I sistemi di gestione del traffico aereo e l'incombente minaccia del crimine: la necessità di un modello organizzativo cyber security centric

di Francesca Castaldo

1. Introduzione

Il largo impiego delle tecnologie digitali applicate alle comunicazioni e all'informazione ha accresciuto a dismisura, negli ultimi anni, 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 sistemi connessi all'acquisizione delle informazioni come i sistemi meteorologici, i satelliti per le comunicazioni, i droni per applicazioni civili, i sistemi di gestione e controllo del traffico aereo o navale.

I sistemi satellitari, le comunicazioni radar civili e militari, gli *UnmannedAerialVehicles* (UAV), i sistemi di controllo del traffico aereo o navale sono, in quasi tutti i casi, sistemi che supportano la movimentazione fisica di persone e merci, dispositivi connessi all'acquisizione delle informazioni e sistemi di supporto ai trasporti

[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.

di vario genere. Si tratta, pertanto, di aree chiave per lasicurezza di una nazione [K.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*[J. Andress, S.Winterfeld, 2014].

Le piattaforme tecnologiche dell'*Air traffic management*(ATM) sono sistemi aperti e interdipendenti, come SESAR[2], in cui l'informazione è l'essenza.Tali strutture perònel nostro Paesenon sono state concepite con un controllo remoto 'security embedded' e, conseguentemente, necessitano nel tempo dello sviluppo di opportune modalità di controllo e della loro correzione [F. Castaldo, 2019].

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.

I sistemi di controllo del traffico aereo italiano sono tra i più sicuri a livello mondiale ma non si deve dimenticare che anche attacchi non direttamente legati alla compromissione di un'infrastruttura critica possano causare comunque danni collaterali rilevanti: basti pen-

[2]SESAR (acronimo dell'inglese *Single EuropeanSky 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.

sare a campagne di *malware*[3],suscettibili dideterminare effetti inaspettati e, in qualche caso, molto gravi sui sistemi di *Air traffic Management* (ATM) o di *Air Traffic Control* (ATC).

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[4], oltre che di preminente interesse tra le minacce emergenti, in particolare nell'ambito del controllo del traffico aereo.

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.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 ne-

[3] 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.

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

vralgica per le attività terroristiche [D. Wright, L. Grego, L. Grounlund, 2005].

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 [P. Rosenzweig, 2013].

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 persistentthreat*[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 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[K. Geers, 2009].

Il sistema di 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 PilotedAir Systems*

[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.

- RPAS)nel flusso ordinario di traffico [U.S. Department of Defense, 2011 b].

La circolazione aerea tra meno di un ventennio sarà effettuata in gran parte dai velivoli pilotati remotamente(i cosiddettidroni)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 [D. Wright, L. Grego, L. Grounlund, 2005].

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 [U.S. Department of Defense, 2011 b].

La sorveglianza dello spettro elettromagneticorappresenta, dunque, uno degli aspetti vitali per garantire la sicurezza di RPAS civili e militari.

Ad aumentare ulteriormente tale complessità 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.

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 [J. Adams, 2001].

A livello nazionale italiano, l'Aeronautica Militare, per quel che concerne la risposta a eventuali minacce, affronta la *Cyber-defence* 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 emergencyresponse team" (CERT)[U. Gori, L.S. 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,Information system* e *Information assurance*) garantendo l'integrità delle comunicazioni e dei dati operativi, la protezione del flusso delle informazioni e adeguati parametri di *business continuity*[7] [W.J. Lynn, 2010].

La sicurezza è uno dei riflessi della sovranità (statale) e il ruolo dello Stato nella protezione dei propri assetti strategici è imprescindibile, in quanto solo lo Stato ha la forza del contrasto attivo e della gestione delle informazioni qualificate per la tutela, attraverso gli organismi di intelligence e di Polizia [F. Castaldo, 2018].

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 "Renega-

[7] 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.

de"[8], anche azioni a più ampio spettro, come l'aumento della percezione e della consapevolezza (*cyber-awareness*) delle problematiche di sicurezza da affrontare insieme a tutti gli stakeholder della Forza Armata, l'intensificazione della formazione e il potenziamneto-dell'addestramento sulle tematiche relative agli aspetti di *CIS Security*, nonché l'introduzione della *cyber-defence* nell'ambito della pianificazione e delle esercitazioni operative, come previsto dall'Alleanza atlantica [M. Colantoni, 2006].

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. Entità ostili nel cyberspace

Il cyberspace, com'è ampiamente noto, è teatro di *warfare* e in esso aleggia lo spettro della multiforme criminalità. Tra le principali organizzazioni criminali si trovano gli *hacktivisti*[9], i criminali cibernetici e i gruppi terroristici in generale.

In realtà organizzazioni terroristiche come al-Qaeda e Isis hanno finora utilizzato lo spazio cibernetico per diffondere la propria propaganda, reclutare nuovi combattenti, finanziare le proprie attività e

[8]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.

[9] Il termine deriva dall'inglese "hacktivism", dato dall'unione di due parole, *hacking* e activism, ed è usato per indicare le pratiche dell'azione diretta digitale in stile hacker. Gli hacktivisti sono, quindi, gli hacker del software, attivisti digitali, guastatori mediatici, militanti politici che considerano i computer e le reti come strumenti di cambiamento sociale e terreno di conflitto.

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*[10]o hanno dato vita a intrusioni negli account di social media, di per sé non particolarmente complessi da violare [A. Klimburg, 2017].

Gli obiettivi preferiti dagli*hacktivisti*, tra cui spicca per notorietà il collettivo di 'Anonymous'[11], sono stati finora le reti di varie istituzioni politiche o pubbliche amministrazioni ritenute in contrasto con i propri valori o la propria ideologia anche se alcuni hacker jihadisti si sono più volte vantati di essere riusciti a penetrare le ben più protette reti militari statunitensi, inglesi e italiane. L'azione di questi soggetti non sembra abbia finora avuto come obiettivo quei sistemi informatici che, se danneggiati o malfunzionanti, potrebbero provocare danni, anche fisici ad individui ed entità [A.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

[10] Il *web defacement*indica la modifica di contenuti della homepage o delle sottopagine di un sito.

[11]*Anonymous* è un fenomeno nato nel 2003 ispirandosi alla pratica della pubblicazione anonima di immagini e commenti su internet e, più in generale, sul web. Negli anni è passato ad indicare una forma di attivismo che identifica singoli utenti o intere comunità online che agiscono anonimamente, in modo coordinato o anche individualmente, per perseguire un obiettivo concordato anche approssimativamente. Il termine viene usato anche come "firma" adottata da gruppi di *hacktivists* che intraprendono proteste o azioni sotto l'appellativo fittizio di "Anonymous" e, più genericamente, per riferirsi ai seguaci della subcultura di internet.

software malevoli hanno contribuito a promuovere l'aumento del fenomeno del crimine online, rispetto a forme più consuete di reato [J. Andress, S.Winterfeld, 2014].

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 [Q. Liang, W.Xiangsui, 2001].

Come precedentemente detto, l'Isis dichiara di possedere competenze avanzate nel settore cyber anche se, ad oggi, non si registrano danni rilevanti alle infrastrutture critiche causati dai terroristi islamici ma solo alcuni isolati casi di*defacement*di siti web o poco altro.

Se è da un lato vero che competenze avanzate sono reperibili anche sul dark market, 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 (come nel caso di Parigi) per cui effettivamente attacchi a infrastrutture critiche sono di fatto minacce legate, più che a bande del terrore, ad attori statuali che possono pensare di inserire *malware*nei sistemi di uno stato nemico, per poi farli detonare nel momento del bisogno [J.A. Green, 2015].

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 [D.H. Gray, A.Head, 2009].Risulterebbe, invece, più semplice per 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"[12]e di "disasterrecovery"[13], che possono permettere al sistema di continuare a lavorare a fronte di fallimenti di parti dello stesso [A. Klimburg, 2017].

La lotta al *cybercrime*necessita di un impianto legislativo e strumentale forte ed efficace ma, soprattutto, di buone capacità tecnico-operative: i cyber-criminali, come abbiamo sottolineato, al di là della loro preparazione e organizzazione, possono causare enormi danni a cose e persone. Discutere di sicurezza dello spazio cibernetico, d'altronde, pare oggi scontato: è inutile parlare di un 'se' proteggere, quanto piuttosto di 'come' proteggere efficacemente.

[12] 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.

[13] Con "disasterrecovery" (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.

4. Protezione 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 *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*, ovvero sull'introduzione di misure atte a resistere agli attacchi informatici preservando le capacità funzionali di un sistema [R.N. Patel, 2016].

L'architettura di ogni infrastruttura protettiva poggia su tre presupposti fondamentali: la sicurezza, utile a proteggere i propri *asse-t*critici da minacce note ed emergenti; la vigilanza, vantaggiosa per aumentare la consapevolezza della minaccia e la localizzazione delle attività antagoniste; la resilienza, fondamentale per potenziare la capacità di pronta reazione agli attacchi.

In base allo scenario operativo -in un normale approccio orientato alla cyber-security - vieneeffettuata un'analisi del rischio di sicurezza del Sistema, che tiene conto delle minacce e della vulnerabilità corrispondenti ai dati da proteggere [Great Britain. Ministry of Defence, 2004].

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 ne-

mico e la zona in cui opera il sistema nonché le misure di sicurezza da adottare [J.A. Green, 2015].

L'analisi di rischio viene utilizzata anche per supportare il processo di certificazione. 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 [U.S. Department of Defense, 2011a].

È opportuno sviluppare, in modo adeguato e approfondito, suggeriscono gli esperti del settore, metodologie di test atte a simulare i cyber attacchi e dotare i sistemi di funzionalità di monitoraggio 'security-oriented'per controllare i sistemi stessi e le reti di comunicazione, oltre che per rilevare tracce di attacchi indesiderati [W.J. Lynn, 2010].

La sicurezza aumenta con la qualità, l'affidabilità e la robustezza di un sistema.

Abbiamo visto precedentemente come i sistemi che utilizzano 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, essere resilienti, recuperare.Ci riferiamo alla resilienza nel dominio cibernetico con riguardo all'introduzione di misure atte a resistere agli attacchi informatici preservando le capacità funzionali di un dato sistema.

I sistemi, pertanto, 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 [Y.Y. Haimes, 2009].

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.

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 *safetycritical*può costituire un pericoloso 'punto di accesso' per un attacco informatico con il pericolo di infettare componenti *safetycritical* [I. Corradini, L. Franchini, 2016].

Idealmente, gli aspetti legati alla sicurezza dovrebberoessere considerati in un'ottica sistemica, per evitare inutili duplicazioni a livello dei sottosistemi o lasciare aree di vulnerabilità.

Per seguire la tecnologia mutevole e mitigare le conseguenze dei cyber attacchi appare, infine,essenziale lo sviluppo di approcci nuovi [J.Andress,S. Winterfeld, 2014].

A livello 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.

5. **L'urgenza di un modello organizzativo *cybersecuritycentric***

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 [P. Rosenzweig, 2013].

L'Atlantic Council, basandosi sulle idee e sulle prassi consolidate in tema di non-proliferazione nucleare, ha stilato nel 2014 un rapporto sulla cyber-deterrenza noto come "Confidence-building measures in cyberspace", che fa da sfondo alle relazioni tra gli Usa e il resto del mondo, in particolare le macroregioni Russia, Cina ed Europa. Questo studio, che ambisce a costituire una sorta di 'grammatica della dissuasione' e dell'equilibrio cibernetico si articola in quattro set di misure proposte, le cosiddette 'confidence-building measure', la cui disamina esula dagli scopi del presente lavoro.[14]

In sintesi, potremmo affermare che il rapporto dell'Atlantic Council lancia una *road map* per la cyber-deterrenza, costituita da misure atte ad aumentare la fiducia tra le macroregioni attualmente differenziate di Usa, Cina, Russia ed Europa, indicando nell'alleanza NATO il punto nodale nevralgico per la loro elaborazione ed implementazione attraverso una via duplice: *bottom-up*, che sollecita gli attori privati rilevanti a tenere in costante considerazione gli interessi pubblici, e *top-down*, che affida comunque al comparto militare e

[14]Per un'analisi approfondita delle*Confidence-building measures in cyberspace* si rimanda, in particolare, a Healey J.M., 2014.

governativo il ruolo di raccordo del dialogo internazionale [J.M. Healey, 2014].

Le nuove forme di manaccia emergente cui abbiamo fatto riferimento impongono oltremodo, oggi più che mai, un incremento di collaborazionetra il comparto 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.

Non meno importante è la consapevolezza che la sicurezza delle informazioni non è soltanto un elemento tecnologico, ma un processo che coinvolge tutta l'organizzazione, a partire dalle persone che la compongono. È quindi fondamentale l'adozione di processi virtuosi, che partano dalla consapevole gestione del rischio e si propaghino in ciascuna componente della struttura, cui è richiesto di partecipare come attore protagonista alla difesa e di considerare la *security* una parte essenziale e trasversale dei processi (dagli investimenti alle operazioni, dalla manutenzione alla gestione dei rapporti con le terze parti) con un approccio volto alla risoluzione continua delle vulnerabilità [J. Caravelli, N. Jones, 2019].

La *cybersecurity* non può, in altri termini, limitarsi alle componenti ICT dei soli comparti difesa, sicurezza e dell'intelligence community, già presidiate dalle singole strutture nazionali preposte, ma deve interessare l'intero universo gestionale delle soluzioni ICT.

Evidentemente la sicurezza delle informazioni gioca un ruolo di primissimo piano all'interno della strategia difensiva delle diverse organizzazioni, pubbliche e private, come elemento pervasivo di tutte le iniziative in corso [U. Gori, 2015].

Un tale modello organizzativo "cyber-security based" è impellente, in particolare, per quelle aziende che operano a vario titolo nel comparto della Difesa e della Security in senso lato. L'organizzazione deve essere permeata a tutti i livelli di cultura della *cyberse-*

curity, che, pertanto, non può continuare ad essere relegata al dipartimento di Information Technology [J. Caravelli, N. Jones, 2019].

Per essere efficace, in altri termini, una configurazione organizzativa basata sulla sicurezza informatica deve coinvolgere tutti i livelli aziendali, dagli impiegati al Consiglio di Amministrazione.

Per raggiungere questo obiettivo, sia a livello istituzionale che aziendale, in Italia è stato recentemente introdotto un Framework nazionale per la *cyber-security*, teso proprio a porre l'attenzione dei Consigli di amministrazione e del 'Comitato Rischi' aziendale verso le minacce che arrivano dal *cyberspace*.

In questa cornice è opportuno sottolineare come l'anello debole della catena sia il fattore umano: non è un caso che le aziende non vengano attaccate attraverso le vulnerabilità tecnologiche del proprio perimetro di protezione ma attraverso i propri dipendenti con campagne di *spearphishing*[15], in modo da penetrare nell'organizzazione attraverso una vulnerabilità umana[16] [I. Corradini, L. Franchini, 2016].

6. Considerazioni per il futuro

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 af-

[15] Con il termine *spearphishing* ci si riferisce ad un tipo di truffa in cui viene presa di mira una persona in particolare, più generalmente un dipendente di un'azienda specifica, con lo scopo di estorcergli dati personali (come username, password, numeri della carta di credito) mediante tecniche di ingegneria sociale digitale.

[16] Si pensi, a scopo esemplificativo, ad un dipendente di un'azienda o di una pubblica amministrazione che clicca sul testo di una e-maildi *phishing*in grado di caricare il *malware* direttamente nel proprio computer.

frontato 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 remotonon nasce 'security embedded' e che, pertanto, richiede nel tempo lo sviluppo di opportune modalità di controllo oltre che della loro correzione.

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 e di tecnologie, puntando allo sviluppo di sistemi e soluzioni, puntando sulle eccellenze che l'Italia produce e facendo sistema all'interno di una strategia nazionale di sviluppo della cybersecurity che, se interpretata in quest'ottica, può rendere il Paese competitivo con le più importanti realtà industriali mondiali.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 funzionale 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 [E. Marchetti, 2013].

Gli aspetti di cybersecurity rendono peraltro necessaria la definizione di un'adeguata strategia nazionale per la protezione dell'intera infrastruttura di rete (wired e wireless), con la necessità di dover analizzare ed identificare per tempo le eventuali aree di vulnerabilità e le possibili minacce, così da implementare adeguate forme di protezione, eliminando il rischio o mitigandolo fino a renderlo accettabile [G. Scagnetti, 2013].

In una cornice mondiale fortemente disomogenea dal punto di vista della sicurezza, probabilmente chi per primo riuscirà a definire un'efficiente e resistente infrastruttura informatica imporrà *de facto* i propri standard e la propria regolamentazione a livello mondiale.

Le aziende e gli operatori italiani del settore, in realtà, hanno da tempo assunto un ruolo primario, ponendosi all'avanguardia, in particolare a livello dell'innovazione. Conseguentemente, è di essenziale importanza cercare di preservare il patrimonio tecnologico dell'industria italiana dalle potenziali acquisizioni, da parte di gruppi stranieri, di quelle realtà nazionali rilevantinel settore sicurezza e difesa. Occorrerebbe, poniamo ancora l'enfasi, la definizione di una strategia coordinata delle istituzioni mirante alla crescita e alla competitività delle società italiane che operano in settori strategici.

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 SecurityPractitioners*, Elsevier, Waltham.

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

Castaldo F. (2018), *Fronteggiareilnemico in arene competitive turbolente: l'importanzadella fiducia e dellecapacitàdinamichenellealleanzestrategiche*, «RivistaItaliana di Conflittologia», n.35.

Castaldo F.(2019), *Scenariconflittuali, guerraelettronica e minaccenel cyberspace: sfidestrategiche e organizzativeneifuturiambienti di combattimento*, «RivistaItaliana di Conflittologia», n.36.

Colantoni M.(2006), *Controllo del trafficicoaereo. Principi, regole e procedure*, IBNEditore, Roma.

Corradini I, Franchini L. (2016), *Ingegneriasociale. Aspettiumani e tecnologici*, Themis, Roma.

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., Germani L.S. (2011) (a cura di), *Information Warfare. Le nuove minacce provenientidal cyberspazio alla sicurezza nazionale*, Franco Angeli, Milano.

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

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

Gray D.H, Head A. (2009), *The importance of the internet to the post-modern terrorist and its roleas a form of safe haven*, «European Journal of Scientific Research», 25(3), pp.396-404.

Great Britain. Ministry of Defence (2004), *Delivering Security in a Changing World: Future Capabilities*.

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

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 multistakeholderApproach 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 eglobalizzazione*, 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 contestointernazionale*, «Quaderni IAI», n.7, Edizioni Nuova Cultura, Roma.

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

Presidenza del Consiglio dei Ministri (Dicembre 2013), *Quadro Strategico Nazionale per laSicurezza dello Spazio Cibernetico*.

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

Scagnetti G. (2013), *La geostrategianelcyberspazio*, «RID - RivistaItalianaDifesa», n.7, pag. 45.

Teti A. (2018), *Cyber Espionage e Cyber Counterintelligence: Spionaggio e Controspionaggiocibernetico*, RubbettinoEditore, SoveriaMannelli (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*, 2011.

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