Il fenomeno Cyber Security Skills Shortage italiano nel contesto internazionale

Printed in February 2019

Il fenomeno del Cyber Security Skill Shortage italiano nel contesto internazionale

By Tommaso De Zan

PhD Researcher, Centre for Doctoral Training in Cyber Security

Research Affiliate, Centre for Technology and Global Affairs

University of Oxford

EXECUTIVE SUMMARY

Molti governi tecnologicamente avanzati vedono l'attuale mancanza di professionisti nel mercato del lavoro della cyber security, definita "*Cyber Security skills shortage*" (CSSS), come una minaccia alla loro sicurezza informatica (*T.De Zan, 2019*). Difficoltà nel bilanciare la domanda e l'offerta di lavoro nel settore della Cyber Security sono state ampiamente riscontrate in paesi come l'Australia, il Giappone, il Regno Unito e gli Stati Uniti. Questi sono stati anche tra i paesi più attivi nel produrre strategie e politiche per mitigare tale carenza. Al di là di questi paesi, tuttavia, e nonostante le rivendicazioni circa una mancanza di competenze in sicurezza informatica a livello globale, ci sono solo degli aneddoti sulla presenza di tale fenomeno in altre parti del mondo, in parte dovuto al fatto che la ricerca scientifica svolta sull'argomento finora è stata limitata.

Questo rapporto, finanziato e supportato dalla Fondazione Global Cyber Security Center, cerca di colmare tale lacuna e di fornire una panoramica del CSSS in Italia. Lo studio presenta nuovi dati e informazioni sul fenomeno grazie ad un sondaggio, inviato ai maggiori Security Manager italiani, in aggiunta ad interviste con esperti del mondo accademico e governativo. Inoltre, la ricerca fornisce il quadro delle politiche pubbliche fin ora adottate dal governo italia-

no per contrastare il problema.

Ad oggi l'Italia sembra dover affrontare le stesse problematiche che stanno impedendo di trovare il giusto equilibrio tra domanda e offerta di lavoro nel settore della sicurezza cibernetica anche negli altri paesi tecnologicamente avanzati.

La maggioranza delle persone che ha risposto al sondaggio ha dichiarato di avere sempre o spesso posizioni aperte che fa fatica a ricoprire o a volte non riesce proprio a ricoprire. Dal sondaggio emerge che a volte "*è difficile trovare anche un solo candidato con le giuste capacità e conoscenze*". Più della metà delle organizzazioni intervistate ha mantenuto aperti i posti vacanti per il proprio staff di Cyber Security per almeno 61 giorni, un indicatore che induce a credere che i posti di lavoro vacanti siano effettivamente difficili da colmare.

Come in Australia e negli Stati Uniti, il mercato del lavoro italiano della Cyber Security sembra essere di fronte ad una "*trappola dell'esperienza professionale*". La maggior parte dei datori di lavoro preferisce assumere candidati che abbiano tra 1-3 anni o 4-10 anni di esperienza professionale, anche se è proprio in questa fascia di esperienza professionale che hanno maggiori difficoltà nel reclutamento. Solo una piccola percentuale delle organizzazioni è disposa ad assumere personale senza alcuna esperienza lavorativa. La mancanza di esperienza professionale non è però l'unico ostacolo nell'attuale mercato del lavoro della Cyber Security. Sebbene l'esperienza lavorativa sia una delle principali cause, le stesse hanno ammesso di "*non offrire sempre stipendi e benefit ai livelli del mercato attuale*".
La capacità del sistema educativo italiano di produrre un numero sufficiente di candidati con le giuste conoscenze e competenze costituisce un altro fattore critico. Questo elemento risulta in linea con un sentimento diffuso a livello internazionale sulla necessità di modernizzare l'attuale offerta formativa in cyber security.

In Italia, il problema del CSSS è stato riconosciuto in numerosi rapporti ufficiali e non ufficiali. Nella fattispecie, Il Dipartimento delle Informazioni per la Sicurezza (DIS), divenuto l'organo centrale nell'ecosistema della sicurezza informatica dopo l'adozione della direttiva NIS del 2018, ha riconosciuto che l'Italia ha un "*vasto problema*" in relazione all'educazione della Cyber Security. Tuttavia, ad oggi, non è stata ancora definita una politica nazionale specifica per mitigare il CSSS.

La risposta italiana al CSSS è stata timida e caratterizzata da campagne di sensibilizzazione promosse da singole amministrazioni più che da una strategia collettiva e centralizzata.
Perciò, non stupisce che Il CINI, il Consorzio Interuniversitario Nazionale per l'informatica, abbia sottolineato nel suo Libro Bianco del 2018, come le politiche educative in tema di Cyber Security siano attualmente insufficienti.

Una comparazione diretta con lo sforzo economico posto in essere dal Regno Unito nel campo della politica di sicurezza cibernetica e della sua educazione purtroppo mette in risalto il limitato impegno economico italiano nel settore. Il Regno Unito ha infatti stanziato nella sua strategia 2011-2016 un budget complessivo di £32.8milioni - su un totale di £860 milioni del bilancio pubblico dedicato alla Cyber Security - per l'attuazione dei propri programmi educativi. Dal momento che molte iniziative e progetti che interessano istruzione e formazione sono state riconfermate o ampliate nel nuovo ciclo strategico (2016-2021), è probabile che tale budget supererà di gran lunga quello che è stato previsto per il precedente programma. Nel dicembre 2018, il Governo italiano ha deciso di istituire un nuovo fondo per la difesa informatica per un totale di 3 milioni di euro per il periodo 2019-2021. La mancanza di investimenti generali nella politica di sicurezza cibernetica quindi può parzialmente spiegare perché' la risposta italiana al CSSS sia stata più limitata.
È difficile ipotizzare se l'Italia avesse potuto realizzare sforzi più concreti per l'educazione alla Cyber Security nonostante l'assenza di stanziamenti economici. Tuttavia, in questo contesto di urgenza, è singolare che i nuovi indirizzi operativi previsti nel nuovo Piano Nazionale pubblicato nel 2017 sulla "Promozione e diffusione della cultura della sicurezza. Formazione e istruzione" siano molto simili a quelli proposti nel 2013, in particolare se si tiene in considerazione del fatto che le politiche previste nel precedente Piano Nazionale non fossero così ben mirate come quelle sviluppate da altri pasi con problemi di CSSS simili. Sfortunatamente, questa inerzia nello sviluppo della politica di sicurezza cibernetica ha rallentato l'ideazione di misure che avrebbero potuto incoraggiare un decisivo cambio di passo nella protezione dello spazio cibernetico nazionale.

In sintesi, dati i vincoli di bilancio e la mancata evoluzione della politica di sicurezza cibernetica nazionale, le azioni di Roma per contrastare il CSSS risultano essere in ritardo rispetto a quelle messe in atto da altri paesi affini. A fronte di queste problematiche, il presente rapporto suggerisce di:

• Determinare la portata del CSSS conducendo un'analisi online delle posizioni vacanti nel mercato del lavoro della sicurezza cibernetica italiano;

• Raccogliere maggiori informazioni sulla natura del CSSS, mandando il questionario adoperato in questo rapporto a un campione più rappresentativo rappresentativo di datori di lavoro attivi nell'ambito della sicurezza cibernetica in Italia e conducendo ulteriori interviste;

• Creare un partenariato tra governo, industria e sistema educativo per ideare una soluzione nazionale al CSSS;

• Includere il Ministero dell'Istruzione, dell'Università e della Ricerca all'interno del Tavolo Tecnico Cyber per indirizzare correttamente la politica educativa in sicurezza cibernetica;

• Stanziare un fondo per lo sviluppo e l'implementazione della sicurezza cibernetica nazionale, che deve prevedere un finanziamento destinato esclusivamente all'educazione e allo sviluppo di competenze nella sicurezza cibernetica;

• Nominare una singola amministrazione responsabile per l'ideazione, l'implementazione, il monitoraggio e la valutazione delle politiche per la riduzione del CSSS;

• Trarre ispirazione dalle politiche adottate dal Regno Unito (tra cui la Scozia) come punto di partenza nella definizione delle politiche di mitigazione che potrebbero essere appropriate per risolvere il CSSS italiano;

• Dare priorità a politiche di intervento rivolte alla scuola primaria e secondaria, all'università, e alla transizione scuola-lavoro;

• Stabilire un insieme di metriche per la valutazione dell'efficacia delle politiche definite per il CSSS.

CONTENTS

1. INTRODUZIONE[1]

A seguito della crescente digitalizzazione, dell'aumento di incidenti di sicurezza informatica, della pressione normativa e del progresso della tecnologia ICT, negli ultimi anni la richiesta di esperti in Cyber Security è fortemente aumentata. Tuttavia, l'offerta di tali professionisti non ha equiparato la sua domanda dando la percezione dell'esistenza di uno skill shortage nel campo della Cyber Security, fenomeno che molti paesi tecnologicamente avanzati considerano una minaccia alla loro sicurezza informatica (De Zan, 2019)[2].
Tale difficoltà nel soddisfare la domanda in Cyber Security è stata riscontrata soprattutto in Australia, Giappone, Regno Unito e Stati Uniti; questi paesi sono anche stati tra i più attivi nel mitigare lo shortage attraverso politiche dedicate. Tuttavia, a eccezione di questi esempi e, nonostante le affermazioni di un deficit globale della forza lavoro in Cyber Security, ci sono poche informazioni sulla presenza di tale shortage in altre zone o paesi del mondo.
Questo rapporto, finanziato e supportato dalla *Fondazione Global Cyber Security Center,* cerca di colmare tale lacuna e analizza il fenomeno del Cyber Security Skill Shortage (CSSS) in Italia[3]. Lo studio delle politiche nel settore

[1] Il presente rapporto è una traduzione della versione del testo originale. La versione originale del testo, intitolato "*The Italian Cyber Security Shortage in the International Context*" e scritto in lingua inglese, e' scaricabile dal sito della Fondazione Global Cyber Security Center al seguente indirizzo: https://gcsec.org/policy-interventions-and-the-cyber-security-skills-shortage/. Il testo di riferimento è quello originale in lingua inglese, pertantol'autore non si assume alcuna responsabilita' circa i contenuti della seguente traduzione.

[2] Vedere Allegato I per le dichiarazioni ufficiali sul Cyber Security Skill Shortage dei 12 paesi. I 12 paesi sono stati scelti sulla base del loro ranking nello sviluppo tecnologico dell'International Telecommunication Union ICT e del Global Cybersecurity indexes. L'Allegato è estratto dal Report *Mind the Gap*.

[3] L'autore desidera vivamente ringraziare Elena Mesa Agresti e Marco Fiore per il loro inestimabile supporto nell'organizzazione del sondaggio , nell'individuazione delle iniziative di sensibilizzazione in Cyber Security e per i commenti alle prime bozze del rapporto; Massimo Cappelli e Nicola Sotira per aver concesso l'opportunità di collaborare con GCSEC. L'autore desidera anche ringraziare Bhimsupa Kulthanan per il suo indispensabile editing. Le osservazioni formulate nella versione originale del rapporto sono esclusivamente quelle dell'autore e non rappresentano quelle della Fondazione GCSEC, del Doctoral Training in Cyber Security dell'University of Oxford.

della Cyber Security in Italia è interessante in quanto il paese fa parte di organizzazioni internazionali come Unione Europea e Nato collocandosi tra i primi dieci paesi al mondo per il suo prodotto interno lordo nominale, così rendendolo uno dei principali obiettivi per le varie minacce informatiche. Per questo motivo, capire se il paese soffre della mancanza di professionisti in cyber security e se le politiche adottate per aumentare il numero di professionisti siano efficaci, costituisce una prerogativa di politica pubblica.

Grazie ad un sondaggio inviato ai dirigenti di sicurezza informatica italiani e grazie a interviste con esponenti del mondo della pubblica amministrazione e accademia, questo studio presenta nuovi dati sulla CSSS italiano, rivelando interessanti approfondimenti sulla natura e le caratteristiche di questo fenomeno nazionale. Questa ricerca fornisce, inoltre, un primo resoconto delle politiche adottate dal governo italiano, utilizzando informazioni acquisite da documenti ufficiali tra cui le "strategie" italiane di Cyber Security e le relazioni annuali del Dipartimento delle Informazioni per Sicurezza (DIS) al Parlamento italiano.

Nonostante siano ancora necessari degli approfondimenti per arrivare ad une corretta e completa identificazione del problema, si può affermare che l'Italia risenta delle stesse problematiche che stanno impedendo un corretto bilanciamento tra l'offerta e la domanda di esperti di Cyber Security come in altri paesi. Nonostante questi problemi nel mercato del lavoro, la risposta italiana in termini di politiche pubbliche è stata caratterizzata perlopiù da campagne di sensibilizzazione portate avanti da singole organizzazioni, piuttosto che da una politica coordinata e centralizzata a livello nazionale. Tenendo dunque in considerazione la potenziale crisi della forza lavoro di cyber security, sarebbe necessario portare avanti un serio dibattito su come evitare che il CSSS possa mettere a repentaglio la sicurezza nazionale e lo sviluppo economico nazionale.

Questo rapporto è così organizzato: la sezione 2 riassume i risultati del rapporto "*Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions*" utile a mettere in prospettiva il CSSS italiano; la sezione 3 raccoglie informazioni rilevanti sul CSSS italiano e i relativi interventi di politica pubblica; la sezione 4 analizza il CSSS italiano tenendo conto della prospettiva internazionale delineata nella sezione 2; la sezione 5 suggerisce alcune raccomandazioni basate sull' analisi precedente.

2. IL FENOMENO DEL CYBER SECURITY SKILL SHORTAGE: LA PROSPETTIVA INTERNAZIONALE

Il Report "*Mind the Gap*" ha rilevato che, ad oggi, non sono stati formulati dati certi e rilevanti sull'incidenza e la natura a livello globale del Cyber Security Skill Shortage (*De Zan, 2019*)[4] . Tuttavia, ha anche evidenziato che, almeno in alcuni paesi, vi sono prove tangibili che dimostrano le cause del disequilibrio tra la curva di offerta e quella di domanda del mercato del lavoro della Cyber Security. Questo paragrafo ha l'obiettivo di ripercorre le evidenze analizzate nello studio delle policy di diverse nazioni come Australia, Giappone, Regno Unito (inclusa la Scozia) e Stati Uniti, allo scopo di poter analizzare in parallelo il CSSS italiano nella sezione n.4.

Il Report sostiene che, al di là dei tipici fattori come livelli di disoccupazione, entrate, prodotto interno lordo, tassi di partecipazione[5], il mercato del lavoro della Cyber Security è influenzato anche da molti altri fattori: dal mondo della digitalizzazione, dagli incidenti di sicurezza informatica, dai regolamenti internazionali e non di meno dal progresso dell'Information Communication Technology (ICT). Poiché tutti questi fattori appena citati hanno raggiunto una dimensione ancor più importante e considerevole, la domanda di esperti in Cyber Security è aumentata. Negli Stati Uniti, ad esempio, i posti di lavoro in Cyber Security pubblicati on-line sono aumentati del 91% dal 2010 al 2014 e nuovamente aumentati del 32% dal 2014 al 2018; il numero di 238,158 posti di lavoro presenti nel mercato (on-line) nel 2014 è diventato di 313,735 nel periodo tra settembre 2017 e agosto 2018 (Cyberseek,2018; Burningglass,2015). Tale linea di tendenza probabilmente avrà un andamento esponenzialmente crescente. Negli Stati Uniti il Bureau of Labor Statistics, a riprova di questa repentina evoluzione, stima che la prospettiva di crescita lavorativa di un analista Cyber Security sia "molto più rapida" (circa del 28%) rispetto al tasso di crescita medio di tutte le altre occupazioni (7%) nel periodo compreso tra il 2016 e il 2026 (Bureau of Labor Statistics, 2018).

---

[4] Il Report "*Mind the Gap*" è disponibile in versione integrale e gratuitamente al seguente link: https://bit.ly/2IFgSvI (Febbraio 2019).

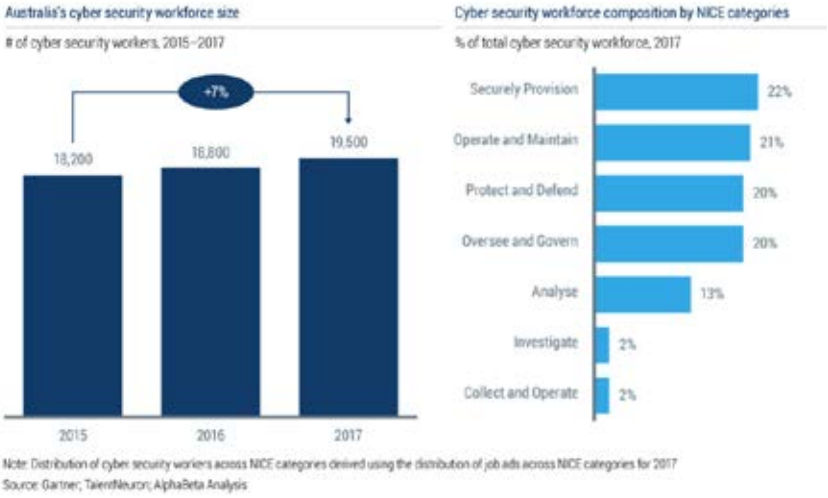
[5] Per *tasso di partecipazione* si intendono gli indicatori del numero di lavoratori compresi tra i 16 e i 64 anni impiegati o che cercano occupazione

Secondo la teoria economica del mercato del lavoro, se dovesse esserci uno shortage in un determinato settore, si dovrebbe notare un aumento dei salari in quello specifico campo, in quanto i datori di lavoro sarebbero disposti a pagare un compenso maggiore per reclutare professionisti specializzati da un bacino più limitato di candidati. Ci sono evidenze empiriche della teoria appena descritta in Australia, Regno Unito e Stati Uniti. In Australia le posizioni in Cyber Security prevedono un salario superiore dell'11% rispetto a tutte le altre occupazioni nel campo IT e dell'81% in più rispetto alle restanti posizioni del mondo del lavoro. Anche i salari in Cyber Security crescono più velocemente rispetto a quelli di altri settori: tra il 2014 e il 2016 un salario previsto per un impiego in Cyber Security è aumentato del 2,7% rispetto ad una crescita media annua delle retribuzioni del 1,7% nel più ampio settore IT (Australia Cyber Security Network, 2017).

Tra il 2015 e il 2016 nel Regno Unito, il tasso medio dei salari è stato di 57.100 sterline annuo con un aumento del 7% rispetto all'anno precedente e del 15% in più rispetto ad altre posizioni specialistiche digitali (Tech Partnership, 2017). Analogamente, un rapporto della società di consulenza Robert Walters ha rilevato che gli specialisti in Cyber Security aumenteranno del 7% nel 2018, molto più della crescita del 3% di sviluppatori e specialisti delle infrastrutture (Bell, 2018). Sempre nel Regno Unito, la remunerazione media per un neo-laureato/junior parte da 28,000 sterline annuali, 45,000 sterline per i profili Senior, 60,000 sterline per i Manager, 80,000 sterline per i responsabili fino a 100,000 sterline per i profili partner/chief executive, il che "ribadisce la rimunerativtà del settore" (RSM and CSIT, 2018). Negli Stati Uniti, la retribuzione media per un analista di Information Security è di $95,510 nel maggio 2017, molto più alta rispetto a un qualsiasi altro impiego nel settore IT (di $84,580) e di tutti gli altri impieghi collegati (di $37,690). Il salario medio annuale di un analista IT è cresciuto dell'11% dal 2012 al 2017 in rapporto alla crescita salariale contenuta all'8% degli altri impieghi (Bureau of Labor Statistics, 2018a).

Un altro importate indicatore che potrebbe suggerire la presenza di questa carenza è il numero delle posizioni che non riescono a essere colmate e che rimangono inoccupate per diverso tempo. In particolar modo queste offerte di lavoro rimangono aperte molto di più rispetto alle altre, questo potrebbe significare che le posizioni vacanti sono "difficili da riempire" e quindi potrebbe esserci una carenza di personale (generalmente più di 2 mesi). A livello nazionale, quattro nazioni hanno evidenziato questa dinamica, nello speci-

fico Australia, Giappone, Scozia e Stati Uniti.
Il Giappone ha visto nel corso degli ultimi anni una esponenziale incremento dello shortage nella Cyber Security. Già nel 2013, il Giappone con la Japanese Cyber Security Strategy, aveva stimato una potenziale carenza in Cyber Security di 80.000 unità rispetto alla forza lavoro totale necessaria di 265.000 unità operative (Information Security Policy Council, 2013).
Secondo una stima successiva del Ministero dell'Economia, del Commercio e dell'Industria giapponese (METI - 2016), lo shortage divenuto già di 132.060 unità, avrebbe superato la soglia di 193.010 nel 2020. Circa la metà delle aziende (utilizzatrici finali) in Giappone ritiene che i loro staff soffrano una carenza di esperti IT e solo il 26% pensa di avere abbastanza talenti in questi ruoli[6].
L'Australian Cyber Security Sector Competitiveness Plan afferma chiaramente che nel settore della Cyber Security la nazione avrà bisogno di un ulteriore numero di esperti compreso tra 7,500 e 11,000 risorse entro il 2026 (Australian Cyber Security Growth Network, 2017).



[6] Ministry of Economy, Trade and Industry (METI) – IT Jinzai report Summary – Lingua originale: http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf - Pag.12

Nel Regno Unito, la Scozia ha stimato di aver avuto tra i 360 e i 480 posti di lavoro vacanti nel 2017, che potrebbero facilmente salire a 620 - 840 nel 2020 in assenza di interventi specifici per aumentare l'offerta (National Cyber Resilience Leaders' Board, 2018).

Infine gli Stati Uniti d'America hanno dichiarato di avere ben 299.000 posti di lavoro ancora disponibili nei settori affini alla Cyber Security dall'agosto del 2017 (*SoC & SoHS, 2018*). Proprio negli U.S.A., CyberSeek, un tool online che analizza il mercato del lavoro e classifica i ruoli di Cyber Security in base al Framework NICE del NIST, riporta tutti gli annunci di lavoro in Cyber Security tra il settembre 2017 e l'agosto 2018. Le principali posizioni sono rinvenibili in "operate and maintain" (26%) e in "securely provision" (24%)[7], analogamente al mercato Australiano e a quello italiano come verrà presentato nei prossimi paragrafi.

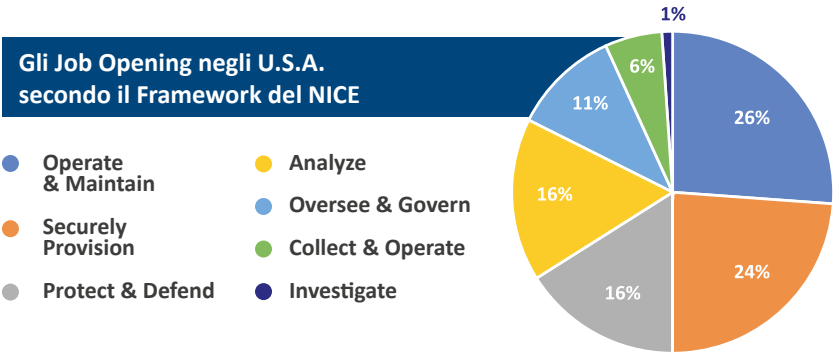


FigurA 1: Job Openings basati sul Framework NICE - Fonte CyperSeek - Novembre 2018

[7] *The National Institute of Standards and Technology (NIST)* ha prodotto una tassonomia – *The National Initiative for Cybersecurity Education (NICE)'s Cybersecurity Workforce Framework* – catalogando, conoscenza, abilità e skill nel mondo della Cyber Security. Il Framework in Cyber Security prevede 7 categorie di alto livello: a*nalyze, collect & operate, investigate, operate & maintain, oversee & govern, protect and defend, securely provision.*

I profili più richiesti	Le certificazioni più richieste	I profili più remunerati
• Cyber Security Engineer	• GIAC	• Cyber Security Architect - $ 129K
• Cyber Security Analyst	• CISM	• Cyber Security Manager - $ 115K
• Cyber Security Manager /Administrator	• CISA	• Cyber Security Engineer - $ 108K
	• CISSP	

Tabella 1: Mercato del lavoro in Cyber Security negli U.S.A. fonte "*CyberSeek che utilizza il Framework NICE del NIST*

Il rapporto "*Mind the Gap*" ha rilevato, inoltre, che mancano solide prove ed elementi per analizzare tutte caratteristiche e la natura dello Skill Shortage data la sua complessità. Le attuali risultanti empiriche del CSSS disponibili a livello internazionale sono imperfette a causa di numerosi problemi metodologici, tra cui questionari mal progettati - quindi l'indeterminatezza dei risultati - nonché la dubbia quantificazione dello Shortage globale. Ciononostante, grazie a un'analisi della documentazione rilevante a livello nazionale e delle politiche sulle specifiche competenze e alle interviste di esperti in materia di Cyber Security, lo studio ha suggerito che ciò che sembra essere particolarmente insufficiente, sono i candidati con anni di esperienza professionale e una combinazione di competenze trasversali.

Il rapporto ha sottolineato che il CSSS è il risultato dell'interazione di più fattori. Sicuramente il sistema educativo deve porre rimedio alla propria difficoltà di formare un numero adeguato di candidati con le competenze e le conoscenze per un ruolo junior nella Cyber Security.
In altre parole, non è sufficiente il numero di laureati in corsi che afferiscono alla Cyber Security e vi è una difficoltà per gli stessi di acquisire competenze e conoscenze adeguate a svolgere un lavoro nella sicurezza informatica. Secondo i datori di lavoro, invece, c'è un disallineamento tra ciò che la stessa industria vorrebbe che gli studenti conoscessero e ciò che il sistema di istruzione e formazione in realtà offre.
In generale gli studenti sono portati a scegliere percorsi professionali più tradizionali a causa di una mancanza di consapevolezza sui vantaggi che una carriera in Cyber Security può offrire. Tra i fattori più influenti nel CSSS c'è sicuramente una evidente carenza di docenti e professori nel sistema educativo, dall'istruzione primaria a quella superiore. Anche i datori di lavoro potrebbero aggravare tale carenza non fornendo opportunità entry-level come

stage e / o apprendistati preferendo assumere professionisti con diversi anni di esperienza professionale (spesso senza specificare con precisione i requisiti dei candidati). Alcuni dati del mercato del lavoro in Australia in Cyber Security mostrano che nell'88% delle posizioni disponibili sono richiesti ben 2 anni di esperienza professionale, rispetto al 66% per qualsiasi altra tipologia di lavoro. (Australian Cyber Security Network, 2017).

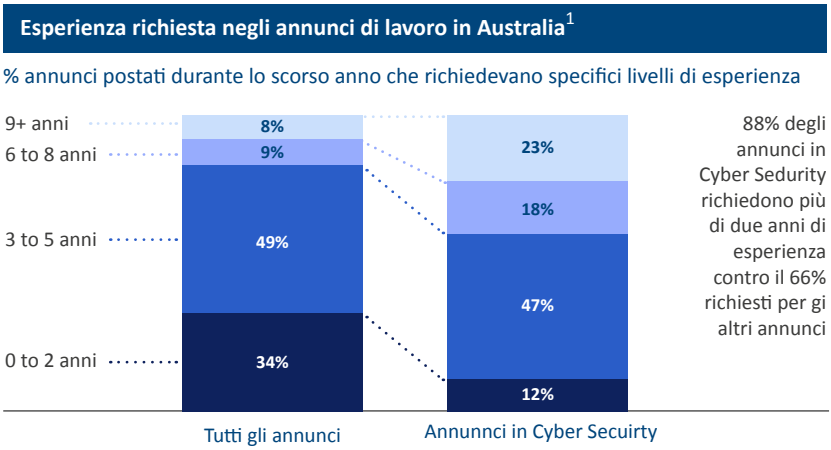


Figure 2 : Esperienza richiesta per gli annunci lavorativi in Australia: Australian Cyber Security Growth Network 2017

I datori di lavoro non offrono formazione adeguata alla forza lavoro e, delle volte, salari in linea con il mercato internazionale non riuscendo a mantenere i propri talenti o ad attirarne altri.
Ulteriori fattori che stanno rendendo il CSSS ancor più complesso sono, tra gli altri, sia il fenomeno migratorio della "fuga di cervelli" che scelgono per il proprio futuro mercati più remunerativi (in particolare gli Stati Uniti) sia l'incapacità nel valorizzare alcune categorie di lavoratori.

Nonostante l'insufficienza di prove concrete, alcuni governi hanno portato avanti politiche per l'implementazione di specifiche soluzioni nazionali. Hanno investito principalmente nell'istruzione superiore, nella ricerca e nella forza lavoro, mentre iniziative più generali hanno interessato la scuola primaria e secondaria, nonché i programmi di formazione professionale e di apprendistato.

Di seguito alcuni esempi di alto livello degli interventi in essere[8] :

Scuola Primaria e Secondaria

- Revisione curriculum (ICT e sicurezza informatica)
- Competizioni in Cyber Security
- Inserimento di esperti di Cyber Security nel corpo docente e formazione del personale

Istituti Professionali e Apprendistato

- Nuovi indirizzi professionali in Cyber Security
- Tirocini tecnici e apprendistato in CYber Security

Università e Ricerca

- Competizioni in Cyber Security
- Borse di studio e sovvenzioni
- Centri Accademici di Eccellenza
- Accreditamenti di laurea da associazioni professionali o enti governativi / orientamento curriculare
  Nuovi programmi in grado di bilanciare l'esperienza pratica e la teoria secondo un approccio multidisciplinare
- Inserimento di discipline di Cyber Security e Awareness in tutti i programmi
- Partenariato Pubblico privato
- Investimenti in progetti di ricerca in Cyber Security e spin-off

Workforce

- Framework delle competenze e skill in Cyber Security
- Programmi di sensibilizzazione per lavoratori
- Programmi di aggiornamento per lavoratori
- Professionalizzazione della figura dell'esperto in Cyber Security
- Ampliamento di tool per il Recruitment

Tabella 2: *"Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions" by T.De Zan (2019)*

Anche se potrebbe sembrare fuorviante parlare di "best practice", è chiaro che alcuni governi sono risultati più "completi" rispetto ad altri nell'affrontare il CSSS[9] .

[8] Per una descrizione specifica delle policy esaminate, "Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions", pp. 40-51 (https://bit.ly/2IFgSvI).

[9] Ci sono due ragioni principali per cui è scientificamente ingiustificabile parlare di "best-practice" nelle policy delle competenze di Cyber Security. Innanzitutto, non è ancora chiaro se le politiche governative abbiano effettivamente affrontato le cause alla radice della CSSS, in parte legate al fatto che finora non sono state prodotte prove così concrete. In secondo luogo, è difficile, se non impossibile, verificare in che misura le misure politiche adottate dai paesi siano state efficaci nell'aumentare la quantità e la qualità dei professionisti della sicurezza informatica. Ciò si verifica principalmente perché le politiche richiedono tempo per produrre l'impatto desiderato (e queste politiche sono relativamente nuove), ma anche perché non molti governi sembrano disporre di metriche per misurare gli effetti delle loro iniziative politiche.

Per "completo" in senso lato si intende che alcuni governi hanno maturato nel tempo una maggiore esperienza e consapevolezza nell'affrontare lo Skill Shortage, coinvolgendo i principali attori del dibattito - cioè i governi stessi, l'industria e il sistema educativo - per ideare soluzioni e attuare politiche rivolte ad un pubblico più ampio. Tale maturità è riscontrabile dall'analisi delle politiche del Giappone, del Regno Unito (e Scozia) e degli Stati Uniti.

L'Allegato II del presente report cerca di entrare vis-à-vis delle policy in materia di Cyber Security adottate dal Regno Unito[10].

Tra il 2011 e il 2016, il Regno Unito ha investito ben 32,8 milioni di sterline per i programmi di formazione ed educazione ed è attualmente in fase di definizione una ulteriore strategia di Cyber Security, che dovrebbe essere pubblicata entro la fine del 2019 (HM Government, 2016; HM Government, 2018)[11]. Ad oggi, le principali iniziative che il Regno Unito ha implementato sono:

• *Scuola Primaria e Secondaria*: la Cyber Security è stata inclusa nei corsi di studio e negli esami di diploma della scuola dell'obbligo; Cyber Security Challenge UK ha organizzato attività extra-curriculari per 23.000 studenti da quando è nata nel 2013; il nuovo Cyber Discovery Program è stato creato per innovare i processi di formazione degli studenti nelle materie di Cyber

[10] La politica del Regno Unito è stata scelta per diversi fattori: il CSSS è stato chiaramente identificato come un problema nella strategia nazionale di Cyber Security; il governo ha perseguito una politica globale rivolta a più gruppi, dalla scuola primaria alla forza lavoro; la politica è stata costantemente sostenuta e si è evoluta nel corso degli anni; sono state progettate e attuate iniziative politiche specifiche e chiaramente discernibili, al contrario di più ampi obiettivi politici; sono disponibili informazioni sul bilancio dedicato a questi programmi politici; esiste un'ampia disponibilità di dati online, in grado di rafforzare i dati raccolti dai documenti della politica di Cyber Security.

[11] La Initial National Cyber Security Skills Strategy è stata pubblicata nel dicembre 2018. Il governo utilizzerà il tale documento per raccogliere consigli e raccomandazioni per l'educazione in Cyber Security. Dopo questa dichiarazione di intenti infatti pubblicherà una strategia finale (entro il 2019). Con questa strategia autonoma, Londra si unirà al comparto di nazioni come il Giappone, Stati Uniti e Scozia, che vantano un documento politico dedicato esclusivamente all'educazione della Cyber Security e alle competenze che integrano una strategia di sicurezza informatica globale.

Security e con il risultato che ben 23.000 studenti hanno aderito alla prima edizione del 2018. La Cyber Security e le competenze digitali verranno implementate in maniera trasversale in tutto il sistema educativo.

• *Istituti professionali e apprendistato*: creato un nuovo apprendistato per la tutela e sicurezza delle Infrastrutture Critiche da parte del governo. L'NCSC (National Cyber Security Centre) ha iniziato il proprio progetto CyberFirst Degree Apprenticeship.

• *Scuola Superiore e Ricerca*: le università hanno istituito nuove e ulteriori borse di studio per le discipline della Cyber Security attraverso specifiche sovvenzioni da parte degli organi preposti. L'NCSC, infatti, ha assegnato borse di studio a studenti che si sono iscritti a corsi di laurea in Cyber Security per le 20 lauree già previste; 17 università sono state riconosciute come centri di eccellenza accademici (ACE) nella ricerca sulla Cyber Security; sono stati istituiti 3 dottorati universitari in Cyber Security e 4 istituti di ricerca dedicati;

• *Forza-lavoro*: è stato lanciato il Cyber Security Skills Immediate Impact Fund un progetto che mira ad aumentare sia il volume che la diversità delle figure professionali oltre che ovviamente le competenze in materia di Cyber Security nel Regno Unito; è stata aperta una consultazione al fine di professionalizzare la Cyber Security entro il 2020. Viene definito con il National Cyber Security Programme un Body of Knowledge per la Cyber Security per aggiornare e sostenere l'istruzione e la formazione professionale nel settore della sicurezza informatica.

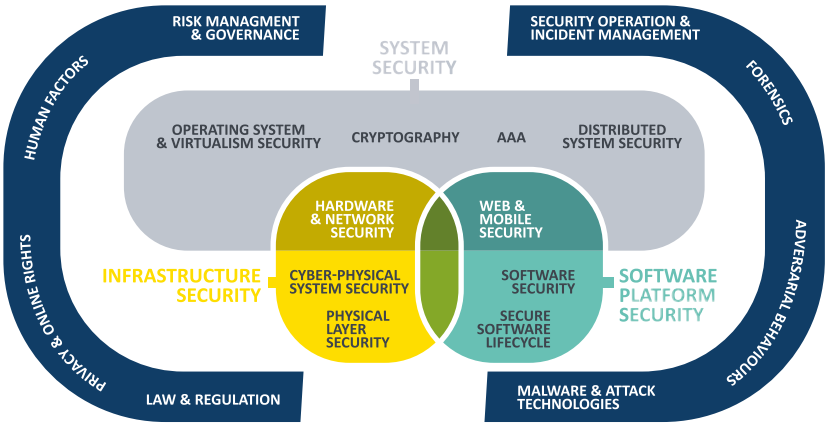


Figure 3 : Cyber Security Body of Knowledge Cluster Diagram

3. IL CONTESTO ITALIANO DELLA CYBER SECURITY

I recenti sviluppi del mercato e della politica internazionale hanno reso la Cyber Security anche per l'Italia un settore particolarmente dinamico sia per il Governo che per le imprese nazionali.
A causa dei ripetuti attacchi ad aziende e enti, perpetrati con malware, gli incidenti informatici sono cresciuti dell'11% solo nel 2017 dando, probabilmente, un impulso al mercato della Cyber Security che ha visto crescere gli investimenti da 728,2 milioni di euro nel 2015 a 896,5 milioni di euro nel 2017 (Rapporto Clusit, 2018; Anitec-Assinform, 2018).
Significativi cambiamenti ci sono stati anche a livello legislativo quando il Governo ha presentato il secondo "Piano Nazionale per la protezione cibernetica e la sicurezza informatica" del 2017 e l'adozione della "Direttiva Network and Information Security" anche più comunemente conosciuta come "Direttiva Nis" recepita dallo stesso Governo italiano nel maggio 2018[12].
Per analizzare nel dettaglio il contesto di riferimento, questa sezione raccoglie le informazioni più rilevanti sul CSSS italiano (3.1) e i relativi interventi strategici (3.2).

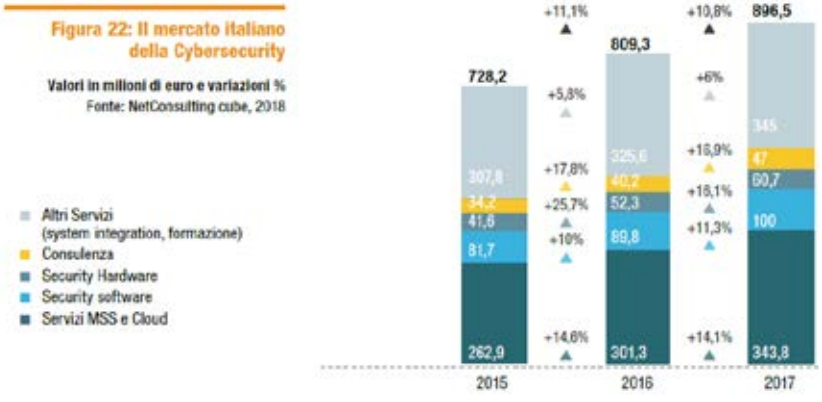


Figure 4 : Il mercato della Cyber Security in Italia. Fonte - Il Digitale in Italia 2018, Anitec-Assinform (2018)

[12] La strategia di sicurezza informatica italiana è composta da due documenti distinti, vale a dire il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" (2013) e il "Piano nazionale per la protezione dello spazio cibernetico e la sicurezza informatica", (2013 e 2017).

3.1 I rapporti del CSSS italiano

In Italia, il CSSS è stato riconosciuto per la prima volta in un documento governativo ufficiale pubblicato nel febbraio 2018. Il documento, la relazione Annuale sulle minacce e le attività di intelligence al Parlamento italiano (Relazione sulla politica per la sicurezza, Allegato: Documento di sicurezza nazionale), è stato rilasciato dal Dipartimento di intelligence sulla sicurezza, che è diventato l'Istituzione centrale nell'ecosistema della sicurezza informatica italiana nel maggio 2018 in seguito all'adozione della direttiva NIS. Il rapporto in questione riconosce che una resilienza cibernetica efficace è il frutto dello sviluppo di una idonea forza lavoro in Cyber Security, ma, tuttavia, evidenzia che in Italia esiste un vasto problema in relazione all'educazione alla sicurezza informatica, che sta interessando sia la forza lavoro operativa che quella futura (*Presidenza del Consiglio dei Ministri, 2018*)[13] .
Altre fonti autorevoli non governative hanno analizzato il fenomeno, fornendo un quadro statisticamente più completo del fenomeno. In particolare sono da menzionare i lavori dell'Osservatorio sulle competenze digitali (Aica et al. 2017), il Cyber Security Barometer (Croci, 2018) e lo studio di Kaspersky Lab (2016).

Scritto dalle quattro più importanti associazioni italiane del settore IT in collaborazione con il Governo italiano[14], l'Osservatorio sulle competenze digitali del 2017, ha rilevato diverse criticità: una estrema esigenza di formare nuove risorse, una carenza di professionisti nel mondo IT e una insufficiente offerta formativa ed educativa del sistema scolastico sono elementi che devono condurre ad un rafforzamento delle politiche esistenti per rafforzare le politiche e le competenze digitali già esistenti e trovare un equilibrio di mercato tra domanda e offerta delle digital skill.

Il rapporto sostiene che le competenze più richieste sono quelle del settore ICT, Informatiche Applicate/di Gestione e della sicurezza: in particolare Cloud Security Architect, Cyber Security Consultant, Cyber Security Architect, Cyber Security Project Manager. Soprattutto nel contesto della nascente In-

[13] p. 11

[14] Le associazioni di settore sono: Aica, Assinform, Assintel, Assinter; AGID (Agenzia per l'Italia Digitale) e MISE (Ministero dell'Istruzione Università e della Ricerca).

dustria 4.0, gli specialisti della Cyber Security sono considerati tra i cinque professionisti più ricercati.

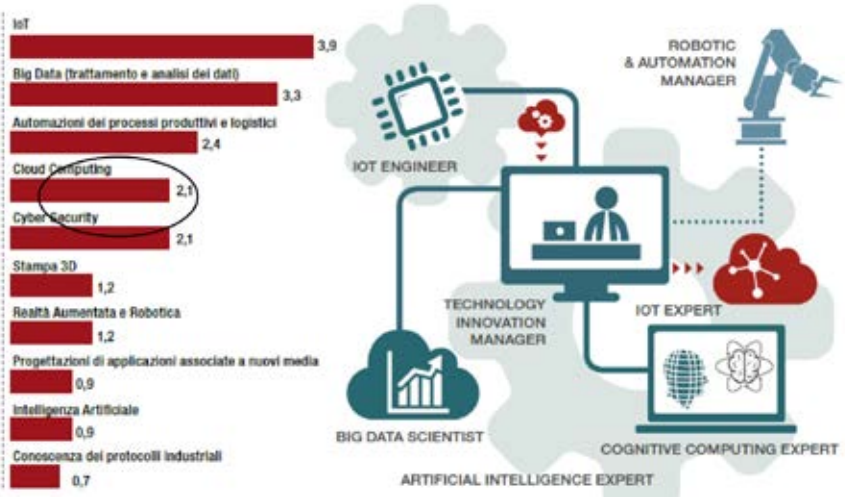


Figure 5 : Le competenze e le specializzazioni più ricercate in Italia - Fonte: Industria 4.0. -Osservatorio Competenze Digitali (2017)

La mancanza di formazione tecnica e di candidati ben preparati, il disallineamento tra la domanda e l'offerta, la difficoltà nell'individuare e trattenere nella propria realtà i talenti, sono le reali minacce che soffocano lo sviluppo e l'acquisizione di competenze digitali[15]. Un'analisi delle offerte di lavoro disponibili tra il 2013 e il 2016 suggerisce un trend annuale in aumento del 26% della domanda di esperti e in generale delle retribuzioni di professionisti del settore ICT. Le nuove professioni emergenti hanno registrato una crescita del 56% e includono i settori della cyber security e cloud computing, dell'IoT, del service development, del service strategy, della robotica, del cognitive e dell'artificial intelligence.

[15] Le tecnologie e i processi aziendali futuri richiederanno forza lavoro capace di combinare conoscenze e competenze tecniche con competenze trasversali quali il pensiero critico, l'intelligenza emotiva, la leadership e la gestione dell'innovazione. In particolare, agli esperti di Cyber Security verrà chiesto di operare in ambienti eterogenei e in continua evoluzione.

Quando è stato pubblicato nel 2017, il rapporto stimava il gap atteso tra domanda e offerta di professionisti ICT nel mercato del lavoro italiano di circa 61.000 - 85.000 lavoratori per il biennio 2016 - 2018. Nello studio si può leggere come "*l'offerta di diplomati e laureati in percorsi di studi attinenti all'ICT, è di circa 71 mila unità per il triennio 2016-18 costituita per il 33% da laureati e il 67% da diplomati, che apparentemente sembrano soddisfare una domanda intermedia tra scenario conservativo e ottimistico.*"[16]
Secondo l'Osservatorio tuttavia le Web Vacancy smentiscono tale dato e "mostrano *una richiesta proporzionata sul 62% di laureati e il 38% di diplomati*."
Il confronto tra domanda e offerta stimato (quindi il suo gap), per il 2017 veniva così individuato:
- *nello scenario conservativo, un deficit di 4.400 laureati ICT a fronte di un eccesso di circa 8.400 diplomati ICT, - nello scenario espansivo un deficit di circa 9.500 laureati e un surplus di diplomati ICT di 5.200*. Risulta rilevante il disallineamento tra domanda e offerta di competenze ICT. Le imprese stanno operando ricerche rivolte a professionisti ICT (laureati) sempre più qualificati perseguendo un *UpSkilling* della propria forza lavoro. Solo recentemente si è assistito a un aumento delle iscrizioni ai corsi di laurea in ICT (+ 9%), ma il 60% non porta a termine i propri studi.
Sono incrementate le iscrizioni per i corsi di laurea che sviluppano temi come Big Data e Cyber Security ma i corsi ICT, in generale, sono fortemente inferiori (nel 50% dei casi) rispetto al totale delle lauree non incentrate nei settori tecnologici.

Il sistema educativo tuttavia non è l'unica fonte di preoccupazione. La formazione professionale all'interno delle aziende è considerata inadeguata o fortemente insufficiente oltre che lo sviluppo professionale e la flessibilità del lavoro. In generale, le collaborazioni tra scuole/università e settore privato non hanno portato risultati attesi e tali accordi non sono stati in grado di aumentare l'offerta di risorse nel campo della Cyber Security come invece è avvenuto nell'area dell'Organizzazione per la cooperazione e lo sviluppo economico. Il coinvolgimento del settore privato è oltremodo ostacolato da un complesso quadro normativo fortemente frammentato, da una scarsa consapevolezza e disponibilità di incentivi finanziari e da una difficoltà nella defi-

[16] Nel 2016, ci sono stati 7.500 laureati ICT, tra cui 4.700 specialisti ICT, laureati in ingegneria informatica o informatica.

nizione di collaborazioni. Alcuni risultati interessanti, che hanno avuto come oggetto di indagine la percezione del fenomeno del CSSS dal punto di vista dei datori di lavoro, sono stati quelli presentati dal Barometro di Cyber Security 2018[17]. I responsabili della sicurezza hanno evidenziato come le lacune principali nelle loro organizzazioni sono dovute da un numero limitato di personale nel proprio staff e da una mancanza di competenze specialistiche. Proprio per contrastare quest'ultimo fenomeno, le organizzazioni prevedono di integrare il proprio personale nel 2019 con le seguenti figure professionali: security analyst, risk analyst, threat intelligence analyst e network security specialist (Croci, 2018)[18]. La società Kaspersky Lab, ad oggi sembrerebbe essere l'unica ad aver promosso un sondaggio a livello internazionale che pone in relazione le carenze di competenze nella Cyber Security in Italia con quelle degli altri principali paesi europei. Il rapporto in questione ha rilevato che il 30% degli intervistati italiani, al quesito: "è difficile trovare abbastanza professionisti della sicurezza informatica da reclutare", rispondono che sono "fortemente d'accordo"; il dato interessante che si può notare è come con tale percentuale statistica l'Italia si posizioni al secondo posto dopo la Spagna tra le nazioni con maggiore difficoltà a reclutare professionisti. (Kaspersky Lab, 2016).

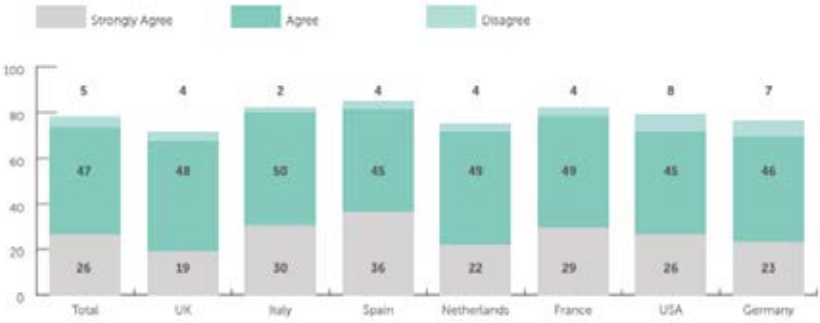


Figure 6 : Sondaggio. Fonte; Kaspersky Lab, 2016

[17] Il sondaggio è stato condotto da NetConsulting Cube, Ca Technologies e Oracle e dal Centro Europeo per la Sicurezza Informatica. Il sondaggio è stato inoltrato a Chief Security Officer, Chied Information Officer, Chief Information Security Officer e Chief Technology Officer di organizzazioni private e istituzioni pubbliche.

[18] https://inno3.it/2018/10/31/barometro-Cyber Security-aziende-pronte-alla-minaccia/

3.2 Nuovi dati sulla CSSS italiana: sondaggi e interviste

Il sondaggio promosso con il presente studio e le interviste effettuate sono state impiegate per raccogliere ulteriori informazioni sul CSSS italiano. In linea con la natura esplorativa di questa ricerca l'indagine ha seguito una specifica metodologia di campionamento[19]. Tale sondaggio[20] online, che garantiva l'anonimato degli intervistati, è stata inviata a 45 CISO italiani appartenenti alle più importanti infrastrutture e organizzazioni nazionali[21] con il supporto della Fondazione Global Cyber Security Center e l'ausilio del CLUSIT e di The Innovation Group[22]. Lo studio ha adottato inoltre il Framework del NICE[23]del NIST– National Institute for Standard and Technology (Newhouse et al. 2017) per identificare le conoscenze, le competenze e gli skill mancanti in cyber security nel mercato del lavoro italiano.
La maggior parte degli intervistati proviene da organizzazioni operanti nei settori di consulenza (33%) e settore bancario-finanziario (11%), ma anche le infrastrutture critiche sono state incluse nel sondaggio: telecomunicazioni, trasporti, energia, petrolio e gas (24%), industria manifatturiera (7%) e Pubblica Amministrazione (9%). Più della metà degli intervistati (62%) lavora per organizzazioni che hanno oltre 500 dipendenti con team di Cyber Security di 10(o +) membri (38%). Le interviste faccia a faccia sono state condotte con rappresentanti della pubblica amministrazione e del mondo accademico.

[19] Il metodo utilizzato per il campionamento è di "*type of non probability sampling*". L'obiettivo principale è quello finalizzato a produrre un campione che possa essere logicamente ritenuto rappresentativo della popolazione." (http://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n419.xml). Per una descrizione delle limitazioni del campionamento non probabilistico, vedere Campionamento non probabilistico http://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n337.xml

[20] http://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n105.xml

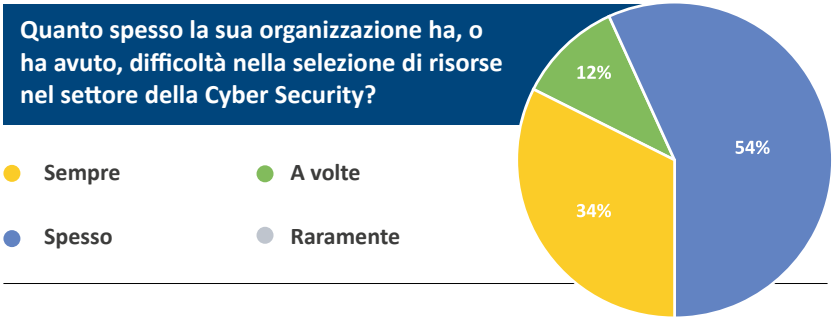
[21] l'Associazione italiana per la sicurezza delle informazioni (https://clusit.it/)

[22] The Innovation Group è una società di servizi che si occupa di organizzazioni di eventi, relazioni di mercato, consulenza e formazione (https://www.theinnovationgroup.it/?lang=en)

[23] NIST, National Institute for Standard and Technology – NICE National Initiative for Cybesecurity Education Workforce Framework, Special Publication 800-181 (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf)

3.2.1 Il Sondaggio

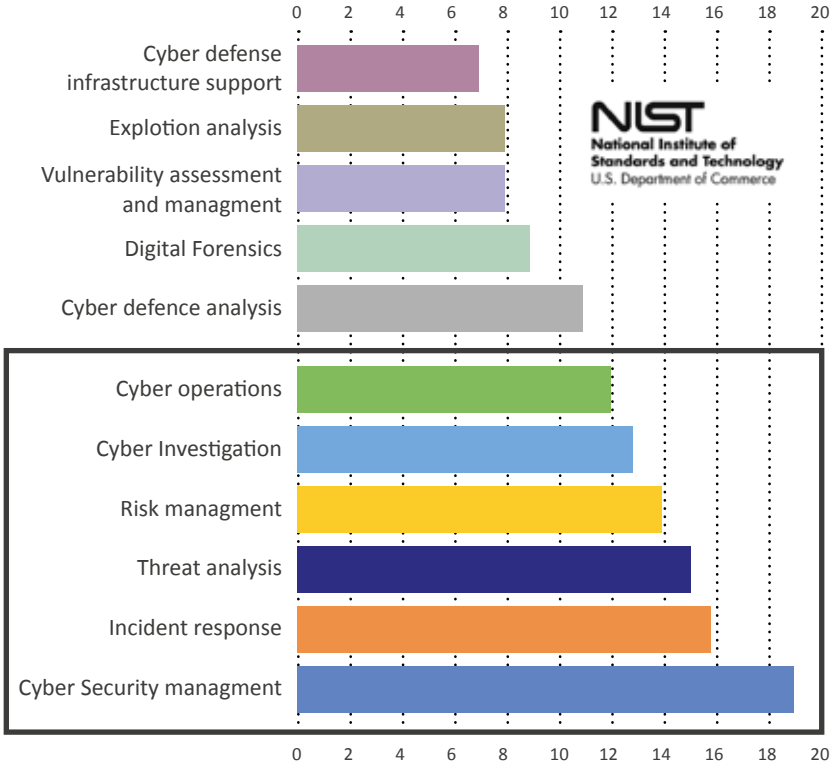
L'indagine ha descritto un quadro decisamente complesso del mercato del lavoro italiano per la Cyber Security. La maggior parte degli intervistati (80%) ha concluso che le loro organizzazioni hanno "sempre o molto spesso" posizioni scoperte in Cyber Security che non possono o non riescono a colmare.
Quando viene chiesto ai Manager quanti candidati siano in possesso dei requisiti minimi di preparazione ed esperienza per una possibile assunzione, il 60% afferma che hanno difficoltà a trovare anche un solo candidato o che perfino sono costretti ad assumere candidati che non sono qualificati per la posizione richiesta.
Inoltre, il 53% ha affermato che le posizioni di Cyber Security sono mantenute aperte tra 61 e oltre 90 giorni, dato che suggerisce come tali posizioni siano realmente difficili da colmare.



Il 56% dei rispondenti ha dichiarato che la propria organizzazione trova maggiore difficoltà ad assumere profili con 4-10 anni di esperienza professionale mentre il 36% profili con 1-3 anni di esperienza.
Apparentemente, le aziende non hanno difficoltà a reclutare neolaureati o candidati senza alcuna esperienza professionale ma la maggior parte delle aziende (58%) afferma che preferirebbe assumere una quantità minore di personale ma con esperienza professionale già acquisita. Non sorprende, infatti, che le organizzazioni di solito richiedano dagli 1-3 anni (51%) e 4-10 anni (42%) di esperienza professionale come requisito minimo. Solo una piccola percentuale di organizzazioni (7%) ha posizioni che non richiedono alcuna esperienza professionale pregressa.

Seguendo le categorie del NICE Cyber Security Workforce Framework le competenze più difficili da reperire sono: Cyber Security management (42%), Incident response (36%), Threat analysis (33%) risk management (31%) and cyber investigation (29%), A queste, per le aziende private, si aggiunge anche la digital forensics (20%).

In quali aree di specializzazione del framework NIST, la sua organizzazione ha maggiore difficoltà ad assumere? (Le definizioni delle specifiche aree sono consultabili al seguente link: https://niccs.us-cert.gov/workforce-development/cyber-security-workfo)

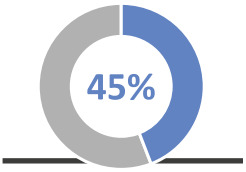


In termini di prerequisiti, le aziende di solito chiedono come titolo minimo per l'assunzione: un diploma di scuola superiore (42%), la laurea triennale (33%) o una laurea magistrale (24%). Ingegneria, Informatica e Cyber Security sono riconosciuti dal 92% degli intervistati come gli indirizzi di studio migliori per ottenere un lavoro in sicurezza informatica entry-level nelle proprie organizzazioni.

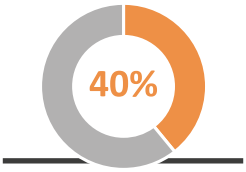
Nel 74% dei casi i CISO richiedono certificazioni professionali e in particolare il 24% le richiede sempre per le proprie posizioni aperte mentre per il 47% rappresentano un importante valore aggiunto. Tra le tipiche certificazioni professionali in Cyber Security, le organizzazioni prediligono la ISO / IEC 27001 nel 69% dei casi e la CISSP nel 56%.

Dall'analisi del sondaggio sembrano emergere altre quattro principali e concomitanti cause che determinano il CSSS sul territorio nazionale. Gli intervistati sostengono che il motivo principale per cui le loro organizzazioni hanno difficoltà o non sono in grado di reclutare personale nella Cyber Security, è la "mancanza di esperienza professionale" (45%) mentre la seconda è "l'incapacità dei datori di lavoro di corrispondere stipendi o sussidi che sono in linea con mercato internazionale "(40%). Altri motivi importanti indicati sono il "basso numero di persone che si candidano" (35%) e la "mancanza di conoscenze teoriche e abilità pratiche dei candidati" (38%).

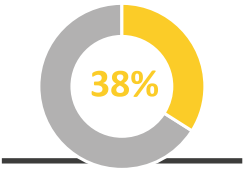
Perchè la sua organizzazione ha difficoltà o non riesce ad assumere personale nel settore della Cyber Security?
Indicare fino a 3 risposte



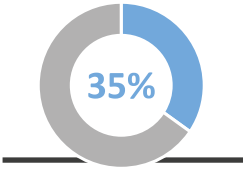
I candidati che non hanno abbastanza esperienza professionale



La mia organizzazione non offre stipendi o benefit adeguati (rispetto al mercato di riferimento)

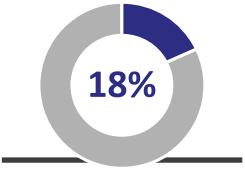


I candidati non hanno ne le conoscenze teoriche, ne le competenze pratiche per svolgere il lavoro richiesto



Non ci sono o sono limitate le candidature per le posizioni aperte

La mia organizzazione ne ha un budget limitato per la Cyber Securiy



La mia organizzazione non offre adeguate opportunità di formazione/ sviluppo professionale

Infatti, alla domanda posta se le organizzazioni sono generalmente soddisfatte delle competenze dei candidati", il 71% degli intervistati dice "solo a volte", indicando come principali cause della propria insoddisfazione: una "conoscenza solo teorica della sicurezza informatica" (71%) e, di nuovo, una mancanza di esperienza professionale (45%).

Infine, il 71% degli intervistati sostiene che il sistema universitario italiano, se pur presenti corsi di laurea rilevanti per la sicurezza informatica come Ingegneria, Informatica e Cyber Security, non fornisce il livello minimo di conoscenze e competenze a un laureato per un primo inserimento nei team di Cyber Security. In generale, le aziende ritengono (53%) che numericamente in Italia non ci siano abbastanza studenti iscritti a tali corsi di laurea.

3.2.2 Le interviste

Il sondaggio è stato supportato da interviste con rappresentati del settore pubblico e del mondo accademico e ha fornito ulteriori dettagli sul CSSS italiano.
Un intervistato ha sottolineato come l'Italia produca pochi professionisti in Cyber Security e come esista una mancanza di competenze a livello manageriale e junior.
Sempre dello stesso avviso, un altro intervistato, ha affermato che ciò che manca davvero in Italia sono professionisti in grado di pensare in modo strategico alla sicurezza informatica, o in altre parole, esperti in grado di stabilire in modo efficace una serie di politiche di sicurezza informatica e guidare una strategia coerente di gestione del rischio di impresa.

Sulle cause dello shortage, un intervistato ha indicato come motivo principale alla base del fenomeno, la mancanza di una adeguata offerta formativa, a cui si aggiunge la mancanza di docenti universitari. Ha aggiunto inoltre che, se è vero che nuove lauree stanno iniziando a nascere, queste sono ancora insufficienti ed eccessivamente focalizzate sulla teoria anziché che sugli aspetti più operativi della Cyber Security. Il sistema educativo italiano, ha affermato l'intervistato, ha reagito in generale lentamente alle nuove tendenze, compresa la formazione informatica. Se ci fossero più lauree in Cyber Security, gli studenti si iscriverebbero volentieri. Una dimostrazione è data dall'iniziativa CyberChallenge.it. L'intervistato ci ha rivelato che già prima che il concorso iniziasse, alcuni dei partecipanti avevano ricevuto offerte di lavoro provenienti, nella maggior parte dei casi, da società straniere non nazionali. A suo parere, questo fenomeno sottolinea la necessità di aumentare il livello della Cyber Security nazionale per controbilanciare la tendenza degli studenti a lasciare il paese per un miglior posto di lavoro con maggiore sicurezza e stabilità all'estero, oltre che prevedere giusti incentivi per frenarne la fuga.
Un altro intervistato ha indicato come una delle principali cause del CSSS in Italia l'assenza di requisiti specifici; non sono chiare le competenze necessarie che Istituzioni e società private richiedono nell'erogazione dei propri servizi di Cyber Security.
Un altro intervistato, invece, ha affermato che la carenza di professionisti in cyber security potrebbe essere collegata alla mancanza della definizione, da parte di Istituzioni e aziende private, di requisiti specifici per erogare servizi di Cyber Security. Secondo lo stesso, il problema può essere ricompreso in una difficoltà più ampia e relativa alla cultura della sicurezza in Italia, sia essa della Pubblica Amministrazione che del settore privato. La sicurezza informatica non è ancora pienamente percepita come una condizione necessaria per le operazioni di business, ponendo i professionisti della Cyber Security nella condizione di non essere sufficientemente supportati dall'ecosistema nazionale. Tuttavia, un intervistato ha affermato che solo alcune aziende italiane stanno richiedendo per l'assunzione titoli accademici, come lauree o master universitari. Allo stesso modo, poche aziende private sarebbero propense a fornire una formazione adeguata o a investire nelle proprie risorse umane.
Un altro intervistato ha ribadito che, se la sicurezza informatica fosse considerata una priorità, i datori di lavoro dovrebbero essere inclini a pagare un salario in linea con i salari internazionali in Cyber Security. Ha riconosciuto poi che, giacché pochissime persone possiedono le conoscenze, le competenze e le capacità per operare in contesti complessi, questi esperti sono estremamente rari e costosi e probabilmente lo saranno anche in futuro.

3.3 Le politiche nazionali per ridurre lo Shortage

Il "Piano Nazionale per la protezione cibernetica e la sicurezza informatica" è stato pubblicato per la prima volta nel febbraio 2013 e ha definito tra i suoi obiettivi la Promozione e diffusione della cultura della sicurezza. Formazione e istruzione. La logica alla base di questo documento era quella di porre l'accento sulla diffusione di una cultura e di una consapevolezza della sicurezza informatica tra la popolazione, ampliando il più possibile i destinatari tra cui il personale del settore pubblico e privato.

Il Piano ha tre obiettivi:

a) *Sviluppo concetti e dottrina*: Analisi del quadro strategico nazionale e un aggiornamento del concetto e delle dottrine relative alle operazioni e alle attività informatiche, miglioramento dell'intesa nazionale su come funziona la deterrenza nello spazio cibernetico;
b) *Promozione e diffusione della cultura della sicurezza informatica*: Organizzare mirate iniziative differenziate per cittadini, studenti, imprese e personale della Pubblica Amministrazione;
c) *Istruzione e formazione*: partecipazione alle iniziative di istruzione e formazione dell'ENISA; aumentare la consapevolezza tra i decision makers sulle minacce informatiche; istruzione per il personale che lavora nelle operazioni informatiche; sviluppo e validazione delle operazioni di Cyber Security con il supporto di training collettivi e training "on-the-job"; raccolta di tutte le prassi di stampo militare disponibili e le attività educative sotto un'entità congiunta; attraverso la partnership con l'Advanced School of Specialization in Telecommunications, l'organizzazione di corsi, seminari e conferenze pubbliche sulla sicurezza delle reti ICT; sviluppare materiale educativo con la Scuola Avanzata per Magistrati e le scuole per il personale amministrativo e penitenziario; sviluppare sinergie con il mondo accademico per definire corsi per la pubblica amministrazione e le imprese; mappa centri di eccellenza nella sicurezza informatica (Presidenza del Consiglio dei Ministri, 2013)

Un nuovo aggiornamento del Piano nazionale per la protezione del cyberspazio e la sicurezza delle ICT è stato pubblicato nel maggio 2017, ma le differenze con il Piano del 2013 sono minime. La principale differenza riguarda la possibilità di collocare le attività di istruzione e formazione sotto la gestione dei centri di eccellenza mettendole a disposizione delle amministrazioni pubbliche, degli alleati NATO, degli Stati membri dell'UE e del personale dei paesi

partner (Presidenza del Consiglio dei Ministri, 2017).

Nella relazione annuale 2017 (febbraio 2018) del *Dipartimento delle Informazioni per la Sicurezza* (DIS), rilasciata al Parlamento italiano, si citano le "varie iniziative che si svolgono a livello locale e nazionale" che stanno tentando di aumentare il livello generale della Cyber Security e delle sue capacità operative (Presidenza del Consiglio dei Ministri, 2018). Sebbene non elencato nel documento, alcune di quelle iniziative potrebbero includere:[24]

Iniziative Nazionali

Be Aware. Be Digital: Una campagna di awareness che ha come destinatari gli studenti e le Piccole e Medie Imprese. Il progetto tra le varie attività prevede lo sviluppo di applicazioni mobili e strumenti di insegnamento digitale per i dipendenti delle PMI;[25]

CyberChallenge.it: Il primo programma italiano di addestramento alla Cyber Security dedicato agli studenti di scuole superiori e università. La Challenge è organizzata dal CINI Consorzio Interuniversitario Nazionale per l'Informatica e dall'Università della Sapienza di Roma; [26]

Laboratorio Nazionale di Cyber Security: è una rete che comprende diverse università e centri di ricerca attivi nell'educazione alla Cyber Security e nella ricerca. Il sito web elenca i principali corsi di laurea e progetti di ricerca in Cyber Security in Italia;[27]

[24] Questa lista non è esaustiva.

[25] Sistema di informazione per la sicurezza della Repubblica (https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/be-aware-be-digital.html).

[26] https://www.cyberchallenge.it/

[27] National Interuniversity Consortium for Informatics (https://www.consorzio-cini.it/index.php/en/national-laboratories/labcs-home).

Vita da social: è una campagna della Polizia Postale promossa sui social media e sulla sensibilizzazione al cyberbullismo;[28]

Generazioni Connesse: è il Safer Internet Centre Italiano, coordinato dal Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) e cofinanziato dalla Commissione Europea ed ha l'obiettivo di essere l'istituto di riferimento nazionale sulla sicurezza digitale per i più giovani. Il programma, attraverso la Commissione, promuove strategie finalizzate a rendere Internet un luogo più sicuro per gli utenti più giovani, promuovendone un uso positivo e consapevole. Esso prevede un Centro di Consapevolezza, due Hotline e una Helpline;[29]

Sicurinrete.it: è un centro nazionale che promuove un uso sicuro dei social media e una maggiore consapevolezza dei diritti e dei doveri di internet di giovani e adulti, promuove campagne di comunicazione e supporto per le persone che hanno esperienze negative online;[30]

L'Autorità Garante per la protezione dei dati (Garante per la protezione dei dati personali) ha pubblicato documenti e promosso campagne di sensibilizzazione con l'obiettivo di sensibilizzare la popolazione su argomenti relativi alla protezione dei dati.[31]

[28] Commissariato di P.S. https://www.commissariatodips.it/uploads/media/COMUNICATO_STAMPA_una_vita_da_social_5__edizione_2018_.pdf

[29] Safer Internet Centre https://www.generazioniconnesse.it/site/it/il-progetto/

[30] Siuri in Rete (https://www.sicurinrete.it/)

[31] Garante per la protezione dei dati personali https://www.garanteprivacy.it/web/guest/home/stampa-comunicazione/vademecum-e-campagne-informative

Una politica che potrebbe anche essere potenzialmente rilevante per la sicurezza informatica è il Piano Nazionale Scuola Digitale (PNSD). Il PNSD è parte di una più ampia riforma scolastica chiamata La Buona Scuola ed entrata in vigore nel 2015. Il Piano ha l'obiettivo di modernizzare il sistema educativo italiano nel contesto della digitalizzazione ma delle 34 iniziative previste nel PNSD non ci sono azioni specifiche sulla sicurezza informatica (CINI, 2018,).

Un'altra politica che potrebbe avere un impatto rilevante sullo sviluppo delle competenze in Cyber Security in Italia è il Piano nazionale per l'Industria 4.0 (Piano Nazionale Industria 4.0), lanciato nel 2017 e successivamente ribattezzato con la denominazione Piano Nazionale Impresa 4.0. Uno degli obiettivi del piano è aumentare le competenze per lo sviluppo di un'industria effettivamente di matrice 4.0. Tra gli obiettivi perseguiti dallo Stato nel documento si legge: il raggiungimento di quota 200.000 studenti universitari e 3.000 manager specializzati nei campi relativi all'industria 4.0; +100% studenti iscritti a scuole tecniche specializzate nei campi relativi all'industria 4.0; 1.400 dottorati di ricerca su argomenti incentrati all'industria 4.0 e nuovi centri di competenza nazionali, che dovrebbero promuovere la formazione avanzata e lo sviluppo di progetti di ricerca industriale e di sviluppo sperimentale. Nel piano d'azione per il 2018, il Governo si è posto l'obiettivo ulteriore di: rafforzare il sistema "ITS" di "Istituti Tecnici Superiori" e aumentare l'iscrizione degli studenti da 9.000 a 20.000 ragazzi tra il 2018 e il 2020 con un investimento di 95 milioni di euro; un fondo di 255 milioni di euro per il periodo 2018-2020 per finanziare progetti di ricerca e innovazione in settori strategici per lo sviluppo del capitale intangibile per aumentare la competitività dell'Italia; incentivi finanziari per incoraggiare la formazione su argomenti di industria 4.0 con un credito d'imposta del 40% sui costi di manodopera del personale con un incentivo massimo per impresa di € 300.000 all'anno. Nonostante gli esperti in Cyber Security siano considerati ad oggi tra i cinque professionisti più ambiti nell'ambito dell'Industria 4.0, non è chiaro se il Piano abbia previsto o includerà qualsiasi disposizione relativa allo sviluppo delle competenze specifiche nel campo della sicurezza informatica.

4. ANALISI

Questa sezione analizza le informazioni raccolte nella sezione 3 in relazione al contesto internazionale che è stato delineato nella sezione 2. Propone quindi due argomentazioni principali. In primo luogo, il mercato del lavoro italiano per la Cyber Security sembra affrontare le stesse problematiche che si stanno riscontrando in altri paesi tecnologicamente ed economicamente sviluppati. In particolare, le problematiche legate a una potenziale "trappola dell'esperienza professionale" e a un sistema educativo poco moderno rischiano di impedire che anche in Italia sia abbia un numero di professionisti adeguato. In secondo luogo, nonostante il CSSS sia stato citato in documenti ufficiali e non ufficiali, non è stata ancora definita una politica nazionale per la formazione delle competenze e dell'impiego nella Cyber Security. Nella misura in cui la sicurezza informatica italiana continuerà a non ricevere un sufficiente investimento economico dedicato e ad avere poca visibilità nell'agenda politica, l'approccio nazionale al CSSS continuerà ad essere in ritardo rispetto a a quello di altri stati. Alla luce di queste sfide, la sezione 5 propone una serie di raccomandazioni.

4.1 L'incidenza dello Shortage

Sebbene manchino ancora alcuni dati per avere un quadro completo sul CSSS, l'Italia si trova ad affrontare le stesse problematiche internazionali che impediscono un giusto equilibrio tra la curva di domanda e offerta in cyber security come in altri paesi. Inoltre, in linea con i risultati internazionali, i nuovi dati emersi e raccolti da questa ricerca suggeriscono che il CSSS italiano è un problema di natura complessa, multidimensionale e che richiede un'azione congiunta di tutte le parti interessate per la sua risoluzione.

Negli ultimi anni, la domanda di professionisti e dei salari ICT in Italia è notevolmente aumentata. Nella misura con cui il mercato della sicurezza informatica sta evolvendo, è probabile che anche la domanda di professionisti della sicurezza informatica sia cresciuta. Infatti, secondo l'Osservatorio 2017 per le competenze digitali, i professionisti della sicurezza informatica sono tra i professionisti più richiesti nell'attuale mercato del lavoro. Tuttavia, non ci sono delle statistiche ufficiali che ci permettano di concludere che la domanda in cyber security sia aumentata, e questo è un dato statistico importante che si dovrebbe ottenere per affrontare il problema in maniera adeguata.

Allo stesso modo, in Italia non abbiamo una quantificazione approssimativa a livello nazionale della portata del CSSS, come in Australia, Giappone, Scozia e Stati Uniti. Tuttavia nel 2017 l'Osservatorio sulle competenze digitali ha fornito una stima generale complessiva della domanda prevista per i professionisti del settore ICT nel periodo 2016-2018 rispetto a una potenziale offerta di candidati. Il rapporto conclude che la domanda è potenzialmente corrispondente all'offerta, ma i potenziali professionisti non avranno le competenze adeguate rispetto alle necessità dei datori di lavoro, che preferirebbero assumere laureati piuttosto che liceali, che secondo le stime dell'Osservatorio costituiscono la parte più cospicua dell'offerta di lavoro[32]. Sebbene questa quantificazione approssimativa del mercato del lavoro ICT complessivo in Italia sia un indicatore importante, si dovrebbe arrivare ad una quantificazione del problema specifica alla Cyber Security per cercare di ottenere la necessaria comprensione del problema al fine di poter porre in essere po-

[32] Il sondaggio ha infatti rilevato che circa il 60% delle organizzazioni preferisce una laurea (triennale e/o Magistrale) come requisito minimo per l'assunzione di un professionista della sicurezza informatica.

litiche opportune.

I risultati di questo rapporto confermano i risultati di altre ricerche e, come osservato in altri paesi, ci sono vari fattori che impediscono un corretto equilibrio tra l'offerta e la domanda nel mercato del lavoro italiano per la Cyber Security. La maggioranza degli intervistati ha riferito di avere sempre/spesso difficoltà, o persino non essere in grado di assumere personale per le proprie posizioni aperte, fino talvolta a non riuscire a colmare la posizione. Dallo studio emerge che a volte è difficile trovare anche un solo candidato con le giuste capacità e conoscenze. Più della metà delle organizzazioni ha mantenuto aperte le posizioni in cyber securityper almeno 61 giorni, un indicatore del fatto che i posti vacanti in materia di sicurezza informatica sono difficili da colmare.

Questi risultati sono in linea con ciò che avviene in altri paesi del mondo.
Come in Australia e negli Stati Uniti, anche il mercato del lavoro italiano per la Cyber Security sembra affrontare una "trappola dell'esperienza professionale", fenomeno che si verifica quando i datori di lavoro offrono posizioni che richiedono molti anni di esperienza professionale, senza però offrire opportunità di ingresso, impedendo così ai giovani laureati di svilupparsi professionalmente. Infatti, la maggior parte dei datori di lavoro chiede ai potenziali candidati tra 1-3 e 4-10 anni di esperienza professionale, nonostante trovare dei professionisti con tutti questi anni di esperienza professionale sia attualmente complesso. Solo una piccola percentuale di organizzazioni ha posizioni che non richiedono alcuna precedente esperienza professionale. Anche in Italia, quindi, i datori di lavoro sembrano avere aspettative non realistiche rispetto ai requisiti che i propri canditati hanno o dovrebbero avere. Se i datori di lavoro non abbasseranno le loro aspettative, probabilmente continueranno ad avere difficoltà nell'assumere personale in Cyber Security. Sebbene il Governo possa aiutare attraverso un intervento mirato la transizione scuola - lavoro, i datori di lavoro dovrebbero essere consapevoli che se quello che non riescono a trovare sono lavoratori specializzati e con molta esperienza professionale, la soluzione a questo problema non è rafforzare il sistema educativo.Se i datori di lavoro considerano l'esperienza professionale come l'unico requisito decisivo, devono essere consapevoli che, per definizione, l'acquisizione di vera esperienza professionale può avvenire solo sul posto di lavoro e non durante la formazione scolastica. Infine, a questo proposito, è interessante notare come gli intervistati hanno evidenziato una mancanza di competenze in Cyber Security non solo tra i professionisti di medio livello ma anche tra

i manager, dimostrando che la percezione e l'interpretazione dello shortage differisce notevolmente a seconda delle persone che vengono interpellate

La mancanza di esperienza professionale non è l'unico ostacolo che il mercato del lavoro della Cyber Security sta affrontando. Sebbene l'esperienza pratica sia al primo posto, le varie organizzazioni ammettono di non offrire stipendi e benefit in linea con il mercato del lavoro. Ciò è particolarmente rilevante all'interno di uno spazio economico come l'Ue, dove la libera circolazione dei lavoratori potrebbe indurre alcuni professionisti a lasciare il proprio paese per una posizione meglio retribuita in altri stati membri. Durante le interviste è stato più volte manifestata la difficoltà delle aziende italiane nel competere con aziende internazionali disposte ad offrire salari più elevati. Il fatto che le aziende italiane non siano propense a retribuire adeguatamente i possibili candidati potrebbe essere un riflesso della mancanza di cultura della sicurezza che sembra permeare l'economia italiana. Un'azienda potrà difficilmente offrire benefit e stipendi che possano indurre candidati a non accettare offerte economiche più cospicue all'estero fino a quando la Cyber Security non verrà considerata come un sottoinsieme del reparto IT o addirittura non alla stregua dei principali reparti operativi dell'organizzazione. Sebbene il governo possa intervenire per migliorare la consapevolezza della sicurezza, questo è qualcosa che i datori di lavoro dovrebbero capire autonomamente, cercando di comprendere il valore di mercato dei professionisti in cyber security e offrendo degli stipendi adeguati.

La capacità del sistema di istruzione e formazione di produrre un numero sufficiente di candidati con le giuste conoscenze e competenze è un altro aspetto giudicato come critico. I datori di lavoro sostengono che pochissimi candidati si propongono per le posizioni aperte e, spesso quest'ultimi non hanno le conoscenze, le abilità e le capacità per svolgere il lavoro richiesto. Secondo la maggior parte degli intervistati, anche una laurea pertinente, di solito in ingegneria, informatica o Cyber Security, non fornisce ancora le conoscenze e le competenze necessarie per ottenere un primo lavoro in Cyber Security. Un intervistato ha confermato che a suo parere uno dei principali problemi alla base della carenza è la mancanza di un'offerta educativa adeguata. Sebbene negli ultimi anni siano stati creati nuovi corsi di laurea e di formazione, l'attuale offerta è ancora scarsa ed eccessivamente focalizzata sulla teoria. Questo elemento con una consapevolezza diffusa a livello internazionale riguardante la necessità di modernizzare l'attuale offerta educativa in tema di Cyber Security.

4.2 Politiche nazionali di intervento

Nonostante l'argomento non sia stato dibattuto così ampiamente come in altri paesi, c'è stato un riconoscimento del problema in diversi rapporti ufficiali e non ufficiali. Tra i più importanti, il Dipartimento delle Informazioni per la Sicurezza (DIS) ha riconosciuto che l'Italia ha un "vasto problema" in relazione all'educazione in sicurezza informatica. Ciò nonostante, non c'è ancora stata una politica univoca per mitigare il problema.

Anche se ovviamente necessarie e qualificanti, le varie campagne di sensibilizzazione che sono state organizzate sembrano perlopiù iniziative sporadiche portate avanti dalle singole amministrazioni piuttosto che il frutto di una singola strategia nazionale coordinata. Nonostante siano chiaramente importanti per la loro natura e per la loro enfasi sull'educazione digitale, politiche pubbliche come il *Piano Nazionale Scuola Digitale e il Piano Nazionale Impresa 4.0.* non prevedono alcuna misura per la formazione o l'educazione in Cyber Security. Inoltre, non è chiaro se una politica come il Piano Impresa, che si pone come obbiettivo l'aumento delle iscrizioni di studenti presso gli Istituti Tecnici, sia adeguata ad affrontare una carenza che è almeno in parte dovuta al basso numero di studenti che si iscrivono e si laureano. A questo fine, una politica che mira ad aumentare il numero degli iscritti e dei laureati in materie affine alla cyber security potrebbe essere più appropriata per risolvere il CSSS.

Pertanto, non sorprende che il CINI abbia affermato nel suo Libro Bianco, dal titolo "Il futuro della sicurezza informatica in Italia" che gli attuali programmi sull'educazione alla sicurezza sono insufficienti. In questo contesto di potenziale urgenza, è singolare che i nuovi indirizzi operativi previsti nel nuovo Piano Nazionale pubblicato nel 2017 sulla "Promozione e diffusione della cultura della sicurezza. Formazione e istruzione" siano molto simili a quelli proposti nel 2013, in particolare se si tiene in considerazione del fatto che le politiche previste nel precedente Piano Nazionale non fossero così ben mirate come quelle sviluppate da altri pasi con problemi di CSSS simili.

Una comparazione diretta con lo sforzo economico posto in essere dal Regno Unito nel campo della politica di sicurezza cibernetica e la promozione della sua educazione purtroppo mette in risalto il basso impegno economico italiano nel settore (si veda la tabella 1 per una comparazione diretta dei di-

versi investimenti fra Italia e Regno Unito in sicurezza cibernetica). Il Regno Unito ha stanziato nella sua strategia per il periodo 2011-2016 un impegno economico complessivo di £32.8 milioni – degli £860 milioni di investimenti previsti nel budget totale per la Cyber Security[33]– per l'implementazione dei programmi educativi. Anche se il budget previsto per le attività educative nel nuovo ciclo strategico (2016-2021) non è noto,[34]vale la pena notare come il nuovo programma extra-curriculare Cyber Discovery, abbia un budget di £20 milioni, che costituisce già il 63% del budget totale che il Regno Unito ha speso per l'istruzione in sicurezza informatica nel precedente ciclo 2011-2016. Poiché molte iniziative dedicate al sistema educativo e alle competenze sono state confermate o ampliate con la nuova strategia 2016-2021, è probabile che il budget per l'educazione alla sicurezza informatica supererà di gran lunga quello già stanziato per l'implementazione delle politiche previste nella strategia precedente (2011-2016). D'altra parte, invece, non è ancora chiaro quanto l'Italia spenda complessivamente per la sicurezza informatica. Come per la Strategia del 2013, la nuova strategia del 2017 ha ribadito che la politica di sicurezza informatica non dovrebbe comportare costi aggiuntivi per l'amministrazione, il che significa che le amministrazioni dovranno fare affidamento sui loro attuali budget per attuare le politiche elencate nel nuovo piano d'azione.[35] Nel 2016, è stato riportato che il governo avesse stanziato 150 milioni di euro per rafforzare le attività del DIS e della Polizia di Stato. Nel 2018, il Governo ha creato un nuovo fondo per la difesa informatica, presumibilmente destinato al ministero della Difesa, per un totale di 3 milioni per il periodo 2019-2021,[36] comunque pochi rispetto alle somme stanziate dal governo britannico In sintesi, la mancanza di risorse finanziarie spiega parzialmente perché la risposta italiana al contrasto del fenomeno dello shortage sia stata fino a questo momento meno incisiva.

---

[33] Budget previsto dal Governo del Regno Unito nel 2011-2016

[34] L'attuale budget totale del Regno Unito per l'implementazione della strategia 2016-2021 è di 2,2 miliardi di euro. - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[35] "Dal presente decreto non derivano nuovi oneri a carico del bilancio dello Stato" (art. 13, "Disposizioni transitorie e finali", Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (Gazzetta Ufficiale n. 87 del 13 aprile 2017).

[36] https://alessandraermellino.it/in-bilancio-un-fondo-di-3-mln-per-la-cyber-security/.

ITALIA		REGNO UNITO
PIL (2018, NOMINALE) – IMF		
$2,086,911 mm		$2,808,899 mm
POPOLAZIONE (2017, UN)		
59,359,900 mm		66,181,585 mm
MEMBERSHIP ISTITUZIONI INTERNAZIONALI		
EU (Direttiva NIS adottata), NATO		EU[30] (Direttiva NIS adottata), NATO
MERCATO DELLA CYBER SECURITY[31]		
€896.5 mm[32]		£5.7 bn[33]
BUDGET PUBBLICO PER CYBER SECURITY		
€3 mm (2019 - 2021)		£1,9 bn (2016 - 2021)
BUDGET PER CYBER SECURITY EDUCATION E SKILLS		
-		£32.8 mm (2011 - 2016)

Tabella 3 : Italia-Regno Unito: comparazione sugli investimenti in sicurezza cibernetica

La politica italiana in materia di istruzione e competenze in sicurezza informatica è stata in gran parte circoscritta a iniziative di sensibilizzazione promosse dalle singole amministrazioni. L'approccio del Regno Unito, invece, è stato caratterizzato da riforme di sistema più ampie, a medio-lungo termine, abbinate a iniziative specifiche con l'obiettivo di ottenere risultati più rapidi. E' difficile ipotizzare se l'Italia avesse potuto realizzare sforzi più concreti per l'educazione alla Cyber Security nonostante l'assenza di stanziamenti economici. Quel che è certo è che l'inerzia nello sviluppo della politica cibernetica nazionale, come testimoniato dall'assenza di una significativa evoluzione degli indirizzi operativi dal Piano Nazionale del 2013 a quello del 2017, ha rallentato l'ideazione di misure che avrebbero potuto incoraggiare un decisivo cambio di passo nella protezione dello spazio cibernetico italiano.

[37] Dato relativo al 29 Marzo 2019.

[38] Poiché questi valori sono stati calcolati utilizzando probabilmente diverse metodologie, dovrebbero essere considerati per alimentare il dibattito

[39] Del 2017 Anitec-Assinform, 2018

[40] 2015/16 riferimento (RSM and CSIT, 2018)

5. LE RACCOMANDAZIONI PER MITIGARE IL FENOMENO IN ITALIA

Alla luce dei problemi evidenziati nella sezione 4, questo studio suggerisce le seguenti raccomandazioni:

• *Determinare la portata del CSSS conducendo un'analisi online delle posizioni vacanti nel mercato del lavoro della sicurezza cibernetica italiano*. Questo studio dovrebbe indicare: se le posizioni in Cyber Security stanno aumentando e se continueranno a farlo nel breve-medio periodo; il livello dei salari nel mercato del lavoro a seconda dell'esperienza professionale; una quantificazione approssimativa dello shortage a livello nazionale con l'utilizzo di una metodologia per la classificazione dei posti di lavoro sulla base di conoscenze, abilità anche specifiche come prestabilito ad esempio dal NICE Cybersecurity Workforce Framework o l'IISP Skills Framework. A questo proposito, si dovrebbe prendere in considerazione il progetto Cyberseek sponsorizzato dal NIST. Infine, ulteriori ricerche dovrebbero indagare il numero di studenti che si laureano in corsi di sicurezza informatica, sia nelle scuole superiori che all'università, per comprendere l'entità del disallineamento tra domanda e offerta in Cyber Security.

• *Raccogliere maggiori informazioni sulla natura del CSSS, mandando il questionario adoperato in questo rapporto a un campione più rappresentativo della popolazione dei datori di lavoro attivi nell'ambito della sicurezza cibernetica in Italia e conducendo ulteriori interviste.* In linea con l'obiettivo esplorativo di questo rapporto e a causa di limiti di tempo, l'indagine ha seguito una metodologia che non ha previsto la randomizzazione del campione che ha risposto al sondaggio. Ciò lascia aperta la possibilità che la popolazione intervistata non possa essere stata interamente rappresentativa del mercato del lavoro della sicurezza informatica. Anche se i risultati ottenuti sono stati significativi in quanto hanno fornito in maniere celere approfondimenti su un argomento poco indagato, l'ideazione e l'implementazione di nuove politiche per ridurre il fenomeno dovrebbero essere precedute da metodi di ricerca scientificamente più rigorosi. Infine, ulteriori interviste dovrebbero fornire un quadro più approfondito delle complesse dinamiche che stanno causando questa mancanza di competenze.

• *Creare un partenariato tra governo, industria e sistema educativo per ideare una soluzione nazionale al CSSS.* Le migliori sedi per avviare un dialogo su come indirizzare il fenomeno in modo olistico sono probabilmente il Tavolo Tecnico Cyber, che è l'entità che riunisce tutti i Ministeri con attività riguardanti la Cyber Security, per la sua posizione centrale all'interno dell'architettura istituzionale italiana per la sicurezza informatica e il Tavolo Tecnico Imprese, in cui siedono i rappresentanti dell'industria e i policymaker per discutere olisticamente delle sfide della sicurezza informatica.

• *Includere anche il Ministero dell'Istruzione, dell'Università e della Ricerca all'interno del Tavolo Tecnico Cyber* per garantire che siano correttamente definite le politiche educative nazionali in materia di sicurezza cibernetica;

• *Stanziare un fondo per lo sviluppo e l'implementazione della sicurezza cibernetica nazionale, che deve prevedere un finanziamento destinato esclusivamente all'educazione e allo sviluppo di competenze di sicurezza*. In assenza di un investimento economico serio, difficilmente i Ministeri potranno essere in grado di far fronte all'ulteriore onere amministrativo e operativo che comporterebbe l'implementazione di un'efficace politica in materia di istruzione e competenze in materia di Cyber Security.

• *Nominare una singola amministrazione responsabile per l'ideazione, l'implementazione, il monitoraggio e la valutazione delle politiche per la riduzione del CSSS*. Al momento, ci sono potenzialmente quattro diverse entità che potrebbero avere un ruolo diretto nella gestione del CSSS: il DIS, Dipartimento delle Informazioni per la Sicurezza, per il suo ruolo centrale e di coordinamento tra le Istituzioni italiane per la sicurezza informatica; il MISE, Ministero dello Sviluppo Economico, come principale interfaccia tra pubblico e privato; l'AGID, Agenzia per l'Italia Digitale, per il suo ruolo all'interno del settore pubblico italiano nella definizione degli standard di sicurezza e infine il MIUR, Ministero dell'istruzione, dell'università e della ricerca. Anche se ovviamente tutti questi attori dovranno necessariamente collaborare per mitigare il problema, una sola entità dovrebbe avere la responsabilità di questa specifica iniziativa, possibilmente con un ruolo chiaro e un budget preciso. Nel caso più entità avessero il compito di promuovere iniziative diverse fra loro, si correrebbe il rischio di frammentazione e quindi rendere le politiche o i vari programmi di intervento meno efficaci.

• *Trarre ispirazione dalle politiche adottate dal Regno Unito (tra cui la Scozia)*

come punto di partenza nella definizione delle politiche di mitigazione che potrebbero essere appropriate per risolvere il CSSS italiano. In questo momento, è difficile riuscire a consigliare delle politiche specifiche per mitigare la carenza di competenza in quanto si sa ancora poco sulla loro efficacia. Tuttavia, poiché è chiaro che alcuni paesi hanno maturato un'esperienza più lunga nel cercare di contrastare il fenomeno, l'Italia potrebbe prendere ispirazione da iniziative internazionali note, tenendo però in considerazione le differenze economiche, politiche e di politiche educative dei Paesi;

• *Dare priorità a politiche di intervento rivolte alla scuola primaria e secondaria, all'università e alla transizione scuola-lavoro*, distinguendo le politiche che dovrebbero aumentare il livello dei professionisti da quelle che invece dovrebbero accrescere la qualità delle loro conoscenze e abilità:

o *Transizione scuola-lavoro*: i datori di lavoro sembrano avere aspettative poco realistiche sulla disponibilità nel mercato del lavoro di professionisti in Cyber Security con diversi anni di esperienza professionale. Tuttavia, attualmente c'è una carenza di tali professionisti non solo in Italia, ma anche nell'attuale mercato globale del lavoro. Pertanto, maggiori sforzi dovrebbero essere intrapresi per assumere giovani laureati con una propensione a lavorare in Cyber Security e offrire loro una formazione rigorosa e personalizzata sul posto di lavoro. Come visto altrove, il Governo potrebbe facilitare questo offrendo una varietà di incentivi finanziari per incoraggiare i datori di lavoro ad offrire opportunità di "primo lavoro" come stage, tirocini, apprendistati e altri ruoli che non richiedono troppi anni di esperienza professionale. Tuttavia, i datori di lavoro dovrebbero anche essere consapevoli del fatto che, date le condizioni dell'attuale mercato del lavoro, è improbabile che potranno assumere e mantenere i talenti della sicurezza informatica a meno che non offrano salari e benefici a livello di mercato. A questo proposito, potrebbero giovare iniziative di sensibilizzazione rivolte volte ad aumentare la consapevolezza sui vantaggi nell'istituzione di adeguati controlli di sicurezza a livello aziendale e nell'offerta di e pacchetti finanziari congrui a quei specialisti che dovrebbero garantire la sicurezza dei sistemi e delle informazioni.

o *Alta formazione*: la mancanza di un'offerta formativa qualitativa

in materia di Cyber Security a livello di universitario in Italia sta ostacolando la creazione di una pipeline sostenibile di professionisti della sicurezza informatica. Il sistema universitario italiano ha reagito più lentamente alle richieste del mercato rispetto ad altri paesi. Sebbene in parte a causa della natura intrinseca del sistema, altri motivi includono l'assenza di docenti e l'alto tasso di abbandono degli studenti che si iscrivono a corsi di laurea che potrebbero essere rilevanti per la Cyber Security. Pertanto, si dovrebbe incentivare un'offerta formativa più ampia e più accessibile. Inoltre, al fine di avere una medesima comprensione di cosa veramente significhi avere le "giuste conoscenze e abilità", tutte le parti interessate potrebbero riunirsi per sviluppare un "curriculum nazionale" di Cyber Security - sulla base di standard internazionali consolidati come ad esempio il Cyber Security Body of Knowledge che l'Università di Bristol sta sviluppando – che dovrebbe essere preso in considerazione dai vari dipartimenti universitari che insegano o vorrebbero insegnare sicurezza. Questa iniziativa potrebbe trarre ispirazione dalle lauree certificate dal NCSC del Regno Unito. [41]

o *Scuola superiore*: alla luce del basso numero di studenti che accedono ai corsi universitari attinenti alla sicurezza informatica, è necessario incentivare più studenti a prendere in considerazione una carriera accademica e / o professionale in questo ambito. Sfortunatamente, non ci sono molti programmi a livello nazionale che possano attrarre studenti fin dalla giovane età. Tuttavia, iniziative di orientamento professionale nelle scuole superiori e competizione di sicurezza informatica potrebbero offrire delle soluzioni (De Zan, 2019). In Italia, CyberChallenge.IT attrae oltre 2000 studenti ogni anno, e se questa iniziativa continua ad aver successo, dovrebbe essere allargata, possibilmente con un investimento diretto del governo come già avviene in altri paesi. Infine ci sono importanti politiche quali il Piano Nazionale Scuola Digitale e il Piano Nazio-

[41] Per un'analisi complementare e più articolata su cosa dovrebbe essere fatto per rafforzare l'educazione alla sicurezza informatica a livello di istruzione superiore, incluso come aumentare il numero di professori e come addestrarli è possibile leggere il documento De Nicola R. and Prinetto P. (2018), Cyber security, l'urgenza di un piano speciale per la formazione superiore e la ricerca, Agenda Digitale, 2018

nale Impresa 4.0 che sono direttamente collegate alle competenze digitali. Queste politiche sono già definite ma non è chiaro se riguardino anche la Cyber Security e, a questo proposito, una possibile soluzione potrebbe essere includerla al loro interno piuttosto che ideare nuove politiche. A tale riguardo, potrebbero essere previsti incentivi per aumentare il numero di "insegnanti in materie ITC" attraverso opportunità di formazione specifiche. Infine si dovrebbero sviluppare campagne mirate ad incentivare le donne a intraprendere percorsi di formazione nella Cyber Security per favorire l'occupazione femminile nel settore.

• *Stabilire un insieme di metriche per la valutazione dell'efficacia delle politiche definite per il CSSS*. Fino ad oggi sono stati valutati in modo rigoroso solo pochi programmi governativi, al punto che non è ancora chiaro quanti studenti o professionisti, che sono stati soggetto delle politiche pubbliche mirate alla risoluzione del CSSS, siano poi stati inseriti nell'ambito della cyber security. Questo vale sia per i governi con politiche di CSSS complesse sia per i paesi con politiche meno complete. La valutazione delle politiche pubbliche è un esercizio complesso che richiede una combinazione di rigore scientifico, impegno finanziario e politico.[42] Se queste valutazioni scientifiche non vengono eseguite, ogni affermazione sull'efficacia di una politica (ad esempio "questa policy ha funzionato) risulta un'affermazione priva di fondamento. Pertanto, la valutazione delle politiche pubbliche dovrebbe essere inclusa in un circolo virtuoso all'interno del quale le lezioni apprese, che susseguono all'implementazione della politica pubblica, devono essere considerate nel processo di revisione delle politiche stesse. Se ciò non avvenisse, ci sarebbe il serio rischio che ogni iniziativa volta a ridurre il CSSS, possa essere tanto inefficace (se non addirittura generare conseguenze negative) quanto uno spreco di risorse pubbliche.

[42] Per una panoramica di ciò che comporta la valutazione delle politiche pubbliche, Magenta Book (HM Government, 2011)

Lista degli Acronomi

CINI	Consorzio Interuniversitario Nazionale per l'Informatica
CSSS	Cyber Security Skills Shortage
DIS	Dipartimento delle Informazioni per la Sicurezza
EU	Unione Europea
ICT	Information Communication Technology
MIUR	Ministero dell'istruzione, dell'università e della ricerca
NATO	North Atlantic Treaty Association
NCSC	National Cyber Security Center
NIS	Network Information Security
NICE	National Initiative for Cyber Security Education
NIST	National Institute of Standards and Technology
PNSD	Piano Nazionale Scuola Digitale
SMEs	Small and Medium Enterprises
U.K.	United Kingdom
U.S.	United States

Allegato I – Dichiarazioni ufficiali sullo Skill Shortage in Cyber Security delle 12 Nazioni

Country	Policy Document	Statement
Australia	Australia's cyber security strategy	"Like many other nations, Australia is suffering from a cyber security skills shortage" (2016).
Estonia	Cyber Security Strategy: 2008-2013 and Cyber Security Strategy: 2014-2017	While the 2008-2013 strategy stated that "there is a growing need for qualified mid-level information security experts in both the public and the private sectors" (2008), there is no direct mention to the lack or need of professionals in the last strategy, notwithstanding the fact that one of the objectives is "Ensuring the next generation cyber security professionals" (2014).
France	French national digital security strategy	"The content and number of initial training and higher education programmes for cybersecurity professions do not meet the needs of businesses and administrations" (2015).
Japan	Cyber Security Strategies	"Cybersecurity workforce development is a pressing task for Japan, as there is a critical domestic shortage of cybersecurity experts, both in quality and quantity" (2015). "Meanwhile, due to lack of expertise in cyber security, it may not be possible for enterprises to move forward […]" (2018).
South Korea	-	-

Country	Policy Document	Statement
Netherlands	National Cyber Security Agenda	"There is a growing demand from the business community and public authorities for innovative solutions to cybersecurity issues and well-trained personnel. This shortage on the labor market leads to scarce cybersecurity knowledge in organizations, which makes them insufficiently resilient to digital threats" (2018).
Norway	Cyber Security Strategy for Norway	"Our citizens, staff and executives in Norwegian companies must be security conscious and increase their information security" (2012).
Singapore	National Cyber Security Masterplan 2018 and Singapore's Cybersecurity Strategy	"The threat posed by increasingly sophisticated cyber-attacks is exacerbated by a shortage of highly skilled defenders. This shortage is not unique to Singapore. […] There is a pressing need to explore new initiatives to boost the numbers and skill levels of cyber security professionals, as well as to retain them in Singapore" (2013). "Today, there is a shortage of cybersecurity manpower around the world. […] To ensure that Singapore has an adequate and well-trained cybersecurity workforce…" (2016).

Country	Policy Document	Statement
Sweden	A national cyber security strategy	"Cyber security knowledge and resources possessed by various organizations, and not least by private individuals, are often limited." […] "The need for skilled personnel in the area of cyber security is also great. A lack of cutting-edge expertise affects both the private and public sectors" (2017).
Switzerland	National strategy for the protection of Switzerland against cyber risks (2012-2017) and (2018-2022)	"The lack of specialists and the acquisition and retention are a great challenge" (2012); "There is currently a lack of specific knowledge and specialists in the various fields relevant to cyber risks" (2017).
United Kingdom	National Cyber Security Strategy 2016-2021	"We lack the skills and knowledge to meet our cyber security needs across both the public and private sector. […] This skills gap represents a national vulnerability that must be resolved." "The UK requires more talented and qualified cyber security professionals" (2016).
United States	Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce	"The United States needs immediate and sustained improvements in its cybersecurity workforce situation" (2018).

Allegato II – Una prospettiva britannica sulla carenza di competenze in materia di Cyber Security e gli interventi di politica pubblica (aggiornati)

Questo allegato fornisce un'approfondita analisi del Cyber Security Skill Shortage nel Regno Unito e le politiche messe in atto per ridurlo, aggiornando l'allegato IV del rapporto sullo scenario internazionale "*Mind the Gap*". L'approccio del Regno Unito è stato scelto per diversi motivi: il CSSS è stato chiaramente identificato come un problema nella strategia nazionale di Cyber Security; il governo ha prodotto politiche trasversali rivolte a più settori, dalla scuola primaria alla forza lavoro; la politica è stata costantemente sostenuta e si è evoluta nel corso degli anni; sono state progettate e attuate iniziative politiche specifiche e chiaramente discernibili, al contrario del circoscrivere meri obiettivi politici; sono disponibili informazioni sulle spese di bilancio dedicato a questi programmi; esiste un'ampia disponibilità di dati online in grado di rafforzare i dati raccolti dai documenti delle policy in Cyber Security. Questo caso studio prima raccoglie i dati disponibili sull'incidenza del fenomeno della sua portata e della sua natura della carenza, in secondo luogo analizza le politiche che sono state progettate per mitigarlo.

La carenza di competenze in Cyber Security nel Regno Unito:
Il governo del Regno Unito ha chiaramente riconosciuto CSSS come una delle principali sfide nella sua strategia di sicurezza informatica 2016-2021: "*Ci mancano le competenze e le conoscenze per soddisfare le nostre esigenze di sicurezza informatica sia nel settore pubblico che in quello privato. [...] Questo gap di competenze rappresenta una vulnerabilità nazionale che deve essere risolta* "(HM Government, 2016).

Sebbene non esistano statistiche ufficiali sul CSSS inglese, ci sono molti dati forniti da organizzazioni che lavorano a stretto contatto con il governo che possono descrivere il fenomeno. Il Tech Partnership stima che nel 2015 tra il 2015 e il 2016 ci siano state quasi 7.000 posizioni in Cyber Security pubblicate con un aumento del 103% rispetto al livello dei precedenti cinque anni e una forza lavoro corrente di 58.000 specialisti. Lo stipendio medio tra il 2015 e il 2016 è stato di 57.100 sterline l'anno, in aumento del 7% rispetto all'anno precedente e del 15% in più rispetto ad altre posizioni specialistiche del set-

tore informatico (Tech Partnership, 2017).
Analogamente, un report della società di consulenza sulle assunzioni "Robert Walters" ha rilevato che gli specialisti in Cyber Security aumenteranno rispetto al 2017 del 7% nel successivo anno, molto più della crescita del 3% previsto per altre posizioni come sviluppatori e specialisti nelle infrastrutture (Bell, 2018). Secondo una recente analisi di RSM, i valori di retribuzione media vanno da 33.000 euro per i ruoli di laureato/junior, 52.000 euro per i ruoli senior, 70.000 euro per i ruoli dirigenziali, 92.000 euro per i ruoli apicali a 115.000 euro per i ruoli partner/chief executive, dato che " ribadisce un premio salariale maggiore rispetto ad altri all'interno del settore della Cyber Security ". Attraverso un sondaggio, la stessa analisi ha rilevato che il 90% degli intervistati, ritiene che vi sia uno shortage nel settore, evidenziando la mancanza di esperienza pratica dei laureati e la mancanza di programmi di formazione personalizzati (RSM e CSIT, 2018). L'Institute of Information Security Professionals (IISP) ha rilevato nel suo sondaggio sulla sicurezza 2017/2018 che la carenza è "più acuta" per ciò che concerne le competenze (18%) e le risorse (18%) piuttosto che l'esperienza (14%) o la mancanza di nuovi operatori (5 %). In uno studio governativo con 51 aziende tra piccole e medie imprese è stato rilevato che lo shortage in Cyber Security, tra le varie cause, sia dovuto dal basso numero di laureati nelle discipline STEM e dalla scarsa consapevolezza che la Cyber Security possa essere un'ottima opzione di carriera. Nell'osservare che i datori di lavoro valutano più l'esperienza che i titoli accademici, è stato riconosciuto che le imprese dovrebbero fare di più per fornire agli studenti un'esperienza pratica attraverso stage e apprendistati (HM Government, 2014).

Politiche per ridurre lo Shortage:
L'approccio del governo britannico per ridurre la carenza di competenze è stato delineato nelle sue due precedenti strategie di sicurezza informatica, ovvero "La Strategia di sicurezza informatica del Regno Unito 2011-2016: Proteggere e promuovere il Regno Unito in un mondo digitale", pubblicato a novembre 2011 e il suo ultimo aggiornamento, la "Strategia nazionale di sicurezza informatica 2016-2021", pubblicata a novembre 2016. Al termine della strategia 2011-2016, il programma nazionale di Cyber Security aveva stanziato 32,8 milioni di sterline (degli 860 milioni di investimento totale previsto per il paese) per programmi di istruzione e formazione delle competenze (HM Government, 2016). Il governo del Regno Unito ha ideato e implementato una politica globale rivolta a tutti e quattro le diverse categorie usate per la classificazione delle politiche internazionali in questa ricerca:

- **Istruzione primaria e secondaria**: Vi sono stati sforzi diretti a includere la Cyber Security nei corsi e negli esami di informatica (GCSE) e a forniture ulteriori di materiale didattico e di apprendimento per lo sviluppo professionale degli insegnanti. Inoltre, è stato istituito il uno specifico programma Cyber Security Challenge per le scuole e, dal 2012, 23.000 studenti hanno avuto accesso ai materiali didattici in materia (Cabinet Office, 2016). Con la nuova Strategia nazionale di sicurezza informatica (2017-2021), è stato creato un programma extra-curriculare con un budget di 20 milioni di sterline per accelerare e sviluppare l'educazione della Cyber Security per studenti dai 14 ai 18 anni. Il programma è iniziato nel 2018 e 23.663 studenti hanno preso parte alla prima fase, con 170 studenti invitati alla fase finale conclusasi nell'estate 2018 (DCMS, 2018a). Secondo il governo, quasi il 38% dei partecipanti al Cyber Discovery non aveva preso in considerazione una carriera in Cyber Security prima della partecipazione al programma, ma la percentuale è scesa all'8% dopo averne preso parte (Kelzi, 2018). Cyber Discovery sarà esteso a Irlanda del Nord e Scozia nel 2019 (DCMS, 2018a). Infine, il Regno Unito ha anche suggerito di integrare la Cyber Security e le competenze digitali all'interno del sistema educativo e progetta di promuovere l'accreditamento dello sviluppo professionale degli insegnanti in materia. (HM Government, 2016). Il NCSC ha avviato inoltre una competizione CyberFirst Girls per ragazze di età compresa tra 12 e 13 anni (Year 7 – 8 in Inghilterra e S2 in Scozia) al fine di ispirare la prossima generazione di giovani donne a prendere intraprendere una carriera nel campo della Cyber Security (NCSC, 2018a).

- **Istituti professionali e apprendistato**: Come prodotto della strategia 2011-2016, la Cyber Security sarebbe dovuta diventare da settembre 2016 una prerogativa per le qualifiche informatiche e digitali per l'istruzione superiore (livelli Regno unito 3 e 4); Sono stati avviati 300 apprendistati sulla sicurezza informatica di livello 4, inclusi 50 all'interno di uffici governativi (HM Government, 2016). La nuova strategia 2016-2021 ha istituito gli apprendistati "CNI" in Cyber Security (Livello 4), rivolti a giovani di età superiore a 16 anni e che non svolgono percorsi di istruzione a tempo pieno (part-time) (DCMS, 2018b). L'NCSC ha creato il proprio programma chiamato CyberFirst nel 2015: l'apprendistato di laurea CyberFirst è un apprendistato di tre anni con uno stipendio iniziale di £ 18.500 e l'assegnazione alla fine del programma di un titolo riconosciuto (NCSC, 2018b). Nel 2016, 20 studenti hanno seguito il programma ma il Regno Unito, secondo le dichiarazioni rilasciate, vorrebbe estenderlo a 1.000 studenti entro la fine del 2020 (HM Government, 2016).

- **Istruzione superiore e ricerca**: la Cyber Security è stata inclusa in tutti i corsi di informatica accreditati dalla British Computer Society e dall'Istituto di ingegneria e tecnologia. Dal 2014, 11 università in tutto il Regno Unito hanno ricevuto sovvenzioni di circa 93.000 euro dall'Accademia di istruzione superiore per migliorare l'insegnamento e l'apprendimento della sicurezza informatica (Higher Education Academy 2018ab). Il NCSC sponsorizza il CyberFirst Bursary, che consiste in una borsa di studio di 4.000 sterline e un'esperienza di lavoro retribuita (NCSC, 2018b) e ha accreditato 31 titoli di laurea e master in Cyber Security (riferimento novembre 2018). Inoltre la stessa Accademia sponsorizza, in collaborazione con UK Research and Innovation, centri di eccellenza accademici (ACE) nella ricerca sulla sicurezza informatica con l'obiettivo di migliorare la portata e la qualità della ricerca in Cyber Security. A novembre 2018, 17 università sono state riconosciute come ACE (EPRSC, 2018). Nel 2013 sono stati istituiti due dottorati in Cyber Security presso la Royal Holloway University e l'Università di Oxford, che genereranno almeno 150 dottori di ricerca entro il 2022. Sono stati creati 4 istituti di ricerca in Cyber Security: Research Institute in Automated Program Analysis and Verification, Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS) and the Research Institute in Secure Hardware and Embedded Systems (RISE). Infine, il Governo del Regno Unito continuerà a sostenere un'educazione in Cyber Security di qualità, colmando in itinere gli eventuali gap specialistici. (Governo HM, 2016).

- **Forza lavoro**: la prima strategia (2011-2016) ha istituito corsi di mentoring e sviluppo per studenti e laureati e creato un hub online ("Inspired Careers"), una piattaforma di gaming e materiale di e-learning per le professioni connesse a risorse umane, contabilità, settore legale e professioni di procurement (Cabinet Office, 2016). L'ultima strategia (2016-2021) ha creato il Cyber Security Skills Immediate Impact Fund, lanciato a febbraio 2018 come pilota, sponsorizza 7 diverse iniziative con l'obiettivo di aumentare rapidamente le dimensioni e la diversità della forza lavoro in Cyber Security nel Regno Unito (DCMS, 2018c). Un altro obiettivo principale della nuova strategia è stato quello di professionalizzare la sicurezza informatica raggiungendo lo status di Royal Chartered entro il 2020, un riconoscimento conferito dalla Regina stessa. Una consultazione aperta tra il governo e le parti interessate è stata chiusa nell'agosto 2018 (DCMS, 2018d).

Nonostante questi sforzi, il Joint Committee on the National Security Strategy, ha affermato nel luglio 2018 di essere "*Colpito dall'apparente mancanza di*

urgenza del governo nell'affrontare divario di competenze cyber di sicurezza in relazione alla Critical National Infrastructure (CNI)." In particolare, il Comitato ha rimarcato che la non-comprensione del fenomeno, che impatta le infrastrutture critiche (CNI) e settori affini, si debba considerare come una carenza di sicurezza e di posti di lavoro per la sicurezza nazionale. (Joint Committee on the National Security Strategy).

Nel mese di dicembre del 2018, il governo del Regno Unito ha pubblicato la Initial National Cyber Security Skills Strategy, che sarà utilizzata dal governo per raccogliere le migliori opinioni per approcciare in modo più efficiente il settore dell'istruzione e le competenze sulla sicurezza informatica, per poi pubblicare un documento strategico completo e definitivo nel 2019. La missione è "aumentare la capacità di cyber security in tutti i settori per garantire al Regno Unito abbia un giusto livello di personale e competenze necessarie per migliorare la postura e la sicurezza per le minacce informatiche auspicandosi di diventare la principale economia digitale del mondo". La strategia afferma che circa 710.000 aziende e 2.200 organizzazioni del settore pubblico hanno un divario tecnico di competenze tecniche di sicurezza informatica, numero che diventa 407.000 per le imprese e 3.300 organizzazioni del settore pubblico, quando si tratta di competenze tecniche di alto livello. Sebbene gli studenti del Regno Unito possano scegliere tra 121 corsi di istruzione superiore a tempo pieno, nell'a.a. 2016/17 erano presenti solo 6.000 studenti con un titolo in Cyber Security; d'altra parte, mentre 47.000 studenti erano iscritti a ulteriori titoli di studio, solo il 670 studiava specificamente la sicurezza informatica nel 2016/17. In generale, il nuovo documento conferma e amplia le politiche precedenti, pur riconoscendo l'importanza delle solide valutazioni e azioni intraprese fino ad oggi. Tra le nuove proposte più rilevanti, il governo del Regno Unito ha annunciato che pubblicherà un corpus completo di conoscenze sulla sicurezza informatica, nominerà degli ambasciatori dell'industria Cyber al fine promuovere le carriere in Cyber Security. Investirà tra il 1 milione di sterline e i 2,5 milioni di sterline per creare un nuovo UK Cyber Security Council per gettare le basi per la standardizzazione della professione (HM Government, 2018).

Riferimenti

Aica, Assinform, Assintel, Assinter (2017), *Osservatorio delle competenze digitali 2017: Scenari, gap, nuovi profili professionali e percorsi formativi*, https://www.agid.gov.it/sites/default/files/repository_files/osservatorio_competenze_digitali_2017.pdf;

Anitec-Assinform (2018), *Il Digitale in Italia 2018: Mercati, Dinamiche, Policy*, Confindustria Digitale, http://ildigitaleinitalia.it/kdocs/1920845/Il_digitale_in_Italia_2018.pdf;

Australian Cyber Security Growth Network (2017), *Cyber Security Sector Competitiveness Plan,* https://www.austcyber.com/wp-content/uploads/2017/04/Cyber-Security-SCP-April2017.pdf;

Bell L. (2018), *Cybersecurity experts to enjoy highest salary increase in 2018,* ITPRO, https://www.itpro.co.uk/business-strategy/careers-training/30433/cybersecurity-experts-to-enjoy-highest-salary-increase-in;

Bureau of Labor Statistics (2018), *Occupational Outlook Handbook: Information Security Analysts,* U.S. Department of Labor, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (visited December, 2018);

Burning Glass (2015), *Job Market Intelligence: Cybersecurity Jobs,* http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf;

Cabinet Office (2016), *The UK Cyber Security Strategy 2011-2016: Annual Report, London,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf;

Consorzio Interuniversitario Nazionale per l'Informatica (CINI) (2018), *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici, ISBN 9788894137330*, https://www.consorzio-cini.it/images/Libro-Bianco-2018-en.pdf;

Clusit (2018), *Rapporto Clusit 2018 sulla sicurezza ICT in Italia*, https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2018_aggiornamento_settembre.pdf;

Cyberseek (2019), *Cybersecurity Supply/Demand Heat Map,* https://www.cyberseek.org/heatmap.html, (visited March 2019);

Croci A. (2018), *Barometro Cybersecurity 2018: le aziende italiane sono pronte alla minaccia?* , Inno 3 SlowLetter, https://inno3.it/2018/10/31/barometro-cybersecurity-aziende-pronte-alla-minaccia/;

De Nicola R. and Prinetto P. (2019), *Cyber security, l'urgenza di un piano speciale per la formazione superiore e la ricerca, Agenda Digitale*, https://www.agendadigitale.eu/sicurezza/cyber-security-lurgenza-di-un-piano-speciale-per-la-formazione-superiore-e-la-ricerca/;

Department for Digital, Culture, Media & Sport (DCMS) (2018a), *Search to find Cyber Security experts of the future*, UK Government, https://www.gov.uk/government/news/search-to-find-cyber-security-experts-of-the-future;

Department for Digital, Culture, Media & Sport (2018b), *Cyber security CNI apprenticeships, UK Government,* https://www.gov.uk/guidance/cyber-security-cni-apprenticeships;

Department for Digital, Culture, Media & Sport (2018c), *Cyber Security Skills Immediate Impact Fund,* UK Government, https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund;

Department for Digital, Culture, Media & Sport (2018d), *Developing the UK cyber security profession,* UK Government, https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession;

De Zan T. (2019), *Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions,* Global Cyber Security Center, Rome, https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf;

Engineering and Physical Sciences Research Council (EPRSC) (2018), Academic Centres of Excellence in Cyber Security Research, UK Research and Innovation, https://epsrc.ukri.org/research/centres/acecybersecurity/;

Ermellino A. (2018), *In Bilancio un fondo di 3 mln per la cyber security,* https://alessandraermellino.it/in-bilancio-un-fondo-di-3-mln-per-la-cyber-security/;

Higher Education Academy (2018a), *Learning and teaching in cyber security 2014 -2016 Projects,* https://www.heacademy.ac.uk/knowledge-hub/learning-and-teaching-cyber-security-2014-2016-projects;

Higher Education Academy (2018b), *Learning and teaching in cyber security 2015 -2017 Projects,* https://www.heacademy.ac.uk/knowledge-hub/learning-and-teaching-cyber-security-2015-2017-projects;

HM Government (2014), *Cyber Security Skills: Business perspectives and Government's next steps,* Department for Business, Innovation and Skills, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf;

HM Government (2016), *National Cyber Security Strategy 2016-2021*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf;

HM Government (2018), *Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability*, A call for views, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767515/Cyber_security_skills_strategy_211218.pdf;

Information Security Policy Council (2013), *Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace*, provisional translation, https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf;

Joint Committee on the National Security Strategy (2018), *Cyber Security Skills and the UK's Critical National Infrastructure: Second Report of Session 2017–19*, HL Paper 172, HC 706, House of Lords and House of Commons, https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf;

Kaspersky (2016b), *The Cybersecurity Skills Gap: A Ticking Time Bomb,* https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf;

Ministero dello sviluppo Economico (2017), *Piano Impresa 4.0: risultati del 2017 – Azioni per il 2018,* Ministero dello Sviluppo Economico, Presidenza del Consiglio dei Ministri, Ministero dell'Economia e delle Finanze, https://www.mise.gov.it/images/stories/documenti/impresa_40_risultati_2017_azioni%202018_rev_eng.pdf;

Ministry of Economy, Trade and Industry (METI) – IT Jinzai report Summary – disponibile in lingua originale al sito: http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf;

National Cyber Resilience Leaders' Board (2018), *Safe, Secure and Prosperous: a Cyber Resilience Strategy for Scotland: Learning & Skills Action Plan for Cyber Resilience 2018-20*, Scottish Government, Edinburgh, ISBN: 978-1-78851-688-4, https://www.gov.scot/binaries/content/documents/govscot/publications/publication/2018/03/learning-skills-action-plan-cyber-resilience-2018-20/documents/00532325-pdf/00532325-pdf/govscot%3Adocument;

National Cyber Security Center (NCSC) (2018a), *Girls Competition,* UK Government, https://www.cyberfirst.ncsc.gov.uk/girlscompetition/;

National Cyber Security Center (2018b), CyberFirst Bursary and Degree Apprenticeship, UK Government, https://www.ncsc.gov.uk/articles/cyber-first-bursary-scheme;

National Cyber Security Center (2018c), *NCSC-certified degrees,* UK Government, https://www.ncsc.gov.uk/information/ncsc-certified-degrees;

Newhouse W., Keith S. Scribner B., Witte G. (2017), National Initiative for Cybersecurity Education (NICE) Workforce Framework, NIST Special Publication 800-181, National Institute of Standards and Technology, U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf;

Presidenza del Consiglio dei Ministri (2013), *The National Plan for Cyberspace Protection and ICT Security,* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf;

Presidenza del Consiglio dei Ministri (2017), *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica,* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf;

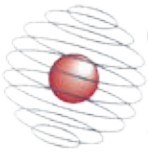
Presidenza del Consiglio dei Ministri (2018), *Allegato. Documento di sicurezza nazionale, Relazione sulla politica dell'informazione per la sicurezza,* Sistema di informazioni per la sicurezza della repubblica, http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf;

RSM and CSIT (2018), *UK Cyber Security Sectoral Analysis and Deep-Dive Review,* for the Department for Digital, Culture, Media and Sport, in conjunction with the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-__June_2018.pdf;

Tech Partnership (2017), *Factsheet: Cyber Security Specialists in the UK*, https://www.tpdegrees.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf;

The Secretary of Commerce (SoC) and Secretary of Homeland Security (SoHS) (2018), *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*, https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf;

GLOBAL
CYBER SECURITY
CENTER



CENTRE FOR
DOCTORAL TRAINING
in CYBER SECURITY

GCSEC - Global Cyber Security Center – Viale Europa, 175 00144 Rome, Italy – www.gcsec.org