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)