ISPI DOSSIER 7 FEBBRAIO 2019

CYBERSECURITY IN ITALIA: IL NODO DELLA FORMAZIONE

Fabio Rugge (ISPI), Samuele Dominioni (ISPI)

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
7 Febbraio 2019

SICUREZZA CIBERNETICA IN ITALIA: IL NECESSARIO "BALZO" CULTURALE

Fabio Rugge
ISPI

Samuele Dominioni
ISPI

La rivoluzione digitale in corso ha già comportato un incremento esponenziale del consumo di prodotti tecnologici da parte di ampie fasce della popolazione che prima non ne usufruivano. Si tratta di un processo che ha luogo a livello nazionale come su scala globale. Tale diffusione ha avuto enorme impatto sulle modalità di produzione e, più in generale, sull'economia: si pensi alla rivoluzione dell'e-commerce, alla gestione digitale degli impianti industriali e della filiera produttiva, al "dato" in quanto nuova risorsa.

Oltre agli impatti economici della rivoluzione digitale, però, si è osservato anche un impatto socio-culturale. Secondo Luciano Floridi, professore di Filosofia ed Etica dell'Informazione all'Università di Oxford, siamo agli albori di una nuova era storica, definita "Iperstoria", nella quale il digitale è diventata parte essenziale dello sviluppo di una società. Floridi differenzia l'Iperstoria dalla Storia e dalla Preistoria non su basi temporali, quanto piuttosto sul "modo di vivere" di una società. In questo senso, vi sono oggi alcune società che vivono ancora nella fase storica, mentre altre si stanno affacciando in quella iperstorica (come l'Italia e le altre nazioni del G7), attestando come le tecnologie informatiche siano all'origine di una vera e propria rivoluzione culturale.

Le conseguenze dell'ingresso massiccio della tecnologia nella quotidianità di tutti noi ha comportato una netta trasformazione di come interagiamo con "l'altro", sia esso una persona fisica o un dispositivo elettronico (come avviene nell'Internet of Things). Tuttavia, la pervasività della tecnologia nelle nostre vite e nella nostra società non genera solo palesi benefici, ma anche la diffusione di nuovi rischi, che derivano in gran parte dalla natura intrinsecamente interconnessa del mondo cibernetico. In questo senso, la propagazione sistemica di un malware può avvenire non solo per comportamenti colposi, ma anche per incuranza e/o ignoranza, con potenziali pericoli

Counselor Fabio Rugge is Head of ISPI's Centre on Cybersecurity, in partnership with Leonardo

Samuele Dominioni is a Research Fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo

per il sistema Paese. Un esempio emblematico è il caso della compagnia di trasporto e logistica danese "Maersk" gravemente danneggiata da un attacco cibernetico nel 2017. Il fattore scatenante che ha permesso la propagazione dell'attacco è stato il comportamento doloso di un suo impiegato in un ufficio ucraino che ha risposto ad un'email infetta del malware "Not Petya". In pochi istanti le operazioni Maersk in 78 terminal in tutto il mondo si sono fermate e nonostante la rapida reazione, l'attacco cibernetico è costato alla compagnia almeno 300 milioni di dollari.

Condizione imprescindibile per poter operare in un contesto nuovo e interconnesso come quello cibernetico, proteggendo il sistema Paese dai rischi che caratterizzano questo dominio, è lo sviluppo non solo di solidi sistemi e procedure di difesa (per esempio per le infrastrutture critiche) e la messa in campo di capacità di reazione rapida (come il Computer Security Incident Response Team, CSIRT), ma anche – e forse primariamente – di una diffusa cultura della sicurezza cibernetica. Quest'ultima, sviluppatasi negli anni Settanta nella stretta cerchia degli esperti informatici e matematici, ha assunto – di pari passo con la diffusione tecnologica – sempre più connotazioni popolari e commerciali. Inoltre, la cultura della sicurezza cibernetica ha anche assunto diverse conformazioni in base alle diverse istanze politiche, strategiche ed ideologiche delle società iperstoriche e di quelle che lo stanno diventando. In ambito strategico sono stati individuati diversi paradigmi di cybersecurity per rispondere alle crescenti minacce provenienti dallo spazio cibernetico: il primo, quello della sicurezza nazionale (focalizzato sulla militarizzazione del quinto dominio); il secondo, quello economico (strutturato sugli attori privati e con un minimo coinvolgimento pubblico); il terzo, che annovera la sicurezza cibernetica tra gli obiettivi fondamentali dello Stato, al pari della sanità pubblica.

Il "modello di sanità pubblica", teorizzato dal Vicepresidente del dipartimento di Security policy della Microsoft, Scott Charney, per il dominio cibernetico, adotta concetti e procedure mutuate dai protocolli in uso per le malattie infettive, quali l'immunizzazione e la quarantena. Per sviluppare un approccio simile, però, è necessario un "balzo culturale" che coinvolga tutti gli utenti di un Paese, in quanto – così come accade per i vaccini – la sicurezza collettiva presuppone l'azione cooperativa di ogni singolo componente. Nel modello di Charney vi sono due attività chiave da promuovere: identificare i dispositivi infetti e garantire standard igienici. La prima azione implica una promozione della cultura della condivisione delle informazioni riguardo lo stato di salute di network e dispositivi. Ad esempio, nel caso un dispositivo sia infetto, l'utente dovrebbe notificarlo e pulirlo prima di accedere nuovamente alle reti informatiche. Per quanto riguarda la seconda attività, Charney ha immaginato un sistema di "certificati di salute" utili a garantire la buona condizione dei dispositivi. Entrambi gli elementi trovano, in questo costrutto, un riscontro nell'impostazione che l'Unione Europea sta promuovendo per la cybersecurity attraverso il GDPR (con l'obbligo di notifica alle autorità per casi di perdita di dati personali) e il prossimo Cybersecurity act (con il sistema di certificazioni per prodotti e servizi digitali).

Quanto fatto finora a livello legislativo, sia a livello nazionale che europeo, è sicuramente importante e lodevole. Tuttavia vi sono ulteriori sforzi da intraprendere per i quali è necessaria una presa di coscienza ampia e condivisa.

Il primo sforzo da compiere è individuale. Come insegna il caso Maersk, la sicurezza collettiva può essere messa a serio repentaglio da sconsiderati, dolosi comportamenti personali, con costi enormi per un'azienda e di conseguenza per il settore produttivo e, nei casi più gravi, di un intero sistema Paese. Pertanto, un significativo "cambio di passo", che equipari il modo in cui ci raffrontiamo ai temi

della sicurezza cibernetica alle basilari norme sociali quali ad esempio quelle che attengono alle più essenziali norme di igiene personale, aumenterebbe significativamente il livello di cybersecurity di un Paese. In questo senso, il legislatore non può che accompagnare – magari con politiche di informazione circa i rischi e di sensibilizzazione sulle necessarie precauzioni – un processo che è eminentemente culturale.

Il secondo sforzo riguarda l'adozione di politiche propositive e non soltanto "punitive" in ambito cibernetico per aumentare la competitività nazionale all'interno di in un mondo sempre più interconnesso e globale. In questo contesto, è necessario promuovere competenze informatiche e tecniche (come, ad esempio, iniziare a insegnare il coding nelle scuole dell'obbligo) necessarie a garantire lo sviluppo economico e la protezione del Paese. A tal fine, vista la scarsezza di risorse umane in tali ambiti, sarà gioco-forza promuovere politiche salariali adeguate e incentivi/vincoli a rimanere evitando così la "fuga di cervelli", specialmente dopo che si è investito in formazione. In sostanza, la capacità di un Paese di formare, diffondere e valorizzare avanzate capacità accademiche e di ricerca scientifica nei settori dell'informatica, oltre che di diffondere e promuovere una cultura della sicurezza cibernetica nuova, è di primaria importanza per la difesa del know-how sul quale poggia la nostra competitività nei mercati globali e per la resilienza complessiva del sistema Paese agli albori, appunto, dell'Iperstoria.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
7 Febbraio 2019

LA FORMAZIONE "DIGITALE" TRA CULTURA E TECNOLOGIA

Luca De Biase

Sole 24 Ore e Università di Pisa

La trasformazione tecnologica è sempre una sfida per la cultura di una popolazione che deve adattarsi a mutamenti quotidiani nell'organizzazione della vita, del lavoro, della produzione, del consumo. E del resto, a sua volta è il frutto di cambiamenti culturali, economici, sociali che rendono l'innovazione tecnologica necessaria e in qualche caso dirompente. In questa dinamica evolutiva, l'adattamento alla trasformazione di contesto e l'innovazione ulteriore sono fenomeni modellati dai sistemi formativi, che sono complessi insiemi di soluzioni per l'addestramento pratico, l'educazione specialistica e l'acculturazione per la socializzazione. Soluzioni che non sono soltanto formali, cioè sviluppate nei contesti dedicati alla formazione, ma che si offrono alla popolazione in molte altre occasioni informali, con effetti formativi che si dipanano tra pari, o grazie all'esperienza sul campo, o addirittura in una serie di momenti acculturanti che si incontrano nell'atto di lavorare, di consumare e di vivere con gli altri. Ogni cultura ha i suoi modi di interpretare tutto questo. Tipicamente, l'Italia trova soluzioni meno formali degli altri paesi, tende a programmare meno degli altri paesi, ha forme di reazione più veloci di quelle che si osservano in altri paesi e si trova in situazioni originali, difficilmente paragonabili a quelle degli altri paesi.

È chiaro che a giudicare dai numeri ufficiali, la situazione italiana è meno che ottimale. Le rilevazioni Desi, l'indice che misura la digitalizzazione dei paesi europei, mostrano che l'Italia resta nelle ultime posizioni. Questo potrebbe indicare che gli italiani non avvertono il bisogno di una modernizzazione digitale: ma non è così, come mostra il boom di investimenti in questo senso che si è verificato nel periodo in cui il governo ha portato avanti una policy di incentivazione all'insegna del piano "industria 4.0". Questo ha accentuato, se possibile, l'evidente disallineamento tra le professionalità richieste dalle imprese

Luca De Biase , Editor di "innovazione" a Il Sole 24 Ore e Nova24 (del quale è stato fondatore); editor della Vita Nòva, magazine per tablet. Docente del master Big Data all'università di Pisa.

e quelle disponibili. Secondo l'edizione 2018 dell'Osservatorio delle Competenze Digitali, la domanda di professionisti della tecnologia digitale è raddoppiata negli ultimi quattro anni e si stima che per il periodo 2018-2020 si creeranno quasi 90mila nuovi posti di lavoro nei settori della tecnologia dell'informazione e della comunicazione. La ricerca è concentrata peraltro in Lombardia, dove si sta formando quasi la metà di questi posti di lavoro. E in generale la domanda specialmente di laureati non trova l'offerta: il 58% dei laureati richiesti, semplicemente, non viene formato dalle università, anche se nell'ultimo anno sono aumentate le iscrizioni a ingegneria. I diplomati invece sono in eccesso e non ci sono abbastanza posti per loro. È chiaro che occorre un aggiustamento del sistema formativo. E non per nulla si parla di accentuare anche il ricorso agli Istituti Tecnici Superiori, per ora poco frequentati dai giovani italiani. In Germania i numeri di coloro che accedono a questo genere di formazione sono quasi cento volte più numerosi.

Certo, l'Italia è sempre difficile da paragonare agli altri paesi e soprattutto è sempre difficile da comprendere nel suo insieme, perché le varie aree del paese sono molto diverse tra loro, le generazioni si sono allontanate, le imprese che esportano si sono trasformate molto più velocemente di quelle che puntano tutto sul mercato nazionale. L'Emilia Romagna, per esempio, si dà soluzioni formative originali, come la nuova università per l'auto da corsa che è stata realizzata per accordo delle varie case automobilistiche della regione e delle quattro università. Inoltre, per esempio, a Parma, un gruppo di imprenditori si sta dando da fare per alimentare la voglia di frequentare corsi tecnici da parte dei giovani delle secondarie. Altrove l'iniziativa del tessuto connettivo sociale è meno sviluppata e la scarsa reattività della scuola pubblica si fa sentire di più. E in effetti lo dimostrano anche i successi delle forme di istruzione tecnica messe in atto da aziende che vendono tecnologia, come, tra le altre, Cisco, Microsoft o Google, che sono riuscite a generare decine di migliaia di nuovi professionisti del digitale con ottimi risultati anche in termini occupazionali.

Ma non è tutto qui. Perché se l'Italia ha quasi sempre trovato soluzioni "creative" ai suoi fabbisogni, oggi ha bisogno di un pensiero sempre più sofisticato sul piano dell'educazione. Il lavoro del futuro richiede capacità specialistiche di primo piano e contemporaneamente propensioni umanistiche spiccate per il lavoro di squadra interdisciplinare che la tecnologia attuale richiede; per lo spirito strategico che l'organizzazione delle imprese moderne abilita e domanda; per la curiosità resa necessaria dalla continua evoluzione delle tecnologie che sfidano ciascuno a prevenire la propria obsolescenza. Da questo punto di vista, paradossalmente, l'Italia non sarebbe messa male: la sua base culturale umanistica è certamente notevole. Ma deve imparare a non disperdere questo vantaggio nel tentativo di inseguire altri sistemi educativi. Ancora una volta il paese è costretto a cercare la sua strada originale. Ma deve coltivare una consapevolezza in più: non basteranno le soluzioni creative e informali, questa volta. Perché la grande chance economica si trova nella valorizzazione dei sistemi culturali di prossimità in un quadro di connessioni internazionali. Per questo occorre la conoscenza delle modalità standard di connessione che il mercato globale richiede. Insomma, c'è bisogno che la cultura locale non si perda nell'omogeneità della globalizzazione e nello stesso tempo che si sviluppi la sua connessione piena al resto del mondo. È questa la sfida e l'opportunità che l'Italia può cogliere.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
7 Febbraio 2019

PROGRAMMI DI FORMAZIONE IN CYBERSECURITY: INFORMATICA, MULTIDISCIPLINARITÀ E...FINANZIAMENTI

Rocco De Nicola
IMT

Paolo Prinetto
CINI

La formazione in cybersecurity viene oggi considerata un obiettivo nazionale negli Stati Uniti e in vari altri paesi, con implicazioni per la difesa nazionale e la sicurezza interna. A titolo di esempio, il National Center of Academic Excellence in Information Assurance/Cyber Defense statunitense svolge un ruolo governativo fondamentale nello sviluppo di standard per l'educazione alla sicurezza informatica e accompagna la definizione e la notevole crescita di corsi di cybersecurity in università, college e altre istituzioni.

La formazione in cybersecurity ha l'obiettivo di colmare, o almeno ridurre, la carenza di forza lavoro a livello planetario. Al fine di stimare il numero di posti di lavoro legati alla cybersecurity disponibili nei prossimi 5 anni, una compagnia statunitense specializzata ha analizzato, nel 2018, i dati sull'occupazione provenienti da media, analisti, fornitori, governi e organizzazioni a livello globale; da questi dati è emerso che ci saranno 3,5 milioni di posizioni di cybersecurity non occupate entro il 2021. Una simile analisi di un'altra azienda, nel 2016, aveva previsto uno "skill shortage" di 2 milioni per il 2019. Anche l'Italia soffre di questo skill shortage, che da noi è accentuato dalla presenza di pochi professori esperti della materia e dal fatto che spesso i nostri studenti trovano impiego oltre confine a condizioni molto migliori di quelle che vengono loro offerte in Italia.

Le figure professionali che servono sono molteplici e vanno dal laureato triennale con specifiche competenze di cybersecurity al dottore di ricerca che garantisce visione, anticipa i cambiamenti e contribuisce alla formazione di nuovi esperti. Occorrerebbe mettere a punto un piano specifico per definire, in modo coordinato con la parte pubblica, le aziende private e le università, le figure professionali formate tramite master, corsi di laurea, e corsi di dottorato, che servono al nostro paese per affrontare i problemi della cybersecurity. Partendo da questo piano, le singole università potranno:

Rocco De Nicola, ordinario di informatica alla Scuola di alta formazione di Lucca (IMT), è direttore del Centro regionale toscano per la cybersecurity, e responsabile formazione al CINI (Consorzio Interuniversitario Nazionale per l'Informatica)

Paolo Prinetto, direttore del CINI (Consorzio Interuniversitario Nazionale per l'informatica).

- ripensare i curricula dei corsi di base in informatica o ingegneria informatica, introducendo la dimensione della sicurezza fin dall'inizio del percorso di studi;
- attivare nuovi insegnamenti universitari su tematiche di cybersecurity da inserire nei curricula esistenti;
- attivare specifici corsi di laurea, soprattutto magistrali, per fornire le competenze e le metodologie atte a garantire una visione di sistema e necessarie per presidiare contesti eterogenei e in continuo cambiamento, tenendo conto di tutti i livelli di rischio;
- attivare corsi di dottorato per formare esperti e ricercatori in grado di capire gli sviluppi della ricerca nel settore della cybersecurity a livello internazionale, prevedere dinamiche di attacco e creare nuovi strumenti di difesa passiva e attiva;
- attivare master che puntino a formare esperti immediatamente operativi, avendo come target non solo neo-laureati, ma anche personale già in organico negli enti e nelle aziende, da sensibilizzare e riqualificare sulle tematiche di cybersecurity.

La definizione di questi nuovi programmi deve però tenere conto del basso numero di studenti che attualmente scelgono discipline scientifiche e tecnologiche e deve perciò essere accompagnata da campagne di informazione e di sensibilizzazione. Tali campagne dovranno essere finalizzate ad attrarre un numero maggiore di giovani, puntando a intercettarli quando non hanno ancora deciso una direzione definita su cui investire le proprie capacità, presentando loro le possibilità di carriera e gli aspetti stimolanti delle attività in cybersecurity. Questo dovrà essere perseguito attraverso il coinvolgimento degli studenti delle scuole superiori e la promozione della partecipazione femminile, sfatando il principio per cui la cybersecurity è un dominio per soli uomini. Particolarmente significativa, al riguardo, la "best practice" rappresentata, in Italia, dal progetto CyberChallenge.IT , mirata alla scoperta e alla valorizzazione dei giovani talenti in ambito cyber.

Va però detto che, al momento, il numero dei docenti e ricercatori di cybersecurity è così basso e distribuito sul territorio nazionale che le università e gli enti di ricerca hanno serie difficoltà ad attivare, in autonomia, programmi di ricerca o di didattica. Inoltre, a livello universitario, il rispetto del soddisfacimento dei requisiti minimi in termini di personale docente imposto dalla normativa vigente fa sì che, in varie sedi, l'attivazione di nuovi corsi di laurea di cybersecurity o di dottorato implicherebbe la chiusura di alcuni dei corsi già esistenti e quindi incontra ovvie resistenze all'interno della governance degli atenei.

Per ovviare a questi problemi, il ministero dell'Istruzione, Università e Ricerca, seguendo l'esempio dei paesi più avanzati, dovrà definire un piano speciale che, partendo dall'attuale situazione di emergenza, preveda l'assegnazione di risorse specifiche, distribuite sul territorio nazionale, in termini di docenti, ricercatori, e finanziamenti di progetti di ricerca per lo sviluppo della formazione superiore e della ricerca in cybersecurity. Questo strumento è indispensabile sia per evitare che nostri ricercatori vadano in Paesi dove la loro professionalità viene meglio riconosciuta e remunerata, sia per incoraggiare il rientro o la venuta dall'estero di ricercatori altamente qualificati. Si auspica che, come avvenuto nel passato per altre aree, come la chimica negli anni Sessanta, venga avviato in Italia un piano straordinario per l'assunzione di ricercatori e professori universitari che si occupano di cybersecurity e, in generale, di trasformazione digitale in tutte le sue componenti: giuridiche, economiche e soprattutto tecnologiche. Solamente una significativa azione straordinaria può aumentare la velocità di creazione della forza lavoro necessaria per difendere il paese, le aziende, i cittadini

da attacchi che diventano sempre più sofisticati e pericolosi.

Per riflettere e avanzare proposte relative alla formazione in cybersecurity, il Laboratorio Nazionale di Cybersecurity del CINI, il Consorzio Interuniversitario Nazionale di Informatica che raggruppa quasi 50 università statali, ha istituito un gruppo di lavoro sulla formazione in cybersecurity che punta a stimolare l'apertura di nuovi corsi di studio a livello di Master, di Lauree Magistrali e di Dottorato di Ricerca, favorendo lo scambio di informazioni tra le varie sedi universitarie su programmi didattici e tecnologie e il coordinamento e la pubblicizzazione delle attività formative in ambito cybersecurity.

Sul sito del laboratorio sono disponibili informazioni e link sulle diverse attività. Si sottolinea inoltre come negli ultimi due anni siano state attivate tre nuovi corsi di laurea magistrale in cybersecurity, aggiungendosi all'unico prima esistente, e come al momento siano allo studio nuove aperture. Per facilitare queste iniziative il laboratorio di Cybersecurity del CINI sta anche lavorando a una proposta di ridefinizione delle specifiche ministeriali per l'accesso a lauree di questo tipo, al fine di permettere l'accesso non solo a informatici o ingegneri informatici, ma anche ad altri ingegneri e a matematici, fisici, economisti e giuristi. La cybersecurity infatti oramai riguarda tantissimi settori della società e per difendere al meglio i sistemi servono competenze sempre più trasversali.

Investire nella formazione e nell'addestramento in cybersecurity fornisce, infine, una risposta unica a molteplici problemi del sistema Paese e si rende indispensabile nell'ambito della progressiva digitalizzazione promossa dal piano Impresa 4.0. Formare le nuove generazioni innescherà un processo virtuoso in cui la classe dirigente e i tecnici del futuro avranno le competenze, il bagaglio culturale e le capacità operative necessarie per confrontarsi con le sfide tecnologiche e scientifiche che cambieranno le nostre vite nei prossimi decenni, mettendo in atto le necessarie iniziative per adattarsi ai continui cambiamenti e ai rischi che ci aspettano in futuro.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
7 February 2019

POLITICHE AZIENDALI DI CYBERSICUREZZA: LA "CYBER HIGIENE"

Luciano Hinna

Universitas Mercatorum di Roma "Tor Vergata"

La parola rischio è nel vocabolario di tutti, ma a giudicare dai comportamenti delle aziende, è ancora nelle conoscenze specifiche di pochi: il rischio, nella sua concezione negativa, è la combinazione tra la probabilità che un evento si verifichi ed i suoi possibili impatti negativi; provare a gestirlo significa agire per diminuire le probabilità, attenuare eventualmente i danni o agire su entrambi i fronti. Se questo è vero per il rischio in genere, lo è ancora di più per il rischio cibernetico.

Prima della metà del Seicento il rischio come grandezza gestibile non esisteva, ma esisteva solo il fato o il Dio avverso e c'era una rassegnazione passiva al destino: non si conosceva ancora il calcolo delle probabilità che è quello che ha consentito di gestire il rischio.

Oggi il rischio sarebbe gestibile, ma in realtà, come nel caso del rischio cibernetico, non lo è perché prima di gestirlo bisognerebbe averne la percezione. Per questo ci si rassegna ai cigni neri: quegli eventi rari che però quando si verificano sono devastanti; in realtà i cigni neri sono solo cigni bianchi come tutti gli altri, che però non riusciamo a vedere in anticipo e che sono il frutto della nostra ignoranza che è, a sua volta, la combinazione di due elementi: scenari in rapido mutamento e carenza di formazione per gestire l'incertezza.

Attraversare una piazza e attraversare una palude non è la stessa cosa: le due cose richiedono approcci diversi e quindi le politiche aziendali dovrebbero prevedere, prima ancora che l'adozione di strumenti tecnici per gestire il rischio cibernetico, l'adozione di strumenti culturali ovvero corsi di formazione/sensibilizzazione sulla gestione del rischio in generale, su quello cibernetico i particolare e, infine, sulla gestione dell'incertezza. Va sviluppata la cultura della palude: non siamo abituati a muoverci con padronanza in una palude dove non valgono le regole certe, le evidenze, le misure definite di ciò

Luciano Hinna, insegna al Master si intelligence economica, da lui creato nel 2012, al Master anticorruzione, e al Master in e-procurement presso l'Università di Roma "Tor Vergata"

che si incontra, di dove si mettono i piedi. Ci vogliono tecniche e capacità diverse, meno legate agli automatismi, alla linearità, alla convinzione che tutto sia riducibile a schemi fissi e prevedibili, altrimenti non si colgono i cambiamenti di scenari che invece ci sono e sono forti.

Infatti, quando si è dentro un cambiamento, o si è parte del cambiamento, come accade spesso alla imprese, non ci si rende conto perfettamente di che cosa sta accadendo; è solo la storia che ci farà poi mettere a fuoco ciò che è accaduto, ma ovviamente a qual punto è troppo tardi per intervenire. Va interpretato il presente prima che diventi storia e cronaca negative; la sicurezza informatica vive oggi questo disagio.

I crimini informatici non potevano esistere se non si fosse realizzata una delle più grandi trasformazioni di scenario della storia: la dematerializzazione. Il telefonino che teniamo in tasca conta tra i 60 e i 100 Giga di memoria e un giga rappresenta un metro cubo di carta stampata in A4 che pesa una tonnellata, che si può rubare o trasferire da una parte all'altra del mondo con un semplice click e si può distrugge con un solo tasto del computer. Quanto tempo doveva bruciare la storica biblioteca di Alessandria prima di andare totalmente distrutta? Questo ci fa comprendere che cosa significhi il cambiamento di scenario tecnologico.

L'elemento da considerare tuttavia non è solo il cambiamento, ma anche l'arco temporale in cui questo cambiamento si è realizzato: un arco temporale ridottissimo. Pensiamo a che cosa è successo con internet che è passata da 0 (1992) a 50 milioni di utenti in soli 4 anni, quando per avere lo stesso numero di utenti la radio ha impiegato 38 anni, la televisione 13 anni ed il telefono ha impiegato 50 anni. Gli utenti Internet erano 3 miliardi nel 2015 e saranno 4 miliardi nel 2019 mentre gli apparati connessi ad internet saranno tre volte e mezza la popolazione della terra. Un'accelerazione di cui non ci rendiamo sempre pienamente conto e che costituisce il liquido amniotico in cui cresce e prospera anche il crimine informatico.

Il secondo elemento con il quale dobbiamo fare i conti è, come accennato, la percezione del rischio ed in particolare del rischio informatico. "Non è mai successo nulla...", "se deve capitare, capita..." sono espressioni di uso comune che tradiscono una impostazione errata della certezza e dell'incertezza. Sottovalutare un fenomeno come un attacco informatico per il semplice fatto che non è mai successo prima è stupido: significa affermare che siamo tutti immortali solo perché nel recente passato nessuno è mai morto prima. I cimiteri sono pieni di persone già morte come sono tanti i casi di attacchi informatici conosciuti ed altri sconosciuti dei quali, magari, siamo stati vittime inconsapevoli. Rassegnarsi al fatalismo – quando una cosa deve succedere succede – significa invece fare un salto indietro di oltre quattrocento anni nell'evoluzione della intelligenza umana, quando si rinunciava a gestire il rischio, ma si subiva il fato e si pregava e si sperava. Può essere questo l'approccio legato al rischio cibernetico? Certamente no. Ma vale la pena chiedersi perché la percezione del rischio è ancora così bassa. Perché la nostra formazione ci ha abituati a gestire la certezza e non siamo abituati a gestire l'incertezza che è invece l'unica cosa certa che esiste. Negare l'incertezza è il frutto di un processo errato di semplificazione: tutti figli di Cartesio affrontiamo un problema complesso spacchettandolo in tanti problemi più semplici, ne affrontiamo uno per volta e facciamo finta che gli altri problemi non esistono o che rimangono statici; in realtà essi sono tutti presenti, sono tutti insieme e mentre ne analizziamo uno gli altri evolvono ancora.

Per affrontare la complessità, inclusa la "cyber-complessità" è necessaria una formazione diversa da quella che abbiamo seguito per anni.

La conclusione è semplice: la sicurezza cibernetica è un problema molto serio, una leggerezza nella sicurezza in-

formatica, un hacker che buca il sistema fa sparire dal mercato un'azienda con la stessa velocità con cui cancelliamo un giga di informazioni, ma se non esiste la percezione del rischio non si può pensare di gestirlo. Non possiamo continuare a coltivare la certezza che è frutto dell'arroganza dell'ignorante ed è l'errore più comune che si possa commettere: ci fa sentire tranquilli nel breve periodo e ci porta a dare eccessiva fiducia ai sistemi di difesa anche se sappiamo che passano velocemente di moda.

E' incoscienza? E' eccessivo orientamento all'azzardo? Forse entrambi, ma non vi è dubbio che serve una dose massiccia di formazione manageriale, prima ancora che tecnica, che faccia sorgere la consapevolezza – l'ignoranza scientifica – della necessità di gestire i rischi strategici che possono mettere in forse la continuità aziendale: quello cyber è uno di questi.

La formazione pertanto diventa una forma di "igiene" intesa come l'insieme dei provvedimenti per la prevenzione di certi rischi specifici.

In questo contesto, i privati e le piccole e medie aziende sono i soggetti più esposti al rischio proprio perché sono quelle categorie con meno cultura manageriale. Secondo l'EY Global Information Security Survey 2018-19 il 65% delle aziende italiane ha registrato almeno un incidente significativo ed il 77% delle imprese italiane non dispone ancora di risorse al livello di sicurezza richiesto. Forse servirebbero vaccinazioni culturali di massa a partire dalle scuole per finire alle università ed al mondo delle aziende sia pubbliche che private.

In estrema sintesi: essere nel cyber spazio non è come stare in una piazza, si deve acquisire la cultura di palude, dove valgono i segnali deboli, dove a fare la differenza sono le sfumature, le sensazioni a pelle, persino le sintesi emozionali. La guardia deve essere alta e crescente perché ci troviamo di fronte ad un rischio che aumenta continuamente e cambia come cambiano gli scenari tecnologici e sociali e, di conseguenza, le forme e la struttura della minaccia.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
7 Febbraio 2019

CYBERDEFENDERS: TALENTI DA SCOPRIRE, PERFEZIONARE E TRATTENERE

Agnese Sollero

NATO

Dopo gli straordinari benefici che la rivoluzione cibernetica ha portato alle nostre società, si sta schiudendo sotto i nostri occhi il suo lato più problematico, che, in un intreccio di rischi e minacce, insidia la nostra privacy, la prosperità dell'economica, nonché la solidità delle strutture di governo e delle democrazie occidentali. Cybersecurity e cyberdefence sono ormai diventate espressioni del linguaggio comune, a testimonianza di una raggiunta consapevolezza della necessità di una corretta gestione dei fattori di rischio del mondo cibernetico. I governi nazionali e le organizzazioni internazionali da tempo sono impegnati nella ricerca delle modalità più appropriate per proteggere dati, imprese, e reti, in un crescendo di investimenti per la sicurezza e la difesa in ambito cyber. Il comparto è in continua espansione, e sembra che la domanda di personale specializzato in grado di occuparsi di queste tematiche non sia accompagnata da un'adeguata offerta di talenti. Si pensi ad esempio che secondo alcune stime, nel settore della cybersecurity, nel 2020 ci saranno 1,5 milioni di posti di lavoro non occupati.1 La partita della difesa in ambito cyber, dunque, sembra giocarsi anche sul piano delle risorse umane e sulla capacità di governi e organizzazioni internazionali di assicurarsi i migliori talenti nelle proprie linee di difesa.

L'ambito della cyberdefence è per sua natura un settore di nicchia che impiega personale altamente specializzato. Tuttavia, possiede allo stesso tempo le caratteristiche di un ambito multisciplinare, che richiede l'interazione e la collaborazione di professionisti di diversi settori. Le "prime linee di difesa" nel mondo cibernetico sono costituite da programmatori, ingegneri e tecnici del settore IT che operano a livello tecnico e operativo. Questi non solo sono impiegati a prevenire possibili attacchi e a rintracciare le vulnerabilità che potrebbero essere sfruttate da eventuali aggressori, ma si trovano in prima linea nella risposta a eventuali incidenti, e in alcuni casi potrebbero

Agnese Sollero, Ananlista, Emerging Security Challenges, NATO.

* Il contenuto di questo articolo riporta le opinioni personali dell'autore, e non riflette le opinioni ufficiali della NATO.

essere impiegati in azioni offensive. Accanto a questi operatori, si può rintracciare un pool di esperti e analisti che hanno il compito di informare la riflessione strategica e il processo decisionale, associando il dato tecnico al dato politico, ed eventualmente alle informazioni fornite dal comparto dell'intelligence. L'apporto di queste diverse professionalità confluisce all'interno della medesima struttura, al fine di produrre una risposta multidisciplinare, multilivello e coerente alle minacce o alle possibili crisi in ambito cibernetico.

Molto spesso, infatti, questi individui sono chiamati a operare in situazioni di crisi. L'abilità di operare sotto pressione e di gestire in maniera efficace problematiche delicate sono componenti fondamentali nel profilo di un cyberdefender. Tali capacità sono continuamente testate e perfezionate durante il percorso professionale grazie a esercitazioni, nazionali e internazionali, di gestione della crisi. Si pensi ad esempio, a Cyber Coalition,2 un'esercitazione in ambito NATO che mira a testare la cooperazione tra la NATO e gli Alleati nel fronteggiare la minaccia cibernetica, oppure a Locked Shields[3], un'esercitazione internazionale che vede diversi team nazionali impegnati nella simulazione della difesa di network nazionali e infrastrutture critiche.

Facendo ora un passo indietro, come avviene la selezione dei cyberdefenders? In particolare, in che modo i governi rintracciano e selezionano i migliori talenti da inserire nelle proprie linee di difesa? Per quanto concerne i profili più tecnici, ovvero quegli specialisti del settore IT che sono impiegati a livello operativo, molti Paesi hanno scelto di giocare d'anticipo e si sono adoperati per individuare le migliori menti da inserire nell'ambito della cyberdefence tra gli universitari e gli studenti della scuole superiori. Esistono diverse competizioni a livello nazionale finalizzate a vedere all'opera i talenti in erba in ambito cyber, così da individuare gli studenti più promettenti, poterli indirizzare verso un percorso di formazione ed eventualmente inserirli in ambito istituzionale come veri e propri cyberdefenders. In Italia, ad esempio, il programma Cyber Challenges propone di creare la nuova generazione di cyberdefenders tra i programmatori in erba delle scuole superiori e delle università italiane. Il programma non vuole essere esclusivamente una sfida e un'opportunità di formazione per i giovani talenti, ma si presenta anche come un'opportunità per le istituzioni per setacciare le giovani risorse e poterle convogliare nella difesa del Paese.[4] Guardando altrove, l'Estonia, all'avanguardia per molti aspetti relativi alla cyberdefence, ha fatto una scelta ancora diversa con la costituzione della cosiddetta Estonian Cyber Defence League. Questa entità è costituita da volontari e si propone di agire in supporto alle istituzioni nazionali nella gestione di possibili crisi. La Estonian Cyber Defence League si presenta come un modello innovativo nel settore poiché va a reclutare direttamente nell'ambito civile dei professionisti altamente qualificati, con competenze in materia IT, legale o in materia di sicurezza, per prepararli a contribuire alla cyberdefence nazionale.[5]

La ricerca del personale adeguato per costituire le proprie linee di difesa in ambito cyber sembra essere une delle sfide che governi e organizzazioni stanno già giocando. Per vincere tale sfida è necessario mobilitare risorse crescenti per individuare, attrarre e formare i nuovi cyberdefenders, nonché formulare una strategia mirata ed efficace per setacciare e riconoscere i nuovi talenti in ambito cyber, con una particolare attenzione verso le nuove generazioni. Sarà una sfida da giocare sul lungo termine, che richiederà una pianificazione strategica, associata alla capacità di formare addetti in grado di adattarsi a minacce in continua evoluzione e di rispondere in maniera multidisciplinare a possibili crisi. Inoltre, le istituzioni, dopo aver inserito i nuovi cyberdefenders nelle proprie linee di difesa, dovranno impegnarsi a trattenere questi talenti, offrendo

una prospettiva professionale che possa competere con le opportunità di carriera nel settore privato. In un quadro che vede una crescente richiesta di professionisti nell'ambito della cybersecurity, trattenere le eccellenze nella strutture nazionali sarà quanto mai fondamentale.

---

1. Harvard Business Review, Cybersecurity Has a Serious Talent Shortage. Here's How

2. NATO, Cyber Coalition helps prepare NATO for today's threats

3. NATO CCDCOE, The Largest International Live-Fire Cyber Defence Exercise in the World to be Launched Next Week

4. Cyber Challenge, https://www.cyberchallenge.it/

5. NATO CCDCOE, The Cyber Defence Unit of the Estonian Defence League – Legal, Political and Organizational Analysis(PDF)

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
7 Febbraio 2019

L'ITALIA NELLE ESERCITAZIONI DI CYBER DEFENCE INTERNAZIONALI

Francesco Vestito

Comando Interforze per le Operazioni Cibernetiche

Il costante progresso tecnologico che caratterizza la nostra era digitale ha da tempo raggiunto un elevato grado di pervasività, chiaramente percepibile da qualsiasi individuo che vive all'interno delle cosiddette nazioni industrializzate e che utilizza, quotidianamente, servizi e strumenti di Information Communication Technology (ICT), tra di loro connessi nel più vasto contesto dell'Internet of Things.

I vantaggi derivanti da questa capillare diffusione tecnologia recano, però, con sé una serie di sfide che le nazioni si trovano ad affrontare. Concetti quali cyber defence e cyber resilience scandiscono oramai le agende dei vari governi internazionali che, al fine di mitigare i rischi derivanti dall'inevitabile esposizione alle minacce cibernetiche (cyber threats) sponsorizzano, con sempre maggior frequenza, iniziative tese a verificare l'efficacia del proprio apparato di difesa cibernetica.

L'Italia segue da tempo questo trend, attraverso la partecipazione a esercitazioni internazionali sia in campo civile che militare.

Nel primo caso l'esercitazione biennale Cyber Europe 2018, importante evento europeo a tema cyber pianificato e condotto dalla European Network and Information Security Agency (ENISA) ha visto, nell'ultima edizione del 2018, la partecipazione nazionale del costituendo Computer Security Incident response Team (CSIRT) - unione di CERT-Nazionale e CERT-PA - operare in stretta sinergia con il Comando Interforze per le Operazioni Cibernetiche (CIOC) dello Stato Maggiore della Difesa, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche della Polizia di Stato e la rete europea dei CSIRT nella gestione e mitigazione di un attacco informatico su vasta scala mirato alle infrastrutture di controllo del traffico aereo.

Francesco Vestito brigadiere generale ITAF, Cyber Commander del Comando Interforze er le Operazioni Cibernetiche (CIOC) in Italia.

Ma è il secondo caso, ovvero la partecipazione della Difesa a esercitazioni con forte connotazione cyber, che esprime, per via di una naturale affinità a tematiche di protezione nazionale e supporto agli altri dicasteri, il maggior numero di iniziative sotto la competenza del CIOC dello Stato Maggiore della Difesa.

In campo NATO, l'Italia è stata una delle prime nazioni a partecipare all'esercitazione Cyber Coalition, giunta, nel 2018, alla sua undicesima edizione e che ha visto la partecipazione di 700 cyberdefenders provenienti da 28 nazioni dell'Alleanza e 5 nazioni/organizzazioni partner che hanno esercitato consolidate procedure internazionali di collaborazione tecnica, sotto il coordinamento dell'Allied Command Trasformation della NATO, al fine di proteggere e difendere il "Cyberspazio dell'Alleanza" nonché condurre operazioni militari all'interno e attraverso di esso.

Un'ulteriore occasione di verifica delle competenze nazionali in campo cyber defence scaturisce dalla stretta collaborazione con il NATO Cooperative Cyber Defence Centre of Excellence di Tallinn, in Estonia, che l'Italia supporta in qualità di Sponsoring Nation. Infatti il Centro di Eccellenza di Tallin, vero e priorio think tank internazionale, organizza, ogni anno, due esercitazioni: la Crossed Swords, evento riservato a personale tecnico dei Red Team e la Locked Shields.

La Locked Shields, in particolare, è la flagship exercise del Centro ed è la più complessa esercitazione live-fire (ovvero attacco-difesa in tempo reale) al mondo; infatti, l'edizione del 2018 ha impegnato i Blue Team di circa 30 nazioni partecipanti nella difesa di sistemi virtuali complessi - come centrali elettriche, reti 4G, sistemi di pilotaggio droni, sistemi di comunicazione - da oltre 2500 attacchi di varia natura.

Non mancano poi iniziative delle singole nazioni che offrono alla NATO, o a nazioni partner, eventi esercitativi organizzati da enti militari mirati a testare l'interoperabilità dei sistemi C4 – Comando, Controllo, Comunicazioni e Informatizzazione (Computer) – della Difesa da utilizzare durante operazioni militari congiunte. Tra di esse l'Italia assicura una partecipazione attiva, ad esempio, alla Bold Quest, esercitazione "trial" (Multinational, Joint, Collaborative Enterprise), organizzata con cadenza annuale dal Dipartimento della Difesa statunitense; così come alla CETATEA, esercitazione di interoperabilità dei Sistemi di C4ISR/CIS (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance/Computer and Information Systems) condotta, annualmente, dall'esercito della Romania.

La prima è caratterizzata dallo sforzo di integrare, in maniera sinergica, diverse capacità del settore militare (Integrated Air Missile Defense, Joint Fire Support, Friendly Force tracking, Coalition Intelligence Surveillance and Recnnaissance, ecc…), nonché fornire adeguata difesa cibernetica alle reti schierate.

La seconda si focalizza, invece, sullo sviluppo, test e validazione di assetti Computer Information Systems (CIS) da utilizzare in future operazioni multinazionali/NATO, ivi inclusi sistemi di supporto logistico, protetti da uno specifico centro per la sicurezza cibernetica.

Infine, negli ultimi anni, si è verificata una notevole crescita di iniziative bilaterali, o derivanti da accordi multinazionali, nel campo dell'integrazione delle capacità di cyber defence dei vari paesi. È il caso, ad esempio, dell'esercitazione SMART CYBER 5+5, evento durante il quale i partecipanti (le nazioni dell'"Iniziativa 5+5 Difesa"), sotto guida portoghese, verificheranno la loro capacità di comunicare e rispondere, in maniera collaborativa, a minacce provenienti dal cyberspazio per migliorare la capacità collettiva di cyber defence all'interno di un framework federato persistente.

Dal variegato panorama esercitativo internazionale presentato, certamente non esaustivo, che vede una sempre maggiore partecipazione dell'Italia, emerge quindi chiara l'indicazione della consapevolezza dell'importanza che tali eventi rivestono e rivestiranno, maggiormente, in futuro. Un futuro dove una delle chiavi del successo nella protezione di assetti e servizi digitali nazionali è rappresentata da un necessario processo di integrazione e validazione delle capacità nel campo della cyber defence in un contesto internazionale sempre più ampio e variegato.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
7 February 2019

THE IMPORTANCE OF INFORMATION SHARING: UNIDIR'S CYBER POLICY PORTAL

UNIDIR

THE UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

The United Nations Institute for Disarmament Research (UNIDIR) recently launched its Cyber Policy Portal – an accessible and up-to-date overview of the cyber policies of all UN Member States and a select number of intergovernmental organizations.

THE IMPORTANCE OF TRANSPARENCY TO CYBER STABILITY

States, regional and international organizations are increasingly acknowledging the important role of transparency and information sharing for cyber stability. Transparency about national cybersecurity strategies and policies serves a range of objectives: in addition to the stabilizing nature of transparency efforts, information sharing has other important benefits including facilitating targeted needs analysis and better focused capacity-building efforts. Accessible, voluntarily shared information can serve as the basis to facilitate common efforts to address the risks related to the use of Information and Communications Technologies (ICTs) while sharing in the benefits of a stable cyber environment.

Recognizing the critical importance of information sharing, the report of the 2012-2013 United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security encouraged States to undertake an "exchange of views and information … on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international cooperation"1. The 2014-2015 GGE report further encouragedvoluntary transparency efforts at the bilateral, subregional, regional and multilateral levels as a confidence-building measure.[2]

BACKGROUND

In 2013, UNIDIR published The Cyber Index: International Security Trends and Realities. This book served as a snapshot

of then-current cyber security activities undertaken by all UN Member States at the national, regional, and international levels. While a useful resource, UNIDIR recognized the need to translate the static information contained in the Index into a dynamic, interactive resource in order to provide timely, policy-relevant information on cyber security issues.

UNIDIR surveyed the availability of existing information on governmental and organizational websites, as well as other online resources.4 The results of that analysis demonstrated that while considerable information is in the public domain, those seeking an overview of national, regional and international cyber policies often need to piece together data from disparate sources, attempt to identify relevant information in foreign languages, and seek to understand different ranking methodologies. Together, these obstacles hinder mapping the cyber policy landscape and the ability to conduct comparative analyses.

Following a rigorous research and design phase to establish the conceptual foundations of this resource,5 the Institute commenced development on an online policy repository that presents the current cyber policy landscapein an objective format.

The Cyber Policy Portal was launched in January 2019 – a user-friendly tool to enhance informed participation in key dialogue and policy processes, and foster further transparency and cyber capacity-building measures. Serving as a reference guide with which to navigate the cyber policy arena, users can access concise yet comprehensive cyber policy profiles of states as well as regional and international organizations.

FEATURES OF THE CYBER POLICY PORTAL

Each state profile provides the user with an overview of the state's cybersecurity policies, national structure, legal framework, and bilateral, regional and multilateral cooperation. Similarly, organization profiles provide an overview of the entity's respective policies, structure, legislation and cooperation with members, non-members, and other organizations. All data available via the Portal is from open source and voluntarily submitted material. Useful features include the ability to compare two or three states or organizations, filter for specific criteria,and export theprofiles.

OUTCOMES

The Portal promotes cyber stability by providing key information about each UN Member State's strategy and policy documents. Situational awareness is critical for states, regional and international organizations wishing to undertake effective and appropriate cyber capacity-building measures. This data will not only help policy makers, risk managers and practitioners to identify specific needs thematically and geographically, but also to tailor their responses. Accessible information on national, regional and international trends and capabilities, as well as comparative analyses, may allow for a better understanding of what constitutes responsible behaviour in cyberspace and will assist States as they prepare for UN Group of Governmental Experts[6] and the Open-Ended Working Group[7], commencing work later this year.

Updates and feedback concerning the Cyber Policy Portal may be sent to unidir@un.org

1. UN General Assembly document A/68/98, para. 26.

2. UN General Assembly document A/70/174, paras. 16(c) and 16(d).

3. See, for example: Global Cybersecurity Index, International Telecommunications Union, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx; F. Hanson, T. Uren, F. Ryan, M. Chi, J. Viola, E. Chapman, 'Cyber Maturity in the Asia Pacific Region 2017' (12 December 2017), Australian Strategic Policy Institute, https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017.

4. See L. Rudnick, D. B. Miller, L. Levy, "Towards Cyber Stability: A User-Centred Tool for Policymakers", 2015, http://www.unidir.org/files/publications/pdfs/cyber-index-2014-en-625.pdf.

5. United Nations General Assembly, "Advancing responsible State behaviour in cyberspace and in the context of international peace and security", 18 October 2018, A/C.1/73/L.37, https://undocs.org/A/C.1/73/L.37.

6. United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security", 18 October 2018, A/C.1/73/L.27/Rev.1, http://undocs.org/A/C.1/73/L.27/Rev.1.