ISSN 2282-6599

RIVISTA DI ECONOMIA E POLITICA DEI TRASPORTI

Anno 2019
Numero 3

R.E.PO.T

Rivista Scientifica della Società
Italiana di Economia dei Trasporti e della
Logistica

DALLA CYBER DEFENSE ALLA CYBER RESILIENCE DELL'INFRASTRUTTURA CRITICA. ALCUNE IMPLICAZIONI STRATEGICHE E ORGANIZZATIVE

Francesca Castaldo[1*]

Sapienza Università di Roma, Dipartimento di Management,

Via del Castro Laurenziano, 9, 00161, Roma, Italia

Negli ultimi anni è aumentata pervasivamente la consapevolezza che alcune delle infrastrutture necessarie al funzionamento della società e dell'economia, e da cui dipende la qualità delle nostre vite, siano vulnerabili rispetto ad eventi naturali gravi e soprattutto nei confronti di minacce antropiche, come gli attentati terroristici. Tali infrastrutture sono considerate 'critiche' perché a loro spetta il compito di garantire il corretto funzionamento del sistema produttivo, economico e sociale e richiedono, pertanto, di essere protette in modo adeguato.
I sistemi che utilizzano in modo intensivo reti di comunicazione e tecnologie digitali per il controllo, nonché scambio di grande quantità di informazioni, come i sistemi di gestione del traffico aereo, sono in particolar modo danneggiabili perché esposti ad attacchi cibernetici, da cui occorre però necessariamente difendersi o, meglio, opporre resistenza e divenire resilienti.
La protezione dell'infrastruttura critica sta imponendo un cambiamento nel paradigma della sicurezza, statuale e non, con uno shift dal topic della difesa a quello della resilienza cibernetica. Tale cambiamento, di ordine tecnologico, non è scevro di interconnessioni e implicazioni sul piano normativo, gestionale, organizzativo e strategico, rappresentando così un'opportunità per i governi e per tutti gli attori, pubblici e privati, coinvolti.

Parole Chiave: infrastruttura critica, minacce, architettura protettiva, sicurezza, cyber defence, cyber resilience

[*] francesca.castaldo@mail.it; francesca.castaldo@uniroma1.it

1. Introduzione

Il largo impiego delle tecnologie digitali applicate alle comunicazioni e all'informazione ha accresciuto a dismisura i rischi legati al cybercrime, che oggi costituisce una delle maggiori minacce alla sicurezza - sia in ambito militare che civile. La minaccia cyber[1] è particolarmente elevata per tutti quei dispositivi connessi all'acquisizione delle informazioni - come i sistemi satellitari, le comunicazioni radar civili e militari, i sistemi meteorologici - e per i sistemi che supportano la movimentazione fisica di persone e merci - come i droni per applicazioni civili, i sistemi di gestione e controllo del traffico aereo o navale.
Si tratta di aree chiave per la sicurezza di una nazione che, per tale motivo, vengono chiamate "infrastrutture critiche" (Geers, 2009).
In questo articolo vogliamo focalizzarci su quella particolare infrastruttura critica rappresentata dai sistemi di controllo del traffico aereo, elemento altamente sensibile e cruciale per una gestione efficace della sicurezza nazionale. Il controllo del traffico aereo, infatti, può diventare l'obiettivo di entità ostili, in quanto infrastruttura che partecipa al sistema dell'aviazione civile, tradizionale obiettivo simbolico delle forze del terrore in uno scenario che plasticamente viene definito di cyber-warfare (Healey, 2014; Rosenzweig, 2013). Essendo non azzerabile il rischio di attacchi di qualunque tipo, come vedremo nei successivi paragrafi, solo l'uso continuato nel tempo di tecnologie allo stato dell'arte e di un modello organizzativo di sicurezza adeguato possono ridurre fortemente tale rischio.

2. La gestione di una infrastruttura critica: il traffico aereo

Il rapporto tra la sicurezza cibernetica e le infrastrutture critiche informatizzate è un tema ampiamente discusso nella fiorente letteratura sulla sicurezza delle informazioni[2], oltre che di preminente interesse tra le minacce emergenti, in particolare nell'ambito del controllo del traffico aereo[3].
Lo sviluppo dell'Information Technology (IT) è il supporto essenziale all'evoluzione dei sistemi di controllo del traffico aereo civile, uno dei settori più importanti per la gestione della sicurezza nazionale e perciò un'area nevralgica per le attività terroristiche (Gori and Lisi, 2014).
Il traffico aereo è connesso alla circolazione di persone e merci, al trasporto in generale, al business, alla politica. Colpirlo consentirebbe di mettere a segno azioni con alte perdite potenziali di vite umane, dando al contempo grande visibilità ad organizzazioni criminali che farebbero risaltare, attraverso i media, la loro bravura e preparazione tecnologica (Gori, 2015).

[1] Il prefisso 'cyber' deriva dalla parola 'cibernetica', che, a sua volta, deriva dal termine greco antico κυβερνήτης (col significato di timone o timoniere, pilota, governatore), ed è molto usato nei termini 'cyberspace', 'cybercrime', 'cyberwarfare', 'cybersecurity', 'cyberstrategy', 'cyberterrorism', tra gli altri.

[2] Si vedano, tra gli altri, Caravelli J., Jones N. (2019); Green J.A. (2015); Lynn W.J. (2010).

[3] La trattazione della minaccia cyber alla gestione del traffico aereo è riconducibile al più ampio campo dell'Air Traffic Management Security (sicurezza dei dati operativi, delle infrastrutture e del personale) da parte delle Aeronautiche Militari.

Il sistema di 'Air Traffic Management' (ATM) è caratterizzato di per sé da una forte complessità tecnologica, che prevede nel prossimo futuro una completa integrazione dei sistemi a pilotaggio remoto (Remote Piloted Air Systems - RPAS) nel flusso ordinario di traffico (U.S. Department of Defense, 2011b). La circolazione aerea tra meno di un ventennio sarà infatti effettuata in gran parte dai velivoli pilotati remotamente (i cosiddetti droni) e controllati tramite sistemi avanzati di telecomunicazione.
Al fine di consentire tale rivoluzione è in corso una revisione del sistema che prevede un'estensiva automazione della gestione delle rotte degli aeromobili, non più canalizzati nelle aerovie ma coordinati da una gigantesca quanto complessa architettura informatica (computer, software e rete), che consentirà la riduzione dei tempi di volo e considerevoli risparmi economici al settore (Castaldo, 2018).
L'impiego crescente del pilotaggio remoto implica la necessità di un'infrastruttura di comunicazione - satellitare e non - sempre più estesa, su una banda elettromagnetica sempre più ampia e su un'architettura distribuita su tutto il territorio. La sorveglianza dello spettro elettromagnetico rappresenta, dunque, uno degli aspetti vitali per garantire la sicurezza di RPAS civili e militari.
Le piattaforme tecnologiche dell'Air Traffic Management (ATM), come SESAR[4], sono sistemi aperti e interdipendenti al cui interno l'informazione è l'essenza. Tali strutture però nel nostro Paese non sono state concepite con un controllo remoto 'security embedded' e, conseguentemente, necessitano nel tempo dello sviluppo di opportune modalità di controllo (Castaldo, 2019).
Ad aumentare ulteriormente la complessità dei sistemi ATM va aggiunto che il trasporto aereo non è immune dall'utilizzo di dispositivi collegati alla Rete, autoreferenziali, con capacità intelligenti (internet delle cose e delle tecnologie 'smart'), difficilmente assoggettabili a un sistema di gestione della sicurezza delle informazioni in grado di ridurne le vulnerabilità. Com'è stato argomentato, i requisiti, gli standard e le procedure che caratterizzeranno tale poderosa infrastruttura informatica dovranno, pertanto, tenere conto di tutte le possibili minacce fisiche, procedurali e, soprattutto, cibernetiche (Adams, 2001; Wright, Grego and Grounlund, 2005).
Il sistema di gestione del traffico aereo, che si configura come infrastruttura critica, è esposto dal punto di vista cyber ad una variegata tipologia di minaccia: 'Advanced persistent threat'[5], che consiste nella possibilità di studiare e pianificare nel tempo un attacco cibernetico come 'effetto sorpresa'; 'Denial of services'[6], nella forma sia di attacchi cyber che di disturbi elettromagnetici; interferenza, ovvero inserimento nello spettro elettromagnetico per ostacolare le operazioni ATM (in quanto le modalità di

[4] SESAR (acronimo di Single European Sky ATM Research, studio di un sistema di gestione del traffico aereo per il cielo unico europeo) è un Programma, attualmente gestito da una public-private partnership, volto a revisionare completamente lo spazio aereo europeo e il suo sistema di gestione del traffico aereo.

[5] Minaccia consistente in un attacco mirato, volto ad installare una serie di malware all'interno delle reti del bersaglio al fine di riuscire a mantenere attivi dei canali che servono a far uscire informazioni di valore dalle reti dell'ente obiettivo.

[6] Attacco volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi server.

attacco cyber si possono miscelare con attacchi e tecniche più tradizionali di guerra elettronica); 'Take control of system', ossia l'importazione di dati falsi e corrotti, con inserimento di malware e con l'accesso e l'introduzione nei sistemi, anche manuale attraverso l'intervento umano (Geers, 2009; Andress and Winterfeld, 2014). Organizzazioni terroristiche (come al-Qaeda o Isis) hanno tradizionalmente utilizzato lo spazio cibernetico per diffondere la propria propaganda, reclutare nuovi combattenti, finanziare le proprie attività e coordinare le operazioni, mentre datano a tempi molto più recenti talune operazioni miranti ad accedere ai servizi informatici di privati o di istituzioni ritenute nemiche. Le tecniche di hacking finora utilizzate si sono, tuttavia, rivelate abbastanza limitate e solo raramente hanno oltrepassato la soglia di web defacement[7] o hanno dato vita a intrusioni negli account di social media, di per sé non particolarmente complessi da violare. Sebbene alcuni hacker jihadisti si siano più volte vantati di essere riusciti a penetrare le ben protette reti militari statunitensi, inglesi e italiane, gli obiettivi preferiti dagli hacktivisti sono stati finora le reti di istituzioni politiche o pubbliche amministrazioni ritenute in contrasto con i propri valori o la propria ideologia. L'azione di questi soggetti non sembra, quindi, abbia finora avuto come obiettivo quei sistemi informatici che, se danneggiati o malfunzionanti, potrebbero provocare danni, anche fisici ad individui ed entità (Teti, 2018).

I criminali cibernetici, dal canto loro, hanno elevato in maniera esponenziale le proprie competenze per l'intrusione nei sistemi informatici. La creazione e la diffusione, nel mercato nero del web, di software malevoli hanno contribuito a promuovere l'aumento del fenomeno del crimine online, rispetto a forme più consuete di reato. Ma l'obiettivo dei criminali cibernetici è precipuamente il profitto e proprio per questo essi possono essere considerati più una minaccia per la sicurezza economica che per quella nazionale.

Solo le organizzazioni terroristiche potrebbero essere intenzionate a colpire le infrastrutture critiche come, appunto, i sistemi di gestione del traffico aereo civile dei Paesi ritenuti avversari ma attualmente essi, a differenza di hacktivisti e criminali cibernetici, che si sono mostrati tecnicamente ben più dotati, non dispongono di capacità di hacking tali da poter costituire un pericolo serio e imminente (Liang and Xiangsui, 2001).

Se è da un lato vero che competenze avanzate sono reperibili anche sul dark market (Klimburg, 2017), dall'altro attacchi alle infrastrutture critiche necessitano comunque di skill informatici molto elevati, oltre che la conoscenza del dominio, per cui un attacco a un sistema di Air Traffic Management (ATM) e di Air Traffic Control (ATC) avrebbe bisogno, per essere progettato, di risorse finanziarie ingenti a fronte di un impatto che potrebbe non essere ampio quanto una mattanza per strada. Per tale motivo, attacchi a infrastrutture critiche sono di fatto minacce legate, più che a bande del terrore, ad attori statuali che possono pensare di inserire, ad esempio, malware nei sistemi di uno stato nemico, per poi farli detonare nel momento del bisogno (Castaldo, 2019).

In altri termini, la possibilità che un hacker possa alterare i sistemi ATM è molto bassa poiché spesso si tratta di sistemi non connessi direttamente a internet e, una volta che l'hacker si è introdotto nel sistema, per creare forti danni c'è bisogno di una conoscenza applicativa molto approfondita per poter alterare ad esempio i piani di volo in modo malizioso (Colantoni, 2006). Risulterebbe, invece, più semplice per

[7] Il web defacement indica la modifica di contenuti della homepage o delle sotto-pagine di un sito.

l'hacker bloccare il funzionamento del sistema una volta penetrato all'interno. In questo caso però paradossalmente la situazione sarebbe meno grave grazie all'esistenza di sistemi di "business continuity"[8] e di "disaster recovery"[9], che possono permettere al sistema di continuare a lavorare a fronte di fallimenti di parti dello stesso (Castaldo, 2018).
L'aeronautica militare italiana risulta pienamente coinvolta nella trattazione della tematica della sicurezza cibernetica, in quanto fornitrice di servizi di controllo estesi a tutto il traffico aereo operativo (OAT) e al traffico aereo generale (GAT) negli spazi aerei di competenza. Se, tuttavia, i sistemi di controllo del traffico aereo italiano sono tra i più sicuri a livello mondiale, non si deve dimenticare che anche attacchi non direttamente legati alla compromissione di un'infrastruttura critica potrebbero causare danni collaterali rilevanti: basti pensare a campagne di malware[10], suscettibili di determinare effetti inaspettati e, in qualche caso, molto gravi sui sistemi di Air traffic Management (ATM) o di Air Traffic Control (ATC).
Com'è stato osservato, a livello nazionale, l'Aeronautica Militare Italiana, per quel che concerne la risposta a eventuali minacce, affronta la Cyber Defense nell'ambito delle predisposizioni che il Sistema-Paese ha già posto in essere, sia a livello normativo che operativo, attraverso strutture ad hoc predisposte denominate "Computer emergency response team" (CERT) (Gori and Germani, 2011).
In questo quadro di riferimento, riveste la massima importanza l'obbligo di assicurare nei servizi dell'Air Traffic management (ATM) adeguati standard dei principi della sicurezza cosiddetti "CIS" (ossia Communication and Information Systems) garantendo l'integrità delle comunicazioni e dei dati operativi, la protezione del flusso delle informazioni e adeguati parametri di business continuity[11] (Green, 2015).
Per l'analisi e il fronteggiamento della minaccia attuale e di prevedibile sviluppo, a livello nazionale, sono state poste in essere, oltre alle specifiche attività correlate al traffico aereo operativo (OAT), al traffico aero generale (GAT) e alla difesa aerea nazionale "Renegade"[12] anche azioni a più ampio spettro, come l'aumento della percezione e della consapevolezza (cyber-awareness) delle problematiche di

[8] Per business continuity si intende, com'è noto, la 'continuità operativa', ovvero la capacità di un'organizzazione di continuare a erogare prodotti e servizi a livelli standard a seguito del verificarsi di un dato incidente.

[9] Con "disaster recovery" (in italiano, recupero dal disastro) nell'ambito della sicurezza informatica si intende l'insieme delle misure tecnologiche e logistico-organizzative atte a ripristinare quei sistemi, dati e infrastrutture necessari all'erogazione di servizi di business per imprese o organizzazioni di varia natura, a fronte di gravi emergenze che ne intacchino la regolare attività.

[10] Termine derivante dalla contrazione di malicious software, riferito ad un programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

[11] Ci si riferisce a dati e informazioni operative, sistemi informativi automatizzati - reti e servizi di comunicazioni terrestri e radio - inclusi i sistemi automatizzati di tipo avionico, piattaforme e sensori, oltre al fattore umano ovvero alla componente del personale.

[12] Vengono chiamati "renegade" in gergo tecnico quegli aerei civili in arrivo o transito nello spazio aereo nazionale, la cui condotta sia potenzialmente pericolosa per la sicurezza in quanto riconducibile ad una possibile azione terroristica.

sicurezza da affrontare insieme a tutti gli stakeholder della Forza Armata, l'intensificazione della formazione e il potenziamento dell'addestramento sulle tematiche relative agli aspetti di CIS Security, nonché l'introduzione della cyber-defense nell'ambito della pianificazione e delle esercitazioni operative, come previsto dall'Alleanza atlantica (Lynn, 2010; U.S. Department of Defense, 2011a).
In altri termini e in sintesi, l'Aeronautica italiana persegue l'obiettivo di conseguire più elevati standard di security per il traffico aereo operativo e quello generale.

3. Protezione dell'infrastruttura critica dalla minaccia cibernetica: dalla Cyber-Defense alla Cyber-Resilience

Ci muoviamo, oggi più che mai, in contesti di rapida evoluzione della tecnologia e delle insidie associate ad essa, che impongono sempre più la necessità di ricorrere a sistemi di protezione dalla minaccia cibernetica, che è in continua ed incessante evoluzione.
Il cyberspace, com'è ampiamente noto, è teatro di warfare e in esso aleggia lo spettro della multiforme criminalità[13].
Il cybercrime rappresenta attualmente una delle maggiori minacce alla sicurezza, sia in ambito militare che civile. La cybersecurity costituisce la risposta a tale minaccia. Essa ha l'obiettivo di garantire confidenzialità, integrità e disponibilità dell'informazione ed è imperniata sulla cyber-resilience (Patel, 2016), ovvero sull'introduzione di misure atte a resistere agli attacchi informatici preservando le capacità funzionali di un sistema (Haimes, 2009).
L'architettura di ogni infrastruttura protettiva poggia su tre presupposti fondamentali: la sicurezza, utile a proteggere i propri asset critici da minacce note ed emergenti; la vigilanza, vantaggiosa per aumentare la consapevolezza della minaccia e la localizzazione delle attività antagoniste; la resilienza (Castaldo e Gatti, 2019), fondamentale per potenziare la capacità di pronta reazione agli attacchi.
In base allo scenario operativo - in un normale approccio orientato alla cyber-security - viene effettuata un'analisi del rischio di sicurezza del 'Sistema', che tiene conto delle minacce e della vulnerabilità corrispondenti ai dati da proteggere (Aven, 2011)[14].
Nello specifico, l'analisi del rischio deve individuare innanzitutto le risorse da proteggere: le componenti - hardware e software - del Sistema, i dati e le informazioni che il sistema deve gestire nonché i dispositivi di memorizzazione. Vengono, in seguito, identificate tutte le possibili minacce al sistema e, per ogni minaccia, tutte le vulnerabilità associate; vengono considerati aspetti quali la capacità del nemico e la zona in cui opera il sistema nonché le misure di sicurezza da adottare (Green, 2015).
Sulla base dell'analisi del rischio si stabiliscono le Contromisure del Sistema, al fine di garantire che la riservatezza, l'integrità e la disponibilità delle informazioni elaborate, memorizzate e trasmesse dal Sistema non siano alterate o compromesse.
Le Contromisure, poi, porteranno alla definizione dei Requisiti di Sicurezza del Sistema, che necessitano di adeguata verifica (Lynn, 2010; U.S. Department of

[13] Tra le principali organizzazioni criminali si trovano gli hacktivisti, i criminali cibernetici e i gruppi terroristici in generale.

[14] L'analisi di rischio viene, peraltro, utilizzata anche per supportare il processo di certificazione.

Defense, 2011a). La sicurezza aumenta con la qualità, l'affidabilità e la robustezza di un sistema.
Abbiamo visto precedentemente come i sistemi che utilizzano in modo intensivo reti di comunicazione e tecnologie digitali per il controllo, nonché scambio di grande quantità di informazioni, siano particolarmente esposti agli attacchi cibernetici; attacchi da cui però occorre necessariamente difendersi o, meglio, opporre resistenza ed essere resilienti, recuperare.
Nel mondo aeronautico, essendo i sistemi complessi e altamente integrati potenzialmente vulnerabili, è necessario che gli aspetti di sicurezza vengano affrontati in tutto il ciclo di vita dello sviluppo dei sistemi (Patel, 2016; Ouyang, 2014).
Analisi di safety e di security, e i relativi standard di certificazione, sono stati a lungo mondi separati: questi mondi ora richiedono un approccio combinato.
La security è indispensabile per la safety. In presenza di cyber attacchi la safety rischia di essere compromessa con conseguenze catastrofiche per cui un errore di progettazione e/o di realizzazione su un componente non safety critical può costituire un pericoloso 'punto di accesso' per un attacco informatico con il pericolo di infettare componenti safety critical (Corradini e Franchini, 2016).
Idealmente, gli aspetti legati alla sicurezza dovrebbero essere considerati in un'ottica sistemica, per evitare inutili duplicazioni a livello dei sottosistemi o lasciare aree di vulnerabilità (Fang, Pedroni e Zio, 2016).
Per seguire la tecnologia mutevole e mitigare le conseguenze dei cyber attacchi appare, infine, essenziale lo sviluppo di approcci nuovi (Patel, 2016; Fujita et al., 2018).
A livello organizzativo aziendale, oltre che naturalmente governativo-istituzionale, è divenuto così imprescindibile investire sullo sviluppo tecnologico per aumentare la resilienza cibernetica in un contesto di evoluzione, o di passaggio, dalla cyber defence alla cyber resilience, laddove la cyber defence cerca di evitare che gli avversari violino i sistemi mentre la cyber resilience mira a rendere i sistemi del cyber spazio più difficili da sfruttare.
I sistemi, nel dominio cyber, sono resilienti allorquando resistono agli attacchi informatici preservando le capacità funzionali e, quando, in caso di soccombenza, sono in grado di ripristinare le proprie funzionalità nel più breve tempo possibile (Haimes, 2009).

4. Alcune implicazioni, considerazioni e indicazioni per il futuro

Il cyberspace, abbiamo affermato, è teatro di warfare e il cybercrime rappresenta, attualmente, una delle maggiori minacce alla sicurezza, sia in ambito militare che civile. Questa minaccia, abbiamo visto, è particolarmente elevata per i sistemi che supportano la movimentazione fisica di persone e merci, come i sistemi di gestione e controllo del traffico aereo. La cyber-security costituisce la risposta a tale minaccia; essa è imperniata sulla cyber-resilience, ovvero sull'introduzione di misure atte a resistere agli attacchi informatici preservando le capacità funzionali di un dato sistema.
Abbiamo visto anche come, nell'ambito delle strategie difensive, sia in atto una transizione dalla cyber-defense alla cyber-resilience. Tale evoluzione mira a rendere le infrastrutture critiche più resilienti rispetto al passato, passando idealmente da un

orientamento debolmente reattivo agli attacchi ad uno idealmente proattivo, con sistemi e strutture ridondanti, in termini informatici, ed ingegneristicamente concepite in modo tale da assicurare un comportamento ottimale, in condizioni standard, e resiliente under attack.
Dalle riflessioni fin qui svolte emerge che, sullo specifico tema della protezione dell'infrastruttura informatica che avrà il compito di gestire il traffico aereo nel prossimo futuro, esso dovrebbe essere affrontato considerando tale infrastruttura come critica, o di servizio critico, ovvero un elemento essenziale per lo sviluppo del Sistema Paese.
Abbiamo altresì affermato, facendo riferimento alla gestione del traffico aereo, che si tratta di una struttura il cui controllo remoto non nasce 'security embedded' e che, pertanto, richiede nel tempo lo sviluppo di opportune modalità di controllo oltre che della loro correzione.
Posto che il rischio di attacco cyber non è eliminabile, ma solo mitigabile, per fronteggiare la molteplice e mutante minaccia occorrono in primis investimenti a livello tecnologico-informatico e di know-how, a livello statuale ma anche industriale. Concepire infrastrutture critiche resilienti sin dal design preliminare richiede, inoltre, accordi strategici di cooperazione pubblico-privato, in particolare tra il comparto militare e quello civile, in un frame normativo, anche europeo, ancora disorganico e perciò migliorabile.
Il dibattito sul conflitto cibernetico ha conosciuto negli ultimi anni un'intensificazione senza precedenti. La cyber-security, tuttavia, rappresentando un ambito relativamente nuovo, richiede un'attenta regolazione, che recepisca stimoli e indicazioni da tutti gli altri comparti. È quindi da ritenere di fondamentale importanza dotarsi, a livello globale, di linee guida e di approcci standardizzati sia in ambito governativo che in quello di infrastrutture critiche. Al riguardo è opportuno sottolineare che l'Italia non si è ancora dotata di una strategia nazionale per la protezione di tali infrastrutture e di una snella organizzazione che definisca gli attori che, a vario titolo, sono responsabili in materia. Servirebbe con urgenza, quindi, un quadro normativo organico per individuare le infrastrutture critiche nazionali e per determinare le modalità di protezione attraverso un sistema sinergico tra istituzioni, operatori e industria (Ouyang, 2014; Marchetti, 2013). Ma affinché la risposta alle minacce cyber non provenga più in futuro solo dai dipartimenti ICT delle diverse organizzazioni, occorre un cambiamento culturale ed organizzativo epocale.
Per pervenire ad un approccio 'cyber security-based' e per aumentare la cyber awareness paiono necessari investimenti in formazione e training, come quelli che negli ultimi tempi ha fatto l'Aeronautica Militare Italiana. Lo stesso sta accadendo in grosse realtà aziendali del comparto aerospazio e difesa, come ad esempio Leonardo S.P.A., che da qualche anno ha creato una divisione Cyber specifica ed investe molto nel cyber security training.
A livello organizzativo, in primis nelle company, sembra impellente un modello 'cybersecurity centric' in cui la cultura della difesa e della resilienza permei tutti i livelli aziendali (Castaldo, 2018). Tenendo conto però che nel cyberspace la vulnerabilità principale sia di tipo umano, permangono in Italia grosse aree da sensibilizzare (si pensi, ad esempio, alla pubblica amministrazione) e c'è molto lavoro ancora da fare nelle organizzazioni complesse d'ogni tipo.
Le nuove forme di manaccia emergente impongono, concludendo, un incremento di collaborazione tra il mondo militare e quello civile. Considerazione, questa, che convince della necessità di un'evoluzione dei rapporti pubblico-privato, fatta di leale cooperazione e di mutuo supporto (Caravelli and Jones, 2019).

Più specificatamente, essendo le infrastrutture critiche, come quella dell'Air Traffic Management, sistemi con molteplici aperture alla minacce cyber, quanto più si capiranno la loro vulnerabilità e i loro impatti, tanto più si sarà in grado di decidere al meglio dove investire in termini di risorse umane, oltre che naturalmente di tecnologie, puntando allo sviluppo di sistemi e soluzioni, basandosi sulle eccellenze che l'Italia produce e facendo sistema all'interno di una strategia nazionale di sviluppo della cyber-security che, se interpretata in quest'ottica, può rendere il Paese competitivo con le più importanti realtà industriali mondiali.

Riferimenti bibliografici

Adams, J. (2001) Virtual Defense, Foreign Affairs, 80 (3), pp. 98-112.

Andress, J., Winterfeld, S. (2014) Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier, Waltham.

Aven, T. (2011) On some recent definitions and analysis frameworks for risks, vulnerability, and resilience, Risk Analysis, 31 (4), pp. 515-522.

Caravelli, J., Jones, N. (2019) Cyber Security: Threats and Responses for Government and Business. Praeger Security International, Westport, Connecticut.

Castaldo, F. (2018) I sistemi di gestione del traffico aereo e l'incombente minaccia del crimine: la necessità di un modello organizzativo cyber-security centric, Rivista Italiana di Conflittologia, 36, pp. 29-48.

Castaldo, F. (2019) Scenari conflittuali, guerra elettronica e minacce nel cyber space: sfide strategiche e organizzative nei futuri ambienti di combattimento, Rivista Italiana di Conflittologia, 37, pp. 59-83.

Castaldo, F., Gatti, M. (2019) Tempestività e resilienza: l'esperienza dei piloti al servizio del business, Rivista Italiana di Conflittologia, 39, pp. 23-41.

Colantoni, M. (2006) Controllo del traffico aereo. Principi, regole e procedure. IBN Editore, Roma.

Corradini, I., Franchini, L. (2016) Ingegneria sociale. Aspetti umani e tecnologici, Themis, Roma.

Fang, Y.P., Pedroni, N., Zio, E. (2016) Resilience-based component importance measures for critical infrastructure network systems, IEEE Transactions on Reliability, 65 (2), pp. 502-512.

Fujita, H., Gaeta, A., Loia, V. Orciuoli, F. (2018) Resilience Analysis of Critical Infrastructures: A Cognitive Approach Based on Granular Computing, IEEE Transactions on Cybernetics, 49 (5), pp. 1835-1848.

Geers, K. (2009) "The Cyber Threat to National Critical Infrastructures: Beyond Theory", The Information Security Journal: A Global Perspective, 18 (1), pp.1-7.

Gori, U. (2015) Cyber Warfare 2014. Armi cibernetiche, sicurezza nazionale e difesa del business. Franco Angeli, Milano.

Gori, U., Lisi, S. (2014), a cura di, Information Warfare 2013. La protezione cibernetica delle infrastrutture nazionali. Franco Angeli, Milano.

Gori, U., Germani, L.S. (2011), a cura di, Information Warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale. Franco Angeli, Milano.

Green, J.A. (2015) Cyber Warfare. A multidisciplinary analysis. Routledge, New York.

Haimes, Y.Y. (2006) On the definition of vulnerabilities in measuring risks to infrastructures, Risk Analysis, 26 (2), pp. 293-296.

Haimes, Y.Y. (2009) On the definition of resilience in systems, Risk Analysis, 29 (4), pp. 498-501.

Healey, J.M. (2014) Confidence-Building Measures in Cyberspace. A multistakeholder Approach for Stability and Security, Atlantic Council.

Klimburg, A. (2017) The Darkening Web: The War for Cyberspace. Penguin Press, New York.

Liang, Q., Xiangsui, W. (2001) *Guerre senza limiti. L'arte della guerra asimmetrica* tra terrorismo e globalizzazione. Libreria Editrice Goriziana, Gorizia.

Lynn, W.J. (2010) Defending a New Domain: The Pentagon's Cyberstrategy, Foreign Affairs, 89(5), pp. 97-108.

Marchetti, E. (2013) Private Military and Security Companies: il caso italiano nel contesto internazionale, Quaderni IAI, 7, Edizioni Nuova Cultura, Roma.

Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering & System Safety, 121, pp. 43-60.

Patel, R.N. (2016) A container-based Approach to Cyber Resilience. Florida Institute of Technology.

Rosenzweig, P. (2013) Cyber Warfare. How Conflicts in Cyberspace Are Challenging America and Changing the World. Praeger, Santa Barbara.

Teti, A. (2018) Cyber Espionage e Cyber Counterintelligence: Spionaggio e Controspionaggio cibernetico. Rubbettino Editore, Soveria Mannelli (CZ).

U.S. Department of Defense (2011a) Department of Defense Strategy for Operating in Cyberspace.

U.S. Department of Defense (2011b) Unmanned Systems Integrated Roadmap FY 2011-2036.

Wright, D., Grego, L., Grounlund, L. (2005) The Physics of Space Security, American Academy of Arts and Sciences, Cambridge, MA.