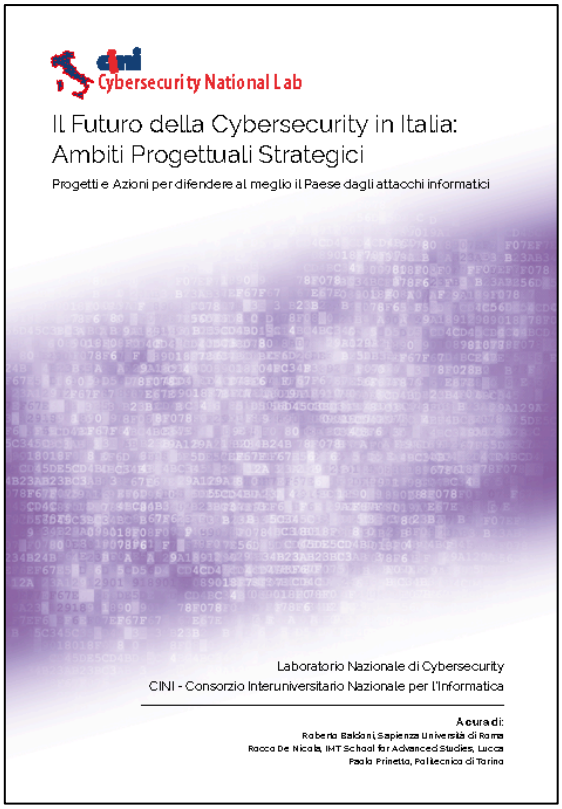

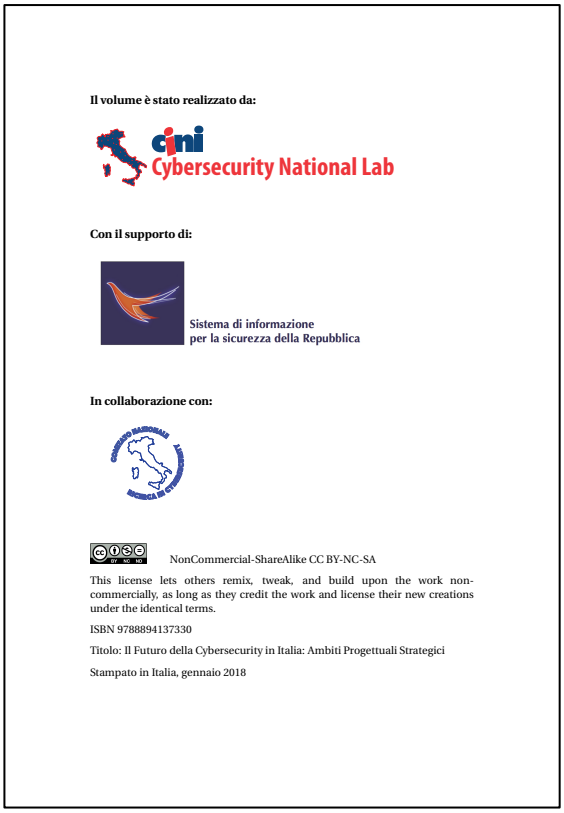

Riassunto e Raccomandazioni

Indice del documento

Il volume completo è scaricabile dal link:
https://www.consorzio-cini.it/images/Libro-Bianco-2018.pdf

1. Introduzione

In questo documento viene fornito un breve riassunto degli aspetti più significativi del volume ***Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici***.

Stampato in Italia nel gennaio 2018, il volume ha visto il coinvolgimento 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.
Il volume, curato dai professori Roberto Baldoni, Rocco De Nicola e Paolo Prinetto, consta di oltre 230 pagine; l'indice dettagliato è riportato in Appendice a questo documento.

2. Scopo del libro e scenario nazionale

Alla fine del 2015, il Laboratorio Nazionale di Cybersecurity del CINI ha realizzato un Libro Bianco 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 nuovo libro bianco 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 si spera 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 ritenuti 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 per tener conto dei cambiamenti tecnologici, normativi, sociali e geopolitici.

Prima di introdurre i diversi ambiti progettuali, il volume dedica un capitolo introduttivo ai pericoli degli attacchi cyber, mettendo in evidenza come 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. Viene poi sottolineato come anche la democrazia possa essere 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 destabilizzare i cittadini di un paese immergendoli in uno spazio informativo non controllato, con un insieme pressoché infinito di sorgenti di notizie.

La figura 1 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.

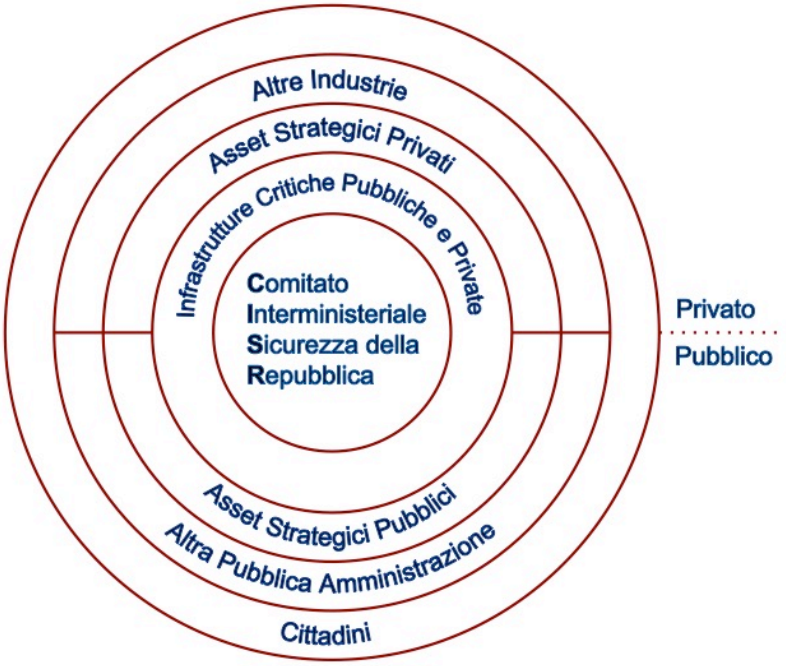

Figura 1: Gli asset pubblici e privati del Paese da difendere

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.

Oltre a questo, il **Capitolo 1** contiene un'analisi dell'estensione degli attacchi cyber in Italia basato su uno studio dei ricercatori della Banca d'Italia e una descrizione dello scenario normativo nazionale ed europeo. Viene descritto il *General Data Protection Regulation* (GDPR) europeo, destinato a sostituire la direttiva sulla protezione dei dati del 1995; il suo scopo principale è riformare, aggiornare e modernizzare la legislazione europea in materia di protezione dei dati per renderla più solida e coerente e direttamente applicabile senza necessità di alcuna norma di recepimento.

Nel capitolo viene anche presentata la nuova normativa nazionale che, a partire dal DPCM Gentiloni, mira principalmente ad alleggerire la gestione delle crisi e ad accentrare le responsabilità, rafforzando il ruolo del Dipartimento delle Informazioni per la Sicurezza, semplificando l'interazione tra una serie di attori e riconducendo a sistema e unitarietà le diverse competenze coinvolte nella gestione delle situazioni di crisi.

3. Ambiti Progettuali

Gli ambiti strategici progettuali sono elencati all'interno dell'indice allegato e vanno dal Capitolo 2 al Capitolo 6. I diversi ambiti progettuali sono stati raccolti in cinque aree operative:

- Infrastrutture e Centri (Capitolo 2)
- Azioni abilitanti (Capitolo 3)
- Tecnologie abilitanti (Capitolo 4)
- Tecnologie da proteggere (Capitolo 5)
- Azioni orizzontali (Capitolo 6).

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 figura 1 verso il punto dove queste possono essere gestite in modo appropriato. Il volume nel **Capitolo 2 (Infrastrutture e Centri)** prende in considerazione gli strumenti e le azioni necessarie a mettere in sicurezza la rete Internet nazionale e i data center della Pubblica Amministrazione e presenta alcune tipologie di centri di competenza da attivare sul territorio nazionale per rafforzare le difese del sistema Paese. Questi centri dedicati alla cybersecurity, distribuiti geograficamente sul territorio e, in alcuni casi, specializzati su singoli settori di mercato, vanno dai centri di Ricerca e Sviluppo ai centri di competenza e supporto all'industria, ai centri per l'analisi delle informazioni, fino ai CERT. Vengono proposti: (i) un *Centro Nazionale di Ricerca e Sviluppo in Cybersecurity,* che ha come compito principale la ricerca avanzata, lo sviluppo di architetture, applicazioni e azioni di varia natura di respiro nazionale; (ii) dei Centri Territoriali di Competenza in Cybersecurity distribuiti sul territorio con valenza di città metropolitana, regionale o interregionale, che si occupano di innovazione in ambito cyber e curano il trasferimento tecnologico, la formazione, la consulenza e il supporto ad aziende locali, PA locali e cittadini; (iii) dei Centri Verticali di Competenza in Cybersecurity dedicati a settori di mercato specifici, quali, ad esempio, energia, trasporti, mercati finanziari.

Una volta realizzata l'infrastruttura basata su Centri per la cybersecurity, occorre sviluppare delle azioni abilitanti per innalzare il livello di sicurezza. Queste azioni, presentate nel **Capitolo 3 (Azioni abilitanti)**, 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. Il capitolo affronta anche le problematiche relative all'anticipo della risposta, e prende in considerazioni tre tipi di attacchi: (i) gli attacchi cibernetici classici attraverso campagne di malware; (ii) gli 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) gli attacchi di tipo fisico, quali quelli terroristici, che sfruttano le potenzialità del cyberspace per portare a compimento le loro azioni. Il capitolo considera anche 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. 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.

Gli strumenti informatici e in generale le tecnologie abilitanti utili 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 vengono considerate nel **Capitolo 4 (Tecnologie abilitanti)**. Vengono dapprima analizzate le sfide poste dalle architetture hardware, che giocano un ruolo fondamentale nell'ottica della cosiddetta *tecnologia nazionale*. Seguono alcuni sistemi verticali, quali la crittografia (in particolare la crittografia postquantum), 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.

Il **Capitolo 5 (Tecnologie da proteggere)** analizza invece le tecnologie da proteggere, quali le comunicazioni wireless, i servizi cloud, le logiche funzionali dei sistemi e, anche nella prospettiva di Impresa 4.0, IoT, sistemi di controllo industriale e robot. Queste tecnologie 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: inserendo adeguate misure di sicurezza all'interno dei sistemi legacy che impiegano tecnologie obsolete e 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 gestite in un cyberspace resiliente.

Il **Capitolo 6 (Azioni orizzontali)** analizza una serie di azioni trasversali rispetto sia alle tecnologie abilitanti sia a quelle da proteggere affrontate 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. Viene messo in evidenza come sia diventata un'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: 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. L'introduzione di sistemi certificati, ben concepiti e sostenibili dal mercato 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.

4. Impatto sulla trasformazione digitale e scenario internazionale

A valle della presentazione delle idee progettuali, il volume, nel **Capitolo 7**, analizza l'impatto della trasformazione digitale su alcuni tra i più importanti settori della società, evidenziando 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, mettendo in evidenza come democrazia, finanza, industria, turismo e cultura possano trarre beneficio da una politica nazionale di sicurezza cyber e come la cybersecurity sia un elemento essenziale per garantire, nel tempo, un adeguato livello di sicurezza alle nostre relazioni, ai nostri affari, alle nostre democrazie.

Il **Capitolo 8** del volume viene poi dedicato alla presentazione delle politiche e delle azioni intraprese da alcune nazioni chiave nello scenario europeo e internazionale, da parte di colleghi Italiani

che da tempo lavorano in Università o Enti di Ricerca stranieri. 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.

5. Raccomandazioni

Nel **Capitolo 9** presenta 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 ritenuti 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.

5.1 Piena implementazione del piano strategico nazionale

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 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.

Si auspica 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 importanti azioni nel settore privato e privato, come quelle già riportate nel DPCM. Altre nazioni hanno sviluppato organizzazioni analoghe, che non hanno alcun scopo commerciale e assistono i governi in attività di analisi e ricerca scientifica, scouting tecnologico e di ingegneria dei sistemi. 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 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, per la creazione e il rafforzamento di startup che sviluppino tecnologia di interesse nazionale.

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 capitolo 3.

5.2 Politica digitale nazionale

Le strategie per garantire la sicurezza cibernetica vanno considerate parte integrante della politica digitale nazionale e questa dovrebbe rientrare sotto la diretta responsabilità politica del Presidente del Consiglio.

A un primo livello, si auspica che il Presidente del Consiglio possa avvalersi di un gruppo di consiglieri, 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, 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 nei diversi settori 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.

5.3 Sicurezza come fattore competitivo

La sicurezza nel dominio cibernetico non può più essere considerata un costo certo di fronte a un danno incerto. 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. 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.

5.4 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 esperti di 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. Al momento, questi corsi di laurea si contano sulla punta delle dita. 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. Vanno create le condizioni per riportare in Italia i nostri migliori cervelli nell'ambito della scienza e dell'imprenditoria nel settore della sicurezza. 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 scienziati e imprenditori, ma anche semplici studenti stranieri verso corsi di laurea all'interno delle loro università.

5.5 Piano straordinario per l'Università

Per essere realizzati, i progetti e le azioni proposte nei capitoli precedenti richiedono una workforce (tecnici, ingegneri, esperti, ricercatori) di dimensioni significative e distribuita sul territorio; per raggiungere questo obiettivo è necessario un piano straordinario per l'assunzione di ricercatori e professori universitari del settore. Si auspica 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 soprattutto tecnologiche. Solamente una significativa azione straordinaria può aumentare la velocità di creazione della workforce necessaria.

5.6 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, e metodologie. È importante pensare a produzioni "nazionali" per applicazioni e/o settori di nicchia ritenuti strategici per la sicurezza nazionale e siccome in Italia non ci sono 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* risulta essere di primaria importanza.

Appendice: Indice del Volume