Cybersecurity Trends

Edizione italiana, N. 1 / 2019

INTERVISTA VIP:

Massimiliano VALERII

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Central Folder:
Cyber Security Skill Shortage

Global Cyber Security

La Fondazione GCSEC è un'organizzazione senza scopo di lucro, creata per promuovere la sicurezza informatica in Italia e nel resto del mondo. Il Centro, fondato e finanziato da Poste Italiane, ha sede a Roma e collabora con Istituzioni Italiane e Internazionali Governative, enti privati, istituti di ricerca e organismi internazionali.
La missione della Fondazione è quella di sviluppare e diffondere la conoscenza e la consapevolezza sulla sicurezza informatica, creando le condizioni per migliorare le capacità, le competenze, la cooperazione e la comunicazione tra i diversi attori coinvolti nell'uso e nella protezione di Internet.

Information Sharing
Creazione di modelli di information sharing pubblico - privato

Threat Intelligence
Analisi di modelli di attacco e delle tecnologie necessarie a velocizzare l'analisi stessa

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione e corsi di specializzazione e master

Fondazione Global Cyber Security Center
Viale Europa, 175 – 00144 Roma
www.gcsec.org

GLOBAL CYBER SECURITY CENTER

Indice

Editoriale

Autore: Nicola Sotira

In uno scenario in cui le minacce informatiche continuano a crescere in intensità e in termini di sofisticazione, le esigenze dei team di sicurezza cambiano costantemente e richiedono personale sempre più specializzato.Molto spesso, però, assistiamo a situazioni in cui affrontiamo il rischio emergente con una mancanza di personale e una difficoltà nell'attrarre e reclutare personale adeguatamente qualificato, una situazione che rappresenta già di per sé un rischio.

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Si verificano deficit di competenze e capacità proprio mentre i principali incidenti di sicurezza danneggiano le performance e la reputazione delle aziende. Formare la forza lavoro del domani nel settore della sicurezza è essenziale per affrontare questa sfida e fornire alle organizzazioni una solidità a lungo termine proprio in termini di sicurezza nell'era digitale. Colmare il vuoto di competenze richiederà alle organizzazioni un cambiamento nell'approccio al reclutamento, alla formazione e alla partecipazione a iniziative di collaborazione. Un approccio troppo rigido e tradizionale per individuare i candidati, con ambienti di lavoro sovraccarichi e insufficienti, richiede chiaramente un mutamento verso nuove tattiche e nuove idee.

GCSEC è attiva sui programmi di awareness e ricerca in ambito UE. Ha infatti sviluppato progetti di Information Sharing, ICS e Smart Grid security, E-crime, Cyber Educational Programme e molto altro. Negli ultimi anni ha organizzato eventi e workshop sulla sicurezza degli ATM, Advanced Persistent Threat, PSD2 Security. Abbiamo già pubblicato studi, come "DNS Health and Security" in collaborazione con ICANN, “Information Sharing and Public-Private Partnerships: Perspectives and Proposals” in collaborazione con UNICRI, “Best Practices in Computer Network Defense: Incident Detection and Response” in collaborazione con la NATO.

Gli studi “Mind the Gap: the cyber security skills shortage and public policy interventions” e “Il fenomeno del Cyber Security Skill Shortage italiano nel contesto internazionale” condotti sullo skill shortage nel settore della cyber security rappresentano l'ultima pietra e il risultato della collaborazione con l'Oxford Centre for Doctoral Training in Cyber Security.

Crediamo che occorra fare di più per preparare i nostri paesi a un mondo digitale migliore e più sicuro. Il primo passo per facilitare la digitalizzazione, in conformità con il terzo pilastro “Trust and Security” della strategia europea per il mercato unico digitale (Digital Single Market Strategy), è quello di riconoscere l'esistenza della carenza di skill e competenze nella sicurezza informatica. In questi studii, abbiamo fornito una panoramica delle politiche adottate dei Paesi e dei pareri degli esperti sui programmi educativi sulla sicurezza informatica, evidenziando alcune raccomandazioni per il futuro. Un focus specifico è stato dedicato al caso italiano. Colmare il divario tra offerta e domanda di lavoro è indispensabile per consentire alle imprese di sviluppare un efficace security posture.

È evidente che individui con competenze, qualifiche ed esperienza richieste non sono disponibili o esigono compensi che non possono essere soddisfatti con i budget esistenti. Poiché molto richiesti, il personale di sicurezza talentuoso si trasferisce regolarmente presso nuovi datori di lavoro cercando salari e progetti migliori presso aziende più prestigiose.

Buona lettura…

Autore: **Marco Obiso,**

Coordinatore per la cyber security, International Telecommunications Union, Ginevra

Caro lettore,

Questo nuovo numero di Cybersecurity Trends sottolinea due punti che sono sempre stati cruciali per l'ITU.

Il primo è quello di promuovere il concetto di cultura digitale in ogni settore e in generale, a livello nazionale, regionale e internazionale, attraverso programmi di capacity building adattati e personalizzati che rispondano alle diverse esigenze in termini di tipologia di entità beneficiarie e di età.

Naturalmente, all'interno del processo di trasformazione digitale, la sicurezza informatica è una questione educativa chiave che deve iniziare il più presto possibile e crescere progressivamente durante tutta la vita di ogni cittadino e professionista.

Una delle sfide da affrontare, tuttavia, è lo sviluppo di programmi di formazione che prendano in considerazione la natura interdisciplinare del cyberspazio, passando da insegnamenti puramente tecnologici, impartiti principalmente con metodologie tradizionali, ad esercizi di team-building interattivi, interattivi e multi-servizio, più adatti alla realtà dinamica del settore ICT.

Il secondo punto è la condivisione di informazioni e conoscenze, tra specialisti con background molto diversi.

La scelta di produrre la rivista evidenziando le più importanti tematiche e sfide "ICT 4.0" e di pubblicarla utilizzando un linguaggio di facile lettura, oltre alla pubblicazione degli articoli sulle minacce emergenti, è un risultato importante. Essere avanti, è naturalmente un must nel nostro campo. Questo tipo di conoscenza potrebbe essere utile per comprendere meglio i possibili rischi legati all'implementazione di nuove tecnologie, mitigandoli per sfruttare al massimo il potenziale del cambiamento di paradigma.

Questo tema, come i precedenti e forse di più, pone una sfida a dinnanzi ognuno di noi su quanto vogliamo essere preparati, ora e domani.

La preparazione è il modo più efficace per aumentare la sicurezza e la nostra missione nell'ITU è quella di assistere gli Stati membri e, di conseguenza, la comunità nel suo complesso, per acquisire conoscenze e costruire le capacità necessarie per contrastare lo "scenario peggiore".

In questo nuovo numero di Cybersecurity Trends, scoprirete che il percorso verso la resilienza può essere molto facile o molto lungo e difficile. La differenza sarà fatta dal livello di consapevolezza, comprensione e conoscenza, tutti elementi fondamentali alla base di un'istruzione e formazione efficace. ■

Il fenomeno del Cyber Security Skill Shortage: un'emergenza globale

Autori: Elena Agresti, Marco Fiore

In uno scenario in cui le minacce informatiche diventano sempre più sofisticate e mutevoli nel tempo, le esigenze dei team di security cambiano costantemente richiedendo personale sempre più specializzato in grado di fronteggiare un contesto in continuo cambiamento.

Purtroppo, tale compito già impegnativo delle imprese di proteggersi contro le minacce cyber è aggravato dallo skill shortage, ovvero la mancanza di competenze nel settore della cyber security. Il fenomeno dello **Skill Shortage, ovvero carenza di competenze, sta diventando una vulnerabilità delle organizzazioni**.

Nel 2017 lo shortage a livello globale **era stimato pari a 1,8 entro il 2022** ma già a fine 2018, secondo una stima di ISC2 **era pari a 2,93 milioni di posti di lavoro[1]. È stimato, inoltre, che tale carenza diventi di 3,5 milioni entro il 2021**.

Per analizzare questo fenomeno e fornire delle indicazioni per la sua mitigazione, la **fondazione Global Cyber Security Center** ha finanziato e supportato un progetto di ricerca condotto dai **ricercatori dell'Università di Oxford[2]**.

L'obiettivo dello studio è stato analizzare le caratteristiche e le cause dello shortage e le azioni intraprese dai 12 Paesi con più alto indice di sviluppo ICT e cyber security[3] per mitigarlo.

Dallo studio emerge un fenomeno molto complesso con cause da imputare a vari fattori. 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.

Solo nel mercato americano da settembre 2017 ad agosto 2018 su 715,715 posizioni aperte ben 313,735, **quasi il 50%, sono rimaste vacanti**.

La carenza di 80.000 unità nel 2013 era divenuta di 132.060 nel 2016 ed è stimato che superi le 193.010 unità nel 2020. 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 le 7,500 e 11,000 risorse entro il 2026 (Australian Cyber Security Growth Network, 2017).

Le figure mancanti sono principalmente quelle tecnico – operative come risulta evidente ad esempio dai mercati australiani e americani in cui i profili più ricercati sono quelli afferenti alle categorie "Operate & Maintain", "Securely Provision" e "Protect & Defend" del framework NICE del NIST.

I dati americani sono stati reperiti tramite CyberSeek, un tool che fornisce uno spaccato dell'offerta e della domanda in Cybersecurity. La carriera professionale è, inoltre, mappata secondo un percorso di carriera professionale da entry-level ad advanced-level. Per ciascun ruolo è indicato il salario medio, i job title associati, la formazione, competenze, skill e certificazioni richieste.

Emerge, ad esempio, che Cybersecurity Engineer, Analyst e Manager/ Administrator sono i profili più richiesti, mentre Cybersecurity Architect, Cybersecurity Manager e Cybersecurity Engineer quelli più remunerati.

Lo Studio ha evidenziato anche una **disomogeneità nella definizione e attuazione delle politiche nazionali** volte a mitigare il fenomeno dello Skill Shortage definite dai 12 paesi più influenti nel settore ICT e cyber security.

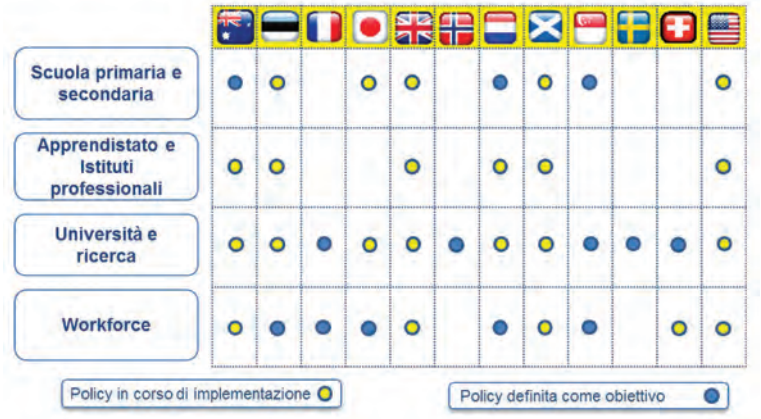


Figura 1: *Politiche nazionali per mitigare il CCSS*

Le politiche sono state analizzate nelle dimensioni: Scuola Primaria e Secondaria, Apprendistato e Istituti professionali, Università e Ricerca, mondo del Lavoro.

I Paesi hanno investito principalmente nel mondo della università e 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.

Lo stato di implementazione e il livello di maturità delle politiche varia di paese in paese ma è possibile affermare che i governi che hanno maturato nel tempo una maggiore esperienza e consapevolezza nell'affrontare lo Skill Shortage e raggiunto un più elevato livello di maturità risultano essere Regno Unito, Giappone e Australia.

Figura 2: *Interventi in essere a livello internazionale*

Il Regno Unito ha operato importanti investimenti. Sono state istituite infatti importanti iniziative governative destinate agli studenti come Cyber First, Cyber Challenge, Cyber Security Discovery e il Cyber Security Skills Immediate Impact Fund. Cyber First mette a disposizione degli studenti diversi percorsi di formazione in cyber security. Il programma prevede borse di studio di 4500 euro nonché attività di apprendistato retribuito e formazione extracurriculare per il periodo estivo. In Cyber First assumono un importante rilievo anche le donne. Al fine di incrementare l'occupazione femminile è stato istituito uno specifico programma Cyber First Girl che comprende anch'esso una gara e che nel 2018 ha contato la partecipazione

BIO

Elena Mena Agresti
Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, opera per la Fondazione GCSEC e la struttura Tutela delle Informazioni di Poste Italiane.
Esperta di compliance, standard internazionali, governancedell'information security, gestione dei rischi, security audit, formazione eawareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security.
È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane eattualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Oracle Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

BIO

Marco Fiore
Marco è un research fellow della Fondazione Global Cyber Security Center di Poste Italiane. Laureato in Giurisprudenza presso La Sapienza di Roma in Procedura Penale. Ha svolto una tesi in "Intercettazioni di messaggistica istantanea Blackberry e utilizzazione probatoria nel processo penale". Dopo gli studi ha svolto la pratica forense e contestualmente portava a termine il Master di II livello "Homeland Security" presso il Campus Bio Medico di Roma dove trasversalmente ha approfondito le tematiche in Security e Privacy e Social Communication. Continua a svolgere ricerche per la Fondazione GCSEC. Tra le varie iniziative rilevanti ha contribuito allo studio del 2019 sul Cyber Security Skill Shortage internazionale Mind the Gap e quello Italiano "Il fenomeno del Cyber Security Skill Shortage italiano nel contesto internazionale". Contribuisce alla gestione e pubblicazione di diverse pubblicazioni sul sito ufficiale della Rivista Cybertrends.it.

di 3.400 ragazze circa, provenienti da 841 scuole. Sempre in tema di Cyber competizioni un'importante iniziativa creata dal governo inglese è il Cyber Discovery. Il programma prevede una challenge per l'apprendimento della cyber security per giovani di età compresa tra i 14 e i 18 anni suddivisa in 4 fasi dove gli studenti vengono formati da esperti del settore con corsi dedicati per poi confrontarsi con vere e proprie sfide online che spaziano da Linux alla crittografia e programmazione. Il piano messo in atto dal Regno Unito è molto variegato. Al fine di combattere il fenomeno dello skill shortage nazionale infatti è stato istituito un ulteriore programma volto a formare e collocare individui che non hanno ancora una occupazione in ruoli di sicurezza informatica e destinato a organizzazioni e associazioni che presentano specifici programmi per aumentare e diversificare le risorse nel campo della Cyber Security.

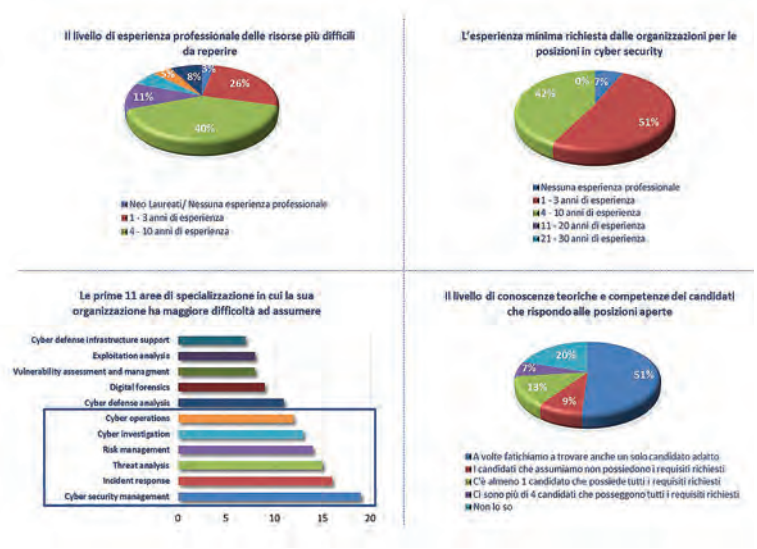
Il fenomeno risulta molto evidente anche in Italia che ha indicato nelle proprie politiche nazionali (es. Piano Nazionale per la protezione cibernetica e la sicurezza informatica) l'obiettivo di aumentare le competenze nel settore della cyber security. **Tuttavia non è stata ancora definita una policy nazionale unica** per ridurre lo skill shortage seppure alcune iniziative siano nate spontaneamente nell'ambito di singoli enti e organizzazioni.

Una politica che potrebbe essere potenzialmente rilevante per la sicurezza informatica è il Piano Nazionale Scuola Digitale, che prevede obiettivi e azioni specifiche per sviluppare le competenze digitali di studenti e docenti e per favorire l'imprenditorialità e il lavoro al fine di colmare il divario digitale sia in termini di competenze che di occupazione.

In Italia, il problema del CSSS è stato riconosciuto in numerosi rapporti ufficiali e non ufficiali. Il Dipartimento delle Informazioni per la Sicurezza (DIS), ha riconosciuto già nel 2017 che l'Italia ha un "vasto problema" in relazione all'educazione della Cyber Security e il CINI (Consorzio Interuniversitario Nazionale per l'informatica,) ha sottolineato nel suo Libro Bianco del 2018, come le politiche educative in tema di Cyber Security siano insufficienti. Gli studi di Kaspersky lab nel 2016, dell'Osservatorio sulle Competenze Digitali del 2017 e il Barometro di Cyber Security nel 2018 confermano la difficoltà italiana nel reclutare professionisti in cyber security.

Al fine di recepire le effettive necessità delle organizzazioni italiane in tutte le sue accezioni è stato proposto sia un sondaggio on- line anonimo e rivolto ai CISO delle principali organizzazioni italiane (+ del 50% delle organizzazioni ha oltre 500 dipendenti), sia sono state condotte delle interviste a rappresentanti della pubblica amministrazione e del mondo accademico.

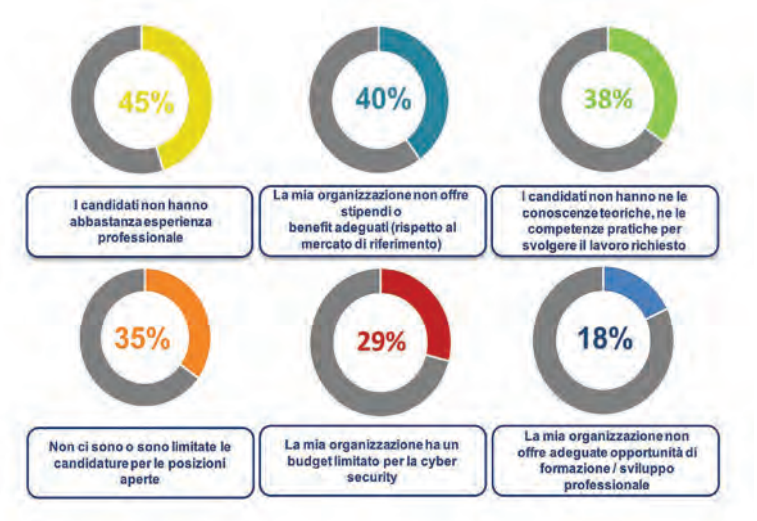
Dal punto di vista delle organizzazioni i CISO italiani hanno riconosciuto una conclamata difficoltà nel trovare risorse per il settore della Cyber Security.



Dal sondaggio condotto infatti emerge che nel 75% dei casi le aziende hanno serie difficoltà ad assumere nel settore della cyber security e che nel 50% dei casi fanno fatica a trovare addirittura anche un solo candidato per la posizione richiesta. Alle posizioni aperte rispondo spesso candidati con poca **esperienza operativa**.

Le competenze maggiormente richieste in Italia risultano essere **cyber security management, incident response, threat analysis, risk mangament, cyber investigation, cyber operations** a cui si affianca, principalmente per il settore privato, la **digital forensics**.

Emerge altresì che, nonostante **«1 - 3 anni» sia l'esperienza professionale minima** richiesta dalle aziende, al fine di coprire le posizioni vacanti le organizzazioni sono **disposte ad assumere anche neo diplomanti** da formare.



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".

I CISO italiani, infatti, imputano tra le principali cause del fenomeno in Italia la mancanza di **competenze pratiche delle risorse** e gli stipendi e i **benefit non adeguati rispetto al mercato internazionale** di riferimento. Infatti, i pochi candidati che in Italia hanno acquisito le competenze **richieste dalle aziende si rivolgono al mercato internazionale che può garantire stipendi nettamente superiori e maggiore stabilità**.

La capacità del sistema educativo italiano di produrre un numero sufficiente di candidati con le giuste conoscenze e competenze costituisce un altro fattore critico. Dal sondaggio si evince, infatti, che in Italia il **sistema accademico** garantisce, soprattutto con lauree in Ingegneria e Informatica, **conoscenze** in cyber security ma **solo teoriche**. Mancano quelle pratiche e operative che consentono l'inserimento immediato nel mondo del lavoro.

Il sistema educativo italiano, ha reagito in generale lentamente alle nuove tendenze, compresa la formazione informatica. A una non adeguata offerta formativa, si aggiunge inoltre la mancanza di docenti universitari. Le nuove lauree stanno iniziando a nascere, ma sono ancora insufficienti ed eccessivamente focalizzate sulla teoria anziché che sugli aspetti più operativi della Cyber Security.

Dalle interviste condotte è emersa, inoltre, la mancanza di una cultura della sicurezza percepita ancora come un costo e un onere e non necessaria e abilitante il business. Le interviste hanno ribadito in più occasioni come in contesti complessi, dove a volte non si riesce a pensare in modo strategico alla sicurezza informatica, gli esperti in cyber security sono particolarmente rari e costosi e i profili maggiormente ricercati non hanno una formazione adeguata per lavorare in contesti immediatamente operativi. Ulteriore fattore critico sottolineato riguardano gli stipendi che essendo **troppo bassi e non in linea con il mercato internazionale contribuiscono alla "fuga dei cervelli" dal territorio nazionale**.

Lo scenario italiano emerso dallo studio non è isolato ma in linea con quello internazionale come emerso dagli studi condotti a livello globale da ISACA[4] che validano i risultati circa la dimensione del fenomeno e i tempi necessari per trovare un candidato qualificato per le posizioni vacanti nelle strutture aziendali, periodo che va dai 30 giorni fino addirittura a sfiorare i 6 mesi (o più). Meno del 50% dei candidati, secondo lo studio di ISACA, non sono propriamente qualificati per rivestire la posizione richiesta dalle stesse organizzazioni, dato che corrobora ancor di più l'importante fattore dell'insufficiente formazione tecnico-operativa e di comprensione del business nel settore della cyber security.

Il fenomeno del CSSS, come già ampiamente dimostrato nel report internazionale "Mind the Gap", è fortemente sentito a livello internazionale e Paesi come il Regno Unito, l'Australia o il Giappone nazioni che ad oggi stanno investendo molto sia in termini economici che di strutturazione di policy mature per contrastare lo shortage.

Paragonando l'Italia con il Regno Unito, uno dei paesi con un approccio sofisticato al cyber security skill shortage, **emerge un minore commitment economico dell'Italia in termini di cyber security e istruzione**.

Il Regno Unito infatti, ha avuto un approccio nazionale al fenomeno soprattutto in termini di politiche e formazione delle giovani generazioni. Tra il 2011 e il 2016, ha investito **38,2 milioni di Euro in programmi di formazione ed educazione** ed è attualmente in fase di definizione una ulteriore strategia per la creazione di skill in cyber security, che dovrebbe essere pubblicata entro la fine del 2019.[5] Ha dedicato alla cyber security **circa un miliardo di euro di budget pubblico** già nel periodo 2011-2016, stanziamento incrementato a 2.2 miliardi per il periodo 2016-2021.[6]

Non è ancora chiaro quanto l'Italia spenda complessivamente per la sicurezza informatica ma il piano strategico 2017 ha ribadito come **la politica di sicurezza informatica non debba comportare costi aggiuntivi per l'amministrazione** e che 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.

Certamente l'Italia potrebbe trarre ispirazione del modello adottato dal Regno Unito, pur tenendo conto delle differenze tra i due Paesi, e mettere in campo alcune iniziative per ridurre il fenomeno dello skill shortage in cyber security.

Potrebbe **definire una soluzione nazionale al fenomeno** del cyber security skill shortage coinvolgendo Governo, Industria e Sistema educativo, designare un **singolo ente nazionale** responsabile delle relative politiche e **stanziare del budget adeguato** senza il quale le amministrazioni italiane difficilmente potranno attuare le politiche in materia di istruzione e competenze.

L'Italia dovrebbe considerare come **priorità le politiche relative al passaggio scuola-lavoro, all'alta formazione e alle scuole superiori e sviluppare campagne per incentivare le donne** a intraprendere percorsi di formazione nella cyber security al fine di favorire l'occupazione femminile nel settore.

I report dello studio internazionale e del caso Italia sono disponibili sul sito della fondazione www.gcsec.org. ■

1 https://www.isc2.org/Research/Workforce-Study
2 Centre for Doctoral Training in Cyber Security, University of Oxford
3 Secondo le stime dell'ITU del 2017
4 ISACA STATE OF CYBERSECURITY 2019 - LEARN ABOUT SEVERAL CLEAR CHALLENGES ENTERPRISES ARE FACING - https://cybersecurity.isaca.org/state-of-cybersecurity
5 È statapubblicatail 21 dicembre 2018 la dichiarazione di intenti - Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views,
6 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Strumenti innovativi per l'awareness aziendale

Autore: Sonia Ciampoli

La ricerca recentemente condotta da GCSEC insieme all'università di Oxford sullo skill shortage solleva diverse questioni interessanti, soprattutto per quelle aziende che hanno una visione chiara dell'importanza della sicurezza informatica e tutta l'intenzione di rendersi protagoniste del futuro cyber che ormai è già qui.

Come mai c'è tanta distanza fra le competenze necessarie e quelle disponibili? Dove e come, a un certo punto, si è inceppato il meccanismo della domanda e dell'offerta? Ma soprattutto, guardando al futuro, cosa può concretamente fare un'azienda per riempire il gap che si è venuto a creare? Come può accompagnare i propri collaboratori e dipendenti in un percorso articolato che li porti a maturare quelle conoscenze e quegli skill di cui c'è attualmente bisogno nel mondo digitale?

Gli strumenti sono noti e tutte le organizzazioni più lungimiranti ne fanno uso costante: corsi di formazione, training on the job, e-learning, iscrizione e collaborazione con gruppi specialistici, etc. Tuttavia, a fronte dei risultati di una ricerca come quella sullo skill shortage, viene spontaneo aggiungere un ulteriore quesito a quelli già elencati poco sopra: questi strumenti noti e diffusi sono realmente efficaci, i migliori disponibili? O forse, in un'epoca così mutata e mutevole come quella che stiamo attualmente vivendo, non si potrebbe pensare ad arricchire e ampliare il panorama educativo e formativo, guardando magari ai cambiamenti di costume intervenuti nel frattempo anche nella società non strettamente digitale?

Oggi ci sono i social network, dove la comunicazione è rapida, immediata, velocissima, e ci sono Netflix, Amazon tv e servizi affini, che hanno trasformato le serie tv in uno dei, se non nel, format più seguito e diffuso, in cui la brevità del singolo episodio o della stagione nel suo complesso è cruciale per fidelizzare lo spettatore.

BIO

Nata a Roma nel 1977, laureata in filosofia alla LUMSA, lavora nella sicurezza informatica da quindici anni.
In Poste si dedica in particolare ai temi legati alla sensibilizzazione e all'awareness, con progetti di diffusione e condivisione di cultura della sicurezza e web content editing, con produzione di contenuti pensati per un pubblico meno tecnico. Nel tempo libero si occupa di divulgazione scientifica.

Pare quindi evidente che, al momento attuale, una comunicazione efficace, anche quando volta all'insegnamento, debba necessariamente uscire dai confini ingessati e rigidi del classico corso di formazione e prediligere forme più "smart", in grado di conquistare l'attenzione e trasmettere il messaggio anche in tempi ridotti. Mezzi di comunicazione che facciano presa sul pubblico medio, non necessariamente il tecnico o l'utente esperto, perché oggi la sicurezza informatica è un tema che riguarda tutti e a tutti deve essere insegnato come tutelare se stessi e le proprie informazioni, non più solo allo sviluppatore super specializzato che deve mantenersi al passo con le evoluzioni tecnologiche.

Non è quindi un caso se di Poste Italiane ha intrapreso per il 2019 un progetto innovativo nel panorama digitale, vale a dire la realizzazione di una mini web serie, in cui l'investigatore interpretato da Alessandro Curioni, editore, imprenditore, giornalista, e autore delle sceneggiature, affronta casi di attacchi informatici realmente accaduti (e ovviamente un po' romanzati a fini narrativi), mostrando come sia possibile diventare vittime di attaccanti malevoli, complici inconsapevoli, strumenti persino, e quali tecniche sia necessario utilizzare per riuscire a capire cosa sia veramente successo.

14 episodi di 5-8 minuti, che spaziano dal phishing, alle truffe del CEO, agli attacchi via Wireless all'Internet of Things, "Le indagini di un cyber investigatore" è fortemente post-moderno, cyber dal montaggio alla fotografia, improntato a una comunicazione lineare adatta a un pubblico meno specializzato, ma con contenuti solidi e rigorosi in grado di superare l'esame anche dello spettatore più tecnico. Senza contare la qualità di scrittura e regia, che lo rendono accattivante anche per semplici serial-addicted.

L'esperimento del CERT di Poste Italiane è innovativo perché è il primo di questo genere in Italia, e probabilmente anche a livello internazionale, se si considera che l'ultima serie a tema informatico è stata Mr. Robot, con l'ormai premio Oscar Rami Malek, che aveva un taglio sicuramente più tecnico e meno family-friendly rispetto a queste pillole realizzate da Alessandro Curioni. Le indagini su una rete senza fili realizzano per la prima volta uno strumento didattico che è in tutto e per tutto anche un prodotto seriale di alto livello.

Si tratta ovviamente di un arricchimento del panorama formativo, non di una soluzione definitiva: nessun filmato può sostituire un percorso di studio articolato, ma la facilità di comunicazione e comprensione offerta da simili media può contribuire a diffondere una reale consapevolezza e cultura della sicurezza informatica, proprio perché si rivolge trasversalmente a un pubblico inclusivo, e tratta la sicurezza per quello che è: un tema che riguarda tutti. ■

Certificazioni professionali e altri strumenti per documentare le competenze in ambito sicurezza

Autore: Giancarlo Butti

La necessità delle aziende di reclutare personale qualificato e quelle dei professionisti ICT di dimostrare le proprie competenze, può avvalersi di alcuni strumenti, quali le certificazioni professionali e i framework delle competenze.

Nell'ambito delle professioni ICT in generale e più specificatamente nell'ambito delle professioni legate alla sicurezza, uno strumento importante per la valutazione delle competenze è rappresentato dalle certificazioni professionali.

Si può avere una visione delle caratteristiche e della molteplicità delle certificazioni di questo tipo, nella pubblicazione **Certificazioni Professionali in Sicurezza Informatica 2.0**, disponibile gratuitamente sul sito del CLUSIT (https://clusit.it/wp-content/uploads/download/Q09_web.pdf).

La pubblicazione raccoglie le certificazioni relative alle competenze:

- sull'organizzazione della sicurezza delle informazioni
- organizzative e tecnologiche
- tecnologiche non legate a prodotti specifici
- tecnologiche legate a prodotti specifici.

Dal punto di vista delle competenze nell'ambito della sicurezza delle informazioni, le certificazioni svolgono un ruolo molto importante e duplice.

Se da un lato il più ovvio ed immediato consiste nell'attestare le competenze professionali di chi acquisisce la certificazione, non meno importante è l'aumento di conoscenze e competenze che i professionisti sono disposti ad acquisire per poterle ottenere.

Conseguire una certificazione comporta di solito il superamento di un esame, conseguentemente, in molti casi questo implica l'acquisizione delle competenze non già possedute, aumentando quindi il proprio bagaglio professionale.

Del resto è sufficiente una breve ricerca on line per individuare quanti corsi sono disponibili per la preparazione agli esami delle più importanti e riconosciute certificazioni professionali e per comprendere, di conseguenza, quanto i professionisti siano disposti ad investire del loro tempo (e denaro) per ottenere tale riconoscimento.

Nella maggior parte dei casi inoltre, tali certificazioni non hanno una validità assoluta, ma necessitano di un mantenimento nel tempo derivante da comprovate attività di formazione.

Questo fa sì che un professionista debba obbligatoriamente mantenere nel tempo un alto livello di formazione, pena la revoca della certificazione.

Molto spesso tali certificazioni sono inoltre "proprietà" di associazioni di professionisti, che operano spesso a livello internazionale e che costituiscono un elemento di garanzia di professionalità che si affianca a titoli istituzionali rilasciati dal normale sistema scolastico e universitario.

Dal punto di vista normativo la regolamentazione delle attività professionali relative alla sicurezza ed all'ICT non organizzate in ordini e collegi è regolato in Italia dalla legge n. 4/2013 ***Disposizioni in materia di professioni non organizzate*** (norma che regola in realtà qualunque professione non rientrante appunto in ordini e collegi).

Tale normativa prevede fra gli altri che un professionista possa ottenere una Certificazione di conformità a specifiche norme tecniche UNI che regolamentano la relativa professione.

In particolare l'articolo 9 2 prevede che:

2. Gli organismi di certificazione accreditati dall'organismo unico nazionale di accreditamento ai sensi del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, possono rilasciare, su richiesta del singolo professionista anche non iscritto ad alcuna associazione, il certificato di conformità alla norma tecnica UNI definita per la singola professione.

Nell'ambito delle professioni ICT UNI ha pubblicato le seguenti norme[1]:

UNI 11506:2017	Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Requisiti per la valutazione e certificazione delle conoscenze, abilità e competenze per i profili professionali ICT basati sul modello e-CF
UNI EN 16234-1:2016	e-Competence Framework (e-CF) - Framework comune europeo per i professionisti ICT in tutti i settori industriali - Parte 1: Framework (modello di riferimento)
UNI 11506:2017	Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Requisiti per la valutazione e certificazione delle conoscenze, abilità e competenze per i profili professionali ICT basati sul modello e-CF
UNI 11621-1:2017	Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e-CF
UNI 11621-2:2017	Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 2: Profili professionali di "seconda generazione"
UNI 11621-3:2017	Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 3: Profili professionali relativi alle professionalità operanti nel Web.
UNI 11621-4:2017	Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 4: Profili professionali relativi alla sicurezza delle informazioni
UNI 11621-5:2018	Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 5: Profili professionali relativi all'informazione geografica
UNI 11697:2017	Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza

BIO

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, whitepaper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN, Università degli studi di Milano.
Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali ed una decina on line. Ha pubblicato 21 fra libri e whitepaper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT…
È socio e proboviro di AIEA, socio del CLUSIT e di BCI.
Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico e GDPR di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti, SOC, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR…
È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMCBI.

In particolare le figure professionali legate alla sicurezza sono regolamentate specificatamente dalla norma UNI 11621-4:2017 ed in parte dalla UNI 11697:2017, come parte delle competenze richieste a chi si occupa di protezione di dati personali.

Come si può notare le prime due norme UNI qui citate fanno riferimento all' e-Competence Framework (e-CF), il framework di competenze europeo (http://www.ecompetences.eu/it/) che mappa diversi profili professionali ICT.

Questo framework consente ai professionisti ICT ed alle aziende di parlare un linguaggio comune e condiviso quando si tratta ad esempio di incrociare domanda ed offerta di lavoro, o di pianificare percorsi di carriera.

A sua volta tale framework si avvale del Quadro europeo delle qualifiche per l'apprendimento permanente (EQF), istituito in base alla RACCOMANDAZIONE 2008/C 111/01/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 aprile 2008.

La Raccomandazione introduce le seguenti definizioni:

f) "risultati dell'apprendimento: descrizione di ciò che un discente conosce, capisce ed e in grado di realizzare al termine di un processo d'apprendimento.

I risultati sono definiti in termini di conoscenze, abilità e competenze;

g) "conoscenze": risultato dell'assimilazione di informazioni attraverso l'apprendimento. Le conoscenze sono un insieme di fatti, principi, teorie e pratiche relative ad un settore di lavoro o di studio.

Nel contesto del Quadro europeo delle qualifiche le conoscenze sono descritte come teoriche e/o pratiche;

h) "abilità": indicano le capacita di applicare conoscenze e di utilizzare know-how per portare a termine compiti e risolvere problemi. Nel contesto del Quadro europeo delle qualifiche le abilità sono descritte come cognitive (comprendenti l'uso del pensiero logico, intuitivo e creativo) o pratiche (comprendenti l'abilità manuale e l'uso di metodi, materiali, strumenti);

i) "competenze": comprovata capacita di utilizzare conoscenze, abilità e capacità personali, sociali e/o metodologiche, in situazioni di lavoro o di studio e nello sviluppo professionale e personale.

Nel contesto del Quadro europeo delle qualifiche le competenze sono descritte in termini di responsabilità e autonomia.

L'allegato II della raccomandazione individua 8 livelli definiti da una serie di descrittori che indicano i risultati dell'apprendimento relativi alle qualifiche a tale livello in qualsiasi sistema delle qualifiche.

Nel contesto del Quadro europeo delle qualifiche, le conoscenze sono descritte come teoriche e/o pratiche secondo questo schema:

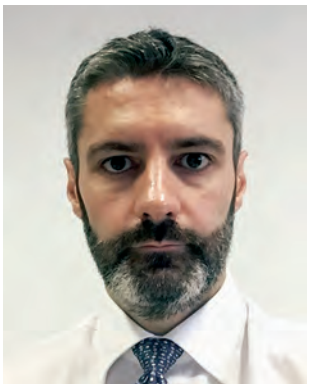
Livello 1	Conoscenze generale di base
Livello 2	Conoscenza pratica di base in un ambito di lavoro o di studio
Livello 3	Conoscenza di fatti, principi, processi e concetti generali, in un ambito di lavoro o di studio
Livello 4	Conoscenza pratica e teorica in ampi contesti in un ambito di lavoro o di studio
Livello 5	Conoscenza teorica e pratica esauriente e specializzata, in un ambito di lavoro o di studio e consapevolezza dei limiti di tale conoscenza
Livello 6	Conoscenze avanzate in un ambito di lavoro o di studio, che presuppongano una comprensione critica di teorie e principi
Livello 7	Conoscenze altamente specializzata, parte delle quali all'avanguardia in un ambito di lavoro o di studio, come base del pensiero originario e/o della ricerca; consapevolezza critica di questioni legate alla conoscenza all'interfaccia tra ambiti diversi
Livello 8	Le conoscenze più all' avanguardia in un ambito di lavoro o di studio e all' interfaccia tra settori diversi

Per i livelli da 5 ad 8 è definita inoltre la Compatibilità con il Quadro dei titoli accademici dell'Area Europea dell'Istruzione Superiore.

Aziende e professionisti della sicurezza hanno quindi a disposizione un insieme articolato di strumenti appositamente creati per confrontarsi nell'ambito di domanda ed offerta di lavoro e per sviluppare carriere professionali basate su criteri ampiamente condivisi. ■

1 L'elenco non vuole essere esaustivo; consultare il sito di UNI www.uni.com

Multidisciplinarità nella gestione degli incidenti

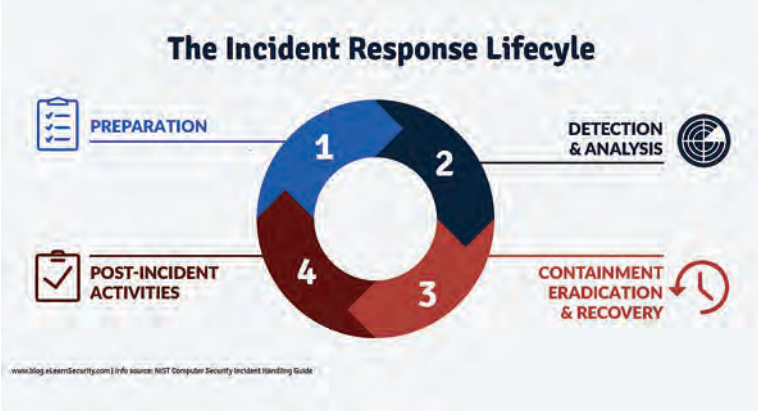


Autore: Massimo Cappelli

La gestione di un incidente è l'attività più critica che un Computer Emergency Response Team (CERT) o un Security Operations Center (SOC) possa affrontare. Nella gestione di un incidente, i fattori da considerare sono molteplici e il tempo per la loro considerazione è ridotto. A questo è necessario aggiungere anche l'elemento *"stress"* che influisce sulle prestazioni e sulle scelte da effettuare.

Per quest'ultimo motivo si ricorda sempre che è fondamentale prepararsi all'evento. La gestione di un incidente non si può improvvisare. I *table top scenario* per oliare gli aspetti di collaborazione e comunicazione e le esercitazioni, per testare le procedure dei dipartimenti coinvolti, dovrebbero essere svolti annualmente per verificare ogni singolo aspetto della gestione e migliorarne l'efficacia e l'efficienza. Le procedure servono a ridurre il tempo di "blocco psicologico" che colpisce chi è coinvolto nella gestione.

Purtroppo, queste attività si sottovalutano perché ritenute di basso valore aggiunto. I dipartimenti coinvolti sono molteplici e le agende dei manager sono spesso disallineate e non permettono momenti comuni di confronto e di test. Questo influisce molto sulle tempistiche e modalità di risposta ad un incidente. Iniziare a gestire un incidente nel momento in cui viene identificato, è troppo tardi. Come nei manuali di Protezione e Difesa Civile, anche nella cyber security il concetto chiave è la prontezza o *"preaparedness"* che si consegue solo con la preparazione.



Alcuni di voi si domanderanno l'attinenza dell'introduzione con il titolo dell'articolo. La risposta è: tutto. Consideriamo il macro-processo di una gestione dell'incidente e verifichiamo come sia fondamentale la preparazione come la multidisciplinarità.

Il primo passo è l'identificazione di un incidente. Un incidente può essere comunicato da un cliente, da un dipendente oppure essere identificato durante la fase di monitoraggio dei servizi.

La prima attività da compiere è un rapido triage per comprendere cosa stia succedendo e quale possa essere l'impatto sui servizi in termini di interruzione, in termini di perdita di riservatezza, di integrità e di disponibilità (RID) delle informazioni ma soprattutto in termini di impatto economico.

La velocità è essenziale per determinare l'impatto ma non è una cosa che si possa fare sul momento. L'impatto si determina sulla base di considerazioni effettuate durante la **fase di preparazione**. Solitamente si dovrebbe

BIO

Massimo Cappelli è operations planning manager presso la Fondazione GCSEC, oltre che responsabile delle attività di Early Warning, Brand Protection, Information Sharing e Cyber Threat Intelligence nella struttura CERT di Poste Italiane. Nella sua passata esperienza ha lavorato come consulente in Booz Allen Hamilton e Booz &Company nella practice Risk, Relisience and Assurance.

utilizzare una **matrice di impatto** dove vengono considerati diversi parametri di valutazione (es. danni alle persone, interruzione di servizio, compromissione RID, perdita economica, perdita di immagine,…) e diversi livelli di criticità (es. verde, giallo, arancione e rosso). Sulla base del triage deve essere determinata la gravità dell'evento da cui poi scaturiranno le azioni da mettere in campo. Ecco che la multidisciplinarità entra in campo già nella fase di valutazione dell'incidente. Per essere più precisi nella fase di preparazione per stilare la matrice di impatto per la valutazione dell'incidente, gli attori che devono essere coinvolti al tavolo, oltre ai profili tecnici, sono sicuramente i *"business owner"* del servizio, il *data protection officer*, il dipartimento di comunicazione/ pubbliche relazioni, il *customer care*, affari legali e regolatorio. Tutte queste figure devono identificare congiuntamente quali siano i livelli di criticità (soglie) per ogni singolo parametro di loro pertinenza. Per ogni livello di criticità verrà poi stabilita una procedura specifica di intervento, di coinvolgimento di altre strutture e livelli manageriali e di comunicazione interna ed esterna.

Le soglie devono essere quantitative e non qualitative. Il potenziale impatto, definito sulla matrice, determina, come già accennato, le azioni da compiere. Se l'impatto è di minor portata, viene gestito solitamente all'interno della struttura tecnica/presidio SOC/CERT. Diversa è la situazione in cui l'impatto è più elevato in termini di disservizi, perdite economiche o reputazionali. In questo caso si avvia una procedura di gestione incidente che coinvolge più strutture. La multidisciplinarità ha la sua massima espressione durante una **crisi** in cui devono essere gestiti più fattori concomitanti. Tralasciando l'aspetto tecnico puramente IT e di sicurezza nella gestione dell'incidente, di seguito presento alcune **discipline** che dovrebbero essere coinvolte nella risoluzione della crisi.

Innanzitutto il *business owner* del servizio. Il *business owner* è quello che riesce a descrivere maggiormente quale possa essere l'impatto diretto di un disservizio o blocco del proprio servizio e tradurlo in perdite economiche (mancati ricavi, stallo produttivo, rallentamenti, …). Il *business owner,* durante la crisi, deve avere già le stime di quali possano essere gli impatti in base al tempo per cui il servizio è rallentato o bloccato. Per questo ci tengo a sottolineare che la maggior parte delle attività deve essere svolta durante il "tempo di pace", come la collezione di tutte le informazioni necessarie a comprendere la portata dell'evento. Più si ha una visione di dettaglio, meglio è. Se si riesce a determinare il flusso dei ricavi derivanti dal servizio, in base allo storico degli anni precedenti, in termini di periodo di riferimento (giorni, ora, etc. etc.) maggiore sarà l'accuratezza della stima. Ovviamente per servizi nuovi, la stima dovrà basarsi su una metodologia. Qualcuno potrebbe anche obiettare che non è detto che ogni periodo sia identico a quello dell'anno precedente. E' vero, ma se non si hanno altre metodologie su cui basarsi, da qualche parte dovremmo pure iniziare.

Altro aspetto e disciplina da considerare è sicuramente la comunicazione. La comunicazione riveste un ruolo chiave nella gestione degli incidenti. Se si comunica male o in ritardo si rischia l'effetto amplificatore dell'impatto. In caso di incidente è opportuno comunicare per primi e non aspettare che le voci trapelino e vengano interpretate o distorte. Il rischio è l'effetto gioco "Acchiappa la talpa" cioè si passa il tempo a smentire invece che a essere fonte primaria di informazione. I fattori principali da considerare nella comunicazione sono i **messaggi** da veicolare e i **canali** da utilizzare in base anche alla tipologia di *stakeholder (target)* da informare. La comunicazione potrebbe essere istituzionale e quindi utilizzare un formato più formale o rivolta ai clienti e quindi utilizzare terminologia più semplice.

© Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, 2012, p. 9 (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf)

La comunicazione però è monca se non si conosce il *target* a cui comunicare. Ecco che entrano in campo altre due discipline che sono il *customer care* e la psicologia/sociologia/antropologia. Il *customer care* è fondamentale per conoscere la propria clientela o gli investitori. Fattori come età, zone geografiche di appartenenza, canali preferenziali per informarsi, tipologia di prodotto/servizio acquisito sono utili a comprendere **quale canale** utilizzare e la frequenza con cui esigono essere aggiornati. La psicologia/sociologia/antropologia, non me ne vogliano gli addetti a tali discipline se le ho condensate in un unico gruppo, è utile a comprendere **quale messaggio** comunicare. Tipologie di clienti diversi potrebbero necessitare di messaggi diversi che riescano ad essere compresi dal cliente. La psicologia serve a definire un messaggio efficace che produca

l'effetto desiderato (rasserenare, allertare,…). La sociologia/antropologia è necessaria per comprendere quali effetti possono derivare dall'incidente. Una crisi può produrre degli effetti a catena, come indignazione, consenso, frustrazione che si diffondono all'interno dei gruppi sociali in maniera diversa. La fuoriuscita di notizie relative a propri dati personali potrebbe essere vissuta in maniera diversa fra un gruppo di teenager e un gruppo di media età o fra popoli di culture diverse.

Oltre agli aspetti di comunicazione, sono rilevanti anche gli aspetti contrattuali relativi alla clientela. Se sono stati definiti dei Service Level Agreement, la funzione di Business e quella di Affari Legali dovranno determinare quali possono essere le conseguenze dirette. Sia nella fase di definizione dell'impatto sia nella fase di risoluzione, sarà determinante quindi comprendere se vi siano clausole specifiche di performance da garantire, se vi siano clausole contrattuali rescissorie, se vi siano particolari indennizzi da considerare. E' importante che queste informazioni siano disponibili già in fase di analisi dell'impatto perché dovrebbero essere considerate all'interno della matrice ma spesso non è così.

L'Ufficio Regolatorio, come quello del Data Protection Officer, dovranno essere chiamati in causa per determinare se eventuali incidenti siano stati causati da inadempimenti della società e se questi inadempimenti, oltre a richiedere specifiche notifiche ai funzionari pubblici preposti o ai clienti stessi, non prevedano potenziali sanzioni.

Infine, si dovrà considerare anche la presenza del Dipartimento Acquisti. La risoluzione di un incidente potrebbe chiedere l'attivazione di contratti extra-budget e la modalità di acquisizione deve essere definita e formalizzata dall'ufficio acquisti in deroga a policy interne di approvvigionamento.

Queste sono solo alcune delle funzioni che, a mio avviso, dovrebbero essere innescate durante una crisi o incidente di alto livello. Per concludere,

ribadisco alcuni elementi fondamentali della gestione degli incidenti: definire un processo di gestione incidente olistico; definire una matrice di impatto quanto più possibile dettagliata; definire le regole di ingaggio sulla base dei livelli di criticità della matrice; testare i flussi di comunicazione fra i vari dipartimenti; effettuare esercitazioni periodiche; preparare diversi scenari di incidente con relative procedure di risposta. Tutto questo deve essere preparato in tempo di pace e pertanto richiede la collaborazione di tutte le funzioni. In futuro l'Intelligenza Artificiale potrebbe cambiare le tempistiche di risposta e anche la rilevanza di alcune funzioni rispetto ad altre ma ce ne occuperemo in altra occasione.

La continuità deriva dalla resilienza, la resilienza deriva dalla prontezza, la prontezza deriva dalla preparazione, la preparazione dal *commitment*.

Ricordiamoci che un incidente gestito male influisce sugli obiettivi aziendali di tutti. ■

"Broadcast yourself!": il digitale esprime un volto della nostra identità

Intervista VIP a Massimiliano Valerii.

Massimiliano Valerii, direttore generale Censis

Autore: Massimiliano Cannata

Otto italiani su dieci utilizzano internet, sette su dieci gli smartphone con connessioni mobili – nel 2009 li usava solo il 15% della popolazione – e altrettanti hanno un account su almeno un social network. Nel caso dei giovani under 30 le percentuali salgono significativamente. Il panorama dell'Italia digitale è in continua crescita, – spiega il direttore generale del Censis Massimiliano Valerii. "Attenti però – sottolinea – alla luce dei numerosi scandali che hanno fatto spalancare gli occhi sui rischi di violazione della privacy con la profilazione degli utenti clienti, dobbiamo renderci conto dell'importanza che rivestono le professionalità specifiche che si occupano di tutela della privacy e di sicurezza informatica". Si tratta di un ulteriore deficit con cui oggi saremo presto costretti a fare i conti.

Direttore, secondo quello che emerge nel 15° Rapporto Censis* sui media digitali e la fine dello star system *come è cambiato il rapporto degli italiani con gli strumenti della comunicazione?

Basterebbe dire che in dieci anni la spesa per *smartphone* è triplicata. Nell'ultimo anno abbiamo speso 23,7 miliardi di euro per cellulari, servizi di telefonia e traffico dati. E questo è avvenuto negli anni della crisi, mentre gli italiani stringevano i cordoni della borsa e risparmiavano praticamente su tutto. Non dimentichiamo che il valore dei consumi complessivi delle famiglie non è ancora tornato ai livelli pre-crisi. La corsa dei dispositivi della disintermediazione digitale è stata inarrestabile. Battono nuovi record anno dopo anno.

Internet e social network, sono questi gli strumenti che magnetizzano l'interesse soprattutto dei più giovani?

Oggi otto italiani su dieci utilizzano internet, sette su dieci gli smartphone con connessioni mobili – nel 2009 li usava solo il 15% della popolazione – e altrettanti hanno un account su almeno un social network. Nel caso dei giovani under 30 le percentuali salgono significativamente. Siamo entrati nell'era biomedica, caratterizzata dalla trascrizione virtuale e dalla condivisione telematica in tempo reale delle biografie personali attraverso i social network, che sancisce il primato dell'io-utente, produttore esso stesso oltre che fruitore *di contenuti della comunicazione. "Broadcast yourself!", recita il pay-off* di YouTube.

Nuovo e vecchi media a confronto, sono definizioni che reggono ancora, non stiamo rischiando di continuare a usare un vocabolario

BIO

Massimiliano Valerii si laurea in Filosofia all'Università degli studi La Sapienza di Roma. Lavora al Centro studi investimenti sociali (CENSIS) dal 2001, prima come direttore di ricerca e poi come responsabile della comunicazione, dove cura i rapporti con i media, la produzione editoriale, i contenuti web. Oggi è Direttore Generale del Centro studi investimenti sociali (CENSIS) e il curatore dell'annuale «Rapporto sulla situazione sociale del paese», che dal 1967 è considerato uno dei più qualificati e completi strumenti di interpretazione della realtà socio-economica italiana.

***vecchio e poco adatto a descrivere quelle che Baricco nel suo ultimo saggio* The Game *definisce* "tracce di una nuova umanità"?**

Questo è uno dei casi in cui l'uso dell'espressione *"mutazione antropologica"* non cade a sproposito. Perché la grande diffusione dei questi device ha modificato radicalmente i comportamenti delle persone, che oggi si abbandonano a nuovi rituali, piccoli tic e manie mascherate. Il 59% degli italiani che possiedono uno *smartphone*, invece di telefonare, preferisce inviare messaggi per comunicare. Il 55% fa parte di gruppi su servizi di messaggistica come WhatsApp. Il 51% controlla le notifiche del telefono come primo cosa al risveglio o come ultima cosa prima di andare a dormire. Il 48% consulta le previsioni meteo nel corso della giornata. Un'altra piccola ossessione quotidiana riguarda il rapporto con la memoria: il cellulare diventa una protesi utile ai nostri ricordi e alle nostre conoscenze, al punto che il 38% degli utenti, quando non ricorda un nome, una data o un evento, si affida immediatamente alle risposte della rete per fugare ogni dubbio. E il 26% non esce di casa senza portare con sé il caricabatteria del cellulare, per il timore di rimanere disconnesso.

Forse non siamo ancora un paese* "On life" *per dirla con Luciano Floridi, comunque il tempo che trascorriamo* on line *è sicuramente aumentato. E' un tempo speso bene?

Grazie ai *device* digitali le persone aumentano il loro potere individuale di disintermediazione, che significa un risparmio netto finale nel loro bilancio personale e familiare. Grazie alle piattaforme digitali scompare la mediazione tra il fornitore dei servizi e l'utente finale, visto che, per esempio, non è più necessario recarsi all'agenzia turistica per prenotare un viaggio oppure in un negozio di calzature per comprare un paio di scarpe. Usare internet per informarsi, per acquistare beni e servizi, per prenotare viaggi e vacanze, per guardare film o seguire partite di calcio, per svolgere operazioni bancarie o entrare in contatto con le amministrazioni pubbliche, significa spendere meno soldi, o anche solo sprecare meno tempo: in ogni caso, guadagnare qualcosa.

E' l'incremento degli utenti dei servizi video digitali che balza agli occhi tra i numerosi dati tutti interessanti della ricerca. Come va interpretata questa tendenza e quali sono le fasce di popolazione più interessata dal fenomeno?

È la grande novità degli ultimi anni. Gli utenti della mobile tv sono aumentati in modo impressionante, dall'1% degli italiani nel 2007 al 26% di oggi. E l'uso di piattaforma video digitali riguarda ormai il 29% dei giovani under 30. È un modo esemplare per spiegare uno dei fenomeni di trasformazione più importante dell'ultimo decennio, cioè il processo di personalizzazione dell'impiego dei media, che ha favorito la desincronizzazione dei palinsesti collettivi e la individualizzazione delle modalità di fruizione dei contenuti di intrattenimento e dei percorsi di accesso alle informazioni, scardinando tendenzialmente la gerarchia tradizionale dei mezzi, che attribuiva alle fonti professionali e autorevoli dell'informazione mainstream un ruolo esclusivo, e allo stesso tempo permettendo di affrancarsi dalla rigida programmazione oraria delle emittenti tradizionali. È un cambiamento che riguarda anche la radio (basta pensare ai servizi di broadcasting online sui siti web delle emittenti), ma che poi si è rafforzato con la comparsa sulla scena di giganti planetari come Netflix.

La *"cara vecchia radio"* ancora protagonista

A proposito. La "cara vecchia radio" rimane un fattore importante di ibridazione, mantenendo fascino ed eterna giovinezza. E' un dato che deve stupirci?

La radio è il mezzo di comunicazione di massa più antico che possediamo (la Rai trasmette programmi radiofonici da oltre novant'anni), ma ha conosciuto una seconda giovinezza perché è in grado di far fluire il messaggio radiofonico su ogni vettore. Non solo gli apparecchi tradizionali in casa o l'autoradio, ma anche via web con il pc o in mobilità con il cellulare. In più, gode di una grande reputazione. È il mezzo ritenuto più credibile e affidabile di tutti gli altri.

Il terreno di diffusione* dell'information society *è lastricato di difficoltà. La ricerca elenca puntualmente alcuni problemi, possiamo riassumere i principali?

La classifica dei principali problemi dell'era digitale secondo gli italiani riflette una visione molto individualistica, prevalentemente centrata su di sé e sull'impatto negativo che le tecnologie digitali possono eventualmente avere sul proprio vissuto quotidiano. Per il 42,5% degli italiani il problema numero uno di internet è la diffusione di comportamenti violenti, dal cyber-bullismo alle diffamazioni e intimidazioni online. Al secondo posto, il 41,5% colloca il tema della protezione della privacy. Segue il rischio della manipolazione delle informazioni attraverso le fake news e poi la possibilità di imbattersi in reati digitali, come le frodi telematiche. Colpisce che solo a grande distanza vengono citati problemi di sistema, per così dire, come l'arretratezza delle infrastrutture digitali del nostro Paese e l'inadeguatezza dei servizi online della pubblica amministrazione.

Anche le aziende italiane hanno avuto le loro difficoltà a "traghettare" nel digitale. Guardando

l'insieme della nostra realtà industriale, sul fronte dell'innovazione come sono messe le nostre imprese?

Come spesso accade in Italia, abbiamo casi di vera eccellenza e una media del sistema di impresa che invece ha maturato molti ritardi nella competizione con gli altri sistemi economici europei. Il problema riguarda soprattutto il sistema pulviscolare delle microimprese, che faticano più delle altre ad adottare i cambiamenti organizzativi e a mettere in bilancio gli investimenti necessari per implementare tutte le innovazioni tecnologiche e digitali che comporterebbero benefici in termini di efficienza e competitività.

Sicurezza, privacy e il lato oscuro di Internet

La sicurezza e la tutela della* Privacy *rimangono un grande tema. Il* Rapporto Clusit *ha evidenziato costi sempre più ingenti in Italia e in Europa, senza contare i danni sempre più alti a carico delle imprese. Qual è la tua riflessione su questo lato "oscuro" di Internet?

Abbiamo avuto un impetuoso avvio del nuovo ciclo della economia della disintermediazione digitale (dall'e-commerce all'home banking, dai rapporti in rete con le amministrazioni pubbliche alla condivisione online di beni e servizi), che determina lo spostamento della creazione di valore da filiere produttive e occupazionali tradizionali in nuovi ambiti. Perché per i cittadini e i consumatori si amplia notevolmente la gamma degli impieghi di internet, che oggi consente di rispondere a una pluralità di bisogni molto più articolati e sofisticati rispetto alla sola esigenza di comunicare, di informarsi e di intrattenersi. Si è così inaugurata una fase nuova all'insegna del primato dello *sharing* sul diritto alla *privacy*: l'io è il contenuto e il disvelamento del sé digitale è diventata la prassi comune. Ma ora ci siamo accorti che questo *trade-off* ha un prezzo troppo alto da pagare.

Cosa vuol dire in concreto?

Che i numerosi scandali ci hanno fatto spalancare gli occhi sui rischi di violazione della privacy con la profilazione degli utenti a scopi commerciali o di propaganda politica. Per non parlare poi dei danni a carico delle imprese causati dai sempre più frequenti attacchi informatici. Siamo in una fase di *impasse* e di transizione. Su questo punto saranno preziose le professionalità specifiche che si occupano di tutela della privacy e di sicurezza informatica: un altro deficit con cui oggi dobbiamo fare i conti.

A proposito di lato oscuro, l'ultimo* Rapporto del Censis *parla di un Paese che dopo il rancore rischia di cedere alla cattiveria. La Rete è un amplificatore di sentimenti spesso negativi. Come si può invertire questa tendenza?

Lo dico con una parola. Anzi, con tre: lavoro, lavoro, lavoro. Il rancore e la cattiveria che hanno invelenito il clima sociale, e che sul web trovano una espressione preferenziale, hanno delle profonde radici sociali. Dipendono dal blocco dei meccanismi di mobilità sociale e dall'assenza di prospettive di crescita, individuali e collettive. Se si supera il ristagno della crescita, anche le manifestazioni di odio degli *haters* sul web si affievoliranno.

Un'ultima domanda riguarda un nuovo trend che sembra farsi strada. Il crollo in borsa di Apple deve farci pensare che gli* Iphone*, come dice già qualche studioso, fanno già parte del passato?

Tenderei ad escluderlo. Qualcuno aveva parlato anche di "era post-pc", preconizzando la progressiva scomparsa del personal computer, che sarebbe stato sostituito dagli smartphone. In realtà, internet e le connessioni mobili sono i dispositivi d'elezione della soggettività nell'epoca contemporanea. Hanno enormemente amplificato il potere di arbitraggio individuale di ognuno. Impossibile rinunciarci nell'epoca dell'individualismo. ■

L'utilizzo delle chiavi di cifratura per la digital cloud transformation

Autore: Sergio Sironi, Sales Director Southern Europe, Gemalto

Molte aziende stanno affrontando un ulteriore passaggio della *digital transformation*, quello in cui le risorse informatiche vengono trasferite dai data center fisici verso il cloud, che prende il nome di *digital cloud transformation*. Questa trasformazione assume diverse forme: trasferimenti verso cloud privati come Dell o VMware, oppure verso provider pubblici quali Azure o Google. Nella maggior parte dei casi, si predilige una soluzione mista, quello che viene chiamato un ambiente ibrido. Un modello di questo tipo consente alle aziende di mantenere all'interno dei data center applicazioni cruciali difficili da dislocare e di beneficiare dei vantaggi di compliance, scalabilità e flessibilità offerti dal cloud.

BIO

Sergio Sironi è Responsabile della strategia di vendita ed espansione della divisione Gemalto Enterprise & Cybersecurity (ex Safenet) in Sud Europa per le regioni Italia, Malta, Spagna, Portogallo, Israele e Cipro.
Nato a Monza nel 1967, entra in Safenet nel 2014 come Country Manager con il compito di guidare la crescita dell'azienda nella regione, organizzare la distribuzione e i partner Cyber Security in Italia e Malta. Sironi ha maturato oltre 20 anni di esperienza con ruoli di crescente responsabilità nelle vendite e nel business sia in ambito italiano che internazionale principalmente nel settore Sicurezza, Enterprise Software, Hardware ed Embedded. Ha una vasta conoscenza del mercato europeo grazie a vari incarichi svolti in aziende multinazionali americane come Wind River, The MathWorks e OSIsoft dove ha ricoperto ruoli di District Sales Manager e Sales Manager per Italia, Grecia e Malta.

Nonostante questi punti a favore, però, un ambiente cloud ibrido presenta anche alcune sfide per le aziende. Tra queste, una delle più significative è quella legata al tema della protezione dei dati.

Con le informazioni che ora si diramano fra infrastrutture fisiche e virtuali, le aziende devono avere un quadro chiaro di dove sono generati e conservati i dati sensibili. Devono, inoltre, anche saper ricostruire come sono condivisi e se tale condivisione supera i confini sotto il proprio controllo. Solo in questo modo sono in grado di definire una strategia di *data protection* che rifletta realisticamente le proprie esigenze di business.

Sempre più frequentemente questa strategia comprende qualche forma di crittografia. Sarà poi una scelta dell'organizzazione decidere se applicarla a tutte le informazioni o solo ad alcuni dati specificatamente individuati, in ogni caso dovrà stabilire come gestire le proprie chiavi.

Più facile a dirsi che a farsi, perché più chiavi di cifratura vengono create per proteggere i dati diffusi, maggiori sono le sfide che l'azienda dovrà gestire. Molte, al giorno d'oggi, hanno silos dedicati alla conservazione delle diverse chiavi per diverse risorse operative come file server, database e web server. Ma una simile rete distribuita di chiavi non è la soluzione ideale per ottenere l'efficienza e il soddisfacimento dei requisiti del GDPR e di altri standard.

Quindi, cosa possono fare le aziende in risposta a queste difficoltà? Come possono implementare una gestione delle chiavi di cifratura che sia adeguata a un ambiente IT distribuito?

È importante comprendere le più recenti strategie e tendenze in materia di crittografia. Una volta che un'azienda cifra i propri dati, l'intera sicurezza aziendale dipende dalla gestione delle chiavi di cifratura, dalla capacità di generare, distribuire, conservare, ruotare e revocare/distruggerle così come necessario per un'adeguata protezione delle informazioni sensibili cui sono associate.

Un approccio centralizzato alla gestione delle chiavi è cruciale. Le aziende dovrebbero gestire e conservare centralmente ed efficacemente le chiavi di crittografia e le politiche di gestione lungo tutto il loro ciclo di vita e trasversalmente a tutta l'azienda.

Le soluzioni Gemalto, ad esempio, consentono di gestire le proprie chiavi su piattaforme di cifratura eterogenee, offrendo soluzioni proprietarie così come anche supporto nell'uso dello standard KMIP (Key Management Interoperability Protocol).

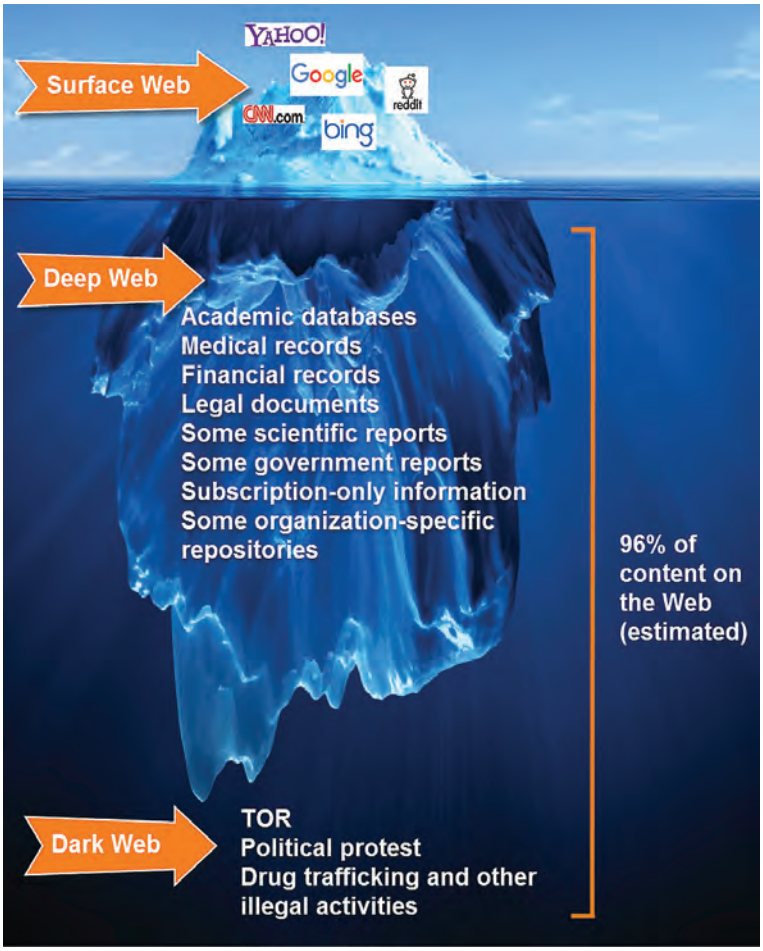
In questo modo, le funzioni preposte alla sicurezza possono monitorare, controllare e gestire chiavi e politiche di crittografia per tutti i dati sensibili, ovunque siano archiviati: cloud, archivi fisici, database o virtualmente ovunque. ■

Un tuffo nel profondo del Dark Web

Autore: Aldo Di Mattia, Principal System Engineer - Team Leader Centre/South Italy di Fortinet

Quello comunemente conosciuto come Web rappresenta solo la superficie, e si riferisce a una piccolissima parte del "www" o del cosiddetto surfing web: circa il 4%.

Gli studi rivelano che questo 4% è rappresentato da contenuti oggi indicizzati dai motori di ricerca noti, come Google e similari, rappresentando una piccolissima parte dei siti web. Da qui derivano due termini che tipicamente vengono usati come sinonimi, ma che in realtà non lo sono: uno è il **Deep Web**, che rappresenta esattamente il restante 96% dei siti che semplicemente non sono indicizzati e che non



è possibile trovare dai comuni motori di ricerca, o dei siti che sono protetti da password. Per accedere al Deep Web, quindi a questo mondo "sommerso", è necessario conoscere l'indirizzo dell'utente a memoria o disporre di credenziali specifiche.

All'interno del Deep Web, esiste il mondo del **Dark Web**. Anch'esso è un contenuto non indicizzato, ma per potervi accedere serve un'ulteriore

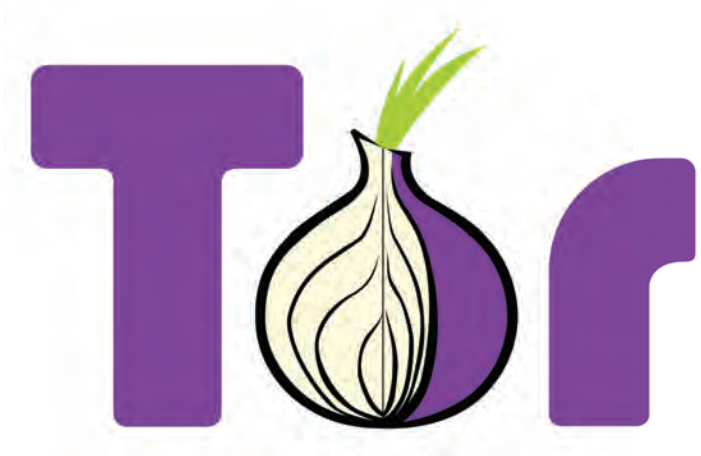
BIO

Aldo Di Mattia si è laureato in informatica all'università La Sapienza di Roma con una tesi sperimentale sulla sicurezza di rete, lavorando poi per due tra i più importanti partner Fortinet nei ruoli di System Engineer, Security Consultant e infine Senior System Engineer and Team Leader. In più di quindici anni di lavoro ha maturato importanti competenze ed esperienze nel settoree, conseguendo nel tempo più di venticinque certificazioni tecniche sui principali vendor di sicurezza informatica e la certificazione indipendente CISSP (ISC2). In Fortinet è entrato nel 2012 con il ruolo di System Engineer, e da inizio 2018 ricopre il ruolo di Principal System Engineer and Team Leader Centre/South Italy.

componente aggiuntiva, ovvero software specifici che consentono di addentrarsi nella cosiddetta DarkNet.

La più famosa e diffusa è **TOR**. Per accedervi è necessario un browser specifico, Firefox, nella versione dedicata rilasciata da TOR. Il suo nome identifica anche il motivo della necessità nel mondo di avere una DarkNet: l'acronimo sta per **"The Onion Router"**, ovvero **"il router a cipolla".** I router a cipolla servono proprio perché la crittografia che viene costruita all'interno della DarkNet è basata su una cifratura a più livelli - come una cipolla, appunto. Anche un sito in chiaro (http, https) all'interno di TOR viene cifrato a più livelli. L'obiettivo è far sì che un messaggio e il suo contenuto siano visibili esclusivamente tra client e server, quindi tra chi eroga un determinato contenuto e chi ha necessità di usufruirne, mentre tutti gli altri all'interno della rete ne sono esclusi.

Un'altra peculiarità delle DarkNet è che nessuno all'interno della rete può vedere quelli che sono gli indirizzi IP reali che nel mondo internet identificano chi è il client e dov'è fisicamente collegato (provider, nazione, città, ecc…), ovvero **dati che permettono a tutti, comprese le forze dell'ordine, di tracciare gli host**. È questa la necessità principale per cui nel mondo esistono TOR e le altre DarkNet: **rendere invisibili i sevizi**, quindi il mascheramento dell'IP e dell'identità, e la cifratura del contenuto. È un modo per accedere a determinati servizi senza lasciare traccia: da TOR è quindi possibile vedere il resto del mondo, ma non viceversa.



Il Dark Web non è, di per sé, un luogo malsano, ma è utilizzato prevalentemente per veicolare contenuti illegali. In certi Stati per esempio, dove determinati siti sono repressi, è possibile accedervi tramite TOR. Alcuni, come **Facebook**, hanno aperto un sito all'interno di TOR per dare la possibilità di accedere a persone che vivono sotto regimi che applicano la censura a siti di questa natura.

Altro esempio di siti "buoni" che hanno scelto di offrire servizi su TOR è **ProPubblica**, una piattaforma indipendente e no-profit con **lo scopo di denunciare gli abusi da parte di governi, imprese, istruzioni**: la versione .onion garantisce ai suoi lettori il completo anonimato per tutelare la loro sicurezza.

Un giro d'affari da milioni di dollari

Da numerosi studi, emerge che i maggiori contenuti diffusi all'interno del dark web sono sicuramente le frodi finanziarie, con una serie di sottodomini che vanno dalla clonazione di carte di credito, all'accesso ad account eBay e PayPal, fino ai codici di accesso a servizi di home banking.

Le analisi dimostrano anche l'esistenza di veri e propri listini: un account bancario online, per esempio, viene venduto a un prezzo tra i 200 e i 500 dollari (a seconda del saldo presente sul conto); un account PayPal o eBay si può acquistare per circa 800 dollari. Esiste quindi una vera e propria rivendita di account, ovvero conti con denaro spendibile. E ancora, documenti falsi come altro servizio frequente all'interno del dark web. Tra i servizi più diffusi negli ultimi anni c'è sicuramente quello di vendita di malware, botnet e attacchi DDoS, e anche in questo caso esistono dei listini: un documento falsificato (carta d'identità o patente) va dai 10 ai 35 dollari, un malware che permette di avere un acceso remoto costa tra i 350 e i 400 dollari, il codice di un malware bancario va dai 900 ai 1500 dollari, oppure 24h di attacco DDoS, quindi botnet a noleggio, possono valere 1500 dollari.

I servizi sicuramente più diffusi all'interno del dark web riguardano quindi la vendita di malware e attacchi a service. Ma i due più grandi, a livello di problematiche e criticità, sono la **pedopornografia** e il **terrorismo**: da un'analisi delle pagine sospette che reindirizzavano a link all'interno di DarkNet, circa 1/3 erano di distribuzione di malware, un 1/3 erano siti per anonimizzare la navigazione, e l'altro terzo erano siti di materiale pedopornografico. L'altra componente, con una percentuale molto piccola, ma sicuramente cruciale, è rappresentata dal terrorismo. In questo caso, le DarkNet vengono sfruttate per influenzare e parlare con jihadisti occidentali, o per diffondere informazioni su come acquistare armi attraverso il dark web.

Armi e droga sono poi gli altri due prodotti maggiormente venduti all'interno del dark web. Un'economia in espansione, considerando che il popolare black market Silk Road nel 2012 contava **un giro d'affari di circa 22 milioni di dollari**, a solo un anno dalla sua nascita. Si tratta di dati in crescita esponenziale.

Le aziende possono contare sulla protezione offerta da Fortinet: nei FortiGate è disponibile il database degli indirizzi IP della rete TOR (exit-node e relay-node) e degli altri proxy di anonimizzazione. Questa lista di oggetti dinamici può essere usata direttamente nelle policy firewall per bloccare la navigazione verso queste reti, e per bloccare l'accesso da queste reti ai propri servizi erogati su Internet. È inoltre possibile utilizzare profili di application control per bloccare o monitorare traffico da e verso sistemi di anonimizzazione, che in questo caso è identificato da firme a livello applicativo. ■

Cybersecurity: la prima linea di difesa contro l'impatto dell'intelligenza artificiale

Autore: Marc-André Ryter

Nei prossimi anni, il ciberspazio sarà confrontato allo sviluppo dell'intelligenza artificiale. Ciò aumenterà notevolmente l'efficacia potenziale degli attacchi informatici e costringerà tutti gli utenti del cyberspazio ad adeguare la loro protezione. Anche se in molti settori potrà beneficiare dell'intelligenza artificiale, l'esercito dovrà affrontare importanti sfide per mantenere le proprie capacità operative.

Introduzione

Lo scopo di questo articolo è quello di dimostrare l'importanza della sicurezza informatica come protezione contro i maggiori rischi che saranno generati dallo sviluppo e dall'integrazione dell'intelligenza artificiale (IA) nel cyberspazio. L'articolo si concentra sulla dimensione tecnica dell'evoluzione, ad oggi in atto, e su ciò che essa implica per le forze armate. Tuttavia, alcune considerazioni etiche o considerazioni sul ruolo dell'uomo in questo mondo di *macchine* - in senso filosofico - saranno inevitabili. Ciò che sta accadendo nel cyberspazio può portare a progressi fantastici, ma può anche diventare una grave minaccia in qualsiasi momento. I rischi che ne conseguono possono mettere a repentaglio la pace e la sicurezza internazionale.

Questa evoluzione è inevitabile e qualsiasi passo indietro è impensabile. L'utilizzo delle nuove tecnologie, in qualsiasi settore, fa parte della vita di tutti individui e della società[1] e i benefici dell'IA giustificano molti compromessi. I progressi nelle tecnologie dell'informazione sono al tempo stesso promettenti e pericolosi. I nuovi strumenti possono promuovere la libertà e lo sviluppo, il progresso e il benessere, ma anche l'oppressione, la frode, la manipolazione e il controllo. I progressi tecnologici andranno a vantaggio di tutti, dai potenti ai deboli, dalle autorità giudiziarie ai gruppi criminali. Di conseguenza, le gerarchie e le autorità possono essere rafforzate o indebolite[2]. Ciò avrà un impatto significativo sulla natura dei conflitti futuri. Se vogliamo controllare la crescita delle nuove tecnologie e soprattutto delle loro applicazioni, è importante anticipare e integrare rischi e opportunità.

L'IA rivoluzionerà la percezione e l'implementazione della sicurezza informatica, che diventerà una missione collettiva e permanente. Gli Stati e le infrastrutture critiche sono già oggi vittime di attacchi volti ad ottenere vantaggi di ogni tipo che siano essi politici, militari o economici. Lo spazio digitale è quindi già un vero e proprio spazio di confronto[3] e gli attacchi informatici sono diventati la realtà quotidiana di una specie di nuova guerra fredda[4]. Le società nel loro insieme, per via delle loro crescenti interconnessioni, diventeranno sempre più vulnerabili. I conflitti tra Stati, imprese o singoli individui potrebbero assumere forme finora ignorate. Ma una cosa è certa, che si tratti di conflitti nazionali o internazionali, politici o economici, tutti avranno una dimensione informatica sempre crescente. L'attore che riesce a

BIO

Colonnello, diplomato in Studi di politica di sicurezza e laureato in Scienze Politiche, Marc-André Ryter collabora con lo Stato Maggiore dell'Esercito svizzero per tutto ciò che riguarda la dottrina militare. Segue gli sviluppi tecnologici per le Forze Armate e gli scenari d'intervento in particolar modo per ciò che concerne la dottrina militare.
Marc-André Ryter può essere contattato all'indirizzo: marcandre.ryter@vtg.admin.ch

prendere il sopravvento nella rete otterrà il sopravvento sul suo avversario[5]. Gli attacchi informatici diventeranno più precisi e veloci. La sicurezza informatica da sviluppare in risposta a questa evoluzione deve essere vista come una costruzione di elementi multipli e complementari per creare un'architettura di sicurezza globale per il cyberspazio. Le capacità militari in questo settore possono, e devono, costituire una parte importante di questa architettura. La portata delle minacce digitali, specialmente quando vengono perpetrate con l'IA, non è ancora ben compresa. Per il momento, è necessario differenziare i rischi per le forze armate dai rischi per le aree civili così da poter immaginare quali azioni bellicose potrebbe intraprendere un aggressore.

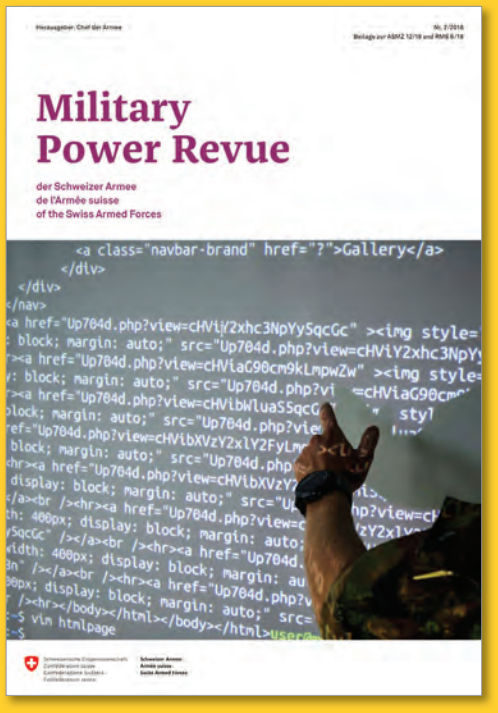
Per questo motivo le forze armate, Esercito Svizzero compreso, devono essere all'avanguardia nella sicurezza informatica.

Prevenire l'invasione del territorio da parte di forze armate straniere può essere considerato il primo livello di deterrenza. Gli aggressori potrebbero rinunciare alle loro azioni di terra se non sono stati in grado di indebolire o paralizzare le forze armate del paese bersaglio prima delle operazioni. La resilienza, che mira ad un rapido recupero della capacità di azione, deve consentire l'impegno di mezzi immediato nonostante che il soggetto sia stato sottoposto ad un attacco informatico o che abbia subito qualche danno. È quindi chiaro che le forze armate hanno un notevole interesse a contribuire alla sicurezza informatica. Le nuove tecnologie che si utilizzeranno in futuro dovranno essere sicure perché devono essere in grado di svolgere la loro missione, anche in un ambiente cibernetico degradato.

Questioni relative allo sviluppo dell'intelligenza artificiale

La sfida centrale sarà quindi quella di sapere come gestire l'evoluzione attuale e le sue conseguenze per le forze armate, poiché questa evoluzione è inevitabile. Occorre individuare i cambiamenti di paradigma, che modificheranno concretamente la natura della vita sociale e delle relazioni tra i paesi. Le caratteristiche del mondo di domani saranno la volatilità, l'incertezza, la complessità e l'ambiguità. Il potere probabilmente sarà proiettato in un nuovo mondo e i conflitti armati convenzionali, come li conosciamo oggi, saranno in futuro solo fenomeni periferici. La sfida sarà quella di trovare un modo per sfruttare al meglio l'introduzione delle nuove tecnologie, proteggendosi al tempo stesso dai grandi rischi che esse creano. In questo contesto, la sicurezza informatica diventerà un obbligo dell'intero Stato e di tutti gli altri attori che possono beneficiare delle opportunità offerte dal ciberspazio o che ne sfruttano il suo regolare funzionamento.

Figura 1: Grande centro di archiviazione dati in Islanda, che dimostra che il ciberspazio si basa anche su infrastrutture fisiche che non possono essere trascurate. (https://www.cio.com/article/2368989/data-center/100152-10-more-of-the-world-s-coolest-data-centers.html#slide8, pagina visitata li 20.07.2018)



L'articolo originale del Col. Marc-André Ryter, redatto in lingua francese, è stato pubblicato nella Military Power Revue of the Swiss Armed Forces (n. 2/2018, pp.18-28). L'esercito svizzero ha accordato alla nostra rivista l'onore di tradurlo in esclusiva e pubblicarlo in lingua italiana. Desideriamp porre i nostri più distinti ringraziamenti al Divisionario Urs Gerber, redattore capo della Military Power Revue, e al Colonnello Marc-André Ryter per la loro disponibilità e per il sostegno accordatoci. Tutti i volumi della Military Power Revue of the Swiss Armed Forces sono gratuitamente fruibili e scaricabili dal sito dell'Esercito Svizzero: http://www.vtg.admin.ch/en/media/publikationen/military-power-revue.html

Nel complesso, la minaccia principale deriva dal fatto che tutte le azioni avviate nel cyberspazio possono causare danni concreti anche negli spazi fisici, colpendo la popolazione civile, o addirittura causando vittime. Devono essere quindi previste le minacce che non esistono ancora e che saranno il risultato dello sviluppo delle nuove tecnologie e dell'IA. La minaccia informatica deve essere posta allo stesso livello della minaccia dei missili balistici o del terrorismo internazionale, per non parlare del fatto che tutte queste minacce possono essere combinate tra loro. Gli attori "non statuali" avranno la capacità di produrre gli stessi effetti degli attori statuali. Tuttavia, occorre tenere presente che gli attacchi, che hanno il potenziale di compromettere la sicurezza nazionale e la stabilità di uno Stato, richiedono risorse considerevoli.

I sistemi devono essere protetti nel loro insieme. Senza protezione, un aggressore può disturbare o interrompere molti servizi essenziali per la popolazione, come la distribuzione di acqua o elettricità, o gli scambi in generale. Ciò può portare rapidamente a gravi disordini sociali. Non sorprende quindi che gli attacchi informatici russi in Ucraina nel 2014 abbiano interessato centrali elettriche, banche, ospedali e sistemi di trasporto, nonché il corretto svolgimento delle elezioni. Gli esperti di teoria dei sistemi ritengono che se il 37% di un'infrastruttura viene distrutta, non funzionerà più. Secondo la *"Revue Stratégique"*[6], è possibile valutare la gravità di un attacco secondo 4 criteri[7]. In primo luogo, è necessario (1) valutare il danno che potrebbe essere arrecato agli interessi fondamentali del paese, (2) analizzare le conseguenti violazioni della sicurezza interna, quindi (3) stimare i danni alla popolazione e all'ambiente e infine (4) all'economia.

Si può dire ad oggi che l'IA svolgerà certamente un ruolo importante nella sicurezza, sia in termini di capacità di difesa che di necessità di attacco. Per alcuni compiti e ruoli nel mondo della sicurezza, l'IA supererà molto probabilmente la capacità umana e porterà sicuramente nuove scoperte andando a controllare nuove tecnologie in una misura che va oltre le possibilità antropiche.

Il ruolo dell'IA per machine learning / deep learning è essenziale. I rapidi progressi in un'ampia gamma di applicazioni si ottengono attraverso l'apprendimento automatico, molto più che attraverso la programmazione. L'intelligenza artificiale permetterà una fusione di mondi reali e virtuali per ottenere una migliore rappresentazione dell'ambiente. Questo apre nuove opportunità di formazione basate sulla maggiore capacità di raccogliere dati, analizzarli molto più rapidamente e sfruttarli istantaneamente.

Figura 2: Migliori capacità di analisi delle immagini con l'IA, che consentirà una migliore preparazione delle operazioni. (https://publiclab.org/wiki/near-infrared-camera, pagina visitata li 30.05.2018)

È prevedibile che l'IA aumenterà le minacce in tre modi diversi: espanderà e diversificherà le minacce esistenti, introdurrà nuove minacce e cambierà il carattere e la natura delle minacce note[8]. Gli attacchi saranno più efficaci, più precisi, più difficili da attribuire ai veri responsabili e sfrutteranno sistematicamente tutte le vulnerabilità. L'IA fornirà anche capacità alle forze armate di identificazione di obiettivi umani (comandanti militari) o la navigazione autonoma. Sarà possibile realizzare campagne di disinformazione su larga scala con una portata inimmaginabile.

Figura 3: Miglioramento delle possibilità di creare immagini generate dal computer per disinformazione. L'originale è a sinistra, l'immagine creata a destra (https://interestingengineering.com/ai-software-generate-realistic-fake-videos-from-audio-clips, pagina visitata li 30.05.2018).

Di conseguenza, l'aumento dell'efficienza sarà una delle principali caratteristiche dei futuri attacchi nel cyberspazio che quindi, saranno preparati ancor meglio e con molta più attenzione[9]. Grazie all'impegno dell'IA, gli attacchi saranno personalizzati e fatti su misura per raggiungere l'obiettivo desiderato. Di fronte a questo nuovo potenziale, l'interoperabilità tra esseri umani e macchine sarà una grande sfida. Una grande sfida connessa quindi sarà quella di trovare la migliore combinazione tra uomo e macchina. Occorre mantenere un certo livello di semplicità in modo che le informazioni possano essere utilizzate rapidamente dagli esseri umani. Troppe informazioni possono rivelarsi controproducenti, a tutti i livelli, in tutte le funzioni se fornite contemporaneamente, soprattutto nei comparti militari.

Una sorta di guerra meccanica, sistemi contro sistemi, non rappresenta fantascienza nel campo della sicurezza informatica. Le macchine d'attacco devono essere in grado di difendersi contemporaneamente da contrattacchi estremamente rapidi provenienti da sistemi precedentemente identificati.

I Robot sono divenuti importanti per la sicurezza in base a tre fattori principali[10]. In primo luogo il loro sviluppo e impiego. I robot infatti si stanno diffondendo e stanno divenendo un fenomeno globale. In secondo luogo la loro adattabilità ai più svariati usi che rappresenta un vero problema di sicurezza, e infine loro l'autonomia, il fattore più rischioso. È infatti possibile che la macchina voglia ribellarsi al controllo del soldato, e voglia portare a termine la missione nel modo che le sembra più razionale. Il controllo da parte dell'uomo potrebbe quindi apparire per la macchina come un elemento distruttivo e pericoloso e che quindi deve essere eliminato per portare a termine la missione. Uno dei maggiori pericoli di questa evoluzione è che alcune decisioni, che richiedono reazioni molto rapide e indiscutibili, potrebbero essere delegate all'IA come ad esempio l'impiego di missili o di armi nucleari[11].

L'IA aumenterà anche l'efficacia degli attacchi informatici APT (Advanced Persistent Threats), che sono i più comunemente usati per lo spionaggio industriale. Questi strumenti sono molto utili per spiare le reti delle forze armate classificate perché sono difficili da localizzare. Grazie a questi APT, gli attori non statuali aumenteranno la propria capacità offensiva proprio come gli attori statali nel campo dello spionaggio.

Ma l'IA ha anche un impatto positivo sull'aumento della sicurezza. Esso apre nuove prospettive sulla capacità di rilevazione, contrasto e risposta agli

attacchi informatici, anche quando il vettore di questi è ancora sconosciuto. L'IA è già coinvolta nel rilevamento di anomalie e malware nel cyberspazio.

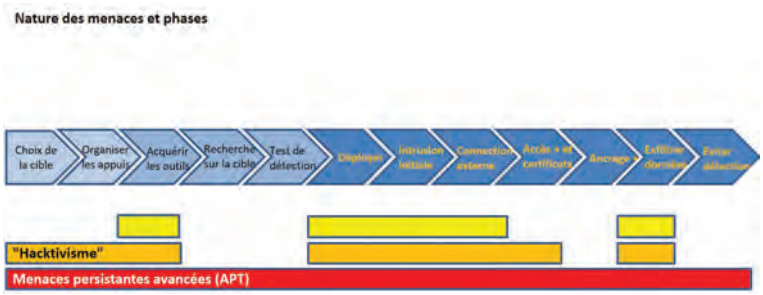


Figura 4: Evoluzione della complessità della minaccia attraverso i PTA, con le loro componenti e fasi.

Impatto sulle forze armate

Di fronte alla notevole minaccia potenziale rappresentata dall'uso dell'IA nel cyberspazio, le forze armate devono essere pronte a sostenere le autorità civili in caso di una grave destabilizzazione della società. Nella maggior parte dei casi, i rischi per le forze armate devono essere dedotti dai rischi per le aree civili, al fine di immaginare quali azioni dolose potrebbe intraprendere un aggressore. Sarà necessario un ambiente sicuro nel ciberspazio, in modo da poter integrare gli sviluppi positivi e da evitare che il loro potenziale generi disastri. Considerando le opportunità e i rischi potenziali, si tratta di definire il modo migliore per le forze armate per sfruttare le opportunità e proteggersi dai rischi. In primo luogo, devono garantire il loro corretto funzionamento al fine di fornire servizi di sicurezza a vantaggio dello Stato.

Figura 5: Esempio di esperti cyber delle forze armate israeliane (IDF). (https://www.blick.ch/storytelling/2018/zukunft/index5.html, pagina visitata li 08.08.2018)

Sicuramente inizierà un nuovo dibattito. Per quanto riguarda i conflitti e i combattimenti, gli sviluppi in corso e le nuove tecnologie si trasformeranno in mezzi per causare ancor più danni attraverso una maggiore precisione ed efficienza nella realizzazione dell'obiettivo. Questi nuovi sistemi permetteranno di distruggere i mezzi dell'avversario in modo più efficace. In questa logica, le nuove tecnologie sono utilizzate solo come vettori per migliorare ciò che è già possibile oggi. Se cambiamo paradigma, è ovvio che dobbiamo chiederci se un nemico può essere sconfitto senza nemmeno combatterlo, con altri mezzi.

Penetrare una rete può anche essere più vantaggioso dell'introduzione di un nuovo insieme di armi. La distruzione fisica dell'avversario non sarebbe quindi né necessaria né fine a se stessa e la natura stessa della guerra non solo evolverà, ma cambierà completamente. L'IA e le armi informatiche hanno un alto grado di flessibilità che consentirà grazie al loro impiego di produrre un'ampia gamma di effetti. L'energia sarà proiettata in un nuovo modo e i conflitti, così come li conosciamo, tenderanno a diventare fenomeni periferici, spesso guidati da intermediari. In questo nuovo tipo di lotta, le possibili conseguenze per le popolazioni civili non appaiono ancora chiare.

Evoluzione della natura dei conflitti e delle forze armate

Di conseguenza, sorgono molte domande sulla natura mutevole dei conflitti. La questione fondamentale è se la guerra informatica diventerà la guerra del futuro, ancor più del confronto con i sistemi d'arma robotica. Questo avrebbe conseguenze molto importanti per la dottrina. L'avversario potrebbe essere sconfitto da azioni nel cyberspazio che lo priverebbero dell'uso di tutte le sue infrastrutture critiche e gli impedirebbero di agire. In secondo luogo, non è chiaro se le armi nucleari e i sistemi d'arma con effetti devastanti saranno ancora utili. Potrebbe infatti essere possibile bloccare la capacità di impegnare quest'ultime attraverso il cyberspazio, o renderle inefficaci. Analogamente, le armi informatiche potrebbero, se necessario, causare tanti danni quanto le armi nucleari. In tal caso, la capacità di sviluppare azioni nel cyberspazio diventerà la chiave del successo, una sorta di deterrente per il futuro. Ciò implica che l'intimidazione di un avversario e la dimostrazione della forza avverrà attraverso il cyberspazio e attraverso azioni che, almeno in una prima fase, avranno probabilmente un impatto scarso o nullo sulla popolazione civile. Ma nel caso di paralisi di interi settori dell'economia di un paese, lo scoppio volontario di disastri tecnologici o ecologici, con molte vittime, o anche durante la manipolazione grossolana del processo democratico, è probabile che siano annunciati veri e propri atti di guerra.

La difesa nel ciberspazio deve quindi far parte degli strumenti di tutte le forze armate se si vuole che esse assolvano la loro missione di difesa e protezione della popolazione civile. La dimensione informatica è una dimensione crescente di tutti i compiti svolti dall'esercito, dalla pianificazione della condotta, alle infrastrutture e ai processi. Tutti gli elementi del cyberspazio svolgono un ruolo di moltiplicatore delle forze coinvolte[12]. Di particolare interesse è il fatto che gli attacchi informatici non solo sono accurati, ma anche molto veloci (velocità della luce). Le forze armate occidentali, che fanno ampio uso di nuove tecnologie impiegate in tutto il mondo, si confrontano costantemente con i rischi associati al loro uso nel cyberspazio. Tale impiego è spesso un prerequisito per lo svolgimento delle loro operazioni, come il consolidamento della pace o gli impegni umanitari in zone remote.

L'importanza del cyberspazio nella pianificazione e nello svolgimento delle operazioni è spesso sottovalutata,

nonostante il fatto che grazie ad essa molti obiettivi militari possano essere raggiunti. E' possibile disturbare e interrompere scambi di dati (comunicazioni di ogni tipo), impedirvene l'accesso, corromperli o danneggiarli infettandoli o rendendoli inutilizzabili. Ma l'obiettivo può essere più facilmente quello di distruggere parte dei dati nei computer o addirittura compromettere le banche dati o bloccare le reti. In generale, è possibile considerare l'implementazione di un malware nei sistemi informatici dell'opponente come un'assicurazione in caso di attacco, o come una preparazione a lungo termine per i casi di contrasti o controversie. In questo caso, c'è un forte interesse a non rilevare l'attacco. D'altro canto, se uno Stato utilizza armi su larga scala nel cyberspazio, con l'intenzione di causare danni significativi al suo avversario, lo fa con una certa finalità, e quindi non ha necessariamente interesse a rimanere nascosto. Al contrario, si rivelerà per ottenere ciò che sta cercando[13].

L'intelligenza artificiale come sfida per le forze armate

Gli attacchi nel cyberspazio saranno sempre più utilizzati perché il tempo, la distanza, la velocità e il ritmo non hanno più un ruolo primario non costituendo più vincoli e potendo anche essere automatizzati. È possibile che gli effetti prodotti dalle azioni nel cyberspazio contro avversari non convenzionali possano essere più difficili da ottenere, o più limitati, se questi ultimi non sfruttano le reti informatiche per i propri processi e i propri sistemi d'arma. Nel caso dell'Ucraina nel 2014, il mantenimento di alcuni controlli manuali ha reso più agevole la reazione dopo un attacco informatico all'infrastruttura di produzione di energia elettrica. Gli attacchi informatici contro l'Estonia, la Georgia e l'Iran non sono stati percepiti da questi paesi come un attacco militare in quanto tale e quindi non hanno avuto alcun impatto sulle loro forze armate. Si tratta di una questione di interpretazione, poiché la distruzione di una capacità chiave si può ritenere sia un attacco all'intero paese. Occorre anche considerare l'importanza che il cyberspazio ha a seconda delle fasi di un conflitto o se, al contrario, tale importanza persiste, eventualmente anche dopo la fine delle ostilità. Sarebbe quindi sbagliato considerare il cyberspazio come uno spazio operativo utilizzato solo o principalmente durante le fasi iniziali di un conflitto e altrettanto che le opportunità, quindi l'importanza del cyberspazio, diminuiscano durante il conflitto.

Nonostante le considerazioni di cui sopra, ci sono ancora alcuni autori che ritengono che la minaccia della cyber-guerra non sia una minaccia grave per le forze armate.

Essi percepiscono le azioni nel cyberspazio come misure parallele al conflitto tradizionale o addirittura ibrido, mentre gli scambi nel cyberspazio sono descritti come schermaglie. Per questo motivo è necessario esaminare in dettaglio l'impatto che l'IA potrebbe avere sulle forze armate. Le conseguenze rivoluzionarie dell'IA sulla sicurezza costringeranno le forze armate a fare un salto di qualità. Non saranno più in grado di accontentarsi delle evoluzioni qualitative per adattarsi ai nuovi prodotti.

In particolare, l'IA e l'e-learning avranno implicazioni decisive per la sicurezza informatica e la guerra informatica. Per quanto riguarda la condotta di un conflitto, il salto qualitativo deve essere considerato alla stregua di quello che si è verificato con l'emergere dell'aviazione.

Più che nello svolgimento di combattimenti dinamici, le forze armate con l'IA avranno un importante vantaggio nell'adempimento della loro missione di sicurezza sociale. L'intelligenza artificiale analizzerà e fonderà l'enorme volume di dati. In particolare nel campo dell'intelligence, le attività che attualmente richiedono molte persone, potranno essere automatizzate. L'esercito avrà una maggiore capacità di raccogliere dati, analizzarli molto rapidamente e utilizzarli immediatamente. La lotta per la superiorità nello spazio dell'informazione diventerà feroce, decisiva.

L'IA genererà opportunità di formazione in mondi che combinano informazioni reali ed elementi virtuali e consentirà, anche a distanza, un livello di prontezza operativa senza precedenti. L'intelligenza artificiale può quindi rivelarsi uno strumento prezioso nella fase iniziale dei conflitti o quando magari un attore non vuole o non è in grado di impegnare truppe per raggiungere l'obiettivo.

Lo spionaggio di sistemi nemici, come misura preparatoria al combattimento, diventerà sempre più importante e sarà il primo passo di una guerra. Questa raccolta di informazioni servirà come base per attività di sovversione, come la mobilitazione a fini politici e l'influenza sull'opinione pubblica, compresa la manipolazione delle informazioni. Sarà inoltre utilizzato per preparare il sabotaggio di impianti, sistemi d'arma, infrastrutture critiche, e il disturbo o la compromissione della natura delle comunicazioni[14]. Tutte azioni, queste, che indeboliscono l'avversario e quindi preparano il campo di battaglia. D'altro canto però è sbagliato assumere che tutte le guerre cominceranno sistematicamente con una fase di guerra informatica, poiché attori isolati saranno sempre in grado di agire direttamente ricorrendo ad azioni violente.

Anche nel campo dei materiali e delle attrezzature in generale, l'IA avrà un impatto importante. Consentirà di controllare le nuove tecnologie molto meglio degli esseri umani. Le nuove capacità dei robot combinate con l'intelligenza artificiale permetteranno di colpire con una precisione millimetrica[15]. La programmazione dei sensori, soprattutto quando possono innescare una risposta automatica, sarà migliorata e diventerà cruciale e concreta. L'automazione accoppiata con l'IA permetterà lo sviluppo di *"fire and forget"* con applicazioni su un gran numero di sistemi; da qui la necessità di sviluppare in parallelo le capacità di controllo umano sull'impiego di queste armi. Le forze armate vorranno sfruttare appieno i vantaggi delle macchine nello svolgimento dei combattimenti. Allo stesso tempo, si parla anche di materiali che non solo sono più leggeri e più isolanti, ma che potrebbero anche cambiare forma e colore. Se questi materiali sono combinati con l'intelligenza artificiale, c'è un grande potenziale per il loro uso, in particolare nel camuffamento, ma anche nel migliorare le prestazioni dei soldati.

Le possibilità dell'intelligenza artificiale nello svolgimento delle operazioni militari

La combinazione della massa di dati disponibili e dell'IA nel cyberspazio indebolirà la volontà di resistere da un punto di vista psicologico. Questa

capacità sarà utile sia per la difesa che per l'attacco. In generale, la progettazione degli attacchi sarà sempre più accuratamente adattata all'obiettivo per garantirne la sua efficacia. Pertanto, nel campo della disinformazione, le possibilità che questi attacchi avvengano si amplificherà e la loro diffusione si realizzerà ad un ritmo molto rapido. L'IA diventerà così un supporto essenziale per lo svolgimento delle operazioni, soprattutto a causa del suo elevato potenziale analitico. L'IA apre nuove dimensioni a questi potenziali miglioramenti, soprattutto nella ricerca delle vulnerabilità dei sistemi opposti.

Figura 6: Foto di ricognizione militare con Interpretazione accurata e automatizzata. (https://www.38north.org/2017/10/udmh102517/ , pagina visitata li 30.05.2018)

L'IA consentirà inoltre di sviluppare supporti ai combattenti attraverso sistemi autonomi. L'estensione della capacità di svolgere autonomamente le missioni sarà una caratteristica della futura forma di combattimento. L'umano, attraverso l'IA, cercherà di reagire ai cambiamenti più velocemente e meglio dell'avversario, il che gli procurerebbe un guadagno sostanziale sul campo di battaglia.

L'IA permetterà di combattere contemporaneamente una moltitudine di sistemi, nel mondo reale e virtuale, e permetterà il contrasto di una successione di attacchi ravvicinati e di diversa natura. Sarà in grado di coordinare le difese, stabilire le priorità e agire con estrema rapidità. L'intelligenza artificiale consentirà, altresì, una migliore analisi degli obiettivi potenziali, soprattutto attraverso controlli incrociati delle informazioni. Ciò vale anche per l'analisi delle immagini collegate ad altri dati come ad esempio l'identificazione delle infrastrutture critiche e il momento migliore per attaccarle. Questo potra avvenire ibridamente sia attraverso attacchi informatici che attacchi convenzionali.

Ma l'intelligenza artificiale può supportare le truppe anche in aspetti meno tecnici, ad esempio nel campo della psicologia con analisi di contenuti violenti che minano il morale delle truppe.

Nel campo della protezione fisica, riduce i rischi, in particolar modo per le ricognizioni nelle zone nemiche o per lo sminamento, operazione queste che potranno essere effettuate da robot.

Sarà possibile preservare gli esseri umani assegnando compiti «3D» *(dirty, dull and dangerous, i.e. sporchi, opachi, pericolosi)* a macchine dotate di IA. Anche il processo decisionale può essere migliorato con l'IA, così come il collegamento di diverse unità, la simulazione operativa per la preparazione delle operazioni. Aumenterà l'efficienza e le prestazioni dei sistemi di combattimento e verranno semplificate le funzioni logistiche di supporto, soprattutto nella manutenzione. Proprio per tali ragioni i computer con IA diventeranno sempre più sistemi d'arma. Le armi informatiche diventeranno così una sorta di super-armi di disturbo[16] e di indebolimento.

Tuttavia, ci sarà sempre una grande differenza tra la sicurezza, che può essere migliorata nelle aree urbane o in alcune infrastrutture come stazioni o aeroporti, dove sono installati un gran numero di sensori come le telecamere di sorveglianza e le cui immagini sono disponibili e possono essere analizzate, e il combattimento dinamico in un ambiente in cui non sono disponibili sensori fissi.

Data la portata dell'azione, durante un'operazione, l'installazione su larga scala di sensori continuerà ad essere un ostacolo che lascerà inevitabilmente spazio a sorprese.

A causa della crescente integrazione dell'IA nei sistemi delle forze armate, il campo di battaglia subirà diversi cambiamenti. In primo luogo, in tutti i settori ci sarà un rimpiazzo su larga scala degli esseri umani con robot autonomi, dalla logistica al combattimento.

Naturalmente, questi robot avranno diversi gradi di autonomia a seconda dei loro compiti. Si tratterà di determinare per ogni compito quale sia il grado minimo di controllo umano richiesto. A lungo termine, gli aerei da combattimento diventeranno parzialmente obsoleti e potranno essere sostituiti da sciami di droni per missioni ben definite.

Questa tendenza sarà sostenuta dal forte calo del costo dei droni. Per le forze di terra si dovrà trovare una soluzione per poter reagire ad un attacco di centinaia o migliaia di droni. Analogamente, cariche esplosive improvvisate diventeranno armi di precisione, moltiplicando il potenziale di qualsiasi gruppo terroristico, ad esempio con un'auto kamikaze che viaggia autonomamente.

Il potenziale dei gruppi armati di destabilizzare una società, come parte di una strategia ibrida, aumenterà. Questi gruppi potrebbero utilizzare robot per effettuare assassinii automatizzati su larga scala di funzionari militari, politici ed economici. Tuttavia, l'IA sarà anche in grado di sostenere il disarmo di questi gruppi identificando le transazioni sospette e, più in generale, identificando potenziali terroristi attraverso l'analisi di blocchi di infomazione. Le difese passive e attive potranno essere migliorate anche per obiettivi di alto valore come le infrastrutture critiche (armature, difese attive, radar UAV, ecc.).

L'apprendimento più o meno automatizzato dell'IA sarà una materia centrale. Una importante vulnerabilità si avrà non appena un aggressore riesce a violare un determinato processo di apprendimento.

Ciò può essere ottenuto aggiungendo elementi di disturbo, come false informazioni su cui si basa l'apprendimento o modificando leggermente la percezione dell'ambiente da parte delle macchine per causare comportamenti diversi e potenzialmente pericolosi.

Ad esempio, il riconoscimento di amici-nemici può essere invertito nella fase di apprendimento o si possono predisporre i sistemi d'arma autonomi, per colpire specificamente i civili.

L'apprendimento automatizzato diventerà un obiettivo in sé, poiché sarà interessante sabotare il potenziale dell'avversario da questa fase, rallentare le capacità di miglioramento dei sistemi d'arma autonomi e spiare o prevenire l'assunzione di funzioni sempre più importanti da parte dei robot con l'IA[17].

Nonostante ciò, l'IA ci costringerà a dare maggiore autonomia alle macchine, per permettere loro di utilizzare il potenziale, soprattutto per quanto riguarda la velocità delle loro reazioni. In questo senso, l'essere umano diventerà un fattore di rallentamento. Se limitassimo l'autonomia e la velocità delle macchine per garantire un miglior controllo, corriamo il rischio che l'avversario sia più veloce. Non ci sarà quindi alcuna scelta e si paventerà il rischio reale che gli esseri umani diventino spettatori di interazioni tra macchine, fino ad includere le battaglie tra loro.

L'esempio dei droni è significativo. L'aumento esponenziale del loro numero per i compiti più diversi è problematico perché aumenterà il rischio di azioni incontrollate. In ultima analisi, si tratterà di individuare i sistemi d'arma che non possono funzionare senza il supporto dell'IA, proprio per adottare misure di protezione adeguate e garantire la ridondanza di tali sistemi.

Le vulnerabilità dell'intelligenza artificiale

La crescente integrazione dell'IA nei sistemi e nei processi dell'esercito solleva molti interrogativi sui possibili effetti negativi e sulle misure necessarie per tenere sotto controllo i rischi. L'obiettivo finale è quello di impedire che sistemi o processi militari siano distolti dal loro uso primario. In generale, il tema è come un ambiente cibernetico degradato possa interferire con la capacità delle forze armate per portare a termine la missione partendo dalla mobilitazione per arrivare al combattimento.

È possibile che gli sviluppi tecnologici, o la loro implementazione nell'esercito, possano essere ostacolati a causa dei rischi connessi. Non appena si parla di armamenti e controlli, più o meno automatizzati, dobbiamo essere in grado di garantire che il controllo sia mantenuto, o che si escluda un'acquisizione o una riprogrammazione da parte dell'avversario. Sarà quindi particolarmente importante rafforzare la sicurezza e la protezione dei sistemi[18].

Le vulnerabilità saranno attivamente ricercate e inevitabilmente attaccate. L'integrazione dei sistemi di IA nelle forze armate sarà soggetta a vincoli significativi ma inevitabili. Una sfida importante sarà quella di trovare la migliore combinazione tra uomo e macchina, per sfruttare al meglio le potenzialità dell'intelligenza artificiale e le sue sinergie. Si tratta di combinare nel modo più rapido possibile l'identificazione delle opportunità e la decisione sulla migliore opzione d'azione e in ogni caso più veloce dell'avversario; tutto questo in modo ripetuto[19].

È importante, soprattutto, evitare che la macchina neutralizzi le funzioni umane o di controllo se non è d'accordo, qualsiasi motivo esso sia, con la decisione dell'uomo. Questo non sarà certamente sempre facile, specialmente in aree in cui l'IA supererà l'intelligenza umana. Gli esseri umani dovrebbero sforzarsi di mantenere al centro la sicurezza delle popolazioni tenendo conto dell'IA.

Per il momento, l'IA dipende ancora da fattori di apprendimento che sono perlomeno iniziati dagli esseri umani. La capacità dell'intelligenza artificiale di reagire e risolvere situazioni nuove e inaspettate, essenziale per le forze armate, sarà un settore prioritario per lo sviluppo. Ciò dimostra tuttavia che sarà necessario sviluppare un nuovo sistema specifico di controllo degli armamenti per le armi autonome, soprattutto per quelle con effetti letali. Dobbiamo fare in modo che gli esseri umani possano disabilitare urgentemente un sistema autonomo che si discosta dalla sua missione. L'IA potrebbe causare problemi inaspettati a causa di effetti imprevedibili causati dalla velocità e dall'accumulo di interazioni. Nel contesto di questa inevitabile evoluzione, la responsabilità ultima per l'impiego di armi autonome deve rimanere in ogni caso con gli esseri umani, e non ci deve essere disimpegno[20].

Uno dei maggiori pericoli insiti in questa evoluzione è che alcune decisioni, che richiedono reazioni molto rapide e indiscutibili, potrebbero essere delegate all'IA, come l'impiego di missili o di armi nucleari[21]. L'IA potrebbe quindi portare ad una nuova corsa agli armamenti, poiché tutti gli attori vorranno migliorare i loro sistemi d'arma con il potenziale dell'IA. L'uso crescente dell'IA sarà quindi un'evoluzione inevitabile, in primo luogo per i suoi benefici, ma anche con tutte le conseguenze nel campo della protezione. Gli esseri umani diventeranno meno determinanti e, allo stesso tempo, le macchine detteranno il ritmo del combattimento in tutte le aree operative e, soprattutto, ne influenzeranno direttamente il risultato. Gli esseri umani dovranno trovare un modo per mantenere il controllo del processo ed eventualmente porre dei limiti alle macchine o alla loro assistenza. Una guerra che utilizza missili autoguidati, carri armati e droni armati, possibilmente guidati a distanza, è un'opzione che deve essere presa in considerazione. Potremmo vedere una sorta di "disumanizzazione" delle guerre del futuro.

Nella conduzione delle operazioni, la tutela delle comunicazioni ha sempre svolto un ruolo essenziale. Tutto ciò ha un impatto positivo solo se è possibile garantire il funzionamento delle proprie comunicazioni allo stesso tempo.

Si può quindi presumere che l'eliminazione delle forze dell'avversario al fine di accaparrarsi la decisione perderà ancora più importanza a favore invece della capacità di raggiungere il cuore del sistema nemico, i suoi centri di gravità, o di attaccarlo per paralizzarlo.

La capacità di riconoscere le finestre di opportunità sarà sempre più importante e decisiva.

Figura 7: I radar sono utilizzati per monitorare continuamente le attività, compresi gli attacchi nel cyberspazio (https://www.journaldugeek.com/2015/01/16/pal-la-cyberguerre-cest-pour-demain/). (pagina visitata li 15.08.2018)

Le «finestre» di opportunità possono essere create «accecando» o ingannando l'avversario. I sistemi di comunicazione delle forze armate contrapposte diventeranno quindi sempre più infrastrutture critiche essenziali. Il loro attacco e la loro distruzione sicuramente paralizzerebbero e quindi sconfiggerebbero gli avversari in un mondo in cui la competenza informativa e la capacità di manipolazione della stessa rappresenterà il vero potere.

La superiorità dello spazio di informazione sarà raggiunta attraverso una maggiore capacità di raccogliere dati, analizzandoli molto rapidamente e utilizzandoli immediatamente sul campo di battaglia. Ci saranno più fonti e sarà più facile diffondere informazioni false o influenzare le decisioni dell'avversario. La propaganda, l'inganno e l'ingegneria sociale, cioè la manipolazione psicologica su larga scala, saranno ottimizzati. Questo servirà anche a confondere l'avversario, interrompendo la sua percezione della situazione più sicuramente che distruggendo il suo equipaggiamento e i suoi sistemi d'arma. Le strutture di comando verticale lasceranno sempre più spesso il posto a strutture in rete altamente flessibili per integrare la cooperazione permanente o temporanea con nuove componenti. Ci saranno quindi certamente cambiamenti significativi anche nell'analisi dei centri di gravità e nella pianificazione degli obiettivi.

Sarà inoltre necessario un equilibrio nel settore delle armi informatiche e del sostegno all'IA che consentirà, come quella nucleare, una nuova forma di deterrenza informatica. Il periodo di transizione tra lo sviluppo di nuove capacità e l'equilibrio delle risorse sarà rischioso. Occorre tener conto del fatto che le applicazioni militari dei sistemi civili di IA non sono così facili da realizzare. La natura della duplicazione di queste tecnologie sarà un fattore importante, eventualmente anche limitante. Una delle dimensioni importanti per l'impegno di sistemi d'arma autonomi è il danno collaterale che potrebbero causare. Spesso si tratta di bilanciare gli interessi in gioco in questo campo, in un contesto che può evolvere ogni secondo. Non si tratta quindi solo della correttezza delle informazioni disponibili, ma di una valutazione di un sistema globale, con un'unica azione che può avere un impatto strategico. La questione dell'autonomia comprende anche la dimensione della responsabilità in relazione alla condotta e alle conseguenze degli impegni di sistemi d'arma autonomi. Alla fine, possiamo immaginare che nel contesto della difesa attiva, uno Stato possa reagire con una risposta solo parzialmente militare, cibernetica e non cibernetica, a cyber-azioni aggressive contro i suoi interessi.

Di fatto, una protezione informatica funzionante e le capacità informatiche consentono all'esercito di svolgere i propri compiti, quindi di condurre le operazioni possibilmente in modo ancora più efficiente e a costi inferiori[22].

L'importanza della difesa informatica per l'Esercito Svizzero

Una difesa informatica efficace e la protezione dei sistemi diventeranno nei prossimi anni la pietra angolare dell'effetto deterrente dell'Esercito Svizzero. Un avversario che non riesce a indebolirla con attacchi cibernetici ci penserà due volte prima di impegnarsi ulteriormente, coinvolgendo rispettivamente i suoi mezzi terrestri e aerei. La sicurezza informatica è essenziale come prima linea di difesa, in quanto può essere una forma di deterrenza contro gli attacchi negli spazi fisici il che non va tuttavia confuso con il concetto di deterrenza nucleare. L'obiettivo è quello di convincere un avversario a rinunciare a un attacco contrastando le operazioni preparatorie nel cyberspazio e nello spazio dell'informazione. Le misure che contribuiscono a questa convinzione devono pertanto essere promosse attivamente. Ciò è particolarmente vero nel caso in cui un avversario scelga una strategia ibrida, che inizia tramite l'indebolimento mirato dello Stato e delle sue forze armate attraverso la dimensione del cyberspazio. È necessario rendere difficile la vita di un potenziale aggressore aumentando i mezzi necessari per il proprio successo. La Svizzera, che non dispone più di un esercito di massa per scoraggiare un potenziale avversario, deve essere all'avanguardia della sicurezza informatica per proteggere i propri sistemi d'arma e le infrastrutture critiche, in modo da non essere indebolita prima di un conflitto. Avere sistemi che utilizzano l'IA possono anche essere un deterrente[23].

La dipendenza dell'Esercito Svizzero dalle infrastrutture civili, in particolare dalle reti di comunicazione, è un fattore che giustifica pienamente lo sviluppo della sicurezza militare nel cyberspazio. È essenziale per l'esercito che anche queste infrastrutture siano ben protette. Da questo punto in poi, è importante integrare la difesa informatica in tutte le esercitazioni militari o di gestione delle crisi, in particolare quelle che coinvolgono anche partner civili. Le relazioni tra l'esercito e le istituzioni civili si intensificano sempre più in entrambe le direzioni, il che significa che in pratica, nell'ambito dell'architettura di sicurezza informatica, l'esercito potrà beneficiare anche del sostegno delle imprese civili, nella misura in cui non dipendono da esse. La ricerca all'interno di *Armasuisse W+T* deve inoltre dedicare maggiori risorse allo studio, allo sviluppo e all'integrazione dell'IA per poter contrastare la ricerca dell'avversario. Inoltre, per quanto riguarda il personale, non va dimenticato che le aziende civili e le forze armate saranno in competizione per gli stessi specialisti. Il sistema della milizia dovrà essere trasformato in un vantaggio, non in un handicap.

Eventuali scontri nel ciberspazio creeranno maggiori aspettative e vincoli per i leader a tutti i livelli, che dovranno essere in grado di agire autonomamente in un dato quadro globale. Chiunque utilizzi una "condotta ordinata" *(Befehlstaktiktik)* con le nuove tecnologie, ad esempio come strumento di controllo permanente per imporre una visione, ne uscirà sconfitto. Task Force modulari, altamente flessibili, con un'ampia gamma di impieghi possibili, in

grado di adattarsi ad un avversario in continua evoluzione, sono le forze del futuro.

In futuro l'Esercito Svizzero avrà bisogno di una struttura di comando molto flessibile, prevista come parte di un sistema di sistemi, in cui la leadership verticale lascia il posto alla leadership tematica, orizzontale e adattabile. È probabile che l'aumento dell'importanza del cyberspazio significhi una diminuzione dell'importanza del dominio del territorio e degli spazi fisici in generale. Questa evoluzione non è quindi insignificante e dovrà essere integrata nei futuri sviluppi dell'esercito anche perché la nozione di "terreno" è sempre stata di notevole rilevanza nella dottrina.

La Cyber-guerra renderà ancora più importante anche l'analisi dei centri di gravità dell'avversario. Tale attività dovrebbe condurre ad uno sforzo massimo sulla protezione dei propri centri di gravità e sulla capacità di agire sui centri di gravità avversi. L'aiuto che l'IA può generare per lo svolgimento dei combattimenti nelle aree urbane sarà decisivo e portà essere un vantaggio notevole proprio perché tali aree rappresentano il principale terreno di intervento dell'Esercito Svizzero.

A causa del rinnovo di molti sistemi d'arma nei prossimi 10-15 anni e del fatto che si prevede che saranno in uso per circa 30 anni, le sfide per la pianificazione degli acquisti saranno molto reali e non possono essere sottovalutate. Questioni come l'utilità futura di carri armati o altri mezzi pesanti come l'artiglieria dovranno essere affrontate. Tuttavia, sarà sempre necessario integrare la dimensione della sicurezza informatica e della ridondanza in caso di attacchi informatici nei processi di acquisizione di questi sistemi. L'Esercito Svizzero dovrà disporre di mezzi informatici adeguati per una preparazione ottimale del campo di battaglia o per bloccare la preparazione dello scenario di attacco di un possibile avversario. A causa degli impegni dell'Esercito Svizzero all'estero, sarà inoltre necessario individuare le possibilità e i limiti delle azioni nel cyberspazio contro avversari non convenzionali.

Sarà inoltre necessario trovare il modo migliore possibile per garantire la sicurezza informatica delle truppe da impegnare in ambienti sfavorevoli.

In sintesi, vi sono 8 sviluppi principali, con le implicazioni del cyberspazio e dell'IA, che interesseranno l'Esercito Svizzero e che dovranno quindi essere monitorati e integrati nella pianificazione dello sviluppo dell'esercito: (1) l'aumento del numero di robot, in tutti i settori, (2) l'abbandono di alcuni sistemi d'arma, sostituiti da nuove tecnologie, (3) nuovi metodi di combattimento derivanti dalle nuove tecnologie, (4) nuove armi, (5) nuovi criteri di potenza e strumenti, (6) la crescente autonomia delle macchine, (7) nuovi problemi legati alle macchine e infine (8) nuovi obiettivi.

Conclusioni

La difesa informatica è diventata una necessità assoluta per proteggere non solo la popolazione e le infrastrutture, ma anche la vita sociale e democratica. Gli attacchi informatici sono la minaccia principale, sebbene questa minaccia sia stata finora mascherata dalla visibilità del terrorismo. Le nuove vulnerabilità appaiono più velocemente, prima che quelle vecchie vengano eliminate. Uno dei problemi principali sarà il costo di una protezione ad ampio spettro.

Figura 8: Importanza delle infrastrutture per il corretto funzionamento del cyberspazio, come le reti che transitano attraverso l'Islanda. (https://askjaenergy.com/2013/02/11/data-centres-in-iceland/, pagina visitata li 20.07.2018)

Gli sviluppi nel cyberspazio e il crescente utilizzo dell'IA in questo spazio operativo modificheranno i parametri a cui siamo abituati. Questo vale sia per gli aspetti civili che per quelli relativi alle forze armate. Le nuove minacce nel cyberspazio non sostituiscono quelle vecchie, ma si aggiungono a quelle già note che rimarranno ulteriori strumenti per attacchi per attori non statuali di ogni tipo (dirottamenti di aerei, imbarcazioni, ecc).

Ma l'esercito è solo uno dei partner e può contribuire alla gestione di una crisi informatica con le proprie risorse, nella misura in cui le disposizioni di legge lo consentono. Non hanno quindi un ruolo guida in questo settore, rispettivamente non dovrebbero farlo se gli organismi civili svolgono il loro ruolo. Ciò non diminuisce la necessità di garantire la loro capacità di fornire i servizi previsti attraverso un'efficace protezione dei loro sistemi e quindi di riconsiderare rapidamente le priorità di assegnazione delle risorse.

Il livello di sicurezza dei sistemi statali, compresi quelli delle forze armate, è una questione centrale. Un livello elevato è essenziale. L'intelligenza artificiale creerà nuove opportunità, rendendole accessibili a più attori.

Caratteristiche geopolitiche come la dimensione del territorio, la popolazione e le risorse naturali non saranno più gli unici attributi del potere di un paese. La rivoluzione determinata dalle nuove tecnologie diffonderà e ridistribuirà il potere, il più delle volte a beneficio degli attori più piccoli e attualmente più deboli. Gli Stati più piccoli e alla punta dell'IA avranno un impatto maggiore[24]. Il pericolo principale sarà senza dubbio uno squilibrio delle risorse che potrebbe spingere uno Stato ad un atteggiamento aggressivo se ha la netta convinzione di vincere o di avere una superiorità nel cyberspazio.

Sarà inoltre necessario un equilibrio nel settore delle armi informatiche e del sostegno all'IA che consentirà, come la deterrenza nucleare, una nuova forma di deterrenza informatica. La regolamentazione del ciberspazio è quindi essenziale per promuovere la cooperazione e consentire la repressione degli abusi. Gli Stati dovranno dotarsi dei mezzi per svolgere un ruolo normativo nel cyberspazio, che al momento sembra alquanto difficile. Se il divario tra Stati ricchi e Stati poveri continua ad aumentare, è prevedibile che si verifichino gravi crisi. I paesi poveri avranno sempre più mezzi per reagire agli abusi del sistema economico globale e saranno in grado, con mezzi relativamente limitati, di

lanciare azioni aggressive nel ciberspazio contro coloro che vengono percepiti come oppressori o approfittatori. Ciò potrebbe generare rischi significativi di destabilizzazione e conflitti.

La questione della responsabilità deve essere risolta il più presto possibile. Nel caso di un problema grave, e questo a causa della difficoltà di individuare un aggressore, sarà necessario essere in grado di attribuire la responsabilità dei fatti. Questo potrebbe essere il proprietario, il programmatore, il costruttore, l'emittente, o anche lo Stato. Questa è una delle più importanti questioni aperte in un mondo sempre più automatizzato. La difficoltà di attribuzione è un problema centrale, anche se può essere considerato come un fattore che calma il gioco, poiché costringe l'attaccante a rimanere misurato nella sua reazione. Tuttavia, questo richiederà anche una soluzione, poiché gli attacchi saranno sempre più efficaci, più precisi, più difficili da attribuire e mirati a tutte le vulnerabilità. Ci saranno anche più attori in grado di effettuare tali attacchi. Il miglioramento della sicurezza non solo deriva dalla necessità di fare le cose meglio, ma anche di farle in modo diverso. Saranno necessarie modifiche comportamentali per ridurre ed eventualmente eliminare i rischi. La sperimentazione è una fase che diventerà sempre più importante, sia per verificare i possibili guadagni in termini di sicurezza, sia per cercare le vulnerabilità al fine di eliminarle. Grazie alle sue crescenti capacità di apprendimento autonomo, l'IA potrebbe in un futuro abbastanza prossimo essere in grado di sviluppare e garantire la sicurezza informatica di un sistema in modo completamente autonomo, cioè senza alcun input umano necessario. Tuttavia, gli esseri umani manterranno un ruolo nel processo di *machine learning*. Una mancanza di interazione potrebbe portare allo sviluppo di macchine nella direzione sbagliata e potrebbe quindi ridurre l'efficacia della sicurezza. L'importanza dell'essere umano, e quindi del soldato, non scomparirà, così come le molte paure che accompagnano lo sviluppo dell'IA. Il rischio reale sarebbe quello di separare gli esseri umani e le macchine, il che porterebbe inevitabilmente a conflitti.

Sarà essenziale che i sistemi militari diventino sufficientemente sicuri da compensare il diffuso aumento delle possibilità della minaccia digitale. È imperativo che tutti gli interessati siano consapevoli della gravità della minaccia. Il rischio nel cyberspazio è un rischio sistemico e non si limita a potenziali attacchi mirati o limitati. In questo contesto, la sicurezza informatica è un deterrente non solo contro gli attacchi informatici, ma anche contro gli attacchi in altre aree operative, poiché l'indebolimento di un avversario nel cyberspazio può essere utilizzato anche come preparazione a un conflitto aperto. Ci si dovrà abituare a un ambiente in cui gli attacchi informatici saranno comuni e sistematicamente tentati, il che potrebbe mettere a repentaglio la stabilità dell'intero ciberspazio. Di conseguenza, potrebbero esserci sempre più scontri tra sistemi, tutti supportati dall'IA, con alcuni che tentano di sfruttare le vulnerabilità altrui. La sicurezza nel mondo virtuale sarà la base per proteggere il mondo reale. Tuttavia, può darsi che l'entità potenziale del danno, compreso il danno collaterale, sia tale da rappresentare un fattore che possa indurre gli aggressori ad usare cautela, specialmente nel caso degli Stati. È infatti molto difficile stimare le conseguenze di attacchi informatici che colpiscono indiscriminatamente tutti i computer e i sistemi di un paese e i cui effetti collaterali sono per definizione imprevedibili. Questo scenario risulta essere del tutto ammissibile con armi autonome basate sull'IA e quindi non più controllate dall'uomo.

L'esercito, e in particolare l'Esercito Svizzero, non ha altra scelta se non quella di proteggersi efficacemente dagli attacchi informatici e dalla diffusione di nuove tecnologie per poter continuare a svolgere la propria missione di protezione della popolazione e del territorio nazionale. È impossibile immaginare forze armate che non hanno una componente informatica. Sottovalutare le nuove sfide legate allo sviluppo del cyberspazio e dell'IA comporta rischi esistenziali per le società. Si possono e si devono adottare misure, spesso sostenute anche dall'IA, per rafforzare la sicurezza nel cyberspazio. Ci sono sei componenti per un'efficace protezione informatica: (1) prevenzione, (2) anticipazione, (3) protezione, (4) individuazione, (5) attribuzione e (6) risposta. La formazione degli "utenti di Internet" e dei media è centrale. L'anticipazione implica la conoscenza delle minacce, per essere in grado di prepararsi a contrastarle, mentre la protezione implica tutte le misure per complicare il compito degli aggressori. L'individuazione deve essere resa possibile dalle misure adottate all'interno dei sistemi stessi. Queste misure diventeranno più importanti, anche se potrebbero complicarsi con lo sviluppo della crittografia. L'assegnazione richiede mezzi specifici di analisi dei segnali. Infine, la reazione riguarda soprattutto i mezzi per riprendere e proseguire le attività, nonché le misure contro l'aggressore stesso. ■

Note :

1. Ryter, Marc-André: La 4ème révolution industrielle et son impact sur les forces armées, MPR I/17, pp. 50–62 (la versione italiana « La Quarta rivoluzione industriale ed il suo impatto sulle Forze Armate » è stata pubblicata in Cybersecurity Trends Italia 2/2018, pp. 14-25)
2. Rid, Thomas: The Rise of the Machines, Scribe Publications, London, 2016, p. 298.
3. Ryter, op. cit., pp. 58–60.
4. Straub, Jeremy: Artificial Intelligence is the weapon of the next Cold War, The Conversation, 29.01.2018, disponibile su: https://theconversation.com/artificial-intelligence-is-the-weapon-of-the-next-cold-war-86086, p.2
5. Anil, Suleyman: How to integrate cyber defence into existing defence capabilities, in Angeli, Franco (Dir.): International Humanitarian Law and New Weapon Technologies, International Institute of Humanitarian Law, San Remo, 2012, p. 152.
6. Anil, op. cit., p. 149.
7. Revue Stratégique de Cyberdéfense, Secrétariat Général de la Défense et de la Sécurité Nationale, Paris, 12.02.2018, disponibile su: http://www.sgdsn. gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf, p. 81.
8. Brundlage, Miles (et al): The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation, February 2018, 99 p., disponibile su: https:// arxiv. org/ftp/arxiv/papers/1802/1802.07228.pdf.
9. Ibid, p. 21.
10. Ibid, p. 39.
11. Straub, op. cit., p. 3.
12. Arquilla, John et Ronfeldt, David: Cyberwar is coming!, Comparative Strategy, vol. 12, no 2, 1993, p. 39
13. Dannreuther, Roland: International Security: the Contemporary Age, Cambridge, Polity Press, 2013, p. 266.
14. Brundlage, op. cit., p. 43.
15. Rid, op. cit., p. 296.
16. Douzet, Frédérick: Cyberguerres et cyberconflits, in: Badie, Bertrand et Vidal, Dominique: Nouvelles Guerres, L'état du monde 2015, La Découverte, Paris, 2014, pp. 111–117
17. Allen, Greg et Chan, Taniel: Artificial Intelligence and National Security, Harvard Kennedy Scholl, Belfer Center for Science and International Affairs, July 2017, p. 46.
18. Villani, Cédric: Donner un sens à l'intelligence artificielle: pour une stratégie nationale et européenne, Mission parlementaire du 8 septembre 2017 au 8 mars 2018, Paris, mars 2018, p. 221, disponibile su: www.aiforhumnaity.fr.
19. Rid, op. cit., p. 300.
20. Brundlage, op. cit., p. 42.
21. Straub, op. cit., p.3.
22. Revue Stratégique de Cyberdéfense, op. cit., p. 52.
23. Straub, op. cit., p. 5.
24. Arquilla et Ronsfeldt, op. cit., p. 26.

L'ALIENAZIONE AI TEMPI DEL WEB

Autore: Massimiliano Cannata

Il saggio di Francesca Re David frutto di un'appassionante conversazione con Lelio Demichelis ***"Tempi (retro) moderni. Il lavoro nella fabbrica-rete"*** (ed. Jaca Book), interroga il lettore sul destino del Sindacato, ma sarebbe più corretto dire sul futuro del lavoro nella *digital society*.

Oltre la fabbrica, intesa come tradizionale luogo della produzione fisicamente bel delimitato, nella nuova realtà dell'*"impresa rete"*, c'è una nuova importante partita da giocare: la difesa del lavoro e dei Diritti fondamentali. Viviamo il tempo delle contraddizioni, una strana epoca in cui ai bagliori del progresso tecnologico stanno facendo da contraltare una crescente sensazione di precarietà, di paura, di incertezza. Risalire la china, invertendo una tendenza negativa che ha assunto i toni drammatici della crisi, è un imperativo che impone a governi e istituzioni di alzare la soglia dell'attenzione. Consapevole di tutto questo, l'autrice alla guida della FIOM (Federazione Impiegati Operai Metallurgici) lancia un messaggio molto preciso: senza l'azione puntuale del sindacato sarà difficile attuare il disegno di una società più giusta, che possa scandire una linea di progresso reale della storia.

Che si potesse aprire una fase di riflessione in tema di civiltà del diritto c'era da aspettarselo. Negli ultimi anni una certa "cattiva" politica, aveva provato a marginalizzare il ruolo dei corpi intermedi, in nome di una disintermediazione dei processi, che di fatto sta rischiando di minare le fondamenta della democrazia occidentale. Per comprendere appieno i pericoli connessi alla deriva *"tecnopolitica"* è utile richiamare l'insegnamento di Stefano Rodotà: *"Nel nuovo spazio globale delle reti digitali – ha scritto il grande giurista - senza un'adeguata evoluzione del diritto, non ci potrà essere né democrazia, né pace tra i popoli mentre stiamo assistendo alla profilazione di nuove modalità di acquisizione del consenso, alle quali non sempre corrisponde una nuova distribuzione del potere. La dimensione della democrazia elettronica non deve essere confusa con la possibilità di essere chiamati a dire un sì o un no, che viene alla fine di un processo di decisione interamente gestito da altri".* Particolarmente eloquente è stato anche il nostro Presidente della Repubblica, che a Modena in occasione della commemorazione della tragica scomparsa del giuslavorista Marco Biagi ha detto, senza usare mezzi termini: *"La teoria secondo la quale occorre emarginare i corpi sociali intermedi ha reso tutti fragili".*

Per avere l'idea della profondità del "baratro" dentro cui stiamo rischiando di cadere basta osservare con spirito critico l'attualità. Mentre gli "algoritmi" decidono chi e dove assumere, i fatti di cronaca ci parlano continuamente di una percentuale drammatica di morti sul lavoro (fenomeno che grida vendetta nel contesto di una società che si dice evoluta e ipertecnologica), della quantità di esuberi generati dalle crisi aziendali, oltre 800 posti in ballo nel caso Sirti, 600 nel gruppo Carrefour, intanto si temono notizie analoghe provenienti dalla grande distribuzione cooperativa. Esiste, inoltre, una preoccupante tendenza al ridimensionamento e alle ristrutturazioni che andrà tamponata al più presto, i casi di Embraco, Amazon, passando per Ryanair e all'ex Seat pagine Gialle, per non parlare della triste vicenda della *Thyssenkrupp*, mettono sul piatto la grande questione della difesa dei diritti inalienabili dei lavoratori. Diritti spesso calpestati, in un totale disconoscimento dei valori della libertà e della dignità dell'uomo, che sono costati secoli di guerre e di faticose conquiste.

"Governare il cambiamento", (tema che verrà dibattuto non a caso sarà al centro dell'XI Congresso SNFIA che si terrà sul Lago di Garda dal 2 al 4 aprile del prossimo) vorrà dire prima di tutto creare le condizioni perché si possa affermare la prospettiva di un "neoumanesimo" solidale, in cui le imprese dovranno prima di tutto porsi il problema di coniugare etica e business, interpretando nella chiave più alta e impegnativa la *mission* di una responsabilità sociale. Bisognerà, in una parola, tornare a battersi, come suggerisce in uno dei suoi ultimi scritti il grande sociologo francese Edgar Morin), per una *"globalizzazione dei diritti, non solo dei mercati"*, per rispondere alle esigenze primarie di milioni di individui, che vivono ai "margini".

Lo studio ha il merito di evidenziare molto bene i lineamenti di un capitalismo che ha mutato profilo e dinamiche, nel contesto che vede una "frantumazione del lavoro" e un'eclissi della Politica (con la p maiuscola). La "metamorfosi" che ha subito un'accelerazione preoccupante in questo difficile decennio segnato dalla crisi, ha avuto origine nella progressiva finanziarizzazione dell'economia, che ha finito col condizionare le scelte decisive di una classe dirigente che troppo spesso ha dimostrato di non essere all'altezza dei compiti. Sono così venuti meno gli assetti organizzativi e produttivi, che avevano retto dalla rivoluzione industriale ad oggi, in una combustione di idee, ma soprattutto di valori che ha lasciato un senso di incertezza, precarietà e disorientamento, molto diffuso nella collettività. Non è ancora chiaro verso quali equilibri stiamo andando.

"Cambiata la scacchiera", come spiega molto bene Alessandro Baricco nel suo bellissimo saggio sulla civiltà digitale *"The Game"*, è mutato anche il nostro assetto mentale e il nostro metodo di conoscenza del mondo. Ora bisogna ritrovare un equilibrato rapporto tra uomo e macchina, per non far risorgere una parola – chiave che attraversa la trattazione: "alienazione". Pensavamo che fosse tramontata, con la fine dei *Tempi moderni* di Chaplin, invece è un termine che risorge, nell'orizzonte di un neo proletariato tecnologico, fuori dal recinto ideologico della lotta di classe, ma di certo non meno destabilizzante per la vita di milioni di individui nei diversi angoli del Pianeta. ■

IN CAMMINO VERSO IL LINGUAGGIO

Autore: Massimiliano Cannata

"Il rumore delle parole" (ed. Rizzoli) come tutti gli scritti di ***Vittorino Andreoli*** è un lavoro impegnativo, che scava nel profondo l'animo umano. L'io narrante si focalizza sull'analisi di quattro termini – chiave: *democrazia, assurdità, bellezza, vecchiaia*, "una tetrade per me magica" come viene spiegato al lettore nella premessa.

Difficile evitare a tutta prima l'accostamento con il celebre saggio di Michel Foucault: *"Le parole e le cose"*. Il problema centrale che animava la ricerca del pensatore francese era riconducibile alla rifondazione delle condizioni di verità del discorso scientifico, in un contesto come quello della contemporaneità che aveva scompaginato in maniera definitiva le categorie tradizionali della conoscenza. In questo caso le questioni in ballo sono altre, ma saremmo comunque fuori strada se pensassimo di avere tra le mani un testo di linguistica in senso stretto. Storia, sociologia, politica, antropologia sono molteplici gli ingredienti disseminati nel racconto del protagonista, che parla da una stanza vuota, connesso alla rete. "La virtualità può essere anche un modo per superare la solitudine". Per chi non ha la fortuna di camminare nel mondo in compagnia, la semplice presenza *on line* di un interlocutore è comunque una provvidenza da benedire. Questa strana figura di docente potrebbe richiamare il protagonista della novella di Pirandello: *"L'eresia catara"*. Costretto a fare le sue lezioni senza un vero pubblico, il professore parlava a dei cappotti vuoti, degli allievi nemmeno l'ombra, malgrado questo continuava a parlare spinto dalla necessità di comunicare. Ecco il primo importante elemento di riflessione: la "solitudine virtuale è meglio del vuoto assoluto" può dunque esistere un lato buono della Rete che forse non abbiamo ancora a sufficienza considerato. Se usato con intelligenza Internet può creare comunità, dando effetto concreto a quell'intelligenza collettiva teorizzata da Pierre Levy.

Ma *"Il rumore delle parole"* è anche, forse più di tutto, un libro sulla vecchiaia di cui non si può e non si deve avere vergogna. *"Sono vecchio"*, parole del protagonista, un'affermazione inusuale nella sua secchezza. Oggi spesso rimane sottaciuta, ingoiata e inespressa, perché soffocata da un alone di pudore, quasi che questa condizione dell'esistenza debba essere negata e conculcata, travolti come siamo dalla velocità, dall'efficienza ad ogni costo, dalla superficialità. Ci aveva già messo sull'avviso Michel Serres tra gli intellettuali oggi più lucidi e influenti, dando alle stampe un *pamphlet* dal titolo molto esplicito: *"Non è un mondo per vecchi"*. Andreoli in maniera implicita ma potente, rincara la dose argomentando con lucidità la ragione per cui sarebbe assurdo negare l'importanza di una stagione dell'esistenza paradigmatica, in quanto specchio fedele di una condizione di fragilità che ci appartiene sempre, fin da quando facciamo il nostro ingresso nel mondo. *"La condizione umana si caratterizza per la fragilità, che è data dal bisogno dell'altro, dal desiderio di conoscere, mentre il potere non ha bisogno dell'altro se non per dominarlo. Questo è l'umanesimo della fragilità, che segna e segnerà le nostre vite… Ho, per questo motivo, studiato da sempre con massimo interesse l'uomo rotto, perché in lui ho sempre ritrovato quella grandezza di cui ogni individuo è portatore. Grazie a questa convinzione riesco a guardare avanti con fiducia, definendomi un pessimista attivo"*.

L'umanesimo della fragilità, *fil rouge* del precedente scritto *"Homo Stupidus Stupidus"*, pubblicato dallo studioso con lo stesso editore, attraversa anche queste pagine. Non c'è da stupirsi: il linguaggio è la "casa dell'essere", come ci ha insegnato Heidegger, "ci parla", facendoci ritrovare l'origine, la strada che dalle radici ci ha condotti fin qui, nella ricerca di un'identità e di un posto nel mondo. La "tetrade" alla fine della trattazione rievoca la morte, ma anche l'eternità, scandendo un tempo non solo mentale ma anche cronologico. Lungo il cammino di questa ricerca che non può trovare risposte definitive ci si potrebbe stupire di trovare una parola quale "assurdità" che dovrebbe essere bandita dal corretto ragionamento. Ma è proprio lo "sguardo di lato" che più accende la scintilla del ricercatore e dello studioso: *"Misurarsi con la dimensione dell'assurdo* – spiega l'autore – *significa ritornare a quello che descrive Kierkgaard in "Timore e tremore". Dio, come è noto, suggerisce ad Abramo di sacrificare il figlio Isacco. Un controsenso, qualche cosa di inaccettabile per qualsiasi genitore. Abramo riesce comunque a trovare una soluzione, va oltre l'assurdo, segue la regola che ha appreso: sa che Dio c'è, ne ha avuto esperienza. Noi di fronte alle contraddizioni che attanagliano l'uomo contemporaneo a differenza di Abramo non facciamo niente, scappiamo. Il grande conflitto, il dramma è proprio questo: c'è una strada indicata dalla civiltà che ci porta verso l'alto, all'opposto ne esiste un'altra che ci porta verso la regressione. Non dobbiamo mai finire di lottare entrare dentro questa contraddizione per superarla, perché a prevalere sia la tensione verso obiettivi di progresso e di crescita umana e civile, perché di questo, mi creda, abbiamo un bisogno estremo e disperato"*.

A conclusione della lettura un monito emerge in maniera netta: nessuno di noi può avere la presunzione di conoscere cosa ci aspetta al di là del mistero, non sappiamo neanche quale sia il confine tra lucidità e follia. Quello che più umilmente possiamo fare è impegnarci a spingere la notte più in là, esercitando la facoltà dell'intelligenza, il valore del rispetto e della tolleranza, cercando di mettere in pratica un metodo di approccio alla realtà fondato sul pensiero critico e sull'ascolto dell'altro. Quell'altro che è *"la provocazione che ci chiama all'essere"* (per dirla con *Alain Badiou*), senza di cui noi stessi non avremmo alcuna seria ragione di stare nel mondo. ■

I BIT E LA LUNA

Autore: Massimiliano Cannata

I *bit e la luna* è una delle tante interessanti metafore del saggio di *Mafe de Baggis*, affascinante e di facile lettura. Il titolo *Luminol* (ed. Hoepli) riporta il lettore non a caso al linguaggio dei film polizieschi e dei gialli, che molto successo riscuotono in questo periodo. Basti pensare ai personaggi intramontabili di *Agatha Christie, George Simenon, Alfred Hitchcock* ormai divenuti dei classici, al grande successo delle serie TV, dominatori dell'audience, che hanno come protagonista *l'ispettore Barnaby,* il *tenente Colombo*, *il commissario Cordier* e per avvicinarci alle nostre latitudini il *maresciallo Rocca, Rocco Schiavone*, fino all'exploit ineguagliabile del *Montalbano* televisivo, prodotto dalla poderosa fantasia di *Andrea Camilleri*. "Basta una semplice riflessione – mi spiega l'autrice – per comprendere la ratio che ha portato alla realizzazione di questo lavoro. A cosa serve il Luminol? A imparare a guardare con attenzione la società che ci circonda, senza cedere alla tirannia della pigrizia e della prima impressione. I media digitali ci permettono di sentire i pensieri delle persone, i loro comportamenti quando pensano di essere invisibili. È incredibile la facilità con cui crediamo che siano le tecnologie a farci comportare male, come se fossimo in un brutto film horror. In realtà le tecnologie fanno emergere chi siamo davvero, chi siamo sempre stati: i veri valori, i veri comportamenti, le vere mancanze. Questo non vuol dire che siano uno specchio, a meno di non pensare che sia uno specchio stregato, perché quello che vediamo ci sembra sempre altro da noi. Sembra che siano sempre gli altri a comportarsi male e quello che vediamo ci condiziona, peggiorandoci quando è sbagliato, migliorandoci quando è sano. Per questo dico che i media digitali non creano i comportamenti, ma quando evidenziano violenza e aggressività condizionano comunque la società, perché peggiorano lo spazio pubblico, in una spirale al ribasso".

Come viene detto molto bene nel corso della trattazione, oggi si avverte una difficoltà di comprensione della nuova realtà in cui siamo immersi. *"Non basta pigiare un bottone per far succedere qualcosa on line",* questa verità non è, purtroppo, evidente a tutti. In particolare quella che preoccupa è l'inadeguatezza delle *élites* non solo di casa nostra, poco preparate a muoversi in un universo in cui viviamo perennemente *on life*. *I "nuovi alfabeti"* del digitale sono diversi dal nostro alfabeto, che ha le caratteristiche dell'univocità e dell'unicità. Vengono citati nel testo molto opportunamente gli studi di Peppino Ortoleva che si soffermava sulla dimensione della complessità, piuttosto che di unilateralità. La sfida di comprendere la sintassi della trasformazione investe in prima battuta il mondo delle aziende. Anche su questo aspetto l'analisi della De Baggis è straordinariamente lucida. "La vera difficoltà, nelle organizzazioni produttive non tanto quella di padroneggiare strumenti e linguaggi. È accettare di dover cedere il palcoscenico a ogni singolo cliente, ciascuno con la sua personalità, proponendo una storia dove il prodotto (o la comunicazione del prodotto) giocano un ruolo minimale ma importante nella soluzione di un problema. È il ruolo dello *storytelling*, che non vuol dire produrre contenuti piacevoli e interessanti (si può fare anche senza narrazioni), ma intrecciare la vita delle persone al *customer journey* di un prodotto e farglielo scoprire (sui social media) o trovare (sui motori di ricerca).

Quando *Pierre Levy,* in un saggio di successo, qualche anno fa parlava del *Virtuale*, come di una nuova categoria dell'essere con cui bisognava fare i conti, che andava affiancata alle vecchie categorie dell'ontologia classica da Aristotele in poi. Aveva probabilmente visto giusto. Spazio, tempo, relazione, sono categorie fluide nell'era delle reti. Ma la categoria che cade più direttamente sotto la lente della De Baggis è quella del tempo, che "nessuno dimostra di capire davvero. Il tempo del digitale, che è un tempo rarefatto e sospeso, non veloce e in fuga. È un tempo da supereroi, in cui puoi fermare tutto e andare avanti e indietro, ma solo se sai che puoi farlo. Non vuole saperlo nessuno: abbiamo creduto alla bufala della rete veloce e fasulla e, così facendo, contribuiamo a renderla tale davvero".

Aspetto particolarmente interessante è il riferimento al celebre saggio di *Eli Pariser (Il filtro quello che Internet ci nasconde, ed. Il Saggiatore, n.d.r.)* in cui per la prima volta appare il termine "bolla" o "camera dell'eco", per definire quell'alone di verità creata che si gonfia alimentandosi nella Rete. In questo tempo dei ragni la sfida della formazione diventa cruciale per orientarsi e comprendere i percorsi di sviluppo della civiltà. Il metodo migliore, ci ricorda in conclusione l'autrice, viene dalle scienze umane, dall'etnografia che è "lo studio antropologico dei comportamenti umani e della scrittura. Internet è uno straordinario campo da gioco per l'antropologo ma anche per il curioso, l'importante essere disposti a considerare i comportamenti osservati come indizi da analizzare e interpretare e non come prove. Per quanto riguarda le bolle, per esempio, uno sguardo privo di pregiudizi dovrebbe confrontare le bolle digitali con le bolle analogiche prima di trarre qualsiasi conclusione". Più equilibrio e meno slogan dunque se non vogliamo "finire nella rete" dei pregiudizi, delle false convinzioni e delle frasi fatte. "La rete è uno strumento che fa parte del mondo, non un mistero da svelare: il mistero sono i comportamenti umani che la rete aiuta a conoscere e a capire meglio". Se solo ce lo ricordassimo più spesso forse qualche passo avanti lo avremmo finalmente compiuto. ■

LO SPETTRO DELLA GRANDE IGNORANZA

Autore: Massimiliano Cannata

"Siamo affetti dalla sindrome del rifiuto per tutto ciò che richiama la qualità. Un fenomeno singolare che viene da lontano, ma che oggi ha assunto i contorni della deriva strutturale". Il recente allarme lanciato dal sociologo Gian Maria Fara in occasione della presentazione dell'ultimo Rapporto Italia dell'Eurispes a tutta prima potrebbe sembrare una battuta ad effetto, in realtà tocca un nervo scoperto che ci riguarda molto direttamente. Mettere al potere politici preparati è diventata una sfida imprescindibile. E' infatti molto strano il nostro rapporto con il potere e con lo Stato. Spesso ci lamentiamo degli attuali uomini al governo, inesperti, impreparati, non hanno esperienza di lavoro e si trovano a guidare ministeri di peso e valenza strategica. Magari non li vorremmo neanche come amministratori di condominio, ma di fatto finiamo con accettarli alla guida del Paese, "votandoli" ma senza ammetterlo. Occorre partire da questa *"pietosa bugia"* connaturata al nostro tratto antropologico, retaggio di antiche dominazioni che hanno annacquato la nostra fiducia nelle istituzioni e dalla considerazione di Fara per comprendere a fondo il saggio di Irene Tinagli *"La grande ignoranza"* (ed. Rizzoli), scritto che ha il merito di mettere a nudo uno scenario inquietante. Con dovizia di dati l'autrice fa, infatti, vedere molto bene come non eravamo mai scesi così in basso: l'attuale classe al potere è la meno attrezzata culturalmente dal dopoguerra ad oggi. "Non possiamo stupirci se consideriamo la scarsa preparazione di chi ha in mano la *Governance* politica. Come si fa a parlare di qualità della democrazia quando siamo il penultimo Paese in Europa per percentuale di laureati, (solo la Romania riesce a fare peggio di noi n.d.r.), mentre non facciamo nulla per rimuovere quegli ostacoli sociali ed economici che dovrebbero permettere a tutti, come prescritto dal dettato costituzionale, di accedere agli studi con pari opportunità?

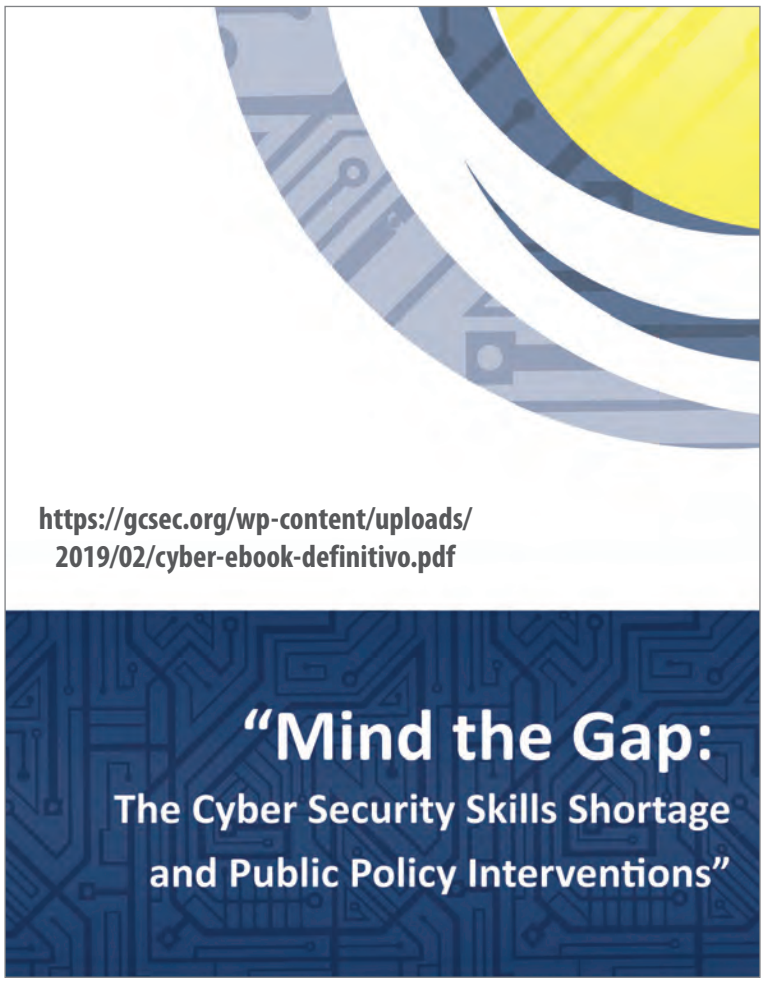
Il lavoro della Tinagli dovrebbe far molto riflettere anche sulla perdita del ruolo e funzione dei luoghi della formazione tradizionale, che hanno costituito la spina dorsale nella costruzione della *leadership* e dei profili della dirigenza pubblica. Occorre ripensarli a partire proprio dall'Università che deve diventare un asset strategico per la costruzione di cittadini consapevoli, dalla mente aperta, animati da una visione alta del bene comune e dal senso del progetto.

Un male si badi bene, quello dell'incompetenza dilagante che ha portato fino allo scriteriato elogio della stupidità, fenomeno non solo italiano. Lo dimostra l'allarme lanciato neanche un anno fa da Tom Nichols docente allo *U.S. Naval War College* e alla *Harvard Extention School*, che ne *"La conoscenza e i suoi nemici"* (saggio uscito negli Stati Uniti, tradotto in Italia dalla *Luiss University Press* e ben presto divenuto un *best seller n.d.r.*) ha sollevato una domanda destinata a segnare quest'epoca densa di mutazioni: Siamo alla fine della competenza? Colti da un misto di preoccupazione e imbarazzo verrebbe da rispondere positivamente, i numeri, infatti, parlano chiaro: parlamentari, ministri e governi annoverano una bassissima percentuale di laureati, cosa che, per quanto ci riguarda, non avveniva neanche alle origini della Repubblica. Negli anni 50 infatti, in un Paese in cui il tasso medio di istruzione era come è noto molto basso, chi occupava gli scranni dell'aula parlamentare aveva le carte molto più in regola rispetto a quanto avviene ai nostri giorni.

La contraddizione in cui viviamo è drammaticamente palese. La società dell'informazione dovrebbe, infatti, celebrare il sapere, quale molla e combustibile essenziale per far andare avanti il mondo, eppure a forza di ripetere che *"uno vale uno"*, stiamo trasformando la Rete, da strumento eccezionale di innovazione e partecipazione a meccanismo di pericolosa semplificazione, che porta a una "narcosi dello schermo". L'individuo è spinto sul baratro dell'ottundimento di ogni autonomia di pensiero, "abbiamo bandito ogni forma di alterità, negato l'altro, per cui ogni spazio della riflessione è ingoiato in una sorta di immanenza satura". Il risultato è che di questo passo *"nessuno varrà niente"*, con conseguenze facilmente immaginabili.

Sarà dunque necessario porre un argine alla democrazia delle scorciatoie per tornare a investire sulla competenza. Oggi siamo infatti di fronte a un paradosso: chi vuole mettere al centro la preparazione viene considerato "diverso" e quindi espulso dalla società, con il risultato che si genera una selezione avversa che ostracizza le migliori intelligenze lasciando il campo della politica ai "peggiori". E' evidente che così sarà impossibile risalire la china, ricollocando il nostro paese nella posizione che gli spetta, in quanto fondatore dell'Europa e patria della civiltà occidentale. ■

Bibliografia - Cybersecurity Trends



https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf

Realizzata per essere esposta nel 2013 all'ITU (l'Unione Internazionale delle Telecomunicazioni), premiata dall'ITU e quindi tradotta ed esposta consecutivamente in 28 città di Romania, Polonia e Svizzera, la mostra è stata tradotta in italiano per le Poste Italiane, col patrocinio della Polizia Nazionale. E stata presentata in anteprima nel 2016 presso la "MakerFaire – European Edition" di Roma (dove ha superato i 130.000 visitatori). In 30 pannelli, l'esposizione illustra l'evoluzione delle tecniche di comunicazione e di manipolazione delle informazioni dai tempi più antichi ai social media usati oggi da tutti. Consente senza essere moralizzatrice di educare giovani ed adulti ad una fruizione consapevole e protetta di Internet.
La mostra è integralmente visitabile sul sito del Distretto di Cyber Security delle Poste Italiane, dove l'esposizione reale è allestita in modo permanente: https://www.distrettocybersecurity.it/mostra-2/

Una pubblicazione

web for business
swiss webacademy

A cura del

GLOBAL CYBER SECURITY CENTER

Redazione:
Laurent Chrzanovski e Romulus Maier (†) (tutte le edizioni)
Per l'edizione del GCSEC:
Nicola Sotira, Elena Agresti

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Indirizzi:
Viale Europa 175 - 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org
Şcoala de Înot nr.18, 550005,
Sibiu, Romania

www.gcsec.org
www.cybersecuritytrends.ro
www.swissacademy.eu

CYBERSECURITY DIALOGUES

www.cybersecurity-dialogues.org

BROUGHT TO YOU BY:

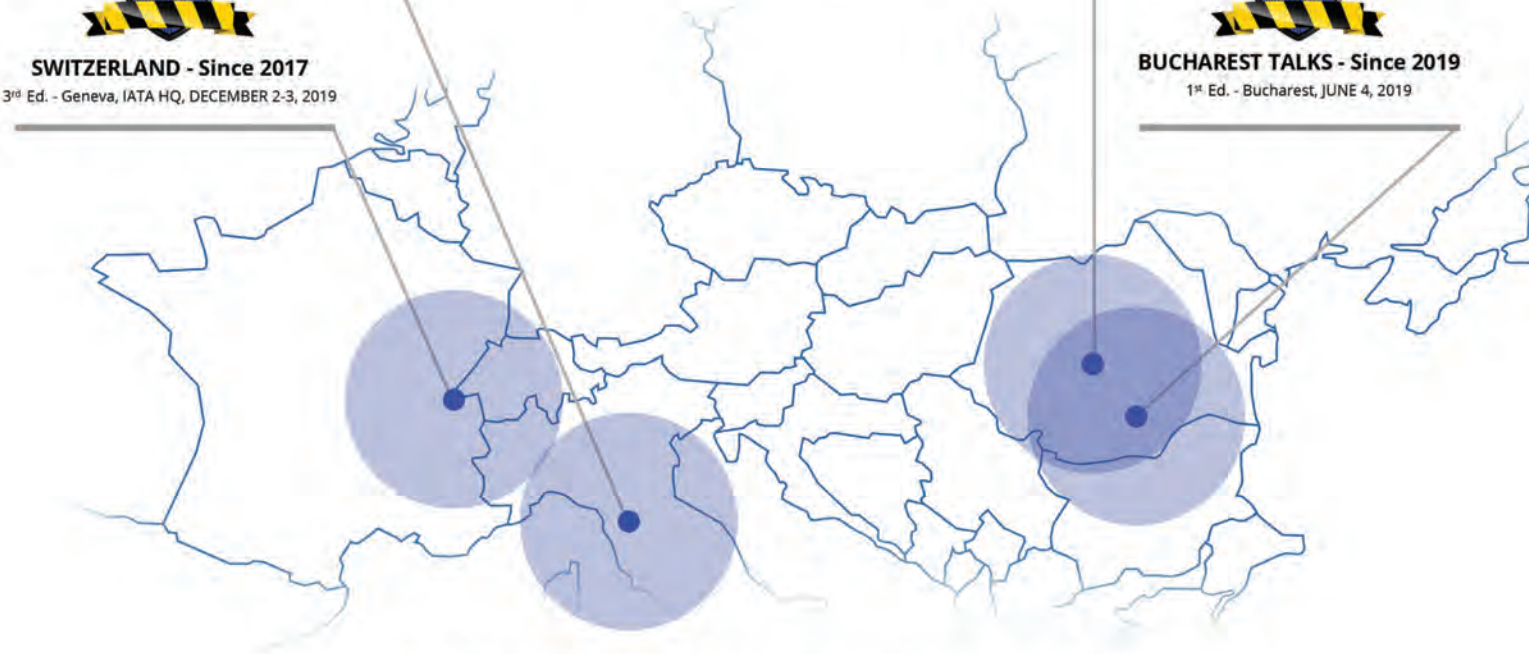
web for your business
swiss webacademy

MEDITERRANEAN - Since 2018
2rd Ed. - Florence, MAY 9-10, 2019

ROMANIA - Since 2013
7th Ed. - Sibiu, SEPTEMBER 12-13, 2019

SWITZERLAND - Since 2017
3rd Ed. - Geneva, IATA HQ, DECEMBER 2-3, 2019

BUCHAREST TALKS - Since 2019
1st Ed. - Bucharest, JUNE 4, 2019



www.cybersecurity-dialogues.org

The only platform with it's own quaterly magazine

https://issuu.com/cybersecuritytrends

web for your business
swiss webacademy

Local Partner / Partner locale:

THALES

Present:

CYBERSECURITY MEDITERRANEAN CONGRESS

2nd Edition

A Southern European Public-Private Dialogue Platform

May 09-10, 2019, Murate IdeaPark, Florence, Italy

www.cybersecurity-mediterranean.it

Under the Patronage of / Con il patrocinio di:

REGIONE TOSCANA

COMUNE DI FIRENZE

POLICE GENEVE

CONFINDUSTRIA Toscana

Confservizi Cispel Toscana

FEDERMANAGER TOSCANA

In collaboration with / Con la collaborazione di:

MIP MURATE IDEA PARK
Idee in Evasione

IATA

GLOBAL CYBER SECURITY CENTER

www.glgsys.ch

In partnership with / In partenariato con:

EUCACS | EUROPEAN CENTER FOR ADVANCED CYBER SECURITY

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

ROMANIA SRI Patria a priori SERVICIUL ROMÂN DE INFORMAȚII

ROMANIA CYBERINT SERVICIUL ROMÂN DE INFORMAȚII

KUDO