formare giovani per la squadra italiana che parteciperà all'ECSC 2018.

Addestramento I *Cyber Range* (si veda il box a pag. 35) possono giocare un ruolo importante per la formazione a tutti i livelli e vari Stati li stanno utilizzando per la formazione in cybersecurity sia civile sia militare. EDURange[20] è una piattaforma finalizzata alla costruzione di scenari e percorsi formativi individuali. L'Arizona Cyber Warfare Range[21] offre percorsi di complessità crescente per l'addestramento individuale. Il Michigan Cyber Range[22] non si limita a riprodurre l'infrastruttura ICT di una singola organizzazione, ma include un'intera città virtuale (Alphaville). Le esercitazioni Locked Shields, eseguite utilizzando il Cyber Range della NATO in Estonia, supportano attività addestrative molto sofisticate dove un team d'attacco, *red team*, si contrappone a molteplici *blue team*, i quali hanno il compito di difendere lo scenario loro assegnato dagli attacchi lanciati dal red team.

6.2.2 Sfide

Le iniziative esistenti in ambito di formazione nel nostro Paese sono purtroppo ancora insufficienti e scontano due grosse carenze: il numero limitato di ricer-

[19] `https://www.cyberchallenge.it`
[20] `http://blogs.evergreen.edu/edurange`
[21] `http://azcwr.org`
[22] `http://www.merit.edu/cyberrange`

catori esperti che possano svolgere funzioni di docenza e un insufficiente coordinamento nazionale tra accademia, scuole superiori, parte pubblica e parte privata per definire le figure professionali necessarie. Inoltre, a livello universitario, benché l'attivazione di nuovi percorsi formativi sia un'esigenza particolarmente sentita, il rispetto del soddisfacimento dei requisiti minimi in termini di personale docente imposto dalla normativa vigente fa sì che, in varie sedi, l'attivazione di nuovi corsi di laurea di cybersecurity implicherebbe la chiusura di alcuni dei corsi già esistenti.

Dal punto di vista dei programmi di formazione per giovani talenti, la sfida principale è quella di intercettarli in una fase del loro percorso di studi in cui non abbiano ancora deciso una direzione definita su cui investire le proprie capacità, presentando loro le possibilità di carriera e gli aspetti stimolanti delle attività in cybersecurity. Questo può essere perseguito attraverso il coinvolgimento degli studenti delle scuole superiori e alla promozione della partecipazione femminile, sfatando il principio per cui la cybersecurity è un dominio per soli uomini.

Per quanto riguarda invece la formazione professionale, è necessario prevedere strumenti di formazione continua. Addestrare sul campo i dipendenti attraverso formazione ed esercitazioni pratiche 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 e il personale esecutivo.

Nelle organizzazioni aziendali private questo tema viene affrontato con diversi livelli di maturità: molto si può ancora fare in quelle realtà medio-piccole che spesso dispongono di minori capacità di investimento ma che rappresentano l'asse portante dell'economia italiana. Ma ancora di più è necessario prevedere uno sforzo su questo tema nel contesto pubblico, dove spesso l'età lavorativa dei dipendenti, la stratificazione dei ruoli ricoperti negli anni o la carenza di fondi per la formazione non contribuiscono allo sviluppo di una sensibilità ai temi della sicurezza: la sfida diventa ancora maggiore in quegli ambiti pubblici che rappresentano infrastrutture critiche per il Paese, quale, ad esempio, la sanità.

In particolare, la preparazione degli operatori che più direttamente devono fronteggiare situazioni critiche (es. attacchi cyber, incidenti di sicurezza, *data breach*, etc.) rappresenta elemento cruciale non solo per una efficace ed efficiente gestione dell'evento quando già occorso, ma anche in ottica di prevenzione e di *lesson learned*. Esempi e best practice di riferimento possono essere presi da settori altamente critici (e.g., in ambito nucleare, aerospaziale, petrolifero, etc.) dove da sempre viene attuata una formazione continua basata su esercitazioni, opportunamente studiate per il contesto specifico mirate a garantire il più alto livello di *resilienza*.

Per questo, sviluppare tecniche e strumenti capaci di automatizzare attività

di supporto alle esercitazioni su possibili attacchi rappresenta una sfida importante. I Cyber Range di prossima generazione possono svolgere questo compito, adeguando la compessità degli scenari considerati ai compiti delle figure professionali coinvolte nelle esercitazioni.

6.2.3 Obiettivi

Tra gli obiettivi più significativi da raggiungere nell'ambito della formazione vanno certamente inclusi i seguenti:

- *Piano per l'alta formazione in cybersecurity* — Occorre prevedere un piano specifico per definire, in modo coordinato con la parte pubblica, le aziende private e le università, figure professionali formate tramite master, corsi di laurea, e corsi di dottorato che, partendo dalle attuali lauree triennali e magistrali in informatica e ingegneria informatica, siano in grado di fornire gli strumenti tecnici e metodologici fondamentali della cybersecurity. In particolare:
  - Le Università dovranno:
    - ripensare i *curriculum dei corsi di base in informatica o ingegneria informatica*, introducendo la dimensione della sicurezza fin dall'inizio del percorso di studi;
    - attivare *nuovi insegnamenti* universitari su tematiche di cybersecurity da inserire nei curriculum esistenti;
    - attivare *corsi di laurea*, soprattutto *magistrali*, per formare il personale necessario per garantire una visione di sistema e presidiare contesti eterogenei e in continuo cambiamento, tenendo conto di tutti i livelli di rischio;
    - attivare *corsi di dottorato* per formare esperti e ricercatori in grado di capire gli sviluppi della ricerca nel settore della cybersecurity a livello internazionale, prevedere dinamiche di attacco e creare nuovi strumenti di difesa passiva e attiva;
    - collaborare alla realizzazione del *Cyber Range nazionale per la formazione* illustrato nel prosieguo di questa sezione;
    - attivare *master* che puntino a formare esperti immediatamente operativi, avendo come target non solo neo-laureati, ma anche personale già in organico negli enti e nelle aziende, da sensibilizzare e riqualificare sulle tematiche di cybersecurity.
    - candidarsi a partecipare come nodi locali ai programmi nazionali di ricerca e formazione di giovani talenti, quali CyberChallenge.IT.

  - Il Ministero dell'Istruzione, Università e Ricerca dovrà definire un piano speciale che, partendo dall'attuale *situazione di emergenza*, preveda l'assegnazione di risorse specifiche (docenti, ricercatori, finanziamenti) per lo sviluppo della formazione superiore e della ricerca in cybersecurity. Questo strumento, come dettagliato nella sez. 9.5, è indispensabile sia per evitare che nostri ricercatori vadano in Paesi dove la loro professionalità viene meglio riconosciuta e remunerata sia per incoraggiare il rientro o la venuta dall'estero di ricercatori altamente qualificati.

- *Piano per l'educazione di base in cybersecurity presso le Scuole* — La strategia di lungo termine deve prevedere l'arricchimento dei programmi presso le scuole di ogni ordine e grado, a partire dal momento in cui gli alunni cominciano a utilizzare in modo autonomo smartphone e dispositivi connessi in rete. L'offerta delle adeguate nozioni di sicurezza, dovrà avere il duplice scopo di introdurre i concetti fondamentali della sicurezza informatica e di rendere i ragazzi consapevoli dei rischi associati a un uso poco accorto della rete e delle applicazioni utilizzate sui loro dispositivi. Per questo è importante:

  - promuovere partnership pubblico-privato per fornire agli studenti incentivi economici (ad esempio mediante borse di studio) per ridurre i costi della formazione in cybersecurity;
  - sponsorizzare programmi di formazione per la ricerca di giovani talenti, promuovendo la partecipazione italiana alle competizioni internazionali come la European Cybersecurity Challenge (ECSC);
  - introdurre nei programmi scolastici elementi obbligatori di sicurezza informatica, introducendo i partecipanti ai concetti di identità digitale, minacce e rischi, strumenti e comportamenti per l'utilizzo sicuro della rete, etc.;
  - predisporre formazione ad hoc per i docenti individuati come potenziali formatori sul tema, stimolando nello stesso tempo lo sviluppo di nuove professionalità all'interno del corpo insegnante;
  - incentivare e potenziare opportunità di esperienze formative nell'ambito di Alternanza Scuola-Lavoro[23] che, sfruttando il connubio sapere e saper fare, offrano ai partecipanti la possibilità di avvicinarsi concretamente alle problematiche della cybersecurity;
  - evidenziare come la trasformazione digitale, che ha cancellato alcune tipologie di lavoro, ne abbia create altre e come le opportunità di impiego e di carriera nel campo della sicurezza informatica siano numerose.

[23] `http://www.istruzione.it/alternanza/`

- *Piano per la formazione professionale in cybersecurity* — Il problema della formazione professionale è ampio e complesso perché, come avviene per la sicurezza sul lavoro, investe non solo i tecnici del settore, ma tutti i dipendenti di una qualunque realtà aziendale, sia nel contesto privato sia nella PA. La formazione e l'aggiornamento professionale attraverso una *formazione professionale permanente* assumono pertanto un ruolo cruciale. Ogni singolo addetto deve infatti comprendere che un errato comportamento in termini di sicurezza può rappresentare l'anello debole della catena di difesa e facilitare accessi malevoli ai sistemi informatici e ai dati rilevanti della propria organizzazione. Al riguardo, in particolare, le aziende e la PA dovranno:

  – mettere in atto programmi di formazione e aggiornamento periodico sulla cybersecurity dedicati a personale non tecnico, come dirigenti, manager, e membri dei vari board;

  – mettere in atto programmi di formazione per colmare le lacune in cybersecurity del personale tecnico di livello intermedio e senior;

  – partecipare come sponsor alle iniziative di formazione dei giovani talenti, assicurandosi il contatto con potenziali candidati da inserire nel proprio organico;

  – definire e attuare specifici programmi di formazione su gestione della sicurezza e del rischio cyber per i profili professionali operanti nel settore dei sistemi di controllo industriali, per far fronte alle complesse sfide che emergono allorquando ci si pone l'obiettivo di proteggere tali sistemi da attacchi informatici;

  – sviluppare piattaforme per la condivisione di informazioni aggiornate su vulnerabilità e minacce rilevate, sia all'interno della singola organizzazione sia lungo l'intera Supply chain. Tali piattaforme devono permettere di migliorare la qualità della formazione e incrementare il livello di consapevolezza sui possibili rischi di sicurezza.

- *Piano Nazionale di formazione e sensibilizzazione dei cittadini* — Finalizzato a fornire alla popolazione le nozioni elementari di cybersecurity e i concetti base della cyber-hygiene; questo piano è analizzato nei dettagli nella sezione successiva.

- *Ricerca di giovani talenti* — Al fine di individuare giovani talenti, è importante non solo coinvolgere gli studenti in una fase iniziale della loro carriera, ma anche promuovere la costruzione di una comunità di esperti che costituisca una piattaforma per il reclutamento dei profili più adatti ai vari ruoli professionali in cybersecurity. Questo può avvenire seguendo

l'andamento della carriera dei giovani che escono dai programmi di formazione iniziali come CyberChallenge.IT[24]. Un primo obiettivo da considerare è il loro coinvolgimento nelle attività di formazione delle classi successive (secondo un modello di *peer education*), per formare nuove generazioni di educatori. Un secondo obiettivo è la promozione di lauree, master e dottorati in cybersecurity. Un aspetto importante e concreto in questo contesto è la realizzazione di un database di giovani esperti e delle loro competenze, mantenuto aggiornato a supporto di un più efficace incontro tra domanda e offerta professionale. Il programma CyberChallenge.IT è il punto di partenza per realizzare questa piattaforma di sviluppo della comunità di cybersecurity italiana del futuro.

- *Cyber Range nazionale per la formazione* — Occorre mirare alla realizzazione di un Cyber Range nazionale dedicato agli aspetti di formazione. Questo potrà abilitare un insieme di attività di grande rilevanza per il Paese: la condivisione del Cyber Range tra mondo della ricerca, PA e mondo produttivo consentirà infatti:
  - all'accademia di potenziare i programmi formativi sulla cybersecurity con sessioni pratiche che permetteranno agli studenti di sperimentare e acquisire capacità immediatamente spendibili nel mondo lavorativo;
  - al mondo della ricerca di sperimentare e valutare l'efficacia di tecniche innovative di cybersecurity in un ambiente controllato;
  - alla PA e al settore privato di addestrare il personale preposto alla cyber defence e di poter altresì valutare sperimentalmente l'efficacia degli strumenti di difesa che si prevede di acquisire.

6.3 Sensibilizzazione e cyber-hygiene

L'utilizzo di Internet è sempre più pervasivo, coinvolgente e, con il passare del tempo, aumenta sempre più il numero di dispositivi connessi in rete, così come le attività che è possibile realizzare con l'ausilio della rete. La rete è oggi, infatti, l'elemento che accomuna diversi contesti, rappresentando lo strumento di comunicazione privilegiato nell'ambito sia personale sia lavorativo: per tutti noi, ormai, la rete è l'infrastruttura su cui viaggiano i nostri dati personali, i dati delle aziende per cui lavoriamo, le nostre idee e i nostri interessi. Senza Internet non possiamo navigare nel Web, usare Facebook, cercare informazioni con Google, inviare e ricevere posta elettronica, spedire messaggi con WhatsApp, fare acquisti e prenotazioni on-line, accedere a molti servizi della PA.

[24] `https://www.cyberchallenge.it`

L'offerta di servizi on-line ha raggiunto straordinari livelli di varietà e diffusione grazie alla facilità d'accesso alle tecnologie mobili e al fiorire di nuove applicazioni in grado di rispondere anche ai bisogni di nicchia degli utenti. Servizi di home banking, di e-government, di sanità elettronica e di e-commerce sono entrati a pieno titolo nella vita dei cittadini che fanno uso del canale digitale per relazionarsi con organizzazioni pubbliche e private.

L'utilizzo esteso dei social media, inoltre, è favorito dalla facilità e dalla condivisione di dati e informazioni che queste piattaforme supportano: in questo contesto di apertura le "naturali" difese di un utente tendono ad abbassarsi a causa, da un lato, del fatto che la comunicazione è mediata da una tecnologia, e, dall'altro, delle aspettative di compiere attività divertenti o interessanti.

I pericoli In uno scenario così ricco di strumenti, di opportunità, e così aperto, la rete diventa spesso fonte di pericoli se non se ne conoscono in misura adeguata limiti e minacce e non si tengono in debito conto gli aspetti di sicurezza. I cittadini sono potenziali oggetti di attacco sia in quanto consumatori di prodotti e servizi digitali sia come membri di organizzazioni.

Siamo pertanto di fronte a un rischio sistemico difficile da gestire, soprattutto in assenza dei meccanismi di controllo tipici delle organizzazioni. Inoltre le limitazioni indotte dall'adozione di meccanismi di sicurezza possono scontrarsi con esigenze contrastanti come l'obiettivo di migliorare l'esperienza d'uso di prodotti e servizi. Un esempio in tal senso lo forniscono i sistemi federati di gestione delle identità, nei quali l'urgenza di raggiungere una massa critica di utenti offrendo servizi utili e immediati si scontra con la necessità di prevenire e individuare furti d'identità mediante articolate procedure per l'identificazione e l'autenticazione. Risulta inoltre difficile contrastare comportamenti indesiderati in contesti interorganizzativi regolati da accordi commerciali in cui le piattaforme digitali forniscono l'infrastruttura per veri e propri ecosistemi di servizi. Basti pensare al fenomeno delle frodi sui sistemi di pagamento mobili con le quali si sottraggono piccoli importi a milioni di utenti tramite sottoscrizioni inconsapevoli ad abbonamenti on-line, innescate tramite forme anche evolute di *phishing* (si veda il box a pag. 28).

Digital Divide aziendale Parafrasando il concetto del *digital divide generazionale*, nei contesti lavorativi si riscontra una evidente separazione tra quelle aziende in cui è preponderante l'utilizzo della tecnologia (nelle quali, quindi, parte del personale ha una competenza, talvolta anche molto approfondita, di strumenti informatici e di sicurezza) e quelle realtà aziendali dove invece l'utilizzo di strumenti tecnologici ricopre un ruolo marginale nello svolgimento dei compiti operativi dei dipendenti.

Interrelazione tra cittadino e mondo del lavoro I più noti attacchi cibernetici sono condotti su larga scala e interessano sia cittadini sia organizzazioni. Tuttavia non è corretto considerare distinti questi due insiemi. Infatti, molto spesso, i cittadini sono anche lavoratori che operano in ambienti digitalizzati in cui le sfere personali e professionali si intersecano esponendo il fianco a pericolosi cortocircuiti in cui la minaccia cibernetica può propagarsi mettendo a rischio le risorse economiche, la protezione dei dati personali, la redditività e la sicurezza di infrastrutture critiche e dei sistemi democratici. L'esposizione al rischio aumenta quando strumenti lavorativi vengono utilizzati anche per attività personali: in questi casi, infatti, gli attacchi possono concretizzarsi non solo in violazione della protezione dei dati personali ma anche in nuove vulnerabilità per l'impresa per cui le vittime lavorano.

Social Engineering (Ingegneria Sociale) – Insieme di tecniche atte a raggirare una persona al fine di ottenerne informazioni riservate. Queste possono essere poi utilizzate in modo fraudolento per portare a termine un attacco, utilizzando strumenti e tecnologie diverse.

Il mondo del lavoro, quindi, riveste un ruolo importante per la sensibilizzazione dei dipendenti ai temi della sicurezza non solo per i fini aziendali di protezione degli asset informativi delle organizzazioni in cui essi operano, ma anche come contributo alla formazione di base che i dipendenti portano nella propria vita personale come privati cittadini. La conoscenza delle minacce derivanti non solo dagli strumenti digitali e dalla rete attraverso malware, ma anche da tecniche di *social engineering*, che si acquisisce nell'ambito lavorativo contribuisce in modo più ampio al rafforzamento della consapevolezza sociale del Paese sui temi della cybersecurity.

6.3.1 Stato dell'arte

A livello europeo, le linee di intervento definite nell'ambito delle competenze digitali di base si fondano su quanto previsto dal pilastro 6 dell'Agenda Digitale Europea (DAE) *Enhancing digital literacy, skills and inclusion*[25] e hanno due obiettivi primari:

- *realizzare la cittadinanza digitale*: accesso e partecipazione alla società della conoscenza, con una piena consapevolezza digitale;
- *realizzare l'inclusione digitale*: uguaglianza delle opportunità nell'utilizzo della rete e per lo sviluppo di una cultura dell'innovazione e della creatività.

[25] `http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/enhancing-digital-literacy-e-skills-and-e-inclusion`

In linea con questi obiettivi, in Italia diversi organismi, a vario titolo, operano per la promozione di iniziative formative indirizzate alla sicurezza. Ad esempio, il *Dipartimento delle Informazioni per la Sicurezza* (DIS) ha promosso una serie di iniziative destinate agli studenti italiani delle scuole medie superiori e delle università per diffondere la cultura della sicurezza attraverso il dialogo con le nuove generazioni. Al riguardo è particolarmente rilevante la campagna *Be aware Be digital*[26] recentemente avviata.

6.3.2 Sfide

In uno scenario così complesso, è necessario un intervento strutturato verso gli utenti finali che tenga conto delle differenze legate alle diverse fasce di età, per i minori adolescenti, i giovani e gli adulti.

Gli adolescenti si muovono con facilità in rete, ma spesso non ne conoscono a fondo meccanismi e limiti e soprattutto non comprendono lo stretto legame esistente tra le azioni nel mondo di Internet e la vita reale; ne sono testimonianza i fatti, talvolta tragici, in cui si trovano coinvolti a causa di fenomeni di cyberbullismo nei social media. Le famiglie si sentono impreparate ad affrontare con competenza il tema e i genitori spesso non sono in grado di dare risposta agli allarmi lanciati dagli adolescenti. La scuola si appoggia alle diverse iniziative esterne oggi esistenti, promosse da aziende, organizzazioni no-profit o dalle stesse istituzioni: tutte iniziative che però, pur nella loro grande utilità, soffrono di una mancanza di continuità e di limitata scalabilità sul territorio nazionale.

I giovani che si affacciano al mondo del lavoro hanno sviluppato nel tempo comportamenti e abitudini, come ad esempio la predisposizione a condividere facilmente informazioni o acquisire informazioni in rete, senza un necessario filtro di pensiero critico. Tali comportamenti possono procurare loro dei rischi sia a livello personale sia per le aziende presso le quali sono impiegati. Servono iniziative strutturate per formare adeguatamente i giovani a diventare dei veri e propri *cittadini della rete*: anche coloro che non hanno seguito percorsi curricolari a indirizzo tecnologico devono poter godere di una formazione digitale in materia di sicurezza, adeguata a un utilizzo maturo degli strumenti tecnologici, basato su comportamenti consapevoli dei rischi e delle proprie responsabilità in rete. Per questo non sono sufficienti interventi spontanei: è necessario pensare a una vera e propria *educazione civica* alla rete, attraverso un programma educativo di portata nazionale, a tutti i livelli, che includa al suo interno la formazione e la sensibilizzazione al tema della sicurezza in Internet.

Gli adulti, in generale, mancano di una percezione del rischio cyber nella sua accezione più ampia. Di conseguenza, non adottano quelle che si possono considerare le regole e i comportamenti base della cosiddetta *cyber-hygiene*.

[26] `https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/be-aware-be-digital.html`

Anche quando tali regole sono conosciute si tende ad aggirarle in favore di un più facile accesso a servizi e informazioni. Si rimane pertanto esposti al pericolo di attacchi su larga scala, che sfruttano comportamenti ingenui quali, a titolo di esempio, le vulnerabilità derivanti dal mancato sistematico aggiornamento del software dei sistemi, dai PC ai tablet agli smartphone. Al riguardo è infatti importante evidenziare come la relazione tra la vulnerabilità dei sistemi e le contromisure di sicurezza non sia statica, bensì dinamica: l'evoluzione delle tecnologie e il continuo adattamento degli strumenti alle esigenze degli utenti rendono necessario un aggiornamento sistematico del software, che in molti casi, per le ragioni più diverse, non è possibile effettuare in modo automatico. Occorre infine sottolineare l'importanza del *comportamento* dei singoli: le protezioni tecnologiche più sofisticate e perfettamente aggiornate sono di fatto del tutto inutili se ciascuno di noi non adotta *comportamenti* sicuri: a titolo di esempio, posso anche usare esclusivamente dispositivi con gli antivirus più aggiornati, ma se poi non sono in grado di riconoscere una mail di phishing e vado su un sito "fake" fornendo le mie credenziali a organizzazioni malevoli, di fatto sto distribuendo a tutti le mie chiavi di casa ...

6.3.3 Obiettivi

Nel contesto nazionale che, come previsto da *Agenda Digitale Italiana*[27], richiede un intervento significativo sul fronte dell'alfabetizzazione digitale della popolazione, è necessario prevedere un percorso per la realizzazione di campagne mirate all'utilizzo sicuro della rete e degli strumenti di comunicazione, per garantire la sicurezza dei singoli e, di riflesso, dell'intero sistema Paese. Per questo, occorre agire con interventi orientati a informare gli utenti al fine di aumentarne la consapevolezza in materia di sicurezza e incidere in modo significativo sui loro comportamenti nell'utilizzo degli strumenti di comunicazione digitale.

È quindi necessario dare vita a un'azione di sistema per una formazione sull'utilizzo sicuro della rete, come iniziativa di accrescimento delle conoscenze tecnologiche e di sicurezza sociale per il Paese, perseguendo i seguenti obiettivi:

- *Framework Nazionale per la sensibilizzazione e l'aggiornamento permanente* — Sviluppare un percorso strutturato a livello nazionale per la definizione di un Framework come modello di riferimento per un aggiornamento permanente sui temi della sicurezza in rete e dell'utilizzo consapevole degli strumenti digitali, all'interno del quale collocare l'azione educativa. Il Framework deve definire un insieme di "contesti" omogenei e, per ciascuno di questi, identificare, grazie al contributo di team di specialisti necessariamente multidisciplinari: (i) obiettivi da raggiungere,

[27] `http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana`

definendo, dove applicabili, anche i relativi Body of Knowledge e i Syllabus; (ii) sequenze di azioni da mettere in atto per raggiungerli; (iii) piani operativi dettagliati, in termini sia di tempistiche sia di risorse.

- *Controlli minimali per cittadini e cyber-hygiene* — (i) Definire un insieme di controlli minimali per cittadini e un insieme di regole base di cyber-hygiene che devono essere sistematicamente seguite. (ii) Identificare e attivare i meccanismi più adatti per la massima diffusione di questi controlli minimali e delle regole base di cyber-hygiene attraverso campagne pubblicitarie e di informazione di massa, sia sui media tradizionali (giornali, radio, tv) sia sui social media.

- *Cooperazione pubblico-privato-terzo settore* — Promuovere e incentivare un modello virtuoso di cooperazione tra pubblico, privato e terzo settore per la valorizzazione e la messa a sistema delle iniziative oggi già atto, nelle forme più disparate, sul territorio nazionale, tra quanti (aziende, organizzazioni, professionisti, associazioni di volontariato, etc.) stanno erogando iniziative formative all'interno della propria mission aziendale o sociale. Questo richiede, a titolo di esempio, la condivisione sia di best practice sia del molto materiale già oggi disponibile, a seguito di una validazione rispetto alle direttive del Framework di cui sopra.

6.4 Gestione del rischio cyber per le imprese

La gestione del rischio cyber assume nel tempo un ruolo di sempre maggiore importanza: quanto più il rischio cyber viene percepito come di livello aziendale, tanto più i responsabili si adoperano per comprenderne gli impatti anche in assenza di una preparazione tecnica specifica in materia.

Il Laboratorio Nazionale di Cybersecurity del CINI ha già lavorato nel corso degli ultimi anni per fornire al Paese strumenti di gestione del rischio che fossero riconosciuti sia da aziende private, indipendentemente dalla loro dimensione, sia da PA, nonché dalle società di consulenza che possono utilizzarli nell'erogazione dei propri servizi di advisory.

Questi strumenti si concretizzano in: (i) il *Framework Nazionale per la Cybersecurity* [10], pubblicato nel 2016 in collaborazione con diversi attori industriali e governativi e adatto ad aziende che, indipendentemente dalla loro dimensione, abbiano già una qualche preparazione in termini di sicurezza; (ii) i *Controlli Essenziali di Cybersecurity* [11], pubblicati nel 2017.

Tutte queste azioni sono state finalizzate a uniformare il linguaggio cyber nei diversi contesti, per una immediata comprensione e un più agevole processo di adozione.

6.4.1 Obiettivi

Alla luce delle esperienze maturate, vengono qui presentate due proposte progettuali basate su questi due documenti e se ne propone la stesura di un terzo, con l'obiettivo di colmare un settore, quello dei singoli cittadini, ancora privo di strumenti dal punto di vista della gestione del rischio cyber.

- *Contestualizzazioni del Framework Nazionale per grandi organizzazioni* — Il Framework Nazionale per la Cybersecurity [10] può essere adattato ai diversi contesti eterogenei presenti nel panorama nazionale tramite la creazione di apposite *contestualizzazioni*. Aziende di settori merceologici diversi hanno infatti, in ambito cyber, requisiti e criticità diverse e peculiari. Questo vuol dire che a seconda di un insieme di fattori (quali settore merceologico, tipo di servizi o prodotti, dimensione, esposizione al rischio, etc.), l'insieme delle pratiche di sicurezza da mettere in atto e i processi necessari possono essere anche molto diversi tra loro.

  Le contestualizzazioni del Framework sono strumenti di altissimo valore, in quanto permettono di strutturare la gestione del rischio cyber delle organizzazioni target. La creazione di una contestualizzazione è tuttavia un'operazione complessa che richiede sia un'elevata conoscenza del dominio applicativo sia una significativa padronanza del Framework Nazionale.

  Il progetto mira alla stesura di contestualizzazioni del Framework per:

  – grandi imprese (a seconda del settore merceologico, es. energetico, edilizia, telecomunicazioni);
  – grandi aziende ospedaliere;
  – grandi PA centrali (es. ministeri);

  a opera di partenariati privato-accademia per il primo caso, pubblico-privato-accademia per gli altri due.

  Le ricadute del progetto saranno molteplici: oltre a innalzare il livello di sicurezza generale del tessuto imprenditoriale e della PA italiana, si avrà una coerenza cross-settoriale nella gestione del rischio e un linguaggio cyber comune condiviso tra privato e pubblico, nonché tra privato e privato, che agevolerà la cooperazione e la condivisione dei requisiti.

- *Divulgazione, promozione e aggiornamento dei Controlli Essenziali per le PMI* — La definizione, l'aggiornamento e la promozione di *controlli essenziali* di cybersecurity per piccole e medie imprese rappresentano un elemento di fondamentale importanza per favorire la diffusione capillare della cultura della cybersecurity nella realtà imprenditoriale nazionale e per produrre una generale diminuzione dell'esposizione del mondo

produttivo al rischio di attacchi cyber. I controlli essenziali rappresentano infatti uno strumento attraverso cui definire un livello minimo di protezione da attacchi cibernetici e favorirne il raggiungimento da parte delle aziende, riducendo così la superficie di attacco e fornendo una base al consolidamento del tessuto produttivo nazionale nei confronti del rischio cibernetico.

Ciò va nella direzione di incrementare la sicurezza dello spazio cibernetico per le piccole e medie imprese, da una parte riducendo il rischio di perdite dovute a incidenti e attacchi, dall'altra aumentando il livello di fiducia di clienti e investitori nazionali e internazionali nei confronti del tessuto produttivo nazionale. Questo, da un lato, crea un vantaggio competitivo per le aziende, mentre, dall'altro, contribuisce alla creazione di un ecosistema di cybersecurity su cui impiantare iniziative più avanzate.

A livello nazionale, controlli essenziali di cybersecurity sono stati per la prima volta definiti nel *2016 Italian Cybersecurity Report*[28] pubblicato dal Laboratorio Nazionale di Cybersecurity del CINI e dal CIS Sapienza[29]. Tali controlli pongono l'attenzione su: identificazione di sistemi e servizi hardware e software utilizzati e relativi livelli di necessità o criticità, rispetto delle normative vigenti e gestione delle responsabilità, uso di soluzioni tecniche adeguate per la protezione dei dati, formazione e gestione del personale addetto, gestione degli incidenti e relativo ripristino. A valle della loro pubblicazione, il rispetto dei controlli essenziali di cybersecurity è stato sottoposto a indagine statistica dall'Università Politecnica delle Marche in collaborazione col CIS Sapienza. Da tale indagine è emerso che alcuni controlli risultano più difficili da soddisfare di altri, come il rispetto delle normative vigenti, l'adeguata formazione del personale e la rapida sostituzione o dismissione di software obsoleto.

Sulla base di tali premesse, occorre proseguire l'azione di divulgazione e promozione di controlli essenziali di cybersecurity. Inoltre, è necessario che tali controlli vengano periodicamente revisionati e aggiornati, al fine di tenere conto dell'evoluzione sia delle minacce sia del livello di cybersecurity di piccole e medie imprese. Tale azione va svolta considerando i livelli stimati di soddisfacimento dei singoli controlli essenziali e introducendo opportune azioni correttive relativamente ai controlli più critici.

Dopo una fase iniziale di adesione volontaria a tali controlli essenziali, occorre procedere alla definizione di una *certificazione nazionale* basata

[28] `http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf`

[29] `https://www.cis.uniroma1.it/`

sui controlli stessi, similmente a quanto fatto nel Regno Unito per i controlli noti come *Cyber Essentials*[30]. Un primo passo in tale direzione è stato fatto con l'emanazione, da parte di AgID, dell'elenco ufficiale di misure minime per la sicurezza ICT che sono di obbligatoria adozione per tutte le PA[31]. Analogamente, è auspicabile che il soddisfacimento di un numero minimo di controlli essenziali, e la relativa certificazione, diventino progressivamente un requisito obbligatorio per la fornitura, da parte di soggetti privati, di prodotti e/o servizi alla PA e non solo.

Il progetto di definizione, aggiornamento e certificazione di controlli essenziali per le PMI si pone i seguenti obiettivi pratici:

- Attivazione di un panel tecnico responsabile della definizione e dell'aggiornamento dei controlli essenziali. In tale contesto, le Università e gli Enti di Ricerca possono contribuire alla costituzione del panel e alle fasi di definizione e aggiornamento dei controlli essenziali, nonché alla pubblicazione dei controlli stessi e dei relativi documenti di accompagnamento. La PA può avere invece il ruolo di garante dell'ente certificatore e di soggetto deputato al rilascio delle relative certificazioni. Il ruolo delle aziende sarà invece quello di sottoporsi all'autovalutazione di rispondenza ai controlli essenziali e richiedere la relativa certificazione al fine di essere incluse nell'elenco pubblico di soggetti certificati.
- Aggiornamento e revisioni periodica della lista dei controlli essenziali e dei relativi documenti di accompagnamento.
- Creazione e mantenimento di un portale per la divulgazione dei controlli essenziali e l'autovalutazione di rispondenza ai controlli stessi.
- Definizione di un ente certificatore che, su richiesta dell'interessato, attui procedure di verifica della rispondenza ai controlli essenziali e ne certifichi l'esito.
- Mantenimento di un database pubblico di imprese che hanno ottenuto la certificazione di rispondenza ai controlli essenziali.

Le ricadute sulla società e sul tessuto produttivo si tradurranno in un generale innalzamento del livello di resilienza delle PMI e non solo, nonché nell'incremento di visibilità e attrattività di quei soggetti che hanno ottenuto e mantenuto la certificazione di rispondenza ai controlli essenziali.

[30] http://www.cyberessentials.org/

[31] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni

Dal punto di vista della ricerca, la creazione e l'aggiornamento di un benchmark di riferimento tramite i controlli essenziali offrirà spunti relativi alla definizione dei controlli stessi e alle loro relazioni con altri standard del settore, a livello sia nazionale sia internazionale.

6.5 Certificazioni sostenibili

Nelle società moderne, che continuano ad affidare alle tecnologie ICT crescenti quantità di informazioni e servizi aventi valore e criticità sempre più rilevanti, la certificazione della sicurezza ICT sta assumendo un ruolo molto importante. Le dichiarazioni dei fornitori di informazioni e servizi circa il loro livello di sicurezza hanno sempre più la necessità di essere integrate da verifiche da parte di soggetti terzi, eseguite, preferibilmente, in accordo a standard internazionali che godano di vasto riconoscimento. Anche a livello istituzionale, sia italiano sia europeo, la certificazione della sicurezza ICT è oggetto di attenzione, come dimostrano le recenti iniziative della Presidenza del Consiglio dei Ministri e della Commissione Europea. La prima, con il DPCM Gentiloni (illustrato nella sez. 1.3.1) e il *Piano Nazionale per la protezione cibernetica e la sicurezza informatica* del marzo 2017 (illustrato nella sez. 1.3.2), ha previsto, tra l'altro, la creazione di un nuovo centro di valutazione e certificazione per la componentistica da utilizzare nelle infrastrutture critiche e strategiche. La seconda, nella comunicazione congiunta al Parlamento e al Consiglio europeo del 13 settembre 2017, con la quale ha tracciato le linee della strategia europea nel campo della cybersecurity (*Cybersecurity Package*[32]), ha manifestato l'intenzione di proporre un *Framework europeo di certificazione della cybersecurity*[33]. Tale framework sarà applicabile a prodotti, servizi e/o sistemi e consentirà una modulazione del livello di certificazione adeguato al contesto applicativo. L'obiettivo della Commissione è duplice: evitare barriere doganali all'interno dell'EU dovute a certificazioni nazionali e abilitare la visione del *Digital Single Market* europeo.

6.5.1 Stato dell'arte

I vari tipi di certificazione attualmente esistenti sono prevalentemente utilizzati su base volontaria e solo raramente, soprattutto in Italia, a seguito di obblighi o di requisiti preferenziali nell'ambito di capitolati per l'acquisizione di beni e servizi. Nel seguito verranno considerate le tre principali forme di certificazioni di sicurezza attualmente esistenti: (i) la certificazione dei sistemi di gestione

[32] `https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en`

[33] `https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework`

della sicurezza ICT utilizzati in un'organizzazione o parte di essa; (ii) la certificazione dei dispositivi ICT, denominata anche *certificazione di prodotto*; (iii) la certificazione delle competenze nel campo della sicurezza ICT.

Certificazione dei sistemi di gestione della sicurezza ICT Tradizionalmente la certificazione dei sistemi di gestione della sicurezza informatica (Information Security Management System[34] - ISMS) è veicolata dalla ISO, che ha ereditato i vecchi standard BS 7799 e la ISO 17799. Le modalità di verifica vengono definite dallo standard ISO/IEC 27001, in base al quale viene verificato il soddisfacimento dei requisiti di sicurezza (denominati *security control*) contenuti nello standard collegato ISO/IEC 27002. Quest'ultimo riporta i requisiti, espressi in linguaggio naturale, nella forma di un catalogo dal quale estrarli sulla base dei risultati dell'analisi dei rischi. Nel catalogo sono anche contenute indicazioni circa le modalità con le quali i requisiti possono essere soddisfatti (*implementation guidance*). È previsto un unico livello di verifica e, quindi, di certificazione.

Lo standard ISO 27001 è sicuramente il più riconosciuto a livello internazionale e quello più recepito e probabilmente efficace, ma è anche uno standard che inizia ad avere necessità di aggiornamento (l'ultima release è del 2013) e comporta costi di applicazione e mantenimento spesso proibitivi, specialmente per aziende di piccole dimensioni e nel caso di ISMS alquanto complessi.

L'evoluzione che si sta manifestando negli ultimi anni mira a certificazioni "leggere", cioè economiche ed efficaci, sul modello di pratiche di sicurezza "quick win". La strada è stata già imboccata dallo UK con i *Cyber Essential*[35], dimostratisi estremamente efficaci in termini di rapporto costi/benefici e suscitando interesse in tutto il mondo. Queste certificazioni sono a diversi livelli: dalle autocertificazioni al livello minimo, alle certificazioni fatte da terzi attraverso sopralluogo per la certificazione di grado più elevato.

In specifici contesti sono stati sviluppati documenti che forniscono idonee indicazioni per l'applicazione dell'ISO 27001. È il caso del Technical Report ISO/IEC TR 27019 sviluppato sulla base dello standard ISO/IEC 27002 e contenente linee guida che consentono di definire ISMS adatti a una tipologia di infrastruttura critica. Infatti il Report è utilizzabile in contesti del settore energetico ove vengono utilizzati sistemi di controllo di processo.

Certificazione dei prodotti ICT Lo standard più noto e utilizzato per certificare prodotti ICT, intesi come componenti e sistemi, continua a essere l'ISO/IEC 15408, meglio noto con il nome di *Common Criteria*[36]. Per i moduli crit-

[34] `https://www.iso.org/isoiec-27001-information-security.html`
[35] `http://www.cyberessentials.org/`
[36] `https://www.commoncriteriaportal.org/`

tografici esistono anche gli standard specifici FIPS 140-2[37] e ISO/IEC 19790[38], 24759 e 17825, questi ultimi utilizzati prevalentemente negli USA.

I Common Criteria prevedono sette livelli di certificazione (EAL1–EAL7), cui corrispondono verifiche più severe sull'oggetto da certificare. Sono utilizzati sia nel contesto della sicurezza nazionale, nel qual caso i fornitori di prodotti sono spesso obbligati a dotarsi di tale tipo di certificazione, sia in quello che il *Piano Nazionale per la protezione cibernetica e la sicurezza informatica* (illustrato nella sez. 1.3.2) definisce il contesto rappresentato dal tessuto produttivo nazionale e dalla cittadinanza. In entrambi i casi esiste un unico organismo nazionale di certificazione di tipo istituzionale in ogni Paese. In Italia, sulla base di appositi decreti della Presidenza del Consiglio dei Ministri, l'Autorità Nazionale per la Sicurezza (ANS) e l'ISCTI del Ministero dello Sviluppo Economico ricoprono, rispettivamente, il ruolo di organismo di certificazione nel contesto della sicurezza nazionale e in quello commerciale. Ciascun organismo di certificazione accredita un certo numero di laboratori di valutazione (denominati Ce.Va. nel primo contesto, LVS nel secondo) che hanno il compito di verificare, sotto la supervisione tecnica dell'organismo di certificazione, se i requisiti contenuti nello standard sono soddisfatti dall'oggetto della certificazione.

Sebbene siano stati certificati con lo standard ISO/IEC 15408 un considerevole numero di prodotti, il suo utilizzo nel contesto commerciale non può considerarsi vasto, a causa di vari fattori che ne hanno frenato la diffusione. A parte, infatti, pochi casi nei quali è stata resa obbligatoria, al di fuori del contesto della sicurezza nazionale la certificazione Common Criteria viene richiesta dai fornitori i quali decidono autonomamente di avvalersene per migliorare l'immagine dei propri prodotti. È evidente però che tale utilizzo prevalente non è possibile con livelli di certificazione bassi che rischierebbero di essere addirittura controproducenti in termini pubblicitari per il prodotto. Conseguentemente, il maggior numero di certificazioni Common Criteria è eseguito a livelli almeno medi (da EAL3 in su) cui corrispondono tempi (almeno alcuni mesi) e costi della certificazione (mediamente dell'ordine delle centinaia di migliaia di euro) alquanto elevati. Altrettanto elevato è il costo del pur importantissimo processo di mantenimento della certificazione che, conseguentemente, non viene spesso attivato, anche perché non indispensabile ai fini pubblicitari suddetti.

La certificazione Common Criteria gode nel contesto commerciale di un riconoscimento piuttosto esteso sia in ambito mondiale, attraverso l'accordo di mutuo riconoscimento CCRA[39], sia in ambito europeo, attraverso l'accordo SOG-IS[40]. Tuttavia il riconoscimento è previsto nel CCRA solo ai bassi livelli di

[37] `https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards`

[38] `https://www.iso.org/standard/52906.html`

[39] `https://www.commoncriteriaportal.org/ccra/`

[40] `https://www.sogis.org/`

certificazione (EAL1 e EAL2) e nel SOG-IS fino a quelli medi (EAL3 e EAL4) in via ordinaria e, secondo specifiche procedure definite per alcune tipologie di prodotti, fino ai massimi livelli di certificazione.

Gli alti costi di certificazione hanno portato alla nascita, in alcuni Paesi europei, di certificazioni di prodotto più leggere che richiedono tempi e costi sensibilmente più limitati e comparabili con quelli delle certificazioni Common Criteria al primo livello di certificazione (EAL1). A titolo di esempio, la Francia, tramite l'ANSSI, rilascia un certificato di sicurezza "di primo livello" chiamato CSPN[41], che eventualmente può essere esteso ai livelli superiori del Common Criteria ed è facilmente ottenibile in un lasso di tempo garantito inferiore alle 8 settimane. Da notare che la certificazione CSPN è richiesta in alcune gare pubbliche. In maniera molto simile, lo UK ha introdotto la Commercial Product Assurance (CPA)[42]: una certificazione per prodotti commerciali di sicurezza off-the-shelf (da scaffale), che ha avuto come driver il governo stesso. Vengono controllate da laboratori autorizzati 11 funzioni di sicurezza, aggiornate con regolarità, con un costo di circa 4.500 Sterline. Anche la CPA è richiesta in vari casi nell'ambito del public procurement. Altri Paesi che si accingono ad attivare certificazioni nazionali leggere sono la Germania e l'Olanda, che le sta già eseguendo a livello sperimentale.

Certificazione delle competenze L'ulteriore dimensione del problema della certificazione è quello della certificazione delle competenze di chi opera nel settore, ai vari livelli di responsabilità. Il tema è diventato oggetto di studio e, successivamente, di tentativi di "standardizzazione" e poi di "normazione" da alcuni anni. In effetti, il mercato ha visto un proliferare di certificazioni rilasciate da organismi vari, molto spesso di natura privata, che si sono sforzati di soddisfare al meglio le esigenze delle aziende e delle organizzazioni.

La certificazione delle competenze richiede: (i) una definizione del dominio di conoscenza (knowledge), (ii) una modalità di declinazione della conoscenza in capacità operative, (iii) una verifica del grado di maturità (proficiency) di questa declinazione, dalla quale consegue il grado di autonomia e responsabilità. È un quadro complesso, all'interno del quale vi sono ampi ambiti di discrezionalità. Esistono però dei sistemi ormai consolidati a livello internazionale, europeo e nazionale, che forniscono delle linee guida, in certi casi operativi e con valore cogente ("norme"). ISO ha prodotto lo schema ISO/IEC NP 27021 (Information technology – security techniques – competence requirements for security management systems professionals[43]), che definisce un quadro di professionalità

[41] https://www.ssi.gouv.fr/administration/produits-certifies/cspn/
[42] https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
[43] https://www.iso.org/standard/61003.html

e uno schema dedicati a figure più operative (ISO/IEC NP 19896-1/2/3 "tester" ed "evaluator"[44]).

L'ente normatore europeo[45] (CEN/TC 428) ha emanato recentemente una norma quadro sulle professionalità ICT ad ampio spettro, la EN 16234-1, che è il risultato di vari anni di attività di un "Consortium Workshop Agreement", il CWA 16458, al quale l'Italia ha partecipato spesso in funzione di leadership. Il contesto europeo ha prodotto una "norma", che, come tale, ha vigore e si applica in tutti i paesi dell'Unione, sostituendo eventuali norme degli enti normatori nazionali (per l'Italia UNI[46]).

La norma generale europea definisce le competenze ICT utilizzando lo schema eCF 3.0[47], che prevede 42 competenze e declina un insieme di 6 famiglie di "profili professionali" articolate in 22 "profili di secondo livello", che includono l'*ICT Security Manager* e l'*ICT Security Specialist*. La definizione delle competenze dello schema eCF si appoggia su un insieme di "conoscenze", cioè una specifica del dominio, volutamente molto scarna e poco articolata. Ne consegue che anche i profili professionali sono definiti, da questo punto di vista, in maniera poco dettagliata. L'Italia ha implementato la norma europea emanando la norma UNI 11506:2016[48], che è una norma quadro, con quattro articolazioni (denominate 11621-1/4). In particolare, la parte 4 (Information security professional profiles) definisce 9 "profili di terzo livello", che si inquadrano quindi nei due profili di secondo livello della norma europea. Da segnalare, sempre in Italia, da parte di AICA, la proposta di livelli diversi di certificazione: a livello intermedio, la certificazione *IT Security*[49] e a livello avanzato, la *ICT Security Specialist*[50], riconducibile all'interno del framework eCF.

In questo quadro normativo agiscono gli attori del mercato: chi vuole offrire un servizio di certificazione alle persone deve necessariamente costruire la sua offerta nel rispetto di questa normativa, oltre che nel rispetto delle altre regole che consentono a un ente di proporsi come "ente certificatore".

6.5.2 Obiettivi

L'obiettivo principale di questa azione sarà quello dell'attivazione del *Centro di Valutazione e Certificazione Nazionale (CVCN)* per la verifica dell'affidabilità della componentistica ICT destinata a infrastrutture critiche e strategiche

[44] https://www.iso.org/standard/71122.html
[45] https://standards.cen.eu/
[46] http://www.uni.com/
[47] http://www.ecompetences.eu/it/
[48] http://www.ithum.it/uni11506
[49] http://www.aicanet.it/it-security
[50] http://www.aicanet.it/per-i-professionisti-ict/servizio-di-certificazione

previsto dal DPCM Gentiloni[51] del 2017. Correttamente, il DPCM affida questo centro al Ministero dello Sviluppo Economico (MiSE) che ha già maturato, come descritto nelle sezioni precedenti, una significativa esperienza nella certificazione di prodotto, attraverso il Ce.Va. dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI), poi nel settore commerciale, a partire dal 2003 quando è stato istituito presso l'ISCTI l'*Organismo di Certificazione della Sicurezza Informatica* (OCSI). Questo centro dovrà sviluppare la strategia nazionale per la parte certificazioni, considerando le seguenti condizioni al contorno:

- *La difficoltà di separare il mercato consumer da quello legato alla sicurezza nazionale* — Il processo di trasformazione digitale e in particolare la diffusione dell'IoT hanno creato i presupposti per una invasione di prodotti commerciali software e hardware all'interno di tutti i settori di mercato, dal mondo consumer alle infrastrutture critiche (che rispondono a criteri di mercato oltre che di servizio pubblico) e alla sicurezza nazionale. Stabilire quindi quali prodotti/servizi certificare per motivi di sicurezza nazionale diventa un esercizio assolutamente non banale.

- *La coesistenza tra certificazioni nazionali e certificazione europea* — La certificazione europea tende a lavorare per la creazione di un digital single market e quindi ad abbattere le barriere che si possono frapporre a livello commerciale per la vendita di prodotti all'interno del mercato europeo e attivare un sistema di fiducia nei servizi su rete da parte dei consumatori. Le certificazioni nazionali lavorano sulla sicurezza nazionale e trovare un equilibrio tra queste certificazioni non sarà facile. Un sistema di certificazione europea garantirà un sistema di mutuo riconoscimento tra gli stati membri, essendo questo la base di ogni trattato dell'Unione. Il mutuo riconoscimento dovrà comunque tenere conto del soddisfacimento di specifici requisiti legati all'interesse nazionale per le infrastrutture critiche e strategiche dei singoli paesi.

- *Certificazione nazionale di prodotti* — Sulla falsariga delle certificazioni nazionali francesi e britanniche, oltre che di quelle sperimentali tedesche e olandesi, l'Italia potrebbe dotarsi di una certificazione nazionale sostenibile in materia di cybersecurity. Questa certificazione, orientata alla sicurezza nazionale e alla protezione delle infrastrutture critiche, dovrebbe essere compatibile con quella europea oltre ad avere costi e tempi predicibili per singola certificazione (*certificazione sostenibile*). Inoltre sarà importante definire un perimetro chiaro per i prodotti certificabili

[51] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf`

in modo che la certificazione possa essere utile alle aziende che dovranno impiegare tali prodotti, ovvero sollevando queste aziende dall'onere della verifica della compliance. Infine è importante che la certificazione sia aggiornabile anche nelle procedure in modo da rispondere a esigenze che possono cambiare a seguito di nuovi tipi di attacchi. La certificazione dovrebbe essere vista dalle aziende non come un inutile costo, ma come un importante passo per rendere più sicuri gli oggetti che popoleranno il cyberspace nazionale. In aggiunta, lo sviluppo di una certificazione nazionale potrebbe portare un indotto importante lavorativo sul territorio, considerando i laboratori di certificazione che dovranno essere attivati sul territorio.

Altri obiettivi progettuali non meno rilevanti possono essere:

- *Certificazione nazionale delle aziende* — Per la sicurezza delle filiere nazionali sarebbe importante introdurre una certificazione nazionale sostenibile in termini di costi per le medie, piccole e piccolissime imprese, che non avrebbero mai le risorse per poter essere certificate tramite standard ISO. Nella stragrande maggioranza dei casi, infatti, gli attacchi alle multinazionali avvengono attraverso la manomissione dei sistemi informativi di alcuni fornitori, in genere aziende piccole o piccolissime, i cui livelli di sicurezza sono certamente molto più bassi ed eterogenei rispetto a quelli delle multinazionali. Occorre quindi elaborare un sistema di certificazioni sostenibili, da usare anche nelle gare delle grandi aziende private, in modo da mettere la committenza nelle condizioni di affidare servizi ad aziende che abbiano un livello minimo di sicurezza garantito.
- *Estensione degli standard per la security alla safety* — Per i dispositivi medici[52] si deve andare oltre la certificazione per la *safety*[53] e considerare anche gli aspetti di security. Le garanzie di security permetterebbero anche di migliorare l'usabilità e la manutenibilità di questi dispositivi (che spesso vengono disconnessi dalla rete a causa dei rischi associati alla presenza di vulnerabilità) in quanto permetterebbero di effettuare aggiornamenti o riconfigurazioni senza correre il rischio di annullamento della certificazione.

[52] `http://www.salute.gov.it/portale/temi/p2_4.jsp?area=dispositivi-medici`

[53] `http://www.salute.gov.it/portale/temi/p2_6.jsp?lingua=italiano&id=8&area=dispositivi-medici&menu=conformita`

CAPITOLO

7 Impatto sugli assi portanti della trasformazione digitale

La trasformazione digitale sta interessando tutti i settori della nostra economia e cambierà profondamente la società, le nostre relazioni e il modo di fare industria. Essa porta tutti noi all'interno della dimensione del cyberspace, che crea un collasso spazio–temporale dove cittadini, organizzazioni, cyber-criminali di ogni zona geografica si trovano a 100 millisecondi di distanza tra loro. In questo contesto la cybersecurity è ovunque: nell'hardware, nei software, nei sistemi di interconnessione, nei processi aziendali o della PA, nei contratti, nelle policy, nel fattore umano, nelle interazioni cybersociali. La cybersecurity diventa quindi l'elemento essenziale di questa nuova dimensione per garantire, nel tempo, un adeguato livello di sicurezza alle nostre relazioni, ai nostri affari, alle nostre democrazie.

Questo capitolo affronta l'impatto della trasformazione digitale su alcuni tra i più importanti settori portanti della società, analizzando come la minaccia stia cambiando in questi settori a causa della trasformazione digitale e come la cybersecurity possa giocare un ruolo chiave per abbattere il rischio legato a tale minaccia.

7.1 Democrazia

Nella società digitale di oggi, e ancor più in quella futura, "cyber is the World of Everything". Questo implica che il cittadino non è solo interessato alla protezione di dati sensibili; le tecnologie digitali si diffondono a macchia d'olio penetrando nel mondo fisico e coinvolgendo vari aspetti della vita quotidiana, dai trasporti ai servizi sanitari, all'ambiente, alle banche, al sistema formativo, al sistema elettorale e ad altri servizi essenziali forniti dalla PA.

Per uno Stato democratico è pertanto indispensabile garantire un buon livello di cybersecurity sia per proteggere la sicurezza nazionale (inclusa la tutela delle libere elezioni e delle campagne elettorali da interferenze esterne) sia per garantire benessere economico e crescita del Paese. Questo richiede un serio impegno a sviluppare strategie nazionali di cybersecurity che allineino i bisogni di sicurezza nazionale con quelli di crescita economica, che promuovano una sicurezza maggiormente proattiva sin dalla progettazione di tutte le politiche digitali e che aumentino la capacità di prevenire, dissuadere e individuare gli attacchi informatici e di rispondere a essi in maniera coordinata con le varie istituzioni coinvolte nell'architettura di cybersecurity.

La sensibilizzazione dei cittadini ai molteplici rischi connessi alla rivoluzione digitale (dalle intrusioni nei computer alla dipendenza digitale, dal furto di dati ai riscatti, dal sabotaggio alle truffe, dalle fake news all'incitamento all'odio on-line) è un altro aspetto importante.

La sfida cyber è molto impegnativa perché le minacce connesse alla rivoluzione digitale corrono più veloci delle politiche pubbliche; per questo è particolarmente importante coinvolgere in modo sempre più intenso Governo, università, centri di ricerca e imprese. Il triangolo virtuoso tra istituzioni, università e mondo imprenditoriale è la precondizione per affrontare le nuove sfide tecnologiche e dare una risposta efficace in ogni democrazia[1].

È fondamentale rafforzare strumenti di cooperazione nella dimensione europea e internazionale ed è necessario che i paesi democratici trovino un minimo comune denominatore partendo dalla piena consapevolezza che le società digitali sono in realtà molto più fragili e vulnerabili di quanto generalmente si pensi. I cittadini possono essere facilmente vittime di intrusioni, campagne di disinformazione, manipolazioni di ogni tipo e i loro diritti fondamentali possono venire erosi: in tale contesto la democrazia stessa, con esiti tragici può diventare la vittima della *cyber unsecurity*.

La cybersecurity e la conoscenza dei rischi ai quali ci espone la pervasività della rete e degli strumenti di interazione diventano pertanto elementi fondamentali per la democrazia nel nostro Paese e nel mondo. Vogliamo qui considerare due aspetti: da un lato la possibilità di utilizzare la rete per diffondere fake news in qualunque parte nel mondo e, dall'altro, la possibilità di ridurre la distanza tra Stato e cittadini utilizzando la rete per consultazioni politiche e di opinione, con i connessi rischi di brogli che questo comporta.

Fake news Da sempre vi sono state campagne di informazione tendenti a polarizzare l'opinione pubblica in specifiche direzioni in caso sia di elezioni sia di conflitti. La facilità con la quale si possono oggi diffondere, da qualunque parte

[1] `http://www.ispionline.it/en/pubblicazione/italy-building-cyber-resilient-society-18229`

del mondo, notizie di qualunque tipo, ha trasformato la rete in un potente strumento per il controllo delle opinioni. Come detto nella sez. 3.4, è fondamentale mettere a punto strumenti per il rilevamento di dinamiche anomale di diffusione, di strumenti di *warning* per gli utenti della rete, ma sopratutto di campagne di sensibilizzazione al fenomeno e all'uso critico della rete che si basino su un approccio scientifico di ricerca delle fonti e sui rischi di rimanere imprigionati nelle cosiddette *echo chamber* (si veda box a pag. 62).

Sistemi di e-Voting In tante nazioni si stanno sperimentando metodi e tecnologie per il voto elettronico; recentemente sono state avanzate varie proposte di utilizzare la *Distributed Ledger Technology* (illustrate nella sez. 4.4) come base di sistemi di voto elettronico in cui non è necessaria la presenza di un'autorità che detiene il controllo sui sistemi informatici sottostanti e che offre agli elettori la possibilità di contare e controllare i voti autonomamente, senza rischi di aggiunta di voti illegittimi. Abbiamo visto, anche in Italia, quanto questi sistemi o piattaforme di voto elettronico possono essere inclini a attacchi, vedi caso dell'hacking della piattaforma Rousseau del Movimento 5 Stelle dell'agosto 2017[2]. Questi strumenti vanno quindi utilizzati con cautela, soprattutto per elezioni generali. Difatti, come già visto nei precedenti capitoli, non esistono sistemi informatici sicuri al 100% e le possibilità di successo di un attacco dipendono da quanto un attaccante è disponibile a investire e, quindi, da quanto si possa potenzialmente guadagnare dall'attacco. Ebbene, nel caso di elezioni politiche possono essere molti i soggetti interessati a investire tanto per governare, controllare o destabilizzare una nazione.

7.2 Servizi essenziali: il caso dell'energia

L'energia elettrica è di fondamentale importanza per l'economia e la società, che dipendono dalla sua disponibilità; un'interruzione dell'alimentazione può avere un impatto diretto sulla fornitura di altri servizi (trasporti, finanza, comunicazioni, approvvigionamento idrico, etc.) per i quali la potenza di backup non sia disponibile o il tempo di ripristino del servizio superi l'autonomia di backup stesso. L'uso crescente di risorse rinnovabili e la poligenerazione portano la rete elettrica (da qui in poi EPES - *Electric Power and Energy System*) a diventare sempre più decentralizzata. La presenza di soggetti (prosumer) che su piccola scala producono energia e la conferiscono in rete rende bidirezionale il flusso energetico.

[2] `http://www.repubblica.it/politica/2017/08/02/news/hacker_online_dimostra_la_vulnerabilita_di_rousseau_ho_bucato_il_sito_dati_a_rischio_-172221493/`

Aumentano gli stakeholder coinvolti nel processo, così come i dispositivi IoT intelligenti connessi alla rete: i dispositivi interconnessi – da quelli di una smart home ai veicoli elettrici – sono sempre più numerosi, dotati di funzioni avanzate e richiedono una gestione sempre più articolata delle smart grid. L'impatto della trasformazione digitale nel settore energetico riguarda l'intera filiera dell'energia: dagli approvvigionamenti agli aggregatori, alla distribuzione e al trasporto, fino alla vendita e al rapporto con i clienti finali. La separazione fra IT (Information Technology) e OT (Operation Technology), tradizionale nella rete elettrica, scompare e i due livelli si compenetrano.

L'ICT diventa quindi il punto di forza della gestione intelligente della rete elettrica del futuro e nel contempo il potenziale punto di debolezza. L'approccio alla sicurezza dei sistemi legacy ICS/SCADA (illustrati nella sez. 5.5) è basato sul paradigma del castello inespugnabile. I limiti di tale approccio sono ben noti e soluzioni tecnologiche per la protezione delle infrastrutture esistenti (senza condizionarne il funzionamento ed evitando interventi invasivi) sono in fase di sviluppo avanzato. Diverso è il discorso per le reti di nuova generazione che, al fine di fornire servizi ai vari utenti/stakeholder e migliorare la QoS/reliability del sistema elettrico (bilanciamento della rete, ottimizzazione dei flussi, etc.), richiederanno un uso più spinto dell'ICT e saranno pertanto potenzialmente più esposte a minacce cibernetiche. La progettazione delle nuove reti elettriche dovrà far leva sulle best practice sviluppate in ambito internazionale per la protezione cibernetica dei sistemi ICT distribuiti, adattandole alle specificità del dominio applicativo. A differenza delle reti elettriche attuali, la sicurezza cibernetica dovrà guidare la progettazione e lo sviluppo delle reti elettriche di nuova generazione.

Le Infrastrutture Critiche in ambito elettrico sono molto varie; tra le altre possiamo citare: (i) grandi impianti classici di generazione termici e idroelettrici; (ii) sistemi di generazione idroelettrica distribuita; (iii) generazione rinnovabile distribuita (eolica, fotovoltaica, etc); (iv) sistemi di trasmissione e distribuzione dell'energia, composti da centinaia di cabine primarie e decine di migliaia di cabine secondarie.

I sistemi telecontrollati e i sistemi distribuiti sono esposti a tutti i rischi correlati a tale contesto. Anche i grandi impianti non possono ormai essere operati in modo isolato: la sicurezza di sistemi, reti e protocolli è pertanto un elemento essenziale. Le possibili minacce possono essere subdolamente veicolate tramite mezzi di natura non connessa come ad esempio media rimovibili o dispositivi ritornati dopo una manutenzione. La rete di telecontrollo delle reti di distribuzione rappresenta un ambito assai complesso per il gran numero di sistemi coinvolti, mentre ancora più granulare è l'infrastruttura dei contatori digitali. È necessario tenere conto delle differenti esigenze dei vari impianti coinvolti e, per ciascuno di questi ambiti, è necessario pertanto sviluppare "by design" un'opportuna strategia di protezione, sia a livello ICT, sia a livello di logiche

operative.

Avvicinandosi alle "foglie" del sistema l'ordine di grandezza degli oggetti cresce e con esso la necessità di individuare una specifica strategia per la sicurezza. Senza adeguate misure di protezione informatica, potrebbe essere violato l'accesso ai sistemi, si potrebbero subire interruzioni di alimentazione, ed effetti a cascata ai sistemi interconnessi e ai servizi energetici: in ultima analisi danni irrimediabili a cose e a persone. Pertanto l'EPES affronterà un crescente numero di sfide, che richiedono lo sviluppo di soluzioni informatiche che contemperino le esigenze della sicurezza con quelle della elevata velocità di comunicazione e garantiscano la facile scalabilità al numero di dispositivi in gioco.

7.3 Finanza

A partire dalla crisi finanziaria del 2008, il mercato bancario italiano ha subito una ristrutturazione che ha visto una diminuzione del numero degli istituti di credito e una riduzione della loro presenza sul territorio. La trasformazione digitale è stata anche l'occasione di un cambiamento radicale dei modelli di business. La diffusione dei servizi bancari erogati tramite dispositivi mobili ha portato all'ingresso di operatori globali come Amazon e Google nell'area dei pagamenti. Con l'entrata in vigore dal gennaio 2018 della Direttiva Europea EU 2015/2366 (*Payment services* - PSD2) è venuto meno il monopolio degli istituti bancari sui servizi di pagamento. L'allargamento dell'ecosistema a operatori non bancari pone vari problemi in termini regolatori e di sicurezza operativa.

La digitalizzazione dei servizi assicurativi ha un elemento specifico: l'interazione con dispositivi mobili IoT, che riguarda i prodotti assicurativi rivolti a dispositivi autonomi come le automobili a guida autonoma e l'erogazione di *assicurazioni a consumo* con premi legati a grandezze misurabili sul campo, compresi gli stili di vita individuali. La digitalizzazione comporta un crescente utilizzo dei dati di contesto associati alle transazioni e raccolti dai dispositivi IoT per l'esecuzione di analitiche on-line. Queste mirano ad abilitare proposte personalizzate e tariffazione dinamica dei prodotti, basate su modelli quantitativi non-attuariali per il calcolo del rischio. Il calcolo on-line di analitiche porta a un aumento della dimensionalità dei dati associati alle singole transazioni. Questa de-normalizzazione dei dati finanziari ha aumentato il loro valore unitario sul mercato illegale e li ha resi un bersaglio più attraente per gli attaccanti.

Negli ultimi anni il settore finanziario ha subito attacchi senza precedenti, caratterizzati da vettori di attacco distribuiti e coordinati. L'analisi degli attacchi permette di individuare tre minacce fondamentali:

- *Compromissione temporanea delle funzionalità dei servizi bancari e assicurativi* — Il corrispondente rischio è accresciuto dall'elevato livello di

interconnessione del sistema bancario e si è aggravato negli ultimi anni anche a causa dei rapidi progressi nella tecnologia di attacco. Oggi, i vettori d'attacco che possono danneggiare il sistema bancario sono grandi sistemi Bot automatizzati e distribuiti. Questi vettori sono difficili da rintracciare e disattivare, anche perché sfruttano dispositivi eterogenei e insospettabili come telefoni cellulari, stampanti e persino giocattoli.

- *Furto organizzato su larga scala di dati bancari e finanziari* — Tipicamente perpetrati attraverso furti episodici (*Data breach*, introdotti nel box a pag. 143) oppure tramite la creazione di falle permanenti (*leaks*) nei processi bancari e assicurativi. La crescente competenza degli attaccanti ha aumentato la loro capacità di iniettare vettori d'attacco mirati non solo agli utenti dei servizi on-line, ma anche alla struttura organizzativa interna dei singoli operatori bancari e assicurativi, tramite attacchi di tipo *spear phishing*, introdotti nel box a pag. 29. I vettori iniettati sfruttano poi errori e debolezze nella configurazione e gestione dei controlli di sicurezza crittografici.

- *Violazione dell'integrità dei dati presenti all'interno del sistema bancario* — Oltre a trafugare i dati del sistema bancario, gli attaccanti possono alterarli, impiegando vettori di attacco diversi, che vanno dai ransomware ai dispositivi IoT e alle false installazioni (*fake install*) che utilizzano emulatori di dispositivi mobili in cloud per fornire false informazioni. Con la crescente diffusione dei servizi finanziari su terminali mobili, questi vettori si prestano a sofisticati attacchi cyber per introdurre dati falsi o fuorvianti nel sistema, inquinando i dati alla base dei modelli di rischio non attuariali menzionati in precedenza. L'attacco può danneggiare la qualità delle analitiche senza essere rilevato, causando un danno permanente al sistema.

Un primo fattore specifico di rischio cyber è il numero crescente di aziende non regolamentate che operano nel settore finanziario. Questi operatori sono molto diversi tra loro per dimensioni e offerta di prodotti, così come per processi e controlli di sicurezza, rendendo più difficile la stima delle probabilità nei modelli per la valutazione del rischio cyber.

Un secondo fattore di rischio riguarda il ruolo del sistema finanziario nel contesto economico nazionale. Le minacce cyber ai servizi bancari critici, oltre a danneggiare i singoli operatori, possono dare origine a un rischio sistemico per la stabilità finanziaria. Per esempio, attacchi coordinati al sistema bancario possono portare a una compromissione della capacità (in termini tecnologici e non finanziari) del sistema di iniettare capitali e liquidità nel sistema delle imprese in particolari momenti congiunturali. La mitigazione di questo rischio sistemico rientra a pieno titolo negli scenari di cyber-warfare.

Un terzo fattore di rischio consiste nella natura prevalentemente difensiva dei controlli di sicurezza attualmente messi in opera dalle banche e dalle altre aziende del settore finanziario. L'aumento delle capacità tecniche degli attaccanti potrebbe rendere a lungo termine insostenibile la difesa senza un'azione di cyber-intelligence che individui i vettori d'attacco più critici.

Per il settore assicurativo, un fattore di rischio aggiuntivo scaturisce dalla difficoltà di garantire la sicurezza dei dispositivi IoT integrati nei nuovi servizi assicurativi, come illustrato nella sez. 5.4.

7.4 Trasporti

Affrontare l'impatto della cybersecurity nell'ambito trasporti richiede l'analisi di tre ambiti tra loro strettamente correlati e interdipendenti: i veicoli, le infrastrutture abilitanti e i servizi.

Nell'ambito dei veicoli intelligenti per il trasporto su strada ricadono tutte le iniziative legate all'*infotainment* e alla guida assistita, con l'obiettivo ultimo dei veicoli a guida autonoma. Nell'ambito dei servizi a valore aggiunto ricadono le iniziative legate alla telemetria (assistenza stradale, manutenzione preventiva), alla sicurezza dei veicoli (assicurazioni personalizzate, antifurto intelligenti), alla *shared-mobility* e, più in generale, alle piattaforme di raccolta e analisi dei dati legati ai veicoli. Nell'ambito, infine, delle infrastrutture intelligenti ricadono oggi tutte le iniziative legate all'ottimizzazione dei consumi e dei flussi e ai cartelli stradali in grado di adattarsi autonomamente alle condizioni di contesto e vi ricadranno, domani, le nuove infrastrutture abilitanti per la gestione del traffico di veicoli a guida completamente autonoma.

Per quanto concerne i veicoli e i servizi, la sempre maggior diffusione di dispositivi IoT, se da una lato permette un incremento del confort per i passeggeri e l'offerta di servizi del tutto innovativi, dall'altro introduce ovvie sfide relative al trattamento della mole di dati generati (Big Data Analytics) e, soprattutto, nuove problematiche di cybersecurity, in termini sia di aumento smisurato della superficie di attacco sia di capillarità e pervasività dei possibili attacchi, come ampiamente analizzato nella sez. 5.4.

È stato anche sottolineato come i nuovi servizi introdotti, potendo essere molto personalizzati, di fatto introducano nuove opportunità e nuove sfide a tutti i livelli, dalla tariffazione alla misura del servizio effettivamente erogato e alla valutazione on-line e dinamica del rischio assicurativo.

Il mondo dei trasporti è regolato da una vasta gamma di standard internazionali e, tradizionalmente, i sistemi impiegati in tale ambito sono sistematicamente progettati con approcci e soluzioni specifiche per affrontare problematiche di safety, di garanzia della qualità del servizio e di tolleranza ai guasti. Al riguardo, è necessario pervenire con urgenza alla definizione di nuovi standard

in grado di integrare quelli esistenti, conglobandovi le problematiche di security introdotti dalle nuove tecnologie e, in particolare, dall'IoT.

In chiusura, è importante evidenziare come sia assolutamente ineludibile un radicale cambio di paradigma in merito alle nuove infrastrutture abilitanti di cui il Paese dovrà necessariamente dotarsi, nel medio/lungo periodo, per permettere sia il traffico di veicoli su gomma a guida completamente autonoma sia l'impiego di droni in ambito urbano. Al di là dei necessari adeguamenti legislativi, occorre prevedere, fin da subito, l'introduzione di norme che vincolino il progetto e la successiva realizzazione di queste nuove infrastrutture al concetto e alla pratica della *Security by design*, non essendo né concepibile né tollerabile che si ripeta, per queste infrastrutture cyber-fisiche, lo stesso errore commesso per quelle informatiche, inizialmente progettate senza considerare minimamente gli aspetti di security.

7.5 Industria

La trasformazione digitale cambierà profondamente il modo di fare industria nel futuro. La nuova industria infatti perderà completamente il concetto di perimetro fisico, tipico degli anni '80, trovandosi così immersa nel cyberspace, con fornitori e clienti in un unico grande blob. L'IoT, l'intelligenza artificiale, il cloud e le tecnologie blockchain stanno eliminando completamente il perimetro spostando dati e servizi al di fuori di esso. Ad esempio, gli algoritmi di intelligenza artificiale richiederanno, per il loro funzionamento, sempre più dati provenienti dalla rete di business aziendale, da quella di missione, dai fornitori e dai clienti, in modo da ottimizzare tutti i processi aziendali, dal facility management, alle vendite, alla produzione, etc. In questo contesto la cybersecurity è ovunque: nell'hardware e nel software utilizzato dall'azienda, nei contratti con i clienti, nella Supply chain, nel fattore umano, etc., diventando un elemento essenziale dell'azienda stessa.

Purtroppo, però, in troppi contesti lavorativi la sicurezza è oggi ancora considerata esclusivamente un onere aziendale. La condizione tipica di gestione della security a livello aziendale è che questa è completamente disallineata dalle altre attività; il problema è poi aggravato dal fatto che, a fronte della maggiore complessità dei prodotti, servizi e sistemi coinvolti, si hanno costi e problemi di gestione in continua crescita.

A livello aziendale esistono numerosi rischi legati alla sicurezza, come ad esempio: perdita di informazioni critiche (personale dipendente, fornitori, utenti, dati delle applicazioni, etc.), interruzione dei processi di business (danneggiamento di sistemi web aziendali, di sistemi e dispositivi mobili in dotazione ai collaboratori aziendali, etc.), danni all'immagine e alla reputazione aziendale.

Purtroppo, a fronte di tali rischi, accade ancora spesso che la security e anche le eventuali situazioni di crisi vengano affrontate a livello individuale, senza alcun protocollo standard di riferimento.

È quindi importante, in primis, che in azienda parta un processo di consapevolezza che deve necessariamente coinvolgere *tutti*: dal CEO al CTO, dal Consiglio di Amministrazione a tutti gli addetti. Consapevolezza che il rischio cyber è un rischio primario per la sopravvivenza dell'azienda: occorre pertanto avviare un corretto processo di formazione del personale e di gestione del rischio cyber basato su best practice internazionalmente riconosciute e approvate almeno a livello nazionale.

Dal punto di vista della Supply chain, non si può prescindere da un'attenzione particolare a cosa entra all'interno del perimetro aziendale in termini di hardware e software. Da qui l'esigenza primaria della presenza di un sistema di certificazione sostenibile che possa aiutare un'azienda a orientarsi sui vari prodotti che può acquisire e/o installare al suo interno, avendo la garanzia di un livello di sicurezza adeguato. Tecnologie e azioni abilitanti dovranno essere considerate guardando al profilo cyber aziendale, agli asset fisici e ai dati da proteggere.

Certamente, in un contesto nazionale, i settori della cantieristica, della meccanica, delle macchine utensili, dell'agroalimentare e del made-in-Italy sono quelli più a rischio poiché rappresentano il cuore pulsante della nostra economia e quindi quelli più appetibili da competitor o da attori statuali. Per affrontare la minaccia in modo adeguato dovranno essere messe in atto appropriate contromisure basate su infrastrutture abilitanti di settore, quali gli ISAO e i Centri Regionali di Competenza (illustrati nella sez. 2.3), interconnessi tra loro e strettamente legati al CSIRT nazionale.

7.6 Turismo e cultura

La trasformazione digitale attualmente in atto in molti settori non può non coinvolgere anche il turismo e le attività ludico-educative che rientrano sotto gli ambiti dei beni culturali e museali e della fruizione di opere di interesse artistico-culturali. Lo *smart tourism* (traducibile in italiano come *turismo intelligente* [40]) è la nuova parola d'ordine per descrivere la crescente dipendenza delle destinazioni turistiche, delle loro industrie e filiere del valore e dei loro visitatori, sfruttando tecnologie ICT che consentono di trasformare enormi quantità di dati in valore aggiunto. L'uso di dispositivi IoT, smartphone e altri dispositivi mobili quali macchine fotografiche e smartwatch, il cloud computing, le tecniche di intelligenza artificiale e machine learning applicate all'analisi delle abitudini di visita dei turisti e ai social network, stanno creando un ecosistema in cui il turista è al centro e viene in modo proattivo indirizzato, guidato, consi-

gliato verso le esperienze più consone alle proprie preferenze e più gratificanti in termini di apprendimento ed esplorazione del territorio, anche di beni minori e di scoperta di nuove realtà [26].

Particolarmente rilevante anche il notevole incremento che queste tecnologie hanno portato alla fruibilità dei beni artistici e museali da parte di visitatori e turisti con disabilità diverse.

Non va poi dimenticato che sempre le medesime tecnologie consentono un monitoraggio più dettagliato e approfondito dello stato di salute dei beni, permettendone una più efficace preservazione e nel contempo ne permettono una visione con informazioni di dettaglio impensabili fino a pochi anni fa.

In analogia con altri settori, questa trasformazione crea però nuovi rischi cyber, sia verso il turista sia verso il bene stesso. La protezione dei dati personali dei turisti può essere violata: applicazioni smart possono, ad esempio, essere manomesse in modo tale da indirizzare flussi di persone da un luogo all'altro, creando danni economici ingenti e/o situazioni critiche di confusione e panico. Le reti di monitoraggio dei beni possono essere compromesse, di nuovo creando falsi allarmi – con conseguenti danni economici – ovvero non lanciando allarmi a tempo debito, portando quindi al danneggiamento irreparabile del bene stesso.

Pertanto la cybersecurity acquista una rilevanza fondamentale anche in questo settore, presentando però alcune peculiarità proprie: da un lato, la necessità, nel valutare possibili manomissioni alle reti di monitoraggio, di avere forti competenze di dominio (sui materiali dei beni, sullo stato di conservazione, etc.) e dall'altro – essendo il dominio a forte componente umana in atteggiamento ludico/ricreativo – la necessità di garantire globalmente la sicurezza delle persone, preservandone nel contempo la riservatezza dei dati personali e controllando l'eventuale insorgere di meccanismi psico-sociali potenziali generatori di panico.

7.7 Comunicazione e stampa

Comunicare la sicurezza informatica è un compito arduo. La complessità delle tematiche, gli attori coinvolti e le caratteristiche dei suoi contenuti hanno finora favorito l'idea che la cybersecurity sia un affare da specialisti. Eppure sappiamo che non è così per un motivo che è sotto gli occhi di tutti: l'allarme che destano nei cittadini le ripetute violazioni della sicurezza informatica di banche, aziende e ministeri di cui la stampa rende conto ormai con una certa frequenza. Certo, questa informazione talvolta viene fatta con un linguaggio da iniziati in un paese come l'Italia dove la cultura informatica di base è ancora arretrata, ma talaltre viene fatto in maniera ipersemplificata, con toni allarmistici e con un linguag-

gio occasionalmente scorretto, che sconta l'incapacità di spiegare la natura, la vastità e la portata del fenomeno.

Complice di tutto questo è anche la crisi del giornalismo e l'assenza di una narrazione condivisa dei fatti che vede gli interessi di parte sovrastare quelli collettivi, ad esempio quando la stampa si trattiene dal fare nomi e numeri di episodi – i data breach – in cui la violazione della sicurezza riguarda le banche che ne garantiscono i debiti, gli inserzionisti pubblicitari, interessi politici organizzati e le carriere, quelle che da una chiara comunicazione dell'accaduto verrebbero stravolte.

Ultima, ma non meno importante, è la scarsa preparazione di chi è chiamato a raccontare le tematiche della cybersecurity in contesti non specialistici e preferisce ritirarsi nella *comfort zone* in cui vengono trattati solo gli argomenti già noti al pubblico e in grado di attirarne l'attenzione con formule sensazionalistiche e sollecitando paure antiche. Situazioni queste che impediscono al giornalismo di esercitare quella doppia funzione di watchdog della democrazia e di manutenzione civica rispetto ai valori fondanti la società.

Eppure non c'è mai stato così tanto bisogno di una buona informazione sui temi della cybersecurity. Ce n'è bisogno per educare le persone, fondare un linguaggio comune, costruire una cultura della sicurezza informatica che parta dalla divulgazione dei suoi temi più rilevanti: la protezione dei dati personali, la libertà, la sicurezza, la salute.

Per tutti questi motivi informare ed educare alla cybersecurity è una sfida che riguarda tutti: cittadini, imprese, istituzioni e università. E, per questo, lavorare su un linguaggio preciso, un linguaggio comune, adeguato a comunicare correttamente i temi della cybersecurity è fondamentale.

Oltre alla sicurezza nazionale, la cybersecurity dovrebbe essere identificata con la protezione dei dati personali che anticipano e definiscono i nostri comportamenti. Ne abbiamo bisogno perché le nostre vite sono definite dal nostro sé digitale che ogni giorno interagisce con realtà il cui core business è proprio l'estrazione e la raccolta dei dati che ci riguardano per rivenderli al miglior offerente. I rischi sono evidenti quando le agenzie di welfare gestiscono in digitale tutto quello che ci rende cittadini con dei diritti (la salute, la pensione, la disoccupazione) e le "cose" dell'IoT non sono governate, a causa di una legislazione insufficiente e arretrata.

In questo scenario è ancora più evidente come la confusione linguistica relativa al mondo della cybersecurity non si giovi di parole che rinviano a concetti deformanti. Ma le parole sono importanti: chi parla male, pensa male. Un esempio è quello della parola *hacker* e delle *attività di hacking*. L'equivalenza errata che identifica la figura dell'hacker con i criminali informatici non solo sollecita paure irrazionali, ma ci priva di una teoria e di una pratica dove invece gli hacker possono essere i migliori alleati della cybersicurezza.

Chiarire i termini all'origine dell'hacking può favorire la mitopoiesi

dell'*hacker "buono"*, dell'*hacker etico* che compendia in sé le migliori qualità delle società moderne: autonomia, indipendenza, libertà. In realtà la genesi della parola hacker aveva un'aggettivazione positiva: i primi hacker erano i burloni dei dormitori universitari ma divennero ben presto quelli che giocando col software ne ottimizzavano le prestazioni. Una cattiva pubblicistica e la nascente industria dei personal computer ha però trasformato nel tempo gli hacker in segreti officianti di pratiche esoteriche. Il bau-bau, l'uomo-nero rappresentato dagli hacker cominciava a incarnare frustrazioni, paure, incertezze personali e sociali. Eppure sono stati degli hacker a costruire i maggiori brand dell'industria informatica, da Bill Gates a Steve Wozniack fino a Page e Brin.

Per fortuna le persone sono spesso più avanti di chi pretende di rappresentarle e indirizzarne il pensiero, così hanno incominciato a contestare quelle stigmate negative tanto a lungo portate dagli hacker e sono diventate consapevoli che essere un hacker, un virtuoso della programmazione, esperto di reti e computer, è la condizione necessaria ma non sufficiente per penetrare abusivamente in un sistema informatico protetto, cosa che inevitabilmente li qualificherebbe come criminali informatici. Questi hacker però possono essere dei formidabili *defender* del nostro cyberspace e molti lo sono. Per questo è importante capire che oggi esistono molte tipologie di hacker. Per quelli che commettono un reato l'aggettivo che li qualifica è criminale. Gli altri dobbiamo cercare di intercettarli e farli crescere in un percorso tecnologico ed etico in modo che diventino la punta di diamante delle nostre polizie del cyberspace. Come abbiamo ricordato nella sez. 3.8, è importante che il legislatore capisca questa differenza di fondo e la qualifichi in modo adeguato.

7.8 Cyber social security

Il cyberspace non rappresenta un mero spazio di interscambio, ma un ecosistema cyber-sociale che si sostanzia nell'esperienza umana in modo sempre più concreto attraverso la progressiva evanescenza del confine materiale/immateriale. Il reale si comprime nella totalizzazione dell'immaginario digitale, in cui il *device* mobile diviene lo specchio aumentato del sé, l'estensione del soggetto il cui spazio-tempo individuale si determina per mezzo della fruizione narcisistico-compulsiva. La sfera privata si disintegra a favore della trasmutazione condivisa della stessa, mentre la frenetica necessità di presenza nelle social media platform, in quanto media narcisistici, colonizza la routine quotidiana dell'*homo digitalis*, di fatto de-socializzandolo, allontanandolo dall'altro per lasciarlo iperconnesso nella solitudine cyber-sociale del selfismo. In tale contesto, la polarizzazione violenta delle audience, favorita dai processi di comunicazione e interazione all'interno dell'ecosistema cyber-sociale, evidenzia la centralità delle dinamiche di demarginalizzazione, riduzione dei freni ini-

bitori, gamificazione, rinforzo positivo, riconoscimento identitario da parte del gruppo dei pari, quali elementi chiave dell'assetto comportamentale deviante e/o criminale.

La transizione dal mondo analogico gerarchizzato al sistema digitale globale, identificata nel passaggio dal XX al XXI secolo, ha favorito un processo che ha profondamente mutato l'essenza identitaria stessa del terrorismo. Internet e le social media platform non rappresentano un territorio di conquista del terrorismo contemporaneo, ma l'ecosistema cyber-sociale entro cui si è sviluppato, evolvendosi in espressioni del tutto nuove rispetto al terrorismo ideologizzato del secolo scorso.

Negli ultimi venti anni, la presenza di materiale di natura terroristica online è passata da una decina di siti a circa diecimila, evidenziando la crescente centralità dell'Internet Jihadism o jihadismo on-line, come complesso fenomeno evolutivo contraddistinto da multidimensionalità, multiattorialità e pervasività. La propaganda, tradizionalmente volta a fondere il singolo nella massa, risulta essere altro rispetto alla cyber-propaganda jihadista che si articola attraverso una strategia di *globalizzazione individualizzata*, cyber-esperienziale, mobile, in grado di superare la necessità di affiliazione diretta, a favore della propagazione cyber-socio-culturale del modus vivendi jihadista, nonché di ridisegnare la realtà e colonizzare la sfera delle percezioni nei soggetti più vulnerabili [3]. Dopo più di un decennio di coltivazione qaedista, l'Islamic State è stato in grado di creare il primo immaginario concretamente globalizzato, sfruttando i social media, viralizzando e sollecitando le pulsioni sadico-violente e reazionarie dei soggetti più vulnerabili, al fine di motivarli, ispirarli e innescarli all'azione terroristica indiscriminata secondo modi operandi sempre più spontanei, asimmetrici e low cost, come tristemente avvenuto a più riprese in Europa negli ultimi due anni. L'*avatarismo terroristico* [2] si diffonde giorno dopo giorno attraverso i siti di file sharing e le social media platform. I Millennial rappresentano al contempo prosumer, follower e influencer costantemente immersi nell'ecosistema cyber-sociale, caratterizzati da vulnerabilità generazionali – principalmente derivanti dall'assenza di un percorso di alfabetizzazione e consapevolezza digitale – che unitamente alle vulnerabilità del singolo possono favorire la cyber-radicalizzazione violenta di soggetti sempre più giovani e vulnerabili attraverso la superficiale complessità che caratterizza l'esperienza disintermediata della jihadisfera, dando vita a due distinte dinamiche di cyber-radicalizzazione violenta [4]:

- *cyber-ecosistemica* — radicalizzazione cyber-sociale attraverso le social media platform;

- *cyber-egosistemica* — radicalizzazione mobile in termini di auto-isolamento cyber-sociale e auto-radicalizzazione.

Oggi, nell'era della post-verità, l'allarmante ridefinizione del concetto di verità, sempre più aderente a quello di condivisione esperienziale in termini additivi ed emotivi, accresce la capacità asimmetrica delle entità terroristiche. Fake news, chatbots e cybertrolling si delineano come le nuove armi della progressiva convergenza cyber-sociale mobile di estremismo, hate speech e terrorismo. L'hybrid warfare jihadista impone, nell'ottica dell'attività di ricerca, analisi, prevenzione, anticipazione e contrasto, la cogente convergenza pubblico-privato sul fronte della cybersecurity in cui si prenda atto sia della rapida evoluzione non-lineare della minaccia sia delle specifiche implicazioni sul piano delle vulnerabilità generazionali e individuali dell'ecosistema cyber-sociale. A tal fine, la strategia di intervento deve essere orientata imprescindibilmente a:

- sviluppare conoscenza, formazione e competenza sulla base di approcci cross-disciplinari che integrino le scienze sociali con le discipline ICT;
- promuovere alfabetizzazione, educazione e consapevolezza digitale a ogni livello, sin dalle prime età, nonché all'interno della famiglia;
- predisporre strategie e tattiche istituzionali di tutela reputazionale in ambiente cyber-sociale;
- strutturare modelli di resilienza e mitigazione basati sulle specifiche dinamiche cyber-sociali, con particolare attenzione all'elemento spazio-temporale;
- promuovere l'istituzione di un contenitore in cui esperti, provenienti dai settori pubblico e privato, cooperino nello sviluppo di scenari evolutivi di vulnerabilità e minacce, attraverso la prospettiva cyber-sociale.

Appare, quindi, evidente come la cybersecurity non possa essere considerata più tale in assenza della sua dimensione cyber-sociale, tra l'altro, sempre più rilevante in termini di devianza e criminalità.

CAPITOLO

8 Lo scenario internazionale

Il presente capitolo considera lo scenario internazionale descritto da colleghi Italiani che da tempo lavorano in Università o Enti di Ricerca straniere. Lo scenario mostra come le diverse nazioni si stiano attrezzando attraverso centri di competenza sulla cybersecurity con adeguato numero di personale, stiano sviluppando programmi di ricerca a livello nazionale e, nel caso della formazione, stiano predisponendo azioni per avere al più presto una workforce appropriata ai loro bisogni di stato sovrano. Il capitolo mette anche in evidenza l'entità delle risorse stanziate dai vari paesi in questo settore strategico.

8.1 Canada

La "Canada's Cyber Security Strategy"[1] creata nel 2010, è basata su tre pilastri fondamentali: mettere in sicurezza i sistemi governativi, favorire la sicurezza delle infrastrutture non governative vitali per il paese, assicurare la protezione dei cittadini canadesi. Un sommario delle misure pratiche poste in essere per l'implementazione della Strategia è presente nel corrispondente Action Plan per gli anni 2010-2015[2]. In sintesi, il governo ha: (i) diviso le competenze delle agenzie coinvolte nella gestione di incidenti di sicurezza, (ii) annunciato lo

[1] Public Safety Canada: Canada's Cyber Security Strategy – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf, ISBN: 978-1-100-16934-7, 2010.

[2] Public Safety Canada. Action Plan 2010-2015 for Canada's Cyber Security Strategy – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf, ISBN: 978-1-100-21895-3. 2013

stanziamento di fondi specifici per la cyber security, (iii) rafforzato la collaborazione con il Department of Homeland Security USA[3] e con imprese private, (iv) lanciato campagne per diffondere una cultura della sicurezza tra il pubblico.

8.1.1 Gestione della cybersecurity: attori, ruoli e finanziamenti

I ruoli e le identità degli attori governativi coinvolti nella gestione degli Incidenti sono definiti nel "Government of Canada Cyber Security Event Management Plan" (GC-CSEMP)[4], che dettaglia come vanno gestiti eventi (incidenti e notizie di vulnerabilità e di possibili attacchi) che coinvolgono (o possono coinvolgere) strutture governative. Gli attori principali del GC-CSEMP formano il nucleo del Cyber Security Event Management Team, gruppo deputato alla gestione degli eventi. Altre strutture sono state create per fronteggiare le diverse problematiche.

Public Safety Canada Public Safety Canada ha tra i suoi compiti la protezione delle infrastrutture critiche e della Cyber e coordina l'implementazione della Strategia. Public Safety Canada cura iniziative di ascolto e sensibilizzazione di cittadini, accademici, imprese e PA e gestisce il portale Get Cyber Safe[5] che contiene notizie e report relativi a recenti attacchi svolti sul territorio canadese. Public Safety Canada incorpora il *Canadian Cyber Incident Response Center*, che ha il compito di coordinare la risposta nazionale ai cyber security threat. Questo centro raccoglie le segnalazioni da parte di infrastrutture critiche, strutture governative e imprese di nuove minacce che possano impattare sulle infrastrutture vitali del paese e diffonde ai propri partner allerte, rapporti e bollettini periodici su cyber threats, vulnerabilità e incidenti. Lavora a stretto contatto con i CERT di UK, USA, Australia e Nuova Zelanda.

Communications Security Establishment Il Communications Security Establishment afferisce al Department of National Defense e si occupa di signal intelligence e information security. Di esso fa parte il Cyber Threat Evaluation Centre che si occupa della detection e dell'analisi tecnica di cyber threats operanti in infrastrutture di rete di interesse nazionale e svolge non solo il ruo-

[3] `https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx`

[4] `https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html`

[5] `https://www.getcybersafe.gc.ca/index-en.aspx`

lo di advisor tecnico, ma anche di sviluppatore e fornitore di strumenti per la gestione di incidenti.

Shared Service Canada Shared Service Canada ha il compito di fornire centri di elaborazione dati e reti a svariate organizzazioni governative. Essenzialmente centralizza la gestione dell'IT governativa. Al suo interno opera il Security Operation Centre che incorpora il Government of Canada Computer Incident Response Team che è l'interfaccia per agenzie governative vittime di un incidente e agisce come coordinatore in tutte le fasi di gestione degli incidenti. Si noti che è invece il Canadian Cyber Incident Response Center a svolgere il ruolo di consulente tecnico e di coordinamento per le infrastrutture critiche.

Treasury Board of Canada Secretariat Il Treasury Board of Canada Secretariat fornisce una direzione strategica al meccanismo di gestione degli Incidenti allo scopo di minimizzare l'impatto e le perdite che possano colpire il governo.

Il GC-CSEMP definisce anche il ruolo di attori secondari, che non sono coinvolti nella gestione di tutti gli eventi ma solo in quelli di particolari gravità o quelli che, per loro stessa natura, rientrano nelle competenze di un particolare attore (Royal Canadian Mounted Police, Canadian Security Intelligence Service, Department of National Defence / Canadian Armed Forces).

Finanziamenti Visto il numero e l'eterogeneità delle strutture governative coinvolte è difficile quantificare con precisione i fondi che il governo alloca specificatamente per la cyber. Per il periodo 2001-11, il 2012 Fall Report of the Auditor General of Canada[6], nota che 13 agenzie, coinvolte a vario titolo nella cyber, hanno ricevuto 780 milioni di dollari canadesi di fondi per emergency management e national security. Inoltre, altri 200 milioni sono stati destinati a progetti che si occupano della protezione delle infrastrutture critiche da cyber threats. Non è chiaro quanti di questi fondi siano stati effettivamente utilizzati per la cybersecurity.

8.1.2 Verso una nuova strategia nazionale canadese

Il governo ha reso disponibile i risultati della consultazione nazionale svolta da PSC[7]. Dal report emergono quattro fondamentali aree di azione: diffondere la

[6] `http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html#hd5b`.

[7] `https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf`.

cultura della sicurezza e una consapevolezza di base; migliorare la preparazione delle forze dell'ordine e dei professionisti che lavorano nella cyber; sviluppare e promuovere standard, best practice, e certificazioni; aumentare i fondi e le risorse per tutte le aree coinvolte nella cyber. Inoltre, emerge come molto sentita la necessità di collaborazione tra governo, accademia e imprese.

Per gli anni dal 2012 al 2019 i Reports on Plan and Priorities riportano fondi per la cyber, assegnati a Public Safety Canada, per circa 80.6 milioni. Per la cyber e l'IT Security per il periodo 2014-2020 viene indicato un budget di circa 760.9 milioni assegnato a Shared Service Canada[8].

8.1.3 Fondi per l'accademia

I fondi disponibili per l'accademia si dividono tra quelli usati per creare centri di ricerca e reti di eccellenza e quelli usati per la ricerca di base.

Reti di eccellenza, centri di ricerca Per agevolare il travaso di know-how verso il settore produttivo, nel 2014 è stata creata la rete di eccellenza SERENE-RISC che include 24 diverse accademie e più di 24 partner non accademici del settore pubblico e privato. Nel 2017, è stato aperto il Canadian Institute for Cybersecurity all'Università di New Brunswick. Uno dei partner principali del centro è IBM. Il centro è presieduto dalla Canada Research Chair in Cybersecurity, Ali Ghorbani.

Ricerca di base Nel 2017 è stata lanciata una call specifica di NSERC in collaborazione con il Department of national Defence. Tra gli ambiti di interesse della call vi è quello della cyber, il finanziamento totale è di $2,4M. Altri fondi destinati alla ricerca sono i Discovery Grant, forniti annualmente da NSERC. Per il periodo 2014-17, limitatamente ai raggruppamenti di Computer Science ed Electrical and Computer Engineering, sono stati identificati fondi totali per progetti con tematiche di cybersecurity per circa $10M. Oltre ai finanziamenti sopra menzionati vi è la Canada Research Chair specifica per la cybersecurity che viene assegnata con cospicui grant settennali.

8.2 Francia

Una prima strategia in materia di cybersecurity è stata sviluppata in Francia all'inizio del 2010, poco dopo la scoperta di un attacco cyber volto a spiare il ministero dell'economia e della finanza. Successivamente, nell'ottobre 2015, l'allora

[8] Shared Services Canada, 2017-2018 Departmental Plan – `https://www.canada.ca/en/shared-services/corporate/publications/2017-18-departmental-plan.html`, ISSN 2371-7912. 2017

primo ministro francese Manuel Valls ha annunciato la strategia nazionale di sicurezza digitale francese, intesa a sostenere la transizione digitale della società francese. Questa strategia è il risultato di un impegno coordinato interdipartimentale per rispondere alle problematiche emergenti sulla sicurezza digitale. La definizione di tale strategia è la conferma che la cybersecurity è considerata dalla Francia come una priorità nazionale e che ora riguarda anche i singoli cittadini. La strategia è caratterizzata da cinque obiettivi che descrivono il ruolo dello Stato nel cyberspace:

1. Garantire la libertà di espressione e di azione della Francia e la sicurezza delle sue infrastrutture critiche in caso di un grande attacco cyber. Questo obiettivo verrà perseguito rafforzando le capacità scientifiche, tecniche e industriali necessarie per proteggere le informazioni nazionali, garantire la sicurezza in rete e sviluppare un'economia digitale affidabile.

2. Proteggere la vita digitale dei cittadini e delle imprese e combattere la criminalità informatica. La Francia aumenterà la sua lotta contro la criminalità informatica e la sua assistenza alle vittime di atti di cyber-violenza.

3. Garantire l'istruzione e la formazione necessarie alla sicurezza digitale. La Francia aumenterà la consapevolezza dei ragazzi sulla sicurezza digitale e sui comportamenti responsabili nel cyberspace, a partire dall'età scolastica. Anche l'istruzione superiore e la formazione continua comprenderanno una sezione dedicata alla sicurezza digitale.

4. Contribuire allo sviluppo di un ambiente che favorisca la fiducia nella tecnologia digitale e che possa rendere la sicurezza digitale un fattore di competitività. La Francia sosterrà lo sviluppo dell'economia e la promozione internazionale dei suoi prodotti e servizi digitali e garantirà la disponibilità di prodotti e servizi digitali con livelli di ergonomia, fiducia e sicurezza adeguati agli usi e alle minacce informatiche.

5. Promuovere la cooperazione tra Stati membri dell'Unione Europea (UE) in modo da favorire un'autonomia strategica digitale europea, garanzia a lungo termine di un cyberspace più sicuro e rispettoso dei nostri valori.

Dal punto di vista pratico, i cinque obiettivi saranno raggiunti grazie alla federazione dello sforzo di molti attori. In particolare: l'ANSSI[9] (*Agence Nationale de la Sécurité des Systèmes d'Information*), è l'attore primario incaricato di misurare e valutare i rischi e gli effetti degli attacchi informatici, rivolti sia agli istituti pubblici sia ai privati; la CNIL[10] (*Commission Nationale de l'Informatique et des Libertés*, i.e., la commissione nazionale dell'informatica e delle libertà) sostiene

[9] `https://www.ssi.gouv.fr/`
[10] `https://www.cnil.fr`

i professionisti affinché possano essere conformi ai regolamenti vigenti e aiuta gli individui privati a controllare i loro dati personali ed esercitare i loro diritti; le agenzie di ricerca pubbliche (CNRS, CEA, INRIA) hanno investito sempre di più in attività di ricerca sulla sicurezza digitale; i cluster regionali (come il polo SCS – *Solutions Communicantes Sécurisées* – nella regione Provenza-Alpi-Costa Azzurra, e il PEC – *Pôle d'Excellence Cyber* – in Bretagna) sostengono le industrie locali finanziando progetti di ricerca e condividendo infrastrutture e piattaforme di sviluppo tra le aziende locali; infine, le agenzie di finanziamento (ANR, FUI, DGA) hanno finanziato vari progetti su problemi correlati alla sicurezza digitale.

8.2.1 Agence Nationale de la Sécurité des Systèmes d'Information

Il ruolo dell'ANSSI è quello di promuovere una risposta coordinata, ambiziosa e proattiva ai problemi di cybersecurity in Francia. Una Legge del 2013 prevede che "il Primo Ministro stabilisce politiche e coordina l'azione del governo nel campo della cybersecurity e della ciber-difesa e a tal fine ha a sua disposizione l'ANSSI".

Oltre a garantire il corretto funzionamento della vita quotidiana e la disponibilità dei servizi informatici che sono diventati intrinsecamente legati alle nostre vite, c'è anche un aspetto economico in gioco. Infatti, è essenziale che le aziende si proteggano da attacchi informatici, al fine di salvaguardarne competenze, know-how e competitività.

L'ANSII coordina il Centro per la valutazione della sicurezza dell'informazione (Centre d'Évaluation de la Sécurité des Technologies de l'Information, CESTI) che è un fornitore di servizi per certificare la sicurezza dei prodotti. Un prodotto per essere certificato deve rispettare le regole del regime di certificazione francese, che permette due tipi di valutazione: la conformità ai Common Criteria e la certificazione della sicurezza del primo livello (Certification de Sécurité de Premier Niveau, CSPN) dei prodotti informatici. La CSPN è stata istituita nel 2008 e permette di attestare la sicurezza di prodotti quali software, sistemi operativi e dispositivi hardware. L'ANSII dispone anche di una congrua rete di CERT (si veda il box a pag. 20).

8.2.2 Commission Nationale de l'Informatique et des Libertés

La *Commission Nationale de l'Informatique et des Libertés* (CNIL) è un'autorità amministrativa indipendente che è responsabile di garantire che l'informatica sia al servizio del cittadino e che non violi l'identità e i diritti umani, la privacy, la libertà individuale e quella pubblica. La CNIL analizza l'impatto delle innovazioni tecnologiche emergenti sulla privacy e la libertà e collabora con le

sue controparti europee e internazionali per sviluppare una regolamentazione armonizzata. Le sue missioni principali sono:

- *Informare e proteggere* — La CNIL informa individui e professionisti e risponde alle loro richieste. Fornisce strumenti pratici e pedagogici e interviene regolarmente per animare azioni di formazione e sensibilizzazione, in particolare nel contesto dell'educazione digitale. Chiunque può contattare il CNIL in caso di difficoltà nell'esercizio dei propri diritti.

- *Accompagnare e consigliare* — La regolamentazione sull'uso dei dati personali si attua attraverso vari strumenti che hanno come obiettivo la verifica di conformità delle organizzazioni; viene offerta ai cittadini la possibilità di commentare progetti di legge e decreti, dando raccomandazioni per semplificare le procedure giuridiche e fare richieste di consulenza.

- *Controllare e sanzionare* — L'ispezione in loco o le interrogazioni permettono alla CNIL di verificare la conformità concreta rispetto alla legge. Un programma di controlli viene elaborato in base ai temi di attualità, ai principali problemi identificati e alle denunce effettuate. La CNIL è responsabile del controllo dei sistemi di video-protezione autorizzati dalle prefetture.

- *Anticipare* — La CNIL rileva e analizza le tecnologie che possono avere impatti significativi sulla privacy ed ha un laboratorio che consente di sperimentare prodotti o applicazioni innovativi. Contribuisce allo sviluppo di soluzioni tecnologiche che proteggano la privacy, consigliando le aziende a tutti i livelli, nello spirito di un'implementazione di privacy-by-design. Per rafforzare la sua efficacia, la CNIL ha creato un comitato di consulenti esterni che contribuiscono alla definizione di un programma annuale di studi e ricerche.

8.2.3 Centri pubblici di ricerca

In Francia, molti sforzi sono stati dedicati alla sicurezza digitale nell'ultimo anno. In particolare, il CNRS (Centre National de la Recherche Scientifique) ha dedicato il 2016 alla sicurezza e recentemente ha creato un gruppo di ricerca (Groupement De Recherche, GDR) dedicato alla sicurezza digitale. Il GDR per la cybersecurity è uno strumento di stimolo per la ricerca scientifica. Gli argomenti trattati dal GDR comprendono la crittografia, la protezione della privacy, la sicurezza di dati multimediali, la sicurezza di reti e infrastrutture, la sicurezza dei sistemi software e hardware, e i metodi formali per la sicurezza.

Il GDR organizza annualmente vari eventi: una scuola estiva in cybersecurity; una settimana d'incontri tra aziende e studenti di dottorato (REDOCS), dove i dottorandi lavorano in gruppi per affrontare problemi reali e per confrontarsi

con le migliori aziende del settore; le "giornate nazionali" (simile a una conferenza) presso la sede CNRS di Parigi; e l'Atelier sur la Protection de la Vie Privée (workshop sulla protezione della vita privata), il cui obbiettivo è quello di riunire ricercatori della comunità francofona il cui lavoro si concentra sulla protezione della privacy e dei dati personali, offrendo loro un forum privilegiato per presentare e scambiare le proprie idee su questo tema. Il workshop è multidisciplinare e mira a riunire ricercatori in informatica, diritto, economia, sociologia e statistica.

8.2.4 Finanziamenti pubblici

L'agenzia di ricerca pubblica (Agence Nationale de la Recherche, ANR), ha finanziato, dal 2012, 35 progetti sulla cybersecurity. Il finanziamento di questi progetti è stato di 6 milioni di euro nel 2012, 3 milioni nel 2013, 6 milioni nel 2014, 1.5 milioni nel 2015 e 3.8 milioni nel 2016.

8.3 Germania

Sin dagli anni 80, il governo tedesco ha mantenuto un atteggiamento aggressivo nello sviluppo delle tecnologie ICT, nello sviluppo di tecnologie a banda larga e nel combattere il digital divide nelle aree rurali. Questo atteggiamento ha permesso alla Germania di diventare leader europeo nel settore dell'ICT e quarto al mondo[11]. I progressi compiuti in questo settore hanno fatto sì che la Germania si confrontasse con le sfide della sicurezza dell'informazione e delle telecomunicazioni in anticipo rispetto ad altri stati europei.

Ad esempio, una delle prime iniziative intraprese dal governo federale tedesco è stata l'istituzione dell'Ufficio Federale per la Sicurezza dell'Informazione (Bundesamt für Sicherheit in der Informationstechnik, BSI) i cui obiettivi, descritti nell'omonima legge, prevedono la protezione delle reti informatiche del governo federale, la verifica e certificazione dei software e servizi, la consulenza per l'amministrazione federale, e, più recentemente, l'allerta da infezioni da malware.

La strategia nazionale sulla cybersecurity e sulla sicurezza informatica è inserita in un contesto di innovazione più ampio che copre tutti i settori strategici ad alta tecnologia. Tale strategia, chiamata "High-Tech Strategie 2020", è descritta in una serie di documenti redatti a partire dal 2006 e aggiornata con cadenza quadriennale. Tale piano viene sviluppato dietro le raccomandazioni di un pa-

[11] `http://www.make-it-in-germany.com/en/for-qualified-professionals/working/industry-profiles/it-and-telecommunications`

nel di esperti che dal 2006 al 2013 ha ospitato prima solo membri della ricerca e dell'industria[12], e, a partire dal 2014, anche membri della società civile.

La cyber e l'IT security vengono affrontate all'interno della priorità "Innovazione per una vita mobile e interconnessa" del piano strategico. In particolare, il governo tedesco riconosce che la messa in sicurezza dell'infrastruttura delle telecomunicazioni e dell'informazione è una delle principali priorità. Le soluzioni ricercate devono offrire integrità, confidenzialità e disponibilità nell'ICT in generale e in particolare nelle infrastrutture critiche per la produzione industriale, la navigazione degli aeroplani, l'industria automobilistica e la gestione del traffico. Inoltre, il governo ritiene prioritaria la ricerca su procedure e tecniche per la difesa da software malevolo[13].

Il piano strategico del 2010 rinnova l'interesse sulle tematiche della sicurezza e introduce una nuova priorità sulle identità digitali. In questo contesto il governo tedesco intende creare processi sicuri per l'autenticazione e la gestione delle identità elettroniche e una infrastruttura affidabile, sicura e flessibile basata sulle nuove carte di identità. I progetti sul tema della sicurezza sono stati rifinanziati per i successivi quattro anni[14].

Il piano strategico del 2014 espande e dettaglia ulteriormente le priorità nel campo di cyber e IT security. Il nuovo piano introduce il termine "Sicurezza Civile" entro la quale vengono racchiuse tutte le priorità nel campo della sicurezza informatica, individuando come aree chiave:

- Cybersecurity: le sfide identificate dal piano riguardano tutte le azioni criminali che possono violare privacy o segreti industriali, mirando all'accesso e alla intercettazione non autorizzata ai dati. Il governo intende dare priorità alla ricerca sull'informatica forense e criminologia. L'implementazione del programma è descritto nel "Cyber Security Strategy for Germany";

- IT security: le sfide in quest'area riguardano la sicurezza informatica e delle reti nel senso classico: affidabilità e sicurezza. Al riguardo, il governo intende sviluppare ulteriori competenze nello sviluppo e la protezione dell'IT. Il governo federale supporta la ricerca nell'IT security con due programmi di finanziamento: "Self-Determined and Secure in the Digital World" per la ricerca accademica, e "IT Security in Industry" per le piccole e medie imprese per migliorare i loro livelli di sicurezza;

[12] http://www.forschungsunion.de/

[13] https://www.fona.de/pdf/publikationen/die_hightech_strategie_fuer_deutschland.pdf

[14] http://www.ibbnetzwerk-gmbh.com/fileadmin/Content/Foerderprogramme%20und%20pdfs/BMBF%20%20Ideen.Innovation.Wachstum%20Hightec2020%202010.pdf

- Identità sicure: la sicurezza delle identità sono l'elemento di particolare interesse per il governo tedesco. Esse sono alla base della privacy, del commercio e degli affari su Internet. Il governo continua a supportare la ricerca nella creazione di nuovi approcci interdisciplinari con un forum "Privacy - Self-Determined Living in the Digital World".

Il piano strategico sulla cybersecurity e sicurezza informatica è implementato attraverso diversi piani. Il primo è puramente di ricerca ed è implementato nel "Self-Determined and Secure in the digital World 2015-2020" e, in parte, nel "Research for Civil Security 2012 – 2017". Questo programma è attuato dal ministero dell'educazione e della ricerca. Il secondo, "Strategia sulla Cyber Sicurezza in Germania", è focalizzato sulla cybersecurity ed è attuato dal ministero degli interni[15].

8.3.1 Implementazione del Piano Strategico

Il ministero federale della ricerca e dell'educazione (Bundesministerium für Bildung und Forschung, BMBF) favorisce lo sviluppo di soluzione ai problemi di sicurezza informatica mettendo a disposizione fondi per la ricerca e l'innovazione (accademica e industriale) e tramite il finanziamento di appositi centri di competenza esclusivamente orientati alla cybersecurity.

ICT 2020 e Research for Civil Security Per affrontare le sfide del piano strategico, il governo Federale ha creato nel 2007 un programma di finanziamento alla ricerca nelle tecnologie per l'informazione e le telecomunicazioni chiamato ICT 2020 (IKT 2020 - Forschung für Innovation) gestito dal BMBF che fornisce fondi per la ricerca in quasi tutte le aree ICT.

Il nuovo piano strategico 2015-2020, *Self-determined and secure in the digital world*, ha considerevolmente ampliato gli argomenti di ricerca nel campo della cybersecurity e copre 17 aree di ricerca organizzate in quattro aree principali:

- Alta tecnologia per l'IT security: Hardware-based trusted platform modules, gestione delle identità digitali, crittografia efficiente e sicura nel lungo termine, comunicazione quantistica, nuove tecnologie di sicurezza;
- Sistemi informativi sicuri, aperti e affidabili: Trasparenza e facilità di utilizzo, protezione da attacchi Internet, sicurezza dimostrabile dei sistemi informatici, IT security in strutture di sistemi eterogenei, protezione della conoscenza e del prodotto;

[15] `https://www.bmbf.de/pub/HTS_Broschuere_eng.pdf`

- Campi di applicazione dell'IT security: Sicurezza informatica per *Impresa 4.0*, sicurezza informatica per le infrastrutture critiche, applicazioni delle tecnologie dell'informazione e della comunicazione nella medicina, sicurezza informatica nel trasporto e nella logistica;
- Privacy e protezione dei dati: Privacy e autodeterminazione nel mondo digitale, cultura Internet e shift dei valori nell'era dell'Internet, privacy e big data.

8.3.2 Centri di Competenza e Azioni Speciali

Il governo federale Tedesco ha anche finanziato la creazione di tre centri di ricerca la cui missione è diventare un punto di riferimento nazionale e internazionale dove raccogliere tutte le competenze sui temi della sicurezza informatica:

- CISPA, Centre for IT Security, Privacy and Accountability in Saarbrücken[16];
- EC SPRIDE, European Centre for Security and Privacy by Design in Darmstadt[17];
- KASTEL, Centre of Competence for Applied Security Technology in Karlsruhe[18],[19].

I centri sono stati finanziati in due fasi: 2011-2015 e 2016-2020. L'ammontare totale del finanziamento del 2011 per i tre centri è stato di 17 milioni di euro su quattro anni. Nel 2015, il governo federale ha rinnovato il finanziamento elevando la somma totale a 41 milioni di euro in quattro anni.

Helmholtz Center on IT Security: CISPA Nel 2017, il governo federale Tedesco, lo stato federato della Saarland, in collaborazione con l'Associazione Helmholtz, hanno deciso di istituire un centro di ricerca sulla cybersecurity e sicurezza informatica a Saarbruecken. Il nuovo centro assorbirà l'attuale centro di competenza CISPA con i suoi 200 ricercatori, con l'obiettivo, nel medio termine, di ospitare più di 500 ricercatori in tutte le aree della sicurezza informatica.

[16] `https://www.bmbf.de/de/geballte-kompetenz-fuer-it-sicherheit-1723.html`

[17] urlhttps://www.bmbf.de/de/groesstes-europaeisches-forschungszentrum-fuer-it-sicherheit-gegruendet-2023.html

[18] `https://www.forschung-it-sicherheit-kommunikationssysteme.de/service/aktuelles/kompetenzzentrum-fuer-it-sicherheitsforschung-kastel-startet-durch`

[19] `https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/kastel`

Il nuovo centro è attualmente in fase di costruzione e diverrà operativo a partire dal 2018[20].

Finanziamenti alle piccole e medie imprese La Germania è uno dei pochi paesi che non offre incentivi alla ricerca e sviluppo sotto forma di credito fiscale. Tuttavia, il BMBF, a partire dal 2007, ha messo a disposizione finanziamenti per sostenere la ricerca nel campo della sicurezza informatica all'interno delle PMI. Le aree nelle quali il governo intende supportare le PMI sono: Privacy e protezione dei dati, IT security in networked systems and applications, secure and trustworthy ICT systems and technologies, procedures and tools for handling IT security incidents. Finora Il BMBF ha approvato un finanziamento superiore al miliardo di euro per più di 1.500 progetti individuali o collaborativi i quali hanno coinvolto circa 2.500 PMI[21].

8.4 Regno Unito

Lo sviluppo della cyber security in Gran Bretagna è stata guidato molto attentamente dal governo e in particolare dal Cabinet Office (equivalente della Presidenza del Consiglio dei Ministri) e dai servizi di sicurezza (equivalente di NSA in USA). La spinta si è focalizzata sia sulle università, per ricerca e formazione, sia sulle aziende e, naturalmente sulle loro relazioni. Nel seguito vengono illustriate le principali caratteristiche di queste iniziative.

8.4.1 Centri accademici di eccellenza in cybersecurity

Nel 2011 il governo lanciò un esercizio per identificare le capacità di ricerca universitaria in cybersecurity esistenti del paese. Otto università (Belfast, Bristol, Imperial College, Lancaster, Newcastle, Oxford, Southampton e University College London) furono inizialmente riconosciute come centri di eccellenza, con l'obiettivo di aiutarle a sviluppare le loro capacità, veicolare risorse e informazione. Nel 2017 i centri di eccellenza sono diventati 14 (con l'ingresso di Birmingham, Cambridge, Edinburgh, Royal Holloway, Surrey e Warwick). La cooperazione tra i vari centri è fortemente sostenuta dal governo con l'obiettivo di favorire un'agenda condivisa a livello nazionale, sia in ambito accademico sia nel mondo industriale e governativo[22].

[20] https://www.saarland.de/dokumente/thema_innovation/2017-03-14_41_Forschungszentrum_fuer_IT-Sicherheit_EN.pdf

[21] https://www.bmbf.de/de/kmu-innovativ-561.html

[22] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496340/ACE-CSR_Brochure_accessible_2015.pdf

8.4.2 Istituti di ricerca in cybersecurity

A corredo della creazione dei centri di eccellenza per la ricerca, il governo ha creato, in fasi successive, quattro istituti di ricerca in cybersecurity, nell'ordine:

- *Research Institute on Science of Cyber Security* – RISCS,
- *Research Institute on Verified Trustworthy Software Systems* – RIVeTSS
- *Research Institute on Trustworthy Industrial Control Systems* – RITICS
- *Research Institute on Hardware Security.*

Gli istituti sono guidati da un direttore che ha la responsabilità di selezionare specifici progetti di ricerca, di promuovere la collaborazione con industrie, e di facilitare la nascita di comunità di ricerca intorno agli istituti.

RISCS[23] si dedica alla comprensione della sicurezza complessiva delle organizzazioni, inclusi le componenti tecnologiche, umane e di processo. Il suo obiettivo principale è quello di supportare le organizzazioni nel loro processo decisionale in ambito cybersecurity, favorendo la corretta analisi dei rischi presenti, dei loro effetti e dei costi/vantaggi delle contromisure applicabili. Lo scopo ultimo è quello di offrire alle organizzazioni gli strumenti più adeguati per prendere decisioni informate sulle politiche di cybersecurity.

RIVeTSS[24] si dedica alla valorizzazione e al finanziamento di attività di ricerca accademica e industriale in ambito cybersecurity, occupandosi in particolare di verifica di programmi. L'istituto riunisce tutte le attività di avanguardia in ambito di analisi e verifica di programmi favorendo lo sviluppo di teorie e strumenti industriali per la verifica di applicazioni reali. L'obiettivo ultimo è offrire strumenti di verifica sempre aggiornati e capaci di stare al passo con la rapida evoluzione di sistemi dello spazio cyber.

RITICS[25] si dedica allo studio in ambito cybersecurity dei sistemi di controllo industriale e delle infrastrutture critiche nazionali. L'istituto coinvolge i più rappresentativi progetti di ricerca accademica nel settore fortemente legati al mondo dell'industria. Questi progetti ambiscono a identificare tre questioni chiave: i pericoli e le minacce reali, i rischi di impresa da considerare, le tecniche all'avanguardia di difesa più efficaci e efficienti.

RIHS[26] si dedica allo studio di tecniche di sicurezza per componenti hardware. L'istituto riunisce virtualmente tutte le attività accademiche del settore, favorendo la creazione di collaborazioni e trasferimento tecnologico nel

[23] `https://www.riscs.org.uk`

[24] `http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/P021921/1`

[25] `https://ritics.org`

[26] `https://www.ncsc.gov.uk/information/research-institute-hardware-security`

mondo dell'industria. In tale ambito, l'istituto favorisce la divulgazione e l'apprendimento del corretto utilizzo nello spazio cyber delle ultime tecnologie hardware.

8.4.3 National Cyber Security Center

Il National Cyber Security Center (NCSC) supporta e finanzia una serie di iniziative a livello nazionali.

Certificazione di corsi di studio in cybersecurity Il governo offre un meccanismo di certificazione per corsi di studio in cybersecurity, con l'obiettivo di garantirne qualità e fruibilità. Questo crea un ciclo virtuoso dal momento che tale certificazione attira i migliori studenti da tutto il mondo, garantendo all'industria il reclutamento continuativo di personale qualificato e la formazione professionale di abilità correlate alla cybersecurity per il personale preesistente. Le certificazioni garantiscono agli studenti una scelta consapevole del loro corso di studio, così da ottenere una qualifica di esperti in cybersecurity altamente spendibile in ambito industriale.

Finanziamento di borse di dottorato in cybersecurity Il governo sovvenziona annualmente un programma di dottorato per studenti dei centri di eccellenza. Il governo assiste annualmente gli studenti offrendo loro tirocini estivi presso NCSC o GCHQ su argomenti d'avanguardia in cybersecurity. La cooperazione tra governo e centri di eccellenza favorisce lo sviluppo di un'agenda di cybersecurity comune tra governo, industria e accademia.

Finanziamento dei centri di alta formazione in cybersecurity Il governo finanzia correntemente due scuole di dottorato in Cybersecurity, a Oxford[27] e Royal Holloway[28]. Questi centri offrono oltre 25 posti di dottorato in cybersecurity interamente sponsorizzati, e forniscono una spina dorsale per l'intero paese capace di assicurate la formazione di nuovi esperti in cybersecurity per l'industria e l'accademia. I centri offrono programmi multidisciplinari di formazione e ricerca che permettono la formazione di esperti capaci di rispondere ai bisogni di cybersecurity in ambiti noti o emergenti del cyber space. La diversità di competenze e abilità favorisce la creazione di tecniche innovative di difesa da attacchi cyber e il loro continuo adattamento nel tempo.

[27] `https://www.cybersecurity.ox.ac.uk/education/cdt`
[28] `https://www.royalholloway.ac.uk/isg/cybersecuritycdt/home.aspx`

8.4.4 Altre Iniziative

Global Cyber Security Capacity Centre Il Global Cyber Security Capacity Centre (GCSCC) è un centro di avanguardia per lo sviluppo e la creazione di programmi di formazione in cybersecurity adeguati e aggiornati alle esigenze del mondo reale. Il ruolo di GCSCC è quello di sviluppare un programma integrato tra tutte le aree di cybersecurity che garantisca alla pubblica amministrazione e all'industria politiche e investimenti in cybersecurity efficaci e effettivi. Le attività sono all'avanguardia in ambito internazionale e coinvolgono attori di primo piano dell'industria e del mondo governativo.

Cyber Invest Cyber Invest[29] è uno schema governativo per incentivare investimenti di industrie private nelle attività di ricerca dei centri universitari di eccellenza. Gli investimenti sono gestiti tramite programmi governativi di finanziamenti alla ricerca e favoriscono la creazione di nuove relazioni tra università, industria e governo allo scopo ultimo di confermare a livello globale il ruolo UK in ambito cybersecurity.

Cyber First Cyber First[30] è uno schema governativo per incentivare studenti delle scuole superiori a intraprendere carriere in cybersecurity. Consiste di un programma di scuole estive di orientamento da intraprendere prima della scelta di un corso universitario. Questo schema offre anche borse di studio per coprire il costo di corsi universitari in cybersecurity. Lo scopo ultimo di questo schema è quello di migliorare le abilità di base in cybersecurity dei futuri professionisti per l'industria.

Cyber Security Academy Una particolare iniziativa di rilevanza nazionale è la Cyber Security Academy dell'Università di Southampton (CSA)[31]. La CSA è un programma di collaborazione tra l'Università e industrie leader nel settore cybersecurity, al momento Defence Science Technology Laboratory (ovvero il laboratorio tecnologico del Ministero della Difesa UK), Northop-Grumman e Roke Manor. L'obiettivo della CSA è favorire la collaborazione tra Università e industria tramite un approccio strutturato basato su quattro elementi fondanti: ricerca, innovazione, formazione e divulgazione. Grazie alla stretta relazione

[29] `https://www.ncsc.gov.uk/articles/cyberinvest-securing-our-future-through-research`

[30] `https://www.gov.uk/government/news/cyber-first-improving-cyber-skills-in-the-uk?`

[31] `https://www.southampton.ac.uk/research/centres/cyber-security-academy.page`

tra i gruppi di ricerca dell'Università, la CSA offre un ampio portafoglio di progetti di ricerca di interesse industriale, un programma annuale di dottorato industriale, consulenza e programmi di formazioni professionale su tematiche di avanguardia di cybersecurity. Al momento, CSA offre programmi di formazione sia per manager, con particolare enfasi sui rischi cyber e sulla nuova regolamentazione Europea in ambito privacy GDPR, sia per tecnici del settore, con particolare enfasi su penetration testing e sistemi blockchain.

8.5 Singapore

Singapore affronta le tematiche di cybersecurity con un approccio basato su un'azione congiunta tra Governo, settore privato e mondo accademico.

L'Agenzia nazionale di Cyber Security (CSA) è l'organo nazionale che sovrintende alle strategie, alle operazioni, all'educazione ed allo sviluppo dell'ecosistema di cybersecurity. Il CSA è un dipartimento del Prime Minister's Office (PMO), organo che si occupa di tutte le questioni di maggior importanza per il Governo, ed è gestita dal Ministro delle Comunicazione e delle Informazioni (MCI).

Con un approccio prevalentemente top-down, il Governo di Singapore crea una serie di direttive che tipicamente si concretizzano in un progetto di legge e sono implementate con l'ausilio del settore privato e del mondo accademico. In particolare il disegno di legge per la cybersecurity nazionale, presentato nella seconda metà del 2017 e in approvazione nel 2018, prevede sostanziali investimenti pubblici e privati che mirano alla creazione di un ecosistema nazionale di cybersecurity.

Tra gli obiettivi principali del Governo si distingue la costruzione di un tessuto nazionale di esperti di cybersecurity. A tale scopo il CSA, in collaborazione con aziende locali ed internazionali leader nel settore, sta creando un'accademia nazionale di training per professionisti di Cybersecurity che saranno impiegati sia in infrastrutture governative che in infrastrutture critiche (CII) come energia, sanità e trasporti con l'intento di fornire più sicurezza e capacità di resilienza alla comunità digitale di Singapore. Il CSA ha anche contribuito alla stesura delle linee guida per i sistemi di controllo industriale utilizzati nelle infrastrutture critiche del Paese.

Per incentivare aziende, professionisti e studenti a contribuire in modo significativo all'ecosistema di cybersecurity, il Governo di Singapore organizza il Cybersecurity Awards in cui si riconosce e si premia il talento professionale messo a disposizione del Paese.

A livello internazionale, Singapore lavora a stretto contatto con i CERT nazionali. Ad esempio all'epoca dell'attacco ransomware wannacry il CSA ha scambiato informazioni e strategie con il Regno Unito e ha condiviso l'analisi

con la comunità CERT Asia Pacific. Un'altra area di cooperazione internazionale è rappresentata dalle infrastrutture critiche che hanno impatto oltre il Paese. In questo caso il CSA porta avanti azioni coordinate ed esercitazioni ricorrenti per validare la capacità di reagire a potenziali attacchi realizzati per colpire infrastrutture critiche internazionali come, ad esempio, sistemi di pagamento globali, sistemi di controllo del traffico aereo, etc.

Negli ultimi anni il CSA ha firmato Memorandum of Understanding sulla cooperazione in ambito cybersecurity con le agenzie nazionali di sicurezza di diversi Paesi tra cui, in ordine cronologico, Francia, Regno Unito, India, Olanda, Stati Uniti, Australia, Germania e Giappone.

Dal punto di vista della realizzazione di sistemi e infrastrutture di cybersecurity, Singapore opera secondo una precisa metodologia che parte dalla consapevolezza del problema per arrivare alla soluzione Paese analizzando (mediante installazione e test) tutte le soluzioni tecnologicamente più avanzate disponibili sul mercato e decidendo se uno o più sistemi meritino di essere integrati ed adottati. In seguito alla fase di analisi, che si declina con una valutazione tecnica estremamente accurata talvolta accompagnata da una forte acquisizione di know-how, si decide se procedere con l'adozione delle soluzioni *as-is* oppure realizzare localmente un prodotto che risponda appieno alle necessità del Paese. Questo modus operandi richiede un investimento considerevole sia in termini economici che in termini di effort; esso ha, tuttavia, il vantaggio di fornire una panoramica globale delle strategie presenti sul mercato globale, tramite l'interazione con i maggiori player del settore, con notevoli benefici in termini di crescita di know-how.

A livello di investimenti e finanziamenti, il Governo di Singapore ha stanziato circa 10 milioni di euro tramite il National Research Foundation (NRF), dipartimento del PMO che definisce i trend nazionali di ricerca e sviluppo, per attivare progetti di cyber security ad alto potenziale di commercializzazione o di sviluppo di competenze che rispondano alle esigenze di sicurezza del Paese. Ogni progetto è una collaborazione tra un'azienda del settore privato e un ente di ricerca o accademico. Tra i progetti di maggior interesse si evidenziano quelli basati su tecnologie di machine learning ed intelligenza artificiale, soprattutto in ambito di infrastrutture critiche, che riducono drasticamente i tempi di reazione nel rilevare comportamenti anomali che potrebbero indicare attacchi in corso.

La fondazione nazionale per la ricerca (NRF) in collaborazione con l'Università statale di Singapore (NSU) ha inoltre creato il Singapore Cybersecurity Consortium (SCC), con l'intento di massimizzare le sinergie tra agenzie governative, il settore privato e mondo accademico incoraggiando attività congiunte di ricerca, trasferimento di know-how, training, e technology awareness.

8.6 USA

Negli Stati Uniti la cybersecurity coinvolge diversi dipartimenti e agenzie governative che spesso si focalizzano sugli aspetti della sicurezza informatica più specifici del proprio settore. Gli attori più attivi sono:

1. *Department of Homeland Security* (DHS) — L'interesse del dipartimento per la protezione nazionale è focalizzato sulla protezione delle infrastrutture critiche, tra cui le infrastrutture energetiche e di trasporto e su strumenti per il controllo delle frontiere e dell'immigrazione, quali le tecniche biometriche per l'identificazione e l'autenticazione.

2. *Department of Defence* (DoD) — L'interesse del dipartimento della difesa è focalizzato su varie tematiche di sicurezza sia di base, come le tecniche di difesa da attacchi cyber [32], sia applicative.

3. *Department of Energy* (DoE) — L'interesse del dipartimento dell'Energia è focalizzato sulla protezione delle infrastrutture per l'energia e sullo sviluppo di strumenti per la gestione della sicurezza (quali gestione delle chiavi pubbliche) in tali infrastrutture.

4. *National Institute of Standards and Technology* (NIST) — È attivo da circa 20 anni in tutti gli aspetti della sicurezza informatica per le applicazioni governative e nello sviluppo di standard per la sicurezza (quali lo standard per il modello Role-Based Access Control – RBAC).

5. *Department of Justice* (DoJ) — L'interesse del dipartimento della giustizia è focalizzato sulle problematiche di digital forensics e sull'uso di tecniche digitali per attività investigative e forensi.

6. *National Security Agency* (NSA) — L'interesse dell'Agenzia Nazionale per la Sicurezza è focalizzato su diverse tematiche, tra cui la Cybersecurity Science.

7. *Federal Bureau of Investigation* (FBI) — FBI è la principale agenzia federale per quanto riguarda le indagini relativi ad attacchi informatici da parte di criminali, terroristi e avversari di altre nazioni. In particolare, FBI ha una divisione specializzata nella sicurezza informatica e collabora attivamente con altri dipartimenti governativi, tra cui DoD e DHS, a varie attività relative alla sicurezza informatica. FBI coordina varie iniziative rivolte ad aspetti diversi della sicurezza informatica, tra cui l'Internet Crime Complaint Center, il Cyber Action Team, la National Cyber Forensics and Training Alliance.

[32] `https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf`

A livello governativo, le varie amministrazioni hanno spesso nominato un responsabile nazionale per la cybersecurity (indicato con il termine cybersecurity czar) e la passata amministrazione aveva varato un piano nazionale per la sicurezza informatica[33].

8.6.1 Università e altri enti di ricerca e sviluppo

Le università statunitensi sono molto attive su tematiche di ricerca e su insegnamenti connessi alla cybersecurity. Numerosi atenei hanno, infatti, centri e istituti che si occupano di cybersecurity, spesso con specifiche specializzazioni. Una recente classifica ha elencato le 20 migliori università per la didattica e la ricerca della cybersecurity; le prime 3 università in tale classifica sono Purdue University, Georgia Institute of Technology, University of Washington at Seattle:

- *Purdue University* — oltre a un MS e PhD in cybersecurity, Purdue ha un MS e un PhD in Computer and Information Technology con una specializzazione in cyber forensics. Inoltre i corsi di MS e PhD in computer science hanno svariati insegnamenti relativi alla cybersecurity (tra cui crittografia, sicurezza di reti, sicurezza e privatezza di dati, sicurezza di sistemi, tecniche per lo sviluppo sicuro di software, tecniche analitiche per la sicurezza). Purdue è inoltre la sede del Center for Education in Research in Information Assurance and Security (CERIAS) a cui afferiscono professori e studenti da sei diverse facoltà e da oltre 20 dipartimenti e che svolge ricerca su tutti gli aspetti della cybersecurity, con una forte enfasi multidisciplinare.
- *Georgia Institute of Technology* — ha un master in cybersecurity articolato in tre specializzazioni (sicurezza delle informazioni, sicurezza dei sistemi per l'energia, politiche per la sicurezza). GeorgiaTech è sede dell'Istituto per la sicurezza e riservatezza delle informazioni (Institute for Information Security & Privacy (IISP)).
- *University of Washington at Seattle* — ha una laurea di primo livello (BS) con una specializzazione in "Information Assurance and Cybersecurity (IAC)" con professori dai vari campus dell'università. Ha anche un certificato on-line in cybersecurity, diretto a professionisti e tecnici già in ambito lavorativo. La ricerca è svolta principalmente presso il Security and Privacy Research Lab, che è parte della School of Computer Science and Engineering. Pertanto la ricerca è principalmente focalizzata sugli aspetti più tradizionali della cybersecurity. Ricerca di tipo multidisciplinare è svolta come parte della Cybersecurity Initiative[34] presso l'International

[33] `https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan`

[34] `https://jsis.washington.edu/research/ipi/ipi-cybersecurity/`

Policy Institute (IPI).

Quello che si evince da un'analisi delle initiative di ricerca e didattica è che in molti casi, oltre a tematiche di ricerca tradizionali, ci sono initiative multidisciplinari spesso innovative e di notevole interesse. La didattica è inoltre molto attiva, con percorsi specializzati all'interno dei curriculum di Computer Science e Computer Engineering, ma anche con master dedicati alla cybersecurity e altre iniziative rivolte a professionisti già in ambito lavorativo. C'è da segnalare che in US vi è una fortissima richiesta di studenti con competenze nell'ambito della cybersecurity e le aziende sono pertanto molto attive nel supporto di iniziative didattiche presso le università.

In aggiunta alle università, altre attività di ricerca e sviluppo sono condotte da numerose aziende nel settore ICT (da IBM a Google a Facebook). Oltre a queste ci sono aziende specializzate nella sicurezza informatica (tra cui le ben note Symantec e RSA) e altre organizzazioni e laboratori, come la MITRE Corporation, un'organizzazione no-profit che gestisce centri di ricerca e sviluppo finanziati dal governo federale, ed il MIT Lincoln Lab, fondato nel 1951 per attività connesse alla difesa nazionale.

8.6.2 Finanziamenti

Esistono numerosi programmi di finanziamento a supporto della ricerca sulla cybersecurity. Il programma principale è il programma SaTC (Security and Trustworthy Cyberspace) della NSF, le cui tematiche di ricerca sono allineate con le priorità del governo federale. Il programma, che per il 2018 ha un finanziamento totale di 68 milioni di dollari, finanzia, oltre a progetti di ricerca di base, anche progetti finalizzati alla didattica della cybersecurity. Oltre al programma SaTC, tematiche di cybersecurity sono presenti in numerosi altri programmi della NSF, come ad esempio il programma CPS (Cyberphysical Systems) ed il programma CICI (Cybersecurity Innovation for Cyberinfrastructure). In aggiunta alla NSF, vari dipartimenti governativi (in particolare DHS, DoD, DoE, DoJ) hanno programmi a supporto della ricerca in ambito accademico e per progetti di ricerca congiunti industria-università.

A questo si aggiungono i numerosi programmi di ricerca finanziati dal DARPA che hanno riguardato varie tematiche relative alla cybersecurity, tra cui modelli formali per la cybersecurity dei veicoli militari, e tecniche per la protezione da advanced persistent threats. Finanziamenti sono anche disponibili per progetti relativi a tematiche di privatezza dei dati personali; ad esempio il programma Brandeis (finanziato dal DARPA) ha recentemente finanziato progetti che si occupano di diversi aspetti relativi alla privacy, dallo sviluppo di tecniche efficienti di crittografia per poter operare su dati criptati allo sviluppo di metriche specifiche per la privacy. A queste fonti di finanziamento si aggiungono finan-

ziamenti dalle aziende, in particolarele aziende impegnate in applicazioni per il governo degli US e nel settore aereo-spaziale.

CAPITOLO

9 Conclusioni

La digitalizzazione della nostra vita porta con sé opportunità e minacce. Dobbiamo essere pronti a cogliere le infinite opportunità di sviluppo e gestire la complessità che questa trasformazione introduce. Se non gestita appropriatamente, la complessità diventerà una minaccia difficile da contenere, con conseguenze rilevanti sull'indipendenza e sullo sviluppo del Paese. Per questo, la messa in sicurezza del cyberspace nazionale è un obiettivo strategico da perseguire nel tempo.

Il collasso spazio-temporale generato dal cyberspace e l'anonimato pressoché garantito cambiano il fattore di scala e abbattono il costo di operazioni sempre esistite, quali propaganda, spionaggio e furto, che nel passato erano altamente rischiose, lunghe e difficili da gestire. Le fake news rappresentano, ad esempio, l'evoluzione della disinformazione e della propaganda (*soft power* e дисинформазиа) mirate a destabilizzare e confondere i cittadini di un paese.

Le campagne di *ramsonware*, come *wannacry* e *notpetya*, il phishing, le fake news sono la punta emersa di un iceberg che include tutte le minacce portate dalla trasformazione digitale. La parte sommersa dell'iceberg è caratterizzata da migliaia di campagne giornaliere di attacchi, mirate o a largo spettro, portate avanti da stati sovrani, cyber-criminali e attivisti politici e che hanno come obiettivo le infrastrutture critiche nazionali, le aziende, le infrastrutture governative e i cittadini al fine di sottrarre dati, monitorare comportamenti, controllare funzionamenti, truffare, ...

Come abbiamo visto nei precedenti capitoli, una politica nazionale deve essere multidimensionale e operare lungo diverse direzioni, con un chiaro nucleo centrato sulla tecnologia digitale e sulla sicurezza informatica e deve tener conto che, come per quasi tutti i paesi europei, abbiamo pochissima disponibilità

di hardware nazionale (in genere l'hardware utilizzato è di origine cinese o statunitense), i software vengono molto spesso importati e gli Industrial Control System sono, per la maggior parte, tedeschi.

Una politica corretta di cybersecurity nazionale deve gestire la minaccia derivante dalla trasformazione digitale e mantenerla all'interno di un rischio accettabile nel tempo. Coniugare competitività economica del Paese sulla scena internazionale con la tutela dell'interesse e della sicurezza nazionale è la vera sfida per una politica cyber nazionale.

I recenti attacchi *Meltdown* e *Spectre* (considerati nella sez. 4.1) hanno dimostrato che in un sistema di elaborazione non vi sono parti sicure e purtroppo non esiste una *pallottola d'argento* in grado di risolvere tutti i problemi. Vanno trovate soluzioni articolate per sviluppare computazioni sicure tramite un sistema distribuito da considerarsi intrinsecamente insicuro che, ad esempio, contiene le nostre informazioni sensibili. Questa sarà la principale sfida tecnica del futuro.

Una politica adeguata dovrebbe favorire la creazione di una serie di infrastrutture abilitanti alla cybersecurity nazionale (come quelle descritte nel cap. 2) nel pubblico, nel privato e attraverso partnership pubblico-private. Questo sviluppo deve essere inquadrato all'interno di una strategia nazionale che coordini l'azione dei centri di competenza verticali, connettendo poi a rete centri di competenza omologhi. Organizzazioni pubbliche e private dovrebbero mettere in campo, da sole o attraverso partenariati, le azioni e tecnologie abilitanti e le azioni trasversali riportate, rispettivamente, nei capitoli 3, 4 e 6. Infine, le organizzazioni dovrebbero proteggere le tecnologie che stanno guidando, o guideranno, la trasformazione digitale alla quale saranno sottoposte (cap. 5). La politica nazionale di cybersecurity dovrebbe essere supportata da adeguati finanziamenti pubblici, poiché tutto ciò che abbiamo descritto concerne direttamente la sicurezza nazionale. Tuttavia anche le organizzazioni private dovranno fare la loro parte, destinando risorse adeguate al rafforzamento delle proprie difese, poiché questo sarà di beneficio al mantenimento della loro reputazione e delle loro capacità di continuare a produrre beni e/o erogare servizi.

Una politica corretta di cybersecurity deve vedere i vari dicasteri, l'industria e la ricerca unite e coordinate per costruire un Paese resiliente ai nuovi attacchi che possono impattare direttamente sui nostri valori e sulla nostra democrazia, oltre che sulla nostra prosperità. È un processo continuo, basato non solo sulla tecnologia, ma anche su consapevolezza, formazione e cultura digitale.

In conclusione, nel prosieguo di questo capitolo presentiamo alcune raccomandazioni che, se seguite, permetteranno di rispondere in modo adeguato

alla sfida della trasformazione digitale. Le raccomandazioni non intendono essere esaustive, ma vanno a toccare dei punti che riteniamo essenziali per una corretta implementazione di una politica di sicurezza cibernetica a livello nazionale. Politica che, per sua natura, dovrà necessariamente essere dinamica e in continua evoluzione in base ai cambiamenti tecnologici, normativi, sociali e geopolitici.

9.1 Piena implementazione del Piano Strategico

La velocità con cui gli attacchi si dispiegano richiede un forte coordinamento tra rilevazione della minaccia e risposta e pertanto una piena implementazione del *Piano Strategico Nazionale di Sicurezza Cibernetica*. Il DPCM Gentiloni (vedi sez. 1.3.2) ha il merito di aver ridotto la catena di comando, rispondendo a questa necessità e chiarendo ruoli e responsabilità. Vi è tuttavia il bisogno di provvedere a una veloce creazione e rapida messa a regime delle nuove strutture indicate dal DPCM stesso (*Comando Interforze per le Operazioni Cibernetiche* e il *Centro di Valutazione e Certificazione Nazionale*), il rafforzamento di quelle già esistenti (il *Nucleo Sicurezza Cibernetica* e il *CNAIPIC*) e l'unificazione e il rafforzamento del *CERT-Nazionale* e del *CERT-PA* per realizzare il *CSIRT nazionale* voluto dalla direttiva Europea NIS (vedi sez. 1.2.1).

Auspichiamo inoltre un cambio di passo nella realizzazione di una *Fondazione* che, avendo come unica missione l'interesse del bene pubblico e della sicurezza nazionale, possa essere di supporto a im portanti azioni nel settore pubblico e privato, come quelle già riportate nel DPCM: un *Centro di Ricerca e Sviluppo in Cybersecurity* (vedi sez. 2.3) e un *Laboratorio di Crittografia* (vedi sez. 4.2). Altre nazioni hanno sviluppato organizzazioni analoghe, nelle forme appropriate ai loro ordinamenti. Negli Stati Uniti, ad esempio, il sistema dei *Federally Funded Research and Development Centers* (FFRDC), quali il MITRE[1], agisce in questa direzione. Questi centri, pur essendo organizzazioni di diritto privato, non hanno alcuno scopo commerciale e assistono il governo federale in attività di analisi e ricerca scientifica, scouting tecnologico e di ingegneria dei sistemi. Inoltre in Italia, la Fondazione potrebbe portare avanti altre importanti azioni per la formazione, la sensibilizzazione e il trasferimento tecnologico, attraverso:

- la creazione di una *Cybersecurity Academy* che, sulla falsariga del modello dei conservatori musicali, possa seguire nel tempo la crescita dei talenti scoperti con programmi quali *CyberChallenge.IT*;
- la messa a disposizione di un *fondo di venture capital etico*, previsto dal DPCM Gentiloni, per la creazione e il rafforzamento di start-up che svi-

[1] `http://www.mitre.org`

luppino tecnologia di interesse nazionale (vedi sez. 9.6). Il fondo giocherebbe un ruolo chiave nell'attivazione di un ecosistema cyber tra università e impresa e consentirebbe che le miriadi di prototipi, *proof of concept* e algoritmi innovativi sviluppati dalla ricerca Italiana (e spesso purtroppo lasciati in un cassetto) possano essere trasformati in opportunità di business [9].

È importante individuare e finanziare, seguendo l'esempio di altri paesi europei (vedi cap. 8), dei Centri di ricerca di eccellenza, distribuiti sul territorio nazionale, il cui centro stella sia il Centro Nazionale di Ricerca e Sviluppo in Cybersecurity. Questi centri dovrebbero essere focalizzati sulle tecnologie di base essenziali per la cybersecurity (machine learning, data analytics, sistemi operativi, compilatori, ingegneria del software, reti e sistemi distribuiti, architetture hardware, etc.) e su altre materie rilevanti per la cybersecurity, quali giurisprudenza, economia, psicologia e sociologia.

Infine, devono essere sviluppati sistemi di certificazione per hardware/software/firmware a livello nazionale, in un contesto di coesistenza e integrazione con le azioni che si stanno portando avanti a livello europeo. Introdurre sistemi certificati, ben concepiti e sostenibili dal mercato, all'interno di settori come le nostre infrastrutture critiche, può dare maggiori garanzie di buon funzionamento e, allo stesso tempo, fornire una base concreta ai sistemi di anticipo della minaccia e di analisi del rischio descritti nel cap. 3.

9.2 Politica digitale nazionale

Le strategie per garantire la sicurezza cibernetica vanno considerate parte integrante della *politica digitale nazionale*; coinvolgendo il Governo nel suo insieme, queste dovrebbero tutte rientrare sotto la diretta responsabilità politica del Presidente del Consiglio.

A un primo livello auspichiamo che il Presidente del Consiglio possa avvalersi di un gruppo di consiglieri, come già avviene nelle migliori democrazie anglosassoni, che interpreti la trasformazione digitale nei diversi ambiti: economico, giuridico, sociale, tecnologico e industriale. Questo gruppo dovrebbe essere costituito da personalità nazionali di alto livello scientifico, imprenditoriale e governativo, dando vita a un vero *Comitato di esperti*. Il Comitato dovrebbe studiare l'impatto sul sistema Italia di specifiche tecnologie *disruptive*, quali IoT, Intelligenza Artificiale, Pervasive robotic, criptovalute, etc., e definire piani strategici di sviluppo del Paese all'interno di queste trasformazioni. È inoltre importante che il Comitato verifichi che singoli provvedimenti presi dall'esecutivo in ogni settore siano allineati con i possibili cambiamenti imposti

dalla trasformazione digitale, al fine di evitare la promulgazione di norme già obsolete sul nascere o destinate a diventarlo in tempi brevissimi.

A livello operativo, sarebbe 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 PA. La nuova struttura dovrà essere organizzata in modo tale da non rappresentare, come è purtroppo spesso accaduto in Italia, un livello burocratico aggiuntivo teso a verificare adempimenti procedurali in chiave legalistico-giuridica. Essa, al contrario, dovrà essere in grado di pianificare e guidare nel tempo programmi strategici che consentano una trasformazione continua e controllata del Paese, per mantenerlo 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[2]. In quest'ottica, tale struttura dovrebbe anche perseguire l'obiettivo fondamentale di creare le condizioni per la nascita di un *ecosistema cyber nazionale* [9].

9.3 Sicurezza come fattore competitivo

Molte ricerche di istituti importanti e terzi, quali le Banche Centrali Nazionali [16], hanno mostrato come *la sicurezza nel dominio cibernetico non possa più essere considerata un costo certo di fronte a un danno incerto*. L'aumento esponenziale degli attacchi, che diventeranno sempre più intelligenti e complessi, sarà un invariante nel prossimo futuro. Le organizzazioni che non prenderanno le opportune contromisure facendo crescere una cultura della sicurezza al loro interno vedranno gli attacchi fatalmente concentrarsi su di loro, trasformando il danno da incerto a certo. Un'organizzazione che viene bucata subisce, oltre al danno economico dovuto alla sottrazione dei dati, un danno reputazionale che può diventare letale per la sua stessa sopravvivenza.

> *Finanziare in modo oculato, ma adeguato e all'interno di un programma strategico, ricerca e industria in questo settore è prioritario, anche per raggiungere il maggior grado possibile di indipendenza nella prevenzione e nella gestione di rischi relativi ai nostri dati, alle nostre transazioni e alle nostre infrastrutture critiche.*

Quello che abbiamo appena detto per le organizzazioni private o pubbliche si applica perfettamente anche al concetto di organizzazione statuale. L'implementazione di un programma multidimensionale a carattere nazionale per la

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

messa in sicurezza del nostro Paese è sicuramente condizione necessaria per assicurarne *prosperità economica* e, considerando l'integrazione sempre più sviluppata all'interno del cyberspace dei sistemi cyber-fisici, anche della *sicurezza fisica* dei suoi abitanti.

Ovviamente la sicurezza costa, ma va vista come un fattore competitivo di un'azienda e, a livello di sistema Paese, come precondizione indispensabile per garantire la competitività dell'intero sistema produttivo.

9.4 Ridurre l'emigrazione di professionalità

Le figure professionali legate alla sicurezza hanno un mercato mondiale e spesso in Italia ci troviamo a competere con realtà che, oltre confine, offrono condizioni salariali di gran lunga migliori. Il numero di figure professionali legate alla cybersecurity prodotte dalle nostre università è ancora troppo basso, a causa anche dei pochi docenti presenti in Italia su questo settore specifico. È questa una delle cause che, di fatto, impedisce l'attivazione di nuovi corsi di laurea triennale e magistrale in molte università italiane: corsi di laurea che in questo momento si contano purtroppo sulla punta delle dita.

A causa del combinato disposto di una fuga dall'Italia per cogliere opportunità salariali importanti e di una scarsa creazione di figure professionali adeguate rispetto al bisogno, è necessario e urgente 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-off, riuscendo in questo modo a trasformare una debolezza endemica in un fattore di crescita.

Oltre a questi programmi, dobbiamo creare le condizioni per riportare in Italia i nostri migliori cervelli nell'ambito della scienza e dell'imprenditoria nel settore della sicurezza. La mobilità del mercato del lavoro è in questo settore un problema endemico che non attanaglia solo l'Italia: alcuni grandi paesi si stanno muovendo, da un lato per avere a disposizione, tra qualche anno, la workforce necessaria e, dall'altro, per creare le condizioni per mantenerla all'interno dei loro confini. Questo passa, a titolo di esempio, per politiche di prestiti d'onore verso gli studenti: politiche ad esempio già perseguite da Francia e Germania e che potrebbero essere prese in considerazione anche nel nostro Paese per mantenere i neo laureati nelle nostre strutture governative, nella PA e nel sistema industriale nazionale.

Se non si metteranno in atto adeguate politiche, la situazione peggiorerà sensibilmente nei prossimi anni. Si noti, al riguardo, che paesi come la Germania stanno facendo politiche molto aggressive per attirare non solo scien-

ziati e imprenditori, ma anche semplici studenti stranieri verso corsi di laurea all'interno delle loro università.

9.5 Piano straordinario per l'Università

Per essere realizzati, i progetti e le azioni che abbiamo proposto nei capitoli precedenti richiedono una workforce (tecnici, ingegneri, esperti, ricercatori) importante e distribuita sul territorio; per raggiungere questo obiettivo è necessario un piano straordinario per l'assunzione di ricercatori e professori universitari del settore.

Abbiamo visto nel cap. 8 e nella sez. 9.4 come diversi paesi si stiano muovendo per raggiungere, nel più breve tempo possibile, un livello di workforce nel settore della cybersecurity che sia adeguato ai bisogni del paese. Tutto ciò ovviamente passa per l'avere, nel proprio organico, dei ricercatori e dei formatori di alto livello nel settore. Noi auspichiamo che, come avvenuto nel passato per altre aree (e.g., la chimica negli anni '60), venga avviato in Italia un piano straordinario per l'assunzione di ricercatori e professori universitari che si occupano di cybersecurity e, in generale, di trasformazione digitale in tutte le sue componenti: giuridiche, economiche e sopratutto tecnologiche. Solamente una significativa azione straordinaria può aumentare la velocità di creazione della workforce necessaria.

In questo momento il numero dei docenti e ricercatori di cybersecurity è così basso e distribuito sul territorio nazionale che le Università e gli Enti di Ricerca non riescono ad attivare, in autonomia, programmi di ricerca o di didattica. Questo è legato al fatto che la sicurezza è stata sempre considerata un elemento secondario, o al più di supporto, nello sviluppo di esperienze didattiche nel settore dell'Informatica o dell'Ingegneria dell'Informazione. Tuttavia, in questo momento, la creazione di nuove lauree sul territorio nazionale è un elemento essenziale per l'incremento della workforce. Ma questo lo si può fare solo con un adeguato numero di docenti esperti della materia nelle singole università.

A parte la componente legata allo sviluppo di progetti di ricerca, investire nella formazione e nell'addestramento in cybersecurity fornisce una risposta unica a molteplici problemi del sistema Paese e si rende indispensabile nell'ambito della progressiva digitalizzazione promossa dal piano *Impresa 4.0*. Formare le nuove generazioni innescherà un processo virtuoso in cui la classe dirigente e i tecnici del futuro avranno le competenze, il bagaglio culturale e le capacità operative necessarie per confrontarsi con le sfide tecnologiche e scientifiche che cambieranno le nostre vite nei prossimi decenni, mettendo in atto le necessarie iniziative per adattarsi ai continui cambiamenti e ai rischi che ci aspettano in futuro. Va notato che considerazioni del tutto simili sono riportate nel docu-

mento della commissione statunitense istituita per migliorare la cybersecurity negli USA[3].

9.6 Tecnologia nazionale

Nella definizione del cyberspace nazionale occorre necessariamente affrontare anche il problema delle *architetture* dei sistemi impiegati. Il concetto astratto di *architettura* di un sistema di elaborazione complesso si è via via ampliato e include oggi hardware, software, algoritmi, infrastrutture di comunicazione, piattaforme, dati, processi, metodologie, contratti, fattore umano, etc.

Certamente l'Italia ha dei player interessanti, non dei giganti, nel software, nell'integrazione, nelle strutture di comunicazione e in specifici mercati di nicchia che possono essere utili nello sviluppo di pezzi di una architettura nazionale. Ci sono dei settori come l'hardware che abbiamo abbandonato da tempo. Visti i trend nel mercato dei semiconduttori di punta, con investimenti dell'ordine di alcuni miliardi di euro per la messa in opera di una linea di produzione per circuiti integrati dell'ultima generazione, sembra improponibile pensare di arrivare ad avere una produzione nazionale in grado di competere con gli *Over-The-Top*. Potrebbe invece essere certamente ragionevole pensare a produzioni "nazionali" per applicazioni e/o settori di nicchia ritenuti strategici per la sicurezza nazionale, quali ad esempio le *architetture tolleranti le vulnerabilità* introdotte nella sez. 4.1.

Proprio perché non abbiamo i leader dei vari settori della trasformazione digitale, dobbiamo trovare un modo italiano per integrare tecnologia straniera con la tecnologia nazionale all'interno di una architettura domestica della quale dobbiamo avere il completo controllo. Possibilmente definendo una strategia a livello di sistema Paese che permetta di decidere, per ciascuna categoria (o sottocategorie) di componenti e di tecnologie, quali siano da sviluppare a livello nazionale e quali invece possano essere reperite sul mercato estero. Per queste ultime occorre averne ben chiari i limiti e, per le tecnologie ritenute strategiche, dotarsi di quegli strumenti che ci mettano in condizione di poter effettuare sistematicamente le necessarie verifiche sul software e sull'hardware e soprattutto di poterne assumere, in caso di necessità, il pieno e incondizionato controllo. In questo, la creazione e lo sviluppo del *Centro di Valutazione e Certificazione Nazionale* risultano essere di primaria importanza.

[3] `https://www.dropbox.com/s/lgw7bq05bstk2m7/cybersecurity-commission-report-final-post.pdf?dl=0`

Bibliografia

[1] R. Baldoni, R. De Nicola (curatori): “Il futuro della Cybersecurity in Italia”. CINI - Consorzio Interuniversitario Nazionale Informatica, 2015 – https://www.consorzio-cini.it/index.php/it/component/attachments/download/416

[2] A. Antinori: “Generation-t: terrorist infosphere and evolution of lone wolf terrorism”. In “Lone actors - an emerging security threat”, NATO Science for peace and security series, (Richman A. et Sharan Y., NATO IOS Press), 2015.

[3] A. Antinori: “From the islamic state to the ‘Islamic state of mind’. The evolution of the jihadisphere and the rise of the lone jihad”. In “European Police Science and Research Bulletin - Summer 2017” (CEPOL, European Union Agency for Law Enforcement Training), 2017.

[4] A. Antinori: “Jihadi wolf threat. The evolution of terror narratives between the (cyber-)social ecosystem and self-radicalization”. in Proc. 1st European Counter Terrorism Centre (ECTC) conference on online terrorist propaganda, at Europol Headquarters, The Hague, 2017.

[5] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. Hankes Drielsma, P. C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron: “The Avispa Tool for the automated validation of internet security protocols and applications”. In Proc. Computer Aided Verification (CAV 2005), LNCS 3576, pp. 281-285, 2005.

[6] A. Armando, R. Carbone, L. Compagna, J. Cuellar, L. Tobarra: “Formal Analysis of a SAML Web Browser Single Sign-On Protocol: breaking the SAML-based Single Sign-on for Google Apps”. In Proc. 6th ACM Workshop on Formal Methods in Security Engineering. 2008.

[7] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Käsper, S. Cohney, S. Engels, C. Paar, Y.l Shavitt: “DROWN: Breaking TLS Using SSLv2”. in Proc. USENIX Security Symposium 2016, pp. 689-706, 2016.

[8] M. Baldi, M. Bianchi, F. Chiaraluce: “Security and complexity of the McEliece cryptosystem based on QC-LDPC codes”, IET Inf. Secur. 7(3), pp. 212–220, 2013.

[9] R. Baldoni: “L’urgenza di un ecosistema cyber nazionale”; Il Sole24ore, pp. 10, 22 Jan. 2017 – https://www.consorzio-cini.it/index.php/it/component/attachments/download/619.

[10] R. Baldoni, L. Montanari Editors: “Italian Cyber Security Report 2015 - Un Framework Nazionale per la Cyber Security” – http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf, ISBN: 9788894137316, 2016.

[11] R. Baldoni, L. Montanari, L. Querzoni (curatori): “Italian Cyber Security Report 2016 - Controlli Essenziali di Cybersecurity” – http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf ISBN: 978-88-941-3732-3, 2017.

[12] B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi: “Duqu: A Stuxnet-like malware found in the wild”. Budapest University of Technology and Economics, 2011.

[13] K. Bhargavan, B. Blanchet, N. Kobeissi: “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”. In Proc. IEEE Symposium on Security and Privacy, pp. 483-502, 2017.

[14] K. Bhargavan, C. Fournet, M. Kohlweiss: “miTLS: Verifying Protocol Implementations against Real-World Attacks”. In IEEE Security & Privacy Magazine, volume 14, pp. 18-25, 2016.

[15] K. Bhargavan, G. Leurent: “On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN”. In Proc. 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS ’16), pp. 456-467, 2016.

[16] C. Biancotti: “The price of cyber (in)security: evidence from the Italian private sector”. Questioni di Economia e Finanza 407, Banca d’Italia, Dicembre 2017.

[17] B. Blanchet: “An Efficient Cryptographic Protocol Verifier Based on Prolog Rules”. In Proc. 14th IEEE Computer Security Foundations Workshop (CSFW-14), pp. 82-96. 2001.

[18] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, H. J. Chizeck: “To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics” – `https://arxiv.org/abs/1504.04339`, 2015.

[19] F. Buccafurri, G. Lax, D. Migdal, S. Nicolazzo, A. Nocera, C. Rosemberger: “Contrasting False Identities in Social Networks by Trust Chains and Biometric Reinforcement”. In Proc. International Conference on Cyberworlds (CYBERWORLDS 2017), pp. 17–24, IEEE Computer Society, 2017.

[20] G. Caldarelli, M. Cristelli, A. Gabrielli, L. Pietronero, A. Scala, A. Tacchella: “A network analysis of countries? export flows: firm grounds for the building blocks of the economy”. PloS one 7 (10), e47278, 2012.

[21] T. Catarci, F. Leotta, A. Marrella, M. Mecella, D. Sora, P. Cottone, G. Lo Re, M. Morana, M. Ortolani, V. Agate, G. R. Meschino, G. Pecoraro, G. Pergola: “Your Friends Mention It. What About Visiting It?: A Mobile Social-Based Sightseeing Application”. In Proc. International Working Conference on Advanced Visual Interfaces (AVI), pp. 300-301, 2016.

[22] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno: “USENIX Security”, August 10 -12, 2011.

[23] A. Chi-Chih Yao: “How to Generate and Exchange Secrets” (Extended Abstract) In Proc. FOCS, pp. 162-167, 1986.

[24] I. Choi et al.: “Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber”, Opt. Express 22, 23121, 2014.

[25] G. W. Clark Jr., M. V. Doran, T. R. Andel: “Cybersecurity Issues in Robotics”. In Proc. IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), 2017.

[26] T. Collerton, A. Marrella, M. Mecella, T. Catarci: “Route Recommendations to Business Travelers Exploiting Crowd-Sourced Data”. In Proc. 14th International Conference on Mobile Web and Intelligent Information Systems, pp. 3-17, 2017.

[27] D. Coyle: “Best Practices in Data Center and Server Consolidation,” White paper. Gartner, Inc., 2011.

[28] A. Das, J. Da Rolt, G. Di Natale, M.-L. Flottes, B. Rouzeyre, I. Verbauwhede: “Test versus Security: Past and Present”. IEEE Transactions on Emerging Topics in Computing, 2 (1), pp. 50-627, 2014.

[29] A. Durante, R. Focardi, R. Gorrieri: “A compiler for analyzing cryptographic protocols using noninterference”. ACM Trans. Softw. Eng. Methodol. 9(4): pp. 488-528, 2000.

[30] P. Ferrara, E. Burato, F. Spoto: “Security Analysis of the OWASP Benchmark with Julia”. In Proc. 1st Italian Conference on Cybersecurity (ITASEC’17), CEUR Workshop Proceedings 1816, pp. 242-247, 2017.

[31] E. Ferrara, O. Varol, C. Davis, F. Menczer, A. Flammini: “The rise of social bots”. Commun. ACM 59, 7, pp. 96-104, 2016.

[32] R. Focardi, F. Palmarini, M. Squarcina, G. Steel, M. Tempesta: “Mind Your Keys? A Security Evaluation of Java Keystores”. In Proc. NDSS Symposium 2018, to appear.

[33] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik: “Unconditional Quantum Teleportation”, Science 282, pp. 706-709, 1998.

[34] J. Gantz & D. Reisel: “The Digital Universe in 2020: Big Data, bigger digital shadows, and biggest growth in the far east". ICD iView: IDC Analyze the future, 2012.

[35] F. D. Garcia, G. Koning Gans, R. Muijrers, P. Rossum, R. Verdult, R. Wichers Schreur, B. Jacobs: “Dismantling MIFARE Classic”. In Proc. 13th European Symposium on Research in Computer Security: Computer Security (ESORICS ’08), pp. 97-114, 2008.

[36] S. Garfinkel: “Digital forensics research: The next 10 years”. Digital Investigation, 7(Suppl. 1), pp. 64-73, 2010.

[37] C. Gentry: “A Fully Homomorphic Encryption Scheme”. Ph.D. Dissertation. Stanford University, CA, USA, 2009.

[38] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden: “Quantum cryptography”, Rev. Mod. Phys. 74, 145, 2002.

[39] O. Goldreich, S. Micali, A. Wigderson: “How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority”. In Proc. STOC, pp. 218-229, 1987.

[40] U. Gretzel, M. Sigala, Z. Xiang, C. Koo: “Smart tourism: foundations and developments”. Electron Markets, 25, pp. 179-188, 2015.

[41] P. H. Gum: “System/370 extended architecture: Facilities for virtual machines,” in *IBM Journal of Research and Development* 27(6), pp. 530-544, 1983.

[42] T. Heer, O. Garcia-Morchon, R. Hummen, S. Keoh, S. Kumar, K. Wehrle: “Security challenges in the ip-based internet of things”. Wireless Personal Communications, 61(3), pp. 527-542, 2011.

[43] T. Huang: “Surveillance video: the biggest big data". Computing Now, vol. 7, n. 2, 2014.

[44] Y. Hwang: “IoT security and privacy: Threats and challenges”. In Proc. 1st ACM Workshop on IoT Privacy, Trust, and Security (IoTPTS ’15), pp. 1-1, 2015.

[45] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti: “Experimental demonstration of long-distance continuous-variable quantum key distribution”, Nature Photonics 7, pp. 378-381, 2013.

[46] Y. Jin: “Introduction to Hardware Security”. Electronics vol. 4, pp. 763-784. – `http://jin.ece.ufl.edu/papers/Electronics15.pdf`, 2015.

[47] N. M. Karie, H. S. Venter: “Taxonomy of Challenges for Digital Forensics”. Journal of Forensic Sciences, 60(4), pp. 885-893, 2015.

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

[49] K. Lee: “The internet of things (IoT): Applications, investments, and challenges for enterprises”. Business Horizons 58(4), pp. 431-440, 2015.

[50] R. J. McEliece: “A public-key cryptosystem based on algebraic coding theory”. DNS Progress Report, Jet Propulsion Laboratory, CA, Pasadena, pp. 114-116, 1978.

[51] P. McGee: “Amazon to open AI centre in Germany’s Cyber Valley". Financial Times, October 23, 2017.

[52] J. Memmott, D. Alonso, E. Berlow, A. Dobson, J. Dunne, R. Sole, J. Weitz: “Biodiversity loss and ecological network structure”. in Ecological Networks: Linking Structure to Dynamics in Food Webs, Oxford University Press, 2006.

[53] R. Misoczki, J.-P. Tillich, N. Sendrier, P. S. L. M. Barreto: “MDPC-McEliece: New McEliece variants from moderate density parity-check codes” – http://eprint.iacr.org/2012/409.

[54] M. Mori: “Controinformazione: la protezione dei processi decisionali del Sistema-Paese. Istituto Gino Germani di Scienze Sociali e Studi Strategici - Research Paper, 2016 – `http://fondazionegermani.org/`.

[55] S. Nag, C. Eschinger, F. Ng: “Forecast Analysis: Public Cloud Services, Worldwide, 4Q16 Update,” White paper. Gartner, Inc. 2017.

[56] M. Nemec, M. Sýs, P. Svenda, D. Klinec, V. Matyas: “The Return of Coppersmith’s Attack: Practical Factorization of Widely Used RSA Moduli”. In Proc. ACM CCS 2017, pp. 1631-1648, 2017.

[57] M.A. Nielsen, I.L. Chuang: “Quantum Computation and Quantum Information”, Cambridge University Press, 2010.

[58] C. Polycarpou, K. N. Cassemiro, G. Venturi, A. Zavatta, M. Bellini: “Adaptive detection of arbitrarily-shaped ultrashort quantum light states”. Physical Review Letters, 109, 053602, 2012.

[59] W. Quattrociocchi, A. Scala, C. R. Sunstein: “Echo chambers on facebook”, 2016 – `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795110`.

[60] H. Rogers: “Theory of recursive functions and effective computability”, MIT Press, 1987.

[61] M. Rostami, F. Koushanfar, R. Karri: “A Primer on Hardware Security: Models, Methods, and Metrics”. Proceedings of the IEEE, Vol. 102, No. 8, 2014.

[62] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev: “The security of practical quantum key distribution”, Rev. Mod. Phys. 81, 1301, 2009.

[63] A. Semuels: “Why Does Sweden Have So Many Start-Ups?”, The Atlantic, September 28, 2017.

[64] P. W. Shor: “Algorithms for quantum computation: discrete logarithms and factoring”. In Proc. 35th Annual Symposium on Foundations of Computer Science (SFCS ’94), pp. 124-134, 1994.

[65] D. Simshaw, N. Terry, K. Hauser, M. Cummings: “Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks”. Richmond Journal of Law and Technology, Vol. 22, No. 3, 2016.

[66] N. Sklavos, R. Chaves, , G. Di Natale, F. Regazzoni (Eds.): “Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment”, Springer, 2017.

[67] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov: “The First Collision for Full SHA-1”. In Proc. CRYPTO 2017: pp. 570-596, 2017.

[68] M. Stevens, A. K. Lenstra, B. de Weger: “Chosen-prefix collisions for MD5 and applications”. International Journal of Applied Cryptography (IJACT) volume 2(4), pp. 322-359, 2012.

[69] A. Sudhodanan, A. Armando, R. Carbone, L. Compagna: “Attack Patterns for Black-Box Security Testing of Multi-Party Web Applications”. In Proc. Network and Distributed System Security Symposium 2016 (NDSS 2016), 2016.

[70] C. R. Sunstein: “Republic: Divided Democracy in the Age of Social Media”. Princeton University Press, 2017.

[71] G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, P. Villoresi: “Interference at the Single Photon Level Along Satellite-Ground Channels”, Phys. Rev. Lett., vol. 116, no. 25:253601, Jun. 2016.

[72] M. Vanhoef, F. Piessens: “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”. In Proc. ACM CCS 2017, pp. 1313-1328, 2017.

[73] R. Verdult, F. D. Garcia, B. Ege: “Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer”. In Proc. USENIX Security Symposium 2013, pp. 703-718, 2013.

[74] S. Wiesner: “Conjugate coding", Sigact News 15(1), pp. 78-88, 1983.

[75] D. A. Wheeler and G. N. Larsen: “Techniques for Cyber Attack Attribution”. Institute for defence analysis. IDA Paper P-3792, 2007.

[76] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, C. Barbieri: “Experimental verification of the feasibility of a quantum channel between space and Earth”, New J. Phys., vol. 10, no. 3, pp. 33-38, 2008.

[77] T. Xu, J. B. Wendt, M. Potkonjak: “Security of IoT systems: Design challenges and opportunities”. In Proc. 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD ’14), pp. 417-423, 2014.

[78] F. Zappa: “La criminalità informatica e i rischi per l’economia e le imprese a livello italiano ed europeo”. United Nations Interregional Crime and Justice Research Institute - UNICRI, 2014.

[79] Z. Zhang, M. Cheng Yi Cho, C. Wang, C. Hsu, C.Kuan Chen, S. Shieh: “IoT security: Ongoing challenges and research opportunities”. in Proc. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230-234, 2014.

[80] F. Zollo, A. Bessi, M. Del Vicario, A. Scala, L. Shekhtman, S. Havlin, W. Quattrociocchi: “Debunking in a world of tribes”. PloS one 12 (7), e0181821, 2017.

Autori e loro affiliazione

Cosimo Anglano	Università del Piemonte Orientale “A. Avogadro”
Leonardo Aniello	Sapienza Università di Roma
Arije Antinori	Sapienza Università di Roma
Alessandro Armando	Università degli Studi di Genova
Rocco Aversa	Università della Campania *Luigi Vanvitelli*, Caserta
Marco Baldi	Università Politecnica delle Marche, Ancona
Roberto Baldoni	Sapienza Università di Roma
Antonio Barili	Università degli Studi di Pavia
Massimo Bartoletti	Università degli Studi di Cagliari
Cataldo Basile	Politecnico di Torino
Marco Bellini	Consiglio Nazionale delle Ricerche
Francesco Bergadano	Università degli Studi di Torino
Cinzia Bernardeschi	Università degli Studi di Pisa
Elisa Bertino	Purdue University, West Lafayette, USA
Giuseppe Bianchi	Università degli Studi di Roma “Tor Vergata”
Claudia Biancotti	Centro Studi Banca d’Italia
Stefano Bistarelli	Università degli Studi di Perugia
Nicola Blefari Melazzi	Consorzio Nazionale Interuniversitario Telecomunicazioni
Milena Boetti	Università degli Studi di Torino
Andrea Bondavalli	Università degli Studi di Firenze
Silvia Bonomi	Sapienza Università di Roma

Francesco Buccafurri	Università degli Studi Mediterranea di Reggio Calabria
Enrico Cambiaso	Consiglio Nazionale delle Ricerche
Barbara Caputo	Istituto Italiano di Tecnologia
Barbara Carminati	Università degli Studi dell'Insubria
Francesco Saverio Cataliotti	Università degli Studi di Firenze
Tiziana Catarci	Sapienza Università di Roma
Andrea Ceccarelli	Università degli Studi di Firenze
Nicolò Cesa Bianchi	Università degli Studi di Milano
Franco Chiaraluce	Università Politecnica delle Marche, Ancona
Michele Colajanni	Università degli Studi di Modena e Reggio Emilia
Marco Conti	Consiglio Nazionale delle Ricerche
Mauro Conti	Università degli Studi di Padova
Luigi Coppolino	Università degli Studi di Napoli Parthenope
Gabriele Costa	IMT School for Advanced Studies Lucca
Valerio Costamagna	Università degli Studi di Torino
Domenico Cotroneo	Università degli Studi di Napoli Federico II
Bruno Crispo	Università degli Studi di Trento
Rita Cucchiara	Università degli Studi di Modena e Reggio Emilia
Salvatore D'Antonio	Università degli Studi di Napoli Parthenope
Ernesto Damiani	Università degli Studi di Milano
Rocco De Nicola	IMT School for Advanced Studies, Lucca
Alfredo De Santis	Università degli Studi di Salerno
Giuseppe Di Battista	Università degli Studi Roma Tre
Beniamino Di Martino	Università della Campania *Luigi Vanvitelli*, Caserta
Ivo Pietro Degiovanni	Istituto Nazionale di Ricerca Metrologica
Camil Demetrescu	Sapienza Università di Roma
Arturo Di Corinto	Consorzio Interuniversitario Nazionale Informatica
Giuseppe Antonio Di Luna	University of Ottawa, Canada
Giorgio Di Natale	Centre National de la Recherche Scientifique, Francia
Gianluca Dini	Università degli Studi di Pisa
Marco Evangelisti	Università degli Studi di Torino
Daniela Falcinelli	Università degli Studi di Perugia
Gianna Figà Talamanca	Università degli Studi di Perugia
Marco Ferretti	Università degli Studi di Pavia

Massimo Ficco	Università della Campania *Luigi Vanvitelli*, Caserta
Paola Flocchini	University of Ottawa, Canada
Marie-Lise Flottes	Centre National de la Recherche Scientifique, Francia
Riccardo Focardi	Università Ca' Foscari, Venezia
Luisa Franchina	Associazione Italiana Infrastrutture Critiche
Angelo Furfaro	Università degli Studi della Calabria
Giorgio Giacinto	Università degli Studi di Cagliari
Roberto Giacobazzi	Università degli Studi di Verona
Paola Girdinio	Università degli Studi di Genova
Franco Guida	Fondazione Ugo Bordoni
Giuseppe F. Italiano	Università degli Studi di Roma "Tor Vergata"
Daniele Lain	Università degli Studi di Padova
Nicola Laurenti	Università degli Studi di Padova
Antonio Lioy	Politecnico di Torino
Michele Loreti	Università degli Studi di Firenze
Donato Malerba	Università degli Studi di Bari
Luigi Vincenzo Mancini	Sapienza Università di Roma
Alberto Marchetti Spaccamela	Sapienza Università di Roma
Gianluca Marcialis	Università degli Studi di Cagliari
Andrea Margheri	University of Southampton, GB
Andrea Marrella	Sapienza Università di Roma
Fabio Martinelli	Consiglio Nazionale delle Ricerche
Maurizio Martinelli	Consiglio Nazionale delle Ricerche
Luigi Martino	Università degli Studi di Firenze
Fabio Massacci	Università degli Studi di Trento
Marco Mayer	Università degli Studi Link Campus, Roma
Massimo Mecella	Sapienza Università di Roma
Maurizio Mensi	Scuola Nazionale dell'Amministrazione
Alessio Merlo	Università degli Studi di Genova
Marino Miculan	Università degli Studi di Udine
Luca Montanari	Sapienza Università di Roma
Marco Morana	Università degli Studi di Palermo
Gian Domenico Mosco	Università LUISS "Guido Carli"
Leonardo Mostarda	Università degli Studi di Camerino

Vittorio Murino	Istituto Italiano di Tecnologia
Daniele Nardi	Sapienza Università di Roma
Roberto Navigli	Sapienza Università di Roma
Andrea Palazzi	Università degli Studi di Modena e Reggio Emilia
Francesco Palmieri	Università degli Studi di Salerno
Ida Panetta	Sapienza Università di Roma
Andrea Passarella	Consiglio Nazionale delle Ricerche
Alessandro Pellegrini	Sapienza Università di Roma
Gerardo Pelosi	Politecnico di Milano
Giancarlo Pellegrino	Universität des Saarlandes, Saarbrüken, Germania
Giuseppe Pirlo	Università degli Studi di Bari
Vincenzo Piuri	Università degli Studi di Milano
Maurizio Pizzonia	Università degli Studi Roma Tre
Marcello Pogliani	Politecnico di Milano
Mario Polino	Politecnico di Milano
Massimiliano Pontil	Istituto Italiano di Tecnologia
Paolo Prinetto	Politecnico di Torino
Francesco Quaglia	Università degli Studi di Roma “Tor Vergata”
Walter Quattrociocchi	Università Ca’ Foscari, Venezia
Leonardo Querzoni	Sapienza Università di Roma
Massimiliano Rak	Università della Campania *Luigi Vanvitelli*, Caserta
Silvio Ranise	Fondazione Bruno Kessler, Trento
Elisa Ricci	Fondazione Bruno Kessler, Trento
Lorenzo Rossi	Consiglio Nazionale delle Ricerche
Paolo Rota	Istituto Italiano di Tecnologia
Ludovico Orlando Russo	Politecnico di Torino
Pierangela Samarati	Università degli Studi di Milano
Nicola Santoro	Carleton University, Ottawa, Canada
Beppe Santucci	Sapienza Università di Roma
Vladimiro Sassone	University of Southampton, GB
Antonio Scala	Consiglio Nazionale delle Ricerche
Fabio Scotti	Università degli Studi di Milano

Andrea Servida	Commissione Europea
Paolo Spagnoletti	Università LUISS “Guido Carli”, Roma
Luca Spalazzi	Università Politecnica delle Marche, Ancona
Francesca Spidalieri	Salve Regina University, Newport, USA
Fausto Spoto	Università degli Studi di Perugia
Marco Squarcina	Università Ca’ Foscari, Venezia
Stefania Stefanelli	Università degli Studi di Perugia
Alessio Vecchio	Università degli Studi di Pisa
Salvatore Venticinque	Università della Campania *Luigi Vanvitelli*, Caserta
Paolo Villoresi	Università degli Studi di Padova
Aaron Visaggio	Università degli Studi del Sannio, Benevento
Andrea Vitaletti	Sapienza Università di Roma
Stefano Zanero	Politecnico di Milano