IAI
Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

Protezione del traffico aereo civile dalla minaccia cibernetica

di Tommaso De Zan,

Fabrizio d'Amore e Federica Di Camillo

ABSTRACT

L'impiego dell'Ict ha caratterizzato in maniera crescente l'evoluzione dell'aviazione civile. La digitalizzazione e la messa in rete di strumenti tecnologici complessi implicano delle problematiche rilevanti per la sicurezza cibernetica del settore. Il Government Accountability Office ha recentemente sottolineato come alcune vulnerabilità riscontrate nei sistemi statunitensi di gestione e controllo del traffico aereo civile possano, se sfruttate, avere serie conseguenze per la sicurezza. Da tali considerazioni scaturiscono una serie di domande sul caso italiano: su quali tecnologie si basano i nostri sistemi di gestione e controllo del traffico aereo civile? Qual è il loro livello di vulnerabilità? Quali attori possono minacciare tali sistemi? E questi attori hanno le capacità tecnologiche per condurre attacchi cibernetici tali da compromettere queste infrastrutture critiche? Le limitate risorse tecniche e i diversi obiettivi degli attori non statali esaminati in questo studio, le misure messe in campo da Enav e la funzione di prevenzione delle autorità italiane consentono di affermare che il livello di rischio a cui sono esposti nel breve periodo i sistemi Atc italiani è relativamente basso. È tuttavia necessario sottolineare la necessità di mantenere un livello di attenzione alto.

Sicurezza dei trasporti aerei | Sicurezza informatica | Italia

keywords

Protezione del traffico aereo civile dalla minaccia cibernetica

di Tommaso De Zan, Fabrizio d'Amore e Federica Di Camillo*

* Tommaso De Zan è assistente alla ricerca presso il Programma Sicurezza e Difesa dell'Istituto Affari Internazionali (IAI). Fabrizio d'Amore è professore associato presso il Dipartimento di Ingegneria informatica, automatica e gestionale (Diag) "Antonio Ruberti" e membro del Centro di ricerca di Cyber Intelligence and Information Security (Cis) dell'Università di Roma "La Sapienza". Federica Di Camillo è responsabile di ricerca presso il Programma Sicurezza e Difesa dello IAI.

· Studio prodotto nell'ambito del progetto di ricerca "Protezione del traffico aereo civile dalla minaccia cibernetica", condotto dall'Istituto Affari Internazionali (IAI) con il sostegno di Vitrociset.

ISSN 2280-6164

Lista degli acronimi

Acc	Area Control Center
Acars	Aircraft Communications Addressing and Reporting System
Aci	Airports Council International
Ads-B	Automatic Dependent Surveillance-Broadcast
Aftn	Aeronautical Fixed Telecommunication Network
Ais	Aeronautical Information Services
Als	ALerting Service
Amhs	Ats Message Handling Service
Ansp	Air Navigation Service Provider
Aois	Aeronautical Operational Information System
Aro	Air Traffic Services Reporting Office
Artas	Atm Surveillance Tracker and Server
Asm	Air Space Management
Asmgcs	Advanced Surface Movement Guidance and Control System
Atc	Air Traffic Control
Atfm	Air Traffic Flow Management
Atis	Automatic Terminal Information Service
Atm	Air Traffic Management
Atm	Asynchronous Transfer Mode
Atn	Aeronautical Telecommunication Network
Ats	Air Traffic Services
AvSec	Aviation Security
Byod	Bring-Your-Own-Device
Canso	Civil Air Navigation Services Organisation
Centcom	Central Command
Cert	Computer Emergency Response Team
Cia	Central Intelligence Agency
Cidin	Common Icao Data Interchange Network
Cis	Centre for Internet Security
Cis	Cyber Intelligence and Information Security Center
C/M	Civile/militare
Cnaipic	Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche
Cnmca	Centro nazionale di meteorologia e climatologia aeronautica
Cns	Communications, Navigation, Surveillance
Copasir	Comitato parlamentare per la sicurezza della Repubblica
Cpdlc	Controller Pilot Data-Link Communication
Cpni	Centre for the Protection of National Infrastructure
Crco	Central Route Charges Office
Cwp	Control Working Position
DDoS	Distributed denial of service
Dis	Dipartimento delle Informazioni per la sicurezza
DoS	Denial of service
Easa	European Aviation Safety Agency

ISSN 2280-6164

Eatmp	European Air Traffic Management Programme
Egnos	European Geostationary Navigation Overlay Service
Enac	Ente nazionale per l'aviazione civile
Enav	Ente nazionale per l'assistenza al volo
Esarr	Eurocontrol Safety Regulatory Requirements
Essp	European Satellite Services Provider
Faa	Federal Aviation Administration
Fbi	Federal Bureau of Investigation
Fdp	Flight Data Processing
Fdpm	Flight Plan Data Management
Fir	Flight Information Region
Fis	Flight Information Service
Gao	Government Accountability Office
Iata	International Air Transport Association
Icao	International Civil Aviation Organisation
Icc	International Communications Centre
Iccaia	International Coordinating Council of Aerospace Industries Associations
Ics	Industrial Control Systems
Ics-Cert	Industrial Control Systems Cyber Emergency Response Team
Ict	Information Communication Technology
Ids	Intrusion Detection System
Ied	Improvised explosive device
Ietf	Internet Engineering Task Force
Ifalpa	International Federation of Air Line Pilots' Associations
Ifr	Instrument Flight Rules
Ip	Internet Protocol
Ire	Interconnessione reti esterne
Ishd	Islamic State Hacking Division
Isis	Islamic State of Iraq and Syria
Isms	Information Security Management System
Iso	International Organisation for Standardisation
It	Information Technology
Itu	International Telecommunication Union
Lan	Local Area Network
Met	Aviation meteorology
Mpls	Multi Protocol Label Switching
Ms	Moduli di sicurezza
NiprNet	Nonclassified Internet Protocol Router Network
Nmoc	Network Manager Operations Centre
Notam	Notices To Air Men
Nsa	National Security Agency
Oldi	On-Line Data Interchange
Osi	Open Systems Interconnection
Osstm	Open Source Security Testing Methodology
Owasp	Open Web Application Security Project

ISSN 2280-6164

Pens	Pan European Network Services
PoP	Point of Presence
Rfc	Request for comments
Rwy	Runway
Sadis	Satellite Distribution System
Sarps	Standards and Recommended Practices
Scada	Supervisory Control and Data Acquisition
Ses	Single European Sky
Sesar	Single European Sky Atm Research
Siem	Security Information and Event Management
SiprNet	Secret Internet Protocol Router Network
Soc	Security Operation Centre
Sop	Same Origin Policy
Sql	Structured Query Language
Sqli	Sql-injection
Src	Safety Regulation Commission
Svfr	Special visual flight rules
Swim	System-Wide Information Management
Tbt	Torre-Bordo-Torre
Tcp	Transmission Control Protocol
Tls	Transport Layer Security
Tma	Terminal Control Area
Tor	The Onion Router
Tpp	Trans Pacific Partnership
Ttip	Transatlantic Trade and Investment Partnership
Uhf	Ultra high frequency
Uir	Upper Information Region
Vfr	Visual Flight Rules
Vhf	Very high frequency
Vor	Vhf Omnidirectional Radio Range
Vpn	Virtual Private Network
Wan	Wide Area Network
Xss	Cross-site scripting

ISSN 2280-6164

ISSN 2280-6164

Introduzione

Il Government Accountability Office (Gao), agenzia governativa statunitense che fornisce al Congresso servizi di valutazione ed investigazione, ha pubblicato a gennaio 2015 un rapporto[1] in cui si sottolineano alcune vulnerabilità di natura informatica riscontrate nei sistemi di controllo del traffico aereo della Federal Aviation Administration (Faa)[2]. Secondo il Gao, queste debolezze minacciano "la capacità dell'agenzia di assicurare sicurezza e continuità nelle operazioni nel sistema di spazio [aereo] nazionale". L'agenzia conclude affermando che, nonostante la Faa abbia tentato di far fronte a tali criticità, essa non ha ancora trovato soluzione ad alcune vulnerabilità che potrebbero esporre i propri sistemi informatici ad attacchi informatici[3]. In una relazione del 2010 "sulle possibili implicazioni e minacce per la sicurezza nazionali derivanti dall'utilizzo dello spazio cibernetico", il Copasir[4] citava una serie di esempi – ripresi in buona parte dall'esperienza statunitense – sull'eventualità di un attacco ai sistemi di gestione e controllo del traffico aereo (Atm/Atc)[5] a causa dell'impiego sempre più pervasivo delle tecnologie dell'informazione. Il Copasir, in particolare, sollecitava il legislatore e gli organismi della sicurezza nazionale a prestare la dovuta attenzione alla protezione dei sistemi di controllo del traffico aereo, ossia di un'infrastruttura critica funzionale alla protezione di interessi di rango costituzionale (la vita e l'incolumità delle persone in volo e a terra e la libertà di circolazione)[6]. In questa direzione va anche la dichiarazione del Cancelliere dello Scacchiere del Regno Unito George Osborne il quale, annunciando importanti investimenti governativi nel campo della sicurezza cibernetica, ha evidenziato l'alta sensibilità dei sistemi di controllo del traffico aereo[7].

Le relazioni del Copasir e del Gao evidenziano un problema centrale per la sicurezza nazionale, ossia come la crescente dipendenza dei sistemi di gestione e controllo del traffico aereo da tecnologie digitali che utilizzano la rete determini l'inevitabile introduzione di nuove vulnerabilità di natura cibernetica. Da questa considerazione emergono una serie di domande: su quali tecnologie si basano i servizi italiani di gestione e controllo del traffico aereo? I loro sistemi informatici

[1] US Government Accountability Office (Gao), *FAA Needs to Address Weaknesses in Air Traffic Control Systems*, January 2015, http://www.gao.gov/assets/670/668169.pdf.

[2] La Faa è l'agenzia del Dipartimento dei Trasporti che regola l'aviazione civile negli Stati Uniti.

[3] Aaron Cooper, "Report: Air traffic control system vulnerable to cyber attack", in *CNN Politics*, 2 March 2015, http://cnn.it/1FOFlBU.

[4] Comitato parlamentare di controllo per i servizi di informazione e sicurezza e per il segreto di Stato.

[5] Gestione del traffico aereo (Air Traffic Management, Atm) e controllo del traffico aereo (Air Traffic Control, Atc).

[6] Copasir, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, 7 luglio 2010, http://www.senato.it/leg/16/BGT/Schede/docnonleg/19825.htm. Le considerazioni del Copasir si riferiscono prevalentemente alle possibili conseguenze nel caso in cui la minaccia si realizzasse. Nella relazione non viene però espresso un giudizio sullo stato della sicurezza dei sistemi Atm/Atc in Italia.

[7] George Osborne, *Chancellor's speech to GCHQ on cyber security, 17 November 2015*, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

sono vulnerabili? Quali attori che possono minacciare questi sistemi? E questi ultimi hanno le capacità di sferrare attacchi cibernetici tali da compromettere queste infrastrutture critiche?

La presente ricerca si inserisce nel più ampio dibattito riguardante il rapporto fra le infrastrutture critiche informatizzate e la sicurezza cibernetica. Il trasporto aereo è infatti considerato un'infrastruttura critica nella maggior parte dei paesi sviluppati: a Singapore l'aviazione civile è stata riconosciuta come un settore critico per il programma "Critical Infocomm Infrastructure Protection" nel contesto del piano nazionale di sicurezza cibernetica 2018[8]; negli Stati Uniti il settore dei sistemi di trasporto è una delle 18 infrastrutture critiche elencate dalla direttiva presidenziale n. 7 sulla Sicurezza interna, nel contesto del "National Infrastructure Protection Plan"[9]; la Commissione Europea ha identificato i trasporti fra i settori critici nella "Direttiva sulle infrastrutture critiche europee" del 2006; infine, anche il Ministero degli Interni, con il decreto "Individuazione delle infrastrutture critiche informatiche di interesse nazionale" del 2008, identifica come infrastrutture critiche informatizzate "Ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute"[10].

Data la rilevanza per la sicurezza nazionale e la loro interdipendenza, le infrastrutture critiche necessitano di un livello di protezione elevato, non sempre facile da garantire. Il rapporto "2013 Italian Cyber Security Report: Critical Infrastructure and Other Sensitive Sectors Readiness", a cura del Cyber Intelligence and Information Security Center (Cis) dell'Università di Roma "La Sapienza", afferma come l'Italia registrasse dei ritardi rispetto ad altri paesi avanzati nell'implementazione di una strategia cibernetica che tenesse in debita considerazione la protezione di tali infrastrutture. In particolare, il rapporto evidenziava che nei quattro settori analizzati (pubblica amministrazione, aziende di pubblica utilità, grandi industrie e il settore finanziario) fossero presenti strutture informatizzate che, se attaccate con successo, avrebbero potuto provocare gravi conseguenze su scala nazionale ed europea. Gli operatori di questi macro settori non sembravano essere consapevoli di rappresentare dei potenziali obiettivi sensibili[11].

[8] Singapore Ministry of Transport, *Singapore hosts civil aviation cyber security conference. Press release*, 9 July 2015, http://www.news.gov.sg/public/sgpc/en/media_releases/agencies/mot/press_release/P-20150709-1.html.

[9] Kasthurirangan Gopalakrishnan et al., "Cyber Security for Airports", in *International Journal for Traffic and Transport Engineering*, Vol. 3, No. 4 (December 2013), p. 365-376, http://dx.doi.org/10.7708/ijtte.2013.3(4).02.

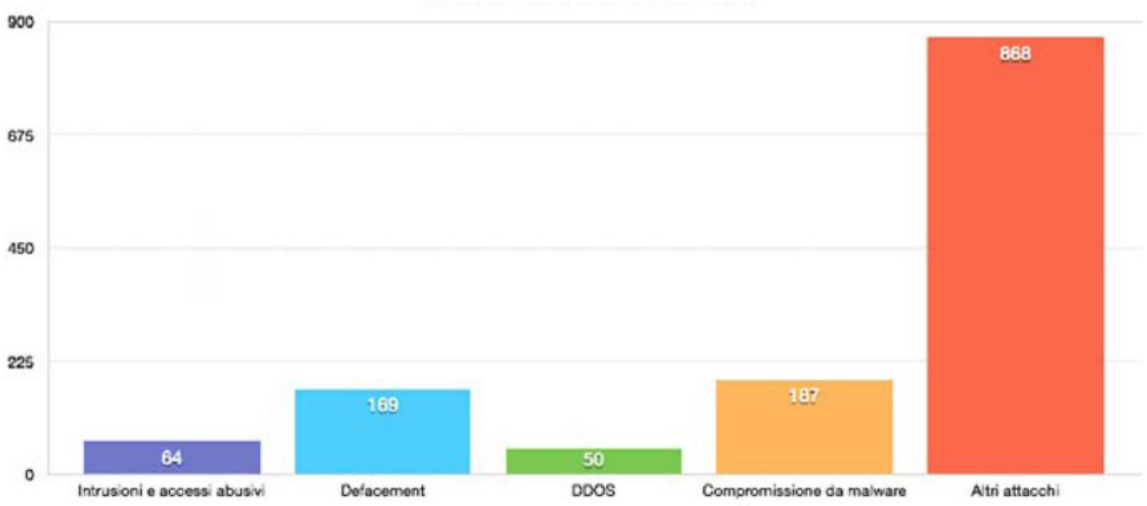
[10] Decreto del Ministero dell'Interno del 9 gennaio 2008, *Individuazione delle infrastrutture critiche informatiche di interesse nazionale*, G.U. n. 101 del 30 Aprile 2008, http://gazzette.comune.jesi.an.it/2008/101/1.htm.

[11] Cyber Intelligence and Information Security Center (Cis), *2013 Italian Cyber Security Report. Critical Infrastructure and Other Sensitive Sectors Readiness*, Roma, Università La Sapienza, December 2013, http://www.cis.uniroma1.it/sites/default/files/allegati/2013CIS-Report.pdf.

ISSN 2280-6164

Eppure i pericoli per questi sistemi informatici sensibili non sono solo potenziali, bensì reali e in aumento. Nel 2014 il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) ha rilevato 1.151 attacchi informatici, di cui 161 di tipo web defacement[12] e 50 di tipo DDoS (distributed denial of service)[13], verso siti internet istituzionali e infrastrutture critiche informatizzate italiane; fra questi vi sono 64 intrusioni e 187 compromissioni dovute a malware[14] che hanno infettato i sistemi di enti istituzionali e imprese private. Nel medesimo periodo sono state segnalate 154 potenziali vulnerabilità e 148 altri possibili attacchi[15].

Figura 1 | Attacchi gestiti dal Cnaipic nel 2014



Fonte: Rapporto Clusit 2015, p. 84.

[12] "Attacco condotto contro un sito web e consistente nel modificare i contenuti dello stesso limitatamente alla home page ovvero includendo anche le sottopagine del sito". Si veda: Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, p. 43, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf.

[13] "Un attacco di tipo denial of service (DoS) mira ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti. Una variante di questo attacco è il DDoS (Distributed Denial of Service), dal funzionamento identico ma realizzato utilizzando numerose macchine attaccanti che insieme costituiscono una botnet". Si veda la voce "denial of service" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#w. Altri strumenti utilizzati da Anonymous includono malware e phishing.

[14] "Codice che sfrutta una vulnerabilità di un sistema permettendo l'esecuzione di codice malevolo, generalmente con lo scopo di acquisire i privilegi di amministratore della macchina colpita". Si veda la voce "exploit" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#e.

[15] Associazione italiana per la sicurezza informatica, *Rapporto Clusit 2015 sulla sicurezza Ict in Italia*, Milano, Astrea, 2015, http://www.business-continuity-italia.it/documenti/Clusit_Rapporto_2015.pdf.

ISSN 2280-6164

ISSN 2280-6164

Lo scopo di questa ricerca è quindi individuare e valutare eventuali vulnerabilità nei sistemi Atm/Atc italiani che potrebbero essere sfruttate dai vari attori operanti nello spazio cibernetico. Si osservano altresì le contromisure di natura organizzativa, tecnologica e di processo poste in essere sia dal fornitore dei servizi della navigazione aerea civile, Enav[16], sia dai presìdi pubblici, in attuazione della strategia cibernetica nazionale e alla luce delle obbligazioni assunte dall'Italia nel quadro convenzionale del diritto internazionale. A tal fine, nel primo capitolo viene introdotto il tema della sicurezza cibernetica nell'ambito dell'aviazione civile. Dopo una breve analisi degli incidenti informatici che hanno colpito il settore, se ne definiscono le principali problematiche e si delinea il perimetro del presente studio. Nel secondo capitolo si spiega che cosa sia un sistema Atm/Atc e le sue funzioni. Nel terzo capitolo sono descritti gli attori considerati dalle autorità dell'aviazione civile come possibili minacce. Nella fattispecie, vengono valutate le competenze tecniche e gli obiettivi delle due principali organizzazione terroristiche, Isis ed Al-Qaeda, di hacktivisti e di criminali cibernetici. Nel quarto capitolo si descrive il ruolo di Enav e le tecnologie da essa impiegate. Vengono poi valutate le possibili minacce cibernetiche dirette contro l'Italia. Nelle conclusioni si offrono degli spunti di riflessione sui risultati della ricerca e sulle possibili evoluzioni del rapporto fra aviazione civile e sicurezza informatica.

1. Sicurezza cibernetica e aviazione civile

"L'aviazione si poggia largamente su computer nelle operazioni a terra e in volo, nonché nella gestione del traffico aereo, e siamo consapevoli di essere un obiettivo"[17].
Tony Tyler, direttore dell'International Air Transport Association

La crescita dell'impiego dell'Information Communication Technology (Ict) nell'aviazione, così come tutte le attività complesse condotte dall'uomo, è un trend che ha caratterizzato il settore in questi ultimi anni. Dallo sviluppo e costruzione di aeromobili, fino agli strumenti di comunicazione e navigazione, passando per le migliaia di connessioni che collegano le varie parti di un aeroporto, il mondo dell'aviazione civile fa impiego massivo delle tecnologie dell'informazione. Come in altri campi, la digitalizzazione e la messa in rete di strumenti così complessi, tuttavia, hanno aggiunto considerevoli problematiche associate alla sicurezza informatica dell'aviazione. Non stupisce perciò che, già nel 2012, un rapporto del Centre for the Protection of National Infrastructure (Cpni)[18] britannico sostenesse che l'interconnessione e l'interdipendenza generate dall'Ict avessero accresciuto la vulnerabilità degli aeromobili e dei sistemi, e di conseguenza l'impatto di eventuali

[16] Ente nazionale per l'assistenza al volo.

[17] Jonathan Gould and Victoria Bryan, "Cyber attacks, drones increase threats to plane safety: insurer", in *Reuters*, 4 December 2014, http://reut.rs/1tRTAOZ.

[18] Autorità governativa britannica che fornisce consigli e raccomandazioni in materia di sicurezza e protezione alle imprese e organizzazioni dell'infrastruttura nazionale.

compromissioni[19]. Nonostante i miglioramenti da un punto di vista economico e gestionale, resta evidente che le vulnerabilità legate al mondo cibernetico presentano dei rischi notevoli per l'aviazione civile.

Figura 2 | Tecnologie Ict nell'aviazione civile

Fonte: American Institute of Aeronautics and Astronautics, *A Framework for Aviation Cybersecurity*, August 2013, p. 8, http://www.aiaa.org/aviationcybersecurity.

L'obiettivo di questa sezione è fornire un quadro introduttivo della relazione fra sicurezza cibernetica e aviazione civile. In prima battuta, si presenteranno gli incidenti di carattere informatico che hanno colpito il settore. Successivamente, si andranno a verificare gli sforzi sostenuti a livello internazionale a contrasto della minaccia cibernetica e la dimensione delle contromisure in atto. Infine, verranno descritte le principali problematiche informatiche che condizionano la sicurezza in volo e a terra.

1.1 Eventi significativi

Storicamente l'aviazione civile ha rappresentato un obiettivo di particolare appetibilità e, nella sua evoluzione storica, si è assistito ad una trasformazione della minaccia sia in termini dimensionali che di modalità di attacco. Dalla tradizionale matrice di aggressione fisica agli aeromobili ed agli aeroporti, si sono registrati eventi di azioni con nuove modalità, tra le quali vanno annoverati episodi ascrivibili alla minaccia cibernetica. Vengono riportati di seguito alcuni esempi di incidenti

[19] Centre for the Protection of National Infrastrucuture, *Cyber Security in Civil Aviation*, August 2012, http://www.cpni.gov.uk/highlights/cyber-security-in-civil-aviation.

ISSN 2280-6164

di natura informatica nel settore dell'aviazione civile[20].

• 2006, luglio: un attacco informatico costringe la Faa americana a disattivare alcuni sistemi di controllo del traffico aereo in Alaska[21].
• 2008, agosto: all'aeroporto spagnolo di Madrid-Bajaras, un trojan[22] in uno dei sistemi principali della compagnia aerea Spanair impedisce la ricezione e l'attivazione di un messaggio d'allarme proveniente dal volo 5022. La mancata segnalazione è fra le cause della collisione dell'aeromobile e della morte dei 154 passeggeri a bordo. Ancora non è stato chiarito se la compromissione dei sistemi attraverso il trojan sia stata intenzionale[23].
• 2009, febbraio: un attacco ai sistemi Faa permette a hacker ignoti di ottenere l'accesso a 48.000 file del personale dell'agenzia americana[24].
• 2011, giugno: tre ingegneri vengono accusati di "interruzione dei servizi informatici" all'interno di un aeroporto, provocando forti disagi per i servizi di check-in e ritardi per una cinquantina di voli[25].
• 2013, luglio: il sistema di controllo dei passaporti agli aeroporti di Istanbul Ataturk e Sabiha Gökçen viene arrestato da un attacco cibernetico, causando il ritardo di numerosi di voli[26].
• 2013: secondo un rapporto del Centre for Internet Security (Cis)[27], nel corso del 2013 circa 75 aeroporti americani sono stati attaccati da prolungate campagne di spear phishing[28].
• 2014, marzo: il volo Malaysia Airlines MH370 scompare dai radar dei controllori di

[20] Gli eventi descritti rappresentano un parziale campionario di tali incidenti. Si noti che la gran parte non riguarda i sistemi Atm/Atc, ad eccezione dell'incidente verificatosi in Alaska nel 2006.

[21] Bernard Lim, "Aviation Security: Emerging Threats from Cyber Security in Aviation – Challenges and Mitigations", in *Journal of Aviation Management*, 2014, p. 84, http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/SAA_Journal_2014.pdf.

[22] "Identifica una categoria di malware le cui funzionalità sono nascoste all'interno di un software apparentemente legittimo facendo sì che l'installazione avvenga in modo inconsapevole da parte dell'utente permettendo in questo modo il controllo da remoto del computer. A causa della specifica modalità di contagio, il malware non è in grado di diffondersi in modo autonomo". Si veda la voce "trojan" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#t.

[23] Roland Heickerö, "Cyber Terrorism: Electronic Jihad", in *Strategic Analysis*, Vol. 38, No. 4 (2014), p. 556, http://dx.doi.org/10.1080/09700161.2014.918435.

[24] Bernard Lim, "Aviation Security: Emerging Threats from Cyber Security in Aviation", cit., p. 84.

[25] Iccaia, *Cyber Security for Civil Aviation*, presented at the Twelfth Air Navigation Conference, Montréal, 19-30 November 2012, http://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf.

[26] Ramon Lopez and Ben Vogel, "Authorities face uphill battle against cyber attacks", in *IHS Jane's Airport Review*, 9 April 2015, http://www.ihsairport360.com/article/6186/authorities-face-uphill-battle-against-cyber-attacks.

[27] Organizzazione non governativa e non-profit statunitense la cui missione è migliorare la prontezza e la capacità reattiva di enti pubblici e privati in merito alla cybersecurity, puntando a risultati di eccellenza attraverso la collaborazione.

[28] Ramon Lopez and Ben Vogel, "Authorities face uphill battle against cyber attacks", cit. "Indica un tipo particolare di phishing realizzato mediante l'invio di Email fraudolente ad una specifica organizzazione o persona. Lo scopo di questi attacchi è tipicamente quello di ottenere accesso ad informazioni riservate di tipo finanziario, a segreti industriali, di stato o militari". Si veda la voce "spear-phishing" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#ss.

ISSN 2280-6164

volo. Il Boeing 777-200ER viene dato per disperso da un comunicato stampa della compagnia malese. Nell'incertezza complessiva dell'evento si deve riportare anche la tesi secondo cui l'aereo sia stato dirottato attraverso un telefono cellulare e/o una penna Usb[29]. L'ipotesi non è mai stata confermata e ha trovato la viva opposizione dei produttori di aeromobili.

• 2014, dicembre: l'azienda Cylance accusa hacker iraniani di aver coordinato attacchi contro i sistemi informatici di più di 16 stati, compresi attacchi ai sistemi di aeroporti e compagnie aeree di Pakistan, Arabia Saudita, Corea del Sud e Stati Uniti[30].

• 2015, febbraio: la Faa scopre diversi malware nei propri sistemi informatici provenienti da email del personale. L'agenzia sostiene di non aver subito danni dall'attacco[31].

• 2015, aprile: la compagnia aerea Ryanair subisce un danno finanziario di circa 3 milioni di sterline a causa di un attacco informatico ai suoi conti bancari[32].

• 2015, giugno: un attacco al network della compagnia di bandiera polacca Lot lascia a terra 10 voli diretti verso Danimarca, Germania e Polonia, provocando il ritardo per altri 10. L'attacco ha compromesso i sistemi che creano i piani di volo[33].

Come testimonia questo elenco – non esaustivo – gli incidenti di natura informatica hanno contribuito a portare la sicurezza cibernetica al centro del discorso nell'aviazione civile. Tali eventi hanno spinto le principali organizzazioni internazionali operanti nel settore a cercare di elaborare delle risposte concrete alle possibili vulnerabilità dei loro sistemi.

1.2 Iniziative a livello internazionale

Attualmente non esiste un approccio olistico e universale al tema della sicurezza cibernetica nell'aviazione civile, anche se sono state lanciate numerose iniziative in questa direzione[34].

[29] Ellie Zolfagharifard, "Hackers are a serious threat to aircraft safety': Aviation chiefs warn of the devastating consequences of a cyber attack", in *Daily Mail Online*, 11 December 2014, http://dailym.ai/1zalBGR; Pierluigi Paganini, "Cyber Threats against the Aviation Industry", in *InfoSec Resources*, 8 April 2014, http://resources.infosecinstitute.com/?p=25456.

[30] Ramon Lopez and Ben Vogel, "Authorities face uphill battle against cyber attacks", cit.

[31] Bart Jansen, "FAA hit by cyberattack, finds no damage", in *Usa Today*, 7 April 2015, http://usat.ly/1yaHNV0.

[32] Jack Elliott-Frey, "The threat in the skies: Have cyber attackers boarded the plane?", in *Insurance Business Blog*, 27 May 2015, http://www.ibamag.com/news/blog-the-threat-in-the-skies-have-cyber-attackers-boarded-the-plane-22592.aspx.

[33] "Polish LOT aeroplanes grounded by computer hack", in *BBC News*, 21 June 2015, http://www.bbc.com/news/world-europe-33219276.

[34] Bart Elias, "Protecting Civil Aviation from Cyberattacks", in *CRS Insights*, 18 June 2015, http://www.fas.org/sgp/crs/homesec/IN10296.pdf. L'Aviation Security (AvSec) Panel Working Group è un gruppo di esperti incaricato dall'Icao di valutare problemi di sicurezza e possibili minacce all'aviazione civile.

ISSN 2280-6164

Nell'ottobre 2012, alla dodicesima conferenza sulla navigazione aerea promossa dall'Icao[35], l'Iccaia[36] ha affermato che "la sicurezza cibernetica è stata identificata come un impedimento di alto livello all'implementazione del Piano globale di navigazione aerea" e che "nuove tecnologie stanno per essere adottate, tecnologie che sono intrinsecamente più vulnerabili ad attacchi cibernetici [...]"[37]. L'associazione invita alla creazione di un gruppo di lavoro con il compito di implementare, gestire e verificare le procedure e le pratiche relative alla sicurezza cibernetica. Nel marzo 2014 l'Icao AvSec Panel[38] chiede un ulteriore sforzo nella valutazione del rischio cibernetico per i sistemi di gestione del traffico aereo basati sulle nuove tecnologie IT[39]. Questo perché nell'Annesso 17 alla Convenzione di Chicago del 1944 sull'aviazione civile, la sicurezza cibernetica è ancora una "pratica raccomandata" e non uno "standard"[40].

Nel 2013 l'Ifalpa[41] ha pubblicato un rapporto dal titolo "Cyber threats: who controls your aircraft?" ("Minaccia cibernetica: chi controlla il tuo aereo?"), identificando come "significativa ed emergente" la minaccia di un possibile attacco cibernetico contro un aereo, le strutture di terra o altri sistemi di rilievo dell'aviazione civile. Il rapporto sottolinea come i dati di navigazione non siano sicuri e che la loro manomissione potrebbe causare notevoli disagi[42].

Nel 2014 Canso[43] ha istituito l'Atm Security Work Group, che ha prodotto, tra l'altro, una "Cyber Security and Risk Assessment Guide" dedicata a promuovere, tra gli Air

[35] L'International Civil Aviation Organisation è l'agenzia specializzata dell'Onu che regola l'aviazione civile mondiale.

[36] International Coordinating Council of Aerospace Industries Associations.

[37] Iccaia, *Cyber Security for Civil Aviation*, cit. Sempre nel 2012, la stessa organizzazione ha emendato uno dei 19 allegati alla Convenzione sull'Aviazione civile internazionale, su cui l'organizzazione si fonda, per includere la dimensione della sicurezza cibernetica.

[38] L'Aviation Security (AvSec) Panel Working Group è un gruppo di esperti incaricato dall'Icao di valutare problemi di sicurezza e possibili minacce all'aviazione civile.

[39] Bernard Lim, "Aviation Security: Emerging Threats from Cyber Security in Aviation", cit. Tra le problematiche attualmente in fase di revisione da parte del gruppo di lavoro vi sono la valutazione di una serie di scenari che possono presupporre attacchi cibernetici diretti contro la cabina di pilotaggio, i sistemi Ict che supportano i moderni sistemi Atm e i sistemi informatici degli aeroporti, come ad esempio i controlli delle partenze e gli schermi con le informazioni di volo. Si veda: Raymond Benjamin, *Opening Remarks to the Conference on Civil Aviation Cyber Security*, 9-10 July 2015, http://www.icao.int/Documents/secretary-general/rbenjamin/20150720_Singapore_Cyber_Security.pdf.

[40] Interviste, novembre 2015. L'Annesso 17 (Misure di sicurezza contro gli atti di interferenza illecita) stabilisce che è obbligo primario degli Stati contraenti salvaguardare la sicurezza dei passeggeri, degli equipaggi, del personale di terra e del pubblico in generale da atti di interferenza illecita verso l'aviazione civile, inclusi attacchi di natura tecnologica alle infrastrutture della navigazione aerea.

[41] L'International Federation of Air Line Pilots' Associations rappresenta circa 100.000 piloti nel mondo.

[42] Ifalpa, "Cyber threats: who controls your aircraft?", in *Ifalpa Position Papers*, No. 14POS03 (5 June 2013), http://www.ifalpa.org/store/14POS03%20-%20Cyber%20threats.pdf.

[43] Civil Air Navigation Services Organisation, associazione che riunisce i fornitori dei servizi alla navigazione aerea, tra cui Enav.

ISSN 2280-6164

Navigation Service Provider (Ansp) associati, l'applicazione delle buone pratiche di settore[44]. Sempre nel 2014 la Iata[45] ha pubblicato un vademecum sulla sicurezza cibernetica nel settore dell'aviazione civile, successivamente aggiornato al luglio 2015[46].

Nel dicembre 2014 Icao, Iata, Aci[47], Canso e Iccaia hanno firmato un piano d'azione per la sicurezza cibernetica dell'aviazione civile (Civil Aviation Cyber Security Action Plan) a coordinamento delle rispettive azioni in contrasto alla minaccia cibernetica. L'obiettivo è quello di "stabilire e promuovere una solida strategia e cultura della sicurezza cibernetica a beneficio di tutti gli attori del settore, attraverso una maggiore condivisione di informazioni quali l'identificazione delle minacce, la valutazione del rischio e le migliori pratiche da adottare"[48].

La convinzione generale, rappresentata anche negli studi dell'Industry High Level Group (Cyber) promosso dall'Icao con Canso, Iata, Aci e Iccaia, si basa sull'assunto che nel settore dell'aviazione civile sia necessario un approccio specifico alla protezione cibernetica. Nonostante ciò, un approccio più generale va comunque considerato, dal momento che le tecnologie in uso nell'aviazione civile sono impiegate anche in altri settori e sono quindi soggette alle stesse minacce informatiche.

Le recenti iniziative a livello internazionale indicano il grado di importanza che la sicurezza cibernetica sta assumendo nell'aviazione civile. A seconda del sistema che si considera, però, sono diverse le vulnerabilità che possono essere sfruttate dai vari attori con intenzioni criminose. Il prossimo paragrafo presenta brevemente i sistemi che, se compromessi, possono costituire un pericolo per l'incolumità degli individui e, in generale, per la sicurezza nazionale.

1.3 Argomenti principali e definizione del perimetro d'indagine

Nel settore dell'aviazione civile sono tre gli obiettivi principali che possono essere soggetti ad un attacco di natura informatica: i sistemi interni di un aeroporto, i sistemi di controllo di un aeroplano in volo e i sistemi di gestione del traffico aereo[49].

[44] Canso, *Cyber Security and Risk Assessment Guide*, 2014, https://www.canso.org/node/753.

[45] L'International Air Transport Association è l'associazione di settore cui aderiscono 260 compagnie aeree, che rappresentano circa l'83 per cento di tutto il traffico mondiale.

[46] Lo scopo della pubblicazione è fornire al lettore un quadro generale dell'argomento, mettere a disposizione delle compagnie aeree uno strumento per la valutazione del rischio legato alla minaccia cibernetica, nonché una guida per l'implementazione di un sistema di gestione della sicurezza cibernetica. Iata, *Aviation Cyber Security Toolkit*, 2nd edition, July 2015, https://www.iata.org/publications/Pages/cyber-security.aspx.

[47] Airports Council International.

[48] Icao, *Aviation Unites on Cyber Threat*, 10 December 2014, http://www.iata.org/pressroom/speeches/Pages/2015-07-09-01.aspx.

[49] Un'altra tematica riguarda i tentativi di frode informatica: il considerevole giro d'affari in questo settore lo rende uno degli obiettivi preferiti dei criminali cibernetici, tanto che secondo alcune stime circa il 50 per cento di tutti tentativi di phishing sono diretti verso le compagnie aeree o i loro

ISSN 2280-6164

Gli aeroporti sono strutture particolarmente vulnerabili alla minaccia cibernetica. Oltre ai sistemi di quelle organizzazioni ed entità che utilizzano internet per operazioni di routine, come ad esempio lo scambio dati e la messaggistica, altri obiettivi possono essere i sistemi Supervisory Control and Data Acquisition (Scada), che spesso controllano i sistemi di ventilazione, del trasporto bagagli, ecc. In futuro, l'aumento di applicazioni mobili collegate alla rete probabilmente creerà ulteriori pericoli per le operazioni interne degli aeroporti. Questi ultimi potranno essere attaccati utilizzando un vasto numero di mezzi, sia fisici (penne Usb, computer, fotocamere digitali, ecc.) che informatici (DoS, phishing[50], trojan, ecc.)[51].

Numerosi esperti di sicurezza informatica hanno sottolineato come l'introduzione del wi-fi sugli aerei abbia prodotto delle falle di sicurezza ragguardevoli. Nel 2013, ad una conferenza della European Aviation Safety Agency (Easa), un esperto di informatica spagnolo, Hugo Teso, ha documentato la possibilità di comandare il sistema di controllo di un aeroplano attraverso uno smartphone. Con un'applicazione software di sua creazione, Teso avrebbe dimostrato di poter guidare un aeroplano in volo e provocarne la caduta[52]. Successivamente, sia la Faa che l'Easa hanno però affermato che la tesi aveva validità limitata perché verificata con un simulatore di volo, e che il metodo di Teso non porterebbe agli stessi risultati se invece venisse impiegato un software operante su una componente hardware certificata per il volo[53]. Nel 2014 Ruben Santamarta ha dimostrato come sia possibile disturbare le comunicazioni satellitari, e quindi interferire con il sistema di navigazione di un aeroplano in volo, tramite il sistema di intrattenimento a bordo, cui si può accedere tramite il wi-fi[54]. Nel luglio 2015 Chris Roberts sarebbe stato in grado di manipolare i sistemi di controllo dell'aeroplano sul quale viaggiava attraverso il sistema di intrattenimento a bordo. Secondo i documenti del Federal Bureau of Investigation

passeggeri. Si veda: Icao, *Aviation Unites on Cyber Threat*, cit.

50 "Truffa via Internet in cui l'aggressore cerca di ingannare la vittima inducendola a fornire informazioni personali, come ad esempio credenziali d'accesso, dettagli sul conto corrente bancario e sulle carte di credito. Si realizza tipicamente tramite l'invio, più o meno mirato, di email che imitano nella grafica e nelle impostazioni siti bancari o postali con le quali si richiede di inviare dati personali". Si veda la voce "phishing" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#p.

51 Kasthurirangan Gopalakrishnan et al., "Cyber Security for Airports", cit.

52 Marcel Rosenbach and Gerald Traufetter, "Cyber-Attack Warning: Could Hackers Bring Down a Plane?", in *Spiegel Online International*, 22 May 2015, http://spon.de/aevsu; Neil McAllister, "FAA: 'No, you CAN'T hijack a plane with an Android app'", in *The Register*, 13 April 2013, http://goo.gl/news/0PmU. Questo tema è stato affrontato in ambito Easa anche in altre occasioni: Cyrille Rosay, *Aviation Cybersecurity Roadmap Research Needs*, Aerodays2015, London, 20-23 October 2015, http://www.aerodays2015.com/wp-content/uploads/sites/20/6H-3-Emmanuel-Isambert.pdf.

53 Neil McAllister, "FAA: 'No, you CAN'T hijack a plane with an Android app'", cit. Airbus ha anche finanziato uno studio indipendente per dimostrare che i sistemi wi-fi di bordo sono del tutto indipendenti dall'avionica e che Acars e Ads-B possono essere chiaramente oggetto di interferenza in quanto sistemi collaborativi che viaggiano su onde radio, ma questo è cosa diversa da un hacker che si impossessa di un aereo. Intervista, novembre 2015.

54 Alcuni rappresentanti di industre che producono sistemi potenzialmente violabili hanno confermato la validità di parte dei risultati della ricerca di Santamarta, pur ridimensionandone il rischio effettivo. Si veda: Jim Finkle, "Hacker says to show passenger jets at risk of cyber attack", in *Reuters*, 4 August 2014, http://reut.rs/1olAeyA.

ISSN 2280-6164

(Fbi), dopo aver collegato il suo computer alla scatola elettronica situata sotto il sedile (seat electronic box), Roberts avrebbe inserito il comando "Clb" ("climb", prendere quota) e il motore dell'aereo avrebbe reagito di conseguenza[55].

Infine, anche i sistemi Atm/Atc sono finiti sotto osservazione per via della crescente dipendenza dall'Ict e dell'interconnessione con altri sistemi e tecnologie. Un rapporto dell'ispettorato generale del Dipartimento dei Trasporti americano ha denunciato nel 2009 le inefficienze e le vulnerabilità dei sistemi Atm di Faa, soprattutto per quel che riguardava le procedure di controllo degli accessi e le capacità di rilevamento di intrusioni illegittime[56]. Un più recente rapporto del Gao (gennaio 2015) ha sottolineato come "vulnerabilità nei controlli di sicurezza esistano e minaccino la possibilità del Faa di garantire la sicurezza delle operazioni nello spazio aereo nazionale"[57]. Le vulnerabilità riscontrate si ritrovano soprattutto nei controlli a prevenzione di accessi non autorizzati, in particolare i controlli per la protezione dei confini dei vari sistemi, l'identificazione e l'autenticazione degli utenti, le autorizzazioni per accedere ai vari sistemi, la criptazione dei dati e il monitoraggio delle attività del Faa. Secondo il rapporto, parte delle debolezze del sistema derivano dalla mancata istituzionalizzazione di un programma per la gestione del rischio cibernetico, come dimostrato dall'assenza di una definizione precisa di ruoli e responsabilità all'interno di Faa.

In merito alla relazione fra sicurezza informatica ed aviazione civile, questo rapporto affronta l'ultima delle tematiche che abbiamo brevemente presentato, ovvero la minaccia cibernetica ai sistemi Atm/Atc.

2. Funzione e componenti dei sistemi Atm/Atc

Un Atm è l'insieme dei servizi delegati alla gestione del traffico aereo. Per circoscrivere il campo di indagine, questa ricerca si soffermerà in particolare sulla componente dei servizi del traffico aereo (Air Traffic Services, Ats) e in particolare sul servizio di controllo del traffico aereo (Air Traffic Control, Atc).

L'obiettivo generale dell'Atm è quello di permettere agli operatori (ad esempio le compagnie aeree) di rispettare gli orari di partenza e di arrivo da loro prefissati e di potersi attenere ai profili di volo da loro preferiti (rotte e quote indicate nei piani di volo), senza mai comprometterne la sicurezza. L'Atm può essere intesa come l'integrazione delle seguenti componenti:
Atm = Ats + Air Traffic Flow Management (Atfm) + Air Space Management (Asm)[58].

[55] Marcel Rosenbach and Gerald Traufetter, "Cyber-Attack Warning...", cit.; Kim Zetter, "Feds Say That Banned Researcher Commandeered a Plane", in *Wired*, 15 May 2015, http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane.

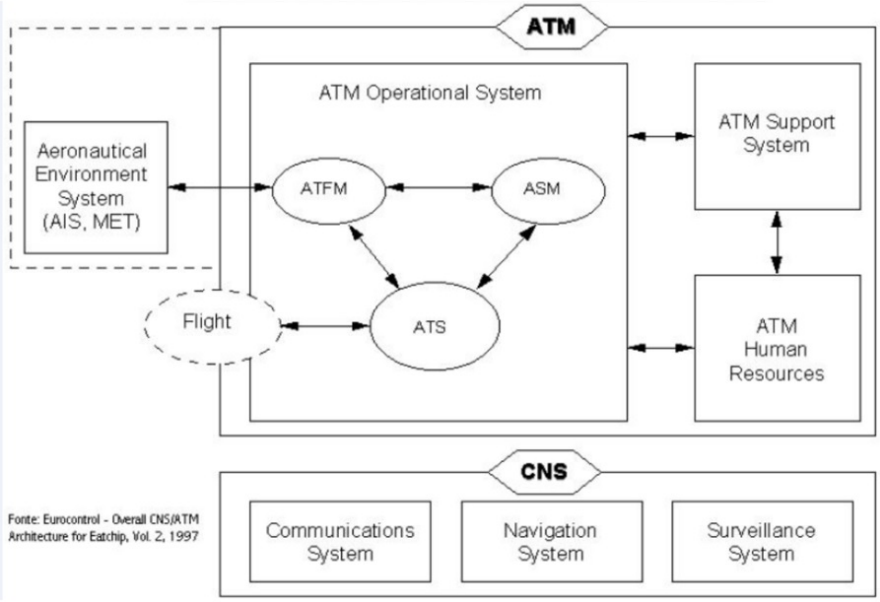
[56] Bart Elias, "Protecting Civil Aviation from Cyberattacks", cit.

[57] Gao, *FAA Needs to Address Weaknesses in Air Traffic Control Systems*, cit.

[58] Enav, "Gestione del traffico aereo", in *Compendio Atc*, settembre 2011, p. 92, http://www.enav.it/

ISSN 2280-6164

Figura 3 | Maggiori elementi sistema Cns/Atm



I servizi Ats sono generalmente forniti dagli Ansp che operano attraverso strumenti e personale presenti presso aeroporti e centri di controllo regionale denominati Area Control Center (Acc), ove è operativa una sala di controllo che attraverso vari sistemi (radar, radio, sensori meteo, ecc.) assicura la gestione delle operazioni. Le figure più rilevanti operanti presso un Ansp sono i controllori del traffico aereo[59], personale specializzato addetto alla fornitura di Ats. Secondo quanto previsto dall'Icao, un Acc è preposto alla fornitura di servizi Ats per una specifica regione. Lo spazio aereo è diviso in regioni denominate regioni di informazioni di volo (flight information region, Fir) e ciascuna Fir è di competenza di una specifica struttura, secondo accordi internazionali stipulati con Icao[60].

L'Atc è un sistema complesso basato su norme nazionali e internazionali, procedure, organizzazioni e strumenti tecnologici finalizzati a: prevenire le collisioni degli aeromobili con altri aeromobili o con ostacoli di diversa natura, organizzare e ottimizzare il flusso del traffico aereo, fornire informazioni e suggerimenti ai piloti per il miglioramento della qualità e dell'efficienza del volo, nonché assistere enti terzi nelle operazioni di ricerca e soccorso. In molti paesi l'Atc fornisce servizi a tutti i voli privati, militari, commerciali e governativi operativi nello spazio aereo corrispondente. A seconda del tipo di volo e della classe di spazio aereo l'Atc può fornire suggerimenti, che il pilota ha discrezione di seguire o meno, o indicazioni

ec5/enav/it/pdf/compendio_77_155.pdf.

[59] Comunemente denominati controllori di volo.

[60] Dimensioni e formati delle Fir possono differire significativamente e in alcuni casi le Fir possono essere suddivise orizzontalmente, limitando in questo caso l'uso del termine Fir allo spazio aereo inferiore e utilizzando la denominazione di "upper information region" (Uir) per quello superiore.

© 2015 IAI
ISSN 2280-6164
DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

che il pilota dovrebbe rispettare obbligatoriamente, salvo nei casi in cui ritenga di deviare dalle indicazioni per ragioni di emergenza[61].

Le procedure di Atc si basano sull'assegnazione dei volumi dello spazio aereo a specifiche classi con la classificazione eseguita dall'Icao, sebbene alcuni paesi ne prevedano adattamenti, in accordo con specifiche esigenze locali. L'Icao introduce sette classi, denominate attraverso le prime sette lettere dall'alfabeto[62]. Nelle classi si fa riferimento al volo a vista (visual flight rules, Vfr), strumentale (instrument flight rules, Ifr) e anche alla forma intermedia volo a vista speciale (special visual flight rules, Svfr). Inoltre, vengono stabilite modalità operative che variano gradualmente da quelle della classe A (implicanti controlli più severi) a quelle della classe G (richiedenti misure meno severe). Per ciascuna delle classi sono definite specifiche caratteristiche come relative condizioni di esistenza, se trattasi di spazio aereo controllato, se sia consentito il volo Ifr/Vfr/Svfr, come sia assicurata la separazione Atc, quali tipi di servizi Ats siano forniti, condizioni minime di visibilità e distanza dalle nubi, obbligatorietà del contatto radio, la necessità di autorizzazione all'ingresso, la modalità di funzionamento del trasponder[63] di bordo, ecc. Le classi da A fino ad E sono relative a spazi aerei controllati, mentre F e G caratterizzano spazi aerei non controllati. I servizi Atc sono previsti per i voli Ifr negli spazi aerei di classe A, B, C, D ed E, e per i voli Vfr negli spazi aerei di classe B, C e D[64].

I servizi Atc interessano tutte le fasi di movimento di un aeromobile: le operazioni al suolo per lo spostamento fra aree di sosta, aree di imbarco/sbarco, aerodromo[65]; le delicate operazioni di decollo/atterraggio; e la crociera. A queste fasi corrispondono specifiche tipologie di Atc, denominate controllo al suolo, controllo locale e controllo d'area.

Il controllo al suolo (ground control), coordinato dalla torre di controllo di un aeroporto, regola e organizza il movimento di aeromobili e veicoli nell'area aeroportuale, inclusi ingresso/uscita nelle/dalle aree di rullaggio (taxiway), piste inattive, aree di stazionamento e piazzali di transito (in partenza, dopo il distacco dal gate; in arrivo, all'uscita delle aree di rullaggio). Ciascun aeromobile, veicolo o persona in movimento nelle aree sottoposte a tale controllo deve essere esplicitamente autorizzato dal controllo al suolo con appositi apparecchi radio Vhf/Uhf.

[61] Il pilota è responsabile della sicurezza dell'aeromobile. Si veda: Icao, *Rules of the Air. Annex 2 to The Convention on International Civil Aviation*, Tenth Edition, July 2005, http://www.icao.int/Meetings/anconf12/Document%20Archive/an02_cons%5B1%5D.pdf.

[62] Solitamente lette attraverso l'alfabeto fonetico Icao: Alpha, Bravo, Charlie, Delta, Echo, Foxtrot, Golf. Si veda Annex 11 (Air Traffic Services), in Icao, *The Convention on International Civil Aviation. Annexes 1 to 18*, http://www.icao.int/safety/airnavigation/nationalitymarks/annexes_booklet_en.pdf.

[63] Ricevitore-trasmettitore che genera un segnale in risposta a una specifica interrogazione.

[64] Icao, Annex 11 (Air Traffic Services), cit.

[65] Area di decollo/atterraggio.

ISSN 2280-6164

ISSN 2280-6164

Il controllo locale, di norma a cura della torre di controllo[66], è responsabile dell'uso delle piste (runway, Rwy), delle aree di rullaggio per l'accesso alle piste, delle fasi di decollo/atterraggio dell'aeromobile (controllo di avvicinamento), per le quali fornisce specifiche autorizzazioni e modalità. In ogni momento è assicurata la separazione fra piste e fra aeromobili. Nella fase preliminare al decollo, il controllo fornisce al pilota, poco prima dell'inizio del rullaggio, le indicazioni di aree di rullaggio, pista e rotta da seguire immediatamente dopo il decollo, con le relative autorizzazioni (clearance delivery). Dati di volo (flight data) è la risorsa, normalmente coordinata con "clearance delivery", che assicura la distribuzione ai piloti di informazioni accurate ed aggiornate, quali ad esempio variazioni climatiche, interruzioni, ritardi nelle operatività al suolo, chiusura di piste, ecc. Ciò è spesso garantito da una registrazione trasmessa in loop su una specifica frequenza (Automatic Terminal Information Service, Atis). L'atterraggio è anch'esso assistito dalla torre di controllo o da un Acc, che fornisce i dettagli di rotta per raggiungere la pista di atterraggio designata. Nel caso di situazioni anomale che interessano un aeromobile in procinto di atterraggio il controllo Locale può emanare la direttiva go-around, indicando al pilota di interrompere le operazioni di atterraggio e di prepararsi a ricevere nuove istruzioni. I controllori che assistono gli aeromobili in avvicinamento gestiscono normalmente aeromobili a una distanza che può arrivare alle 30-50 miglia nautiche dall'aeroporto. Talvolta sono assistiti da sale radar a disposizione dell'aeroporto e di un centro di controllo (o altro aeroporto) vicino.

Il controllo d'area è svolto da un Acc competente per la Fir in cui si trova un aeromobile durante la fase di crociera. Per ciascuna Fir il servizio base Ats consiste nel Servizio informazioni volo (Flight Information Service, Fis) e nel Servizio di allarme (ALerting Service, Als). Le informazioni Fis includono dati meteorologici, attività vulcaniche, presenza in atmosfera di sostanze radioattive o tossiche, modifiche nell'efficienza operativa degli aiuti alla navigazione, cambiamenti nelle condizioni di aeroporto e infrastrutture associate, palloni liberi senza equipaggio, rischi di collisione, dati su imbarcazioni presenti nell'area ed ogni altra informazione rilevante per la sicurezza. Il servizio di allarme è invece fornito per notificare alle autorità competenti l'esistenza di aeromobili che necessitino di ricerca e soccorso, e per assistere tali organismi come necessario.

3. Minacce informatiche ai sistemi Atm/Atc

Nel dicembre 2014 Icao, Iata, Aci, Canso e Iccaia hanno firmato il piano d'azione per la sicurezza cibernetica dell'aviazione civile "per contrastare la minaccia cibernetica, in particolare quella proveniente da hacker, hacktivisti, criminali cibernetici e terroristi"[67]. Similmente, in occasione della conferenza sulla sicurezza cibernetica

[66] I piloti si riferiscono comunemente al controllo locale attraverso il termine controllo di torre.

[67] Icao, *Aviation Unites on Cyber Threat*, cit.

nell'aviazione civile tenutasi a Singapore nell'agosto 2015, il segretario generale dell'Icao Raymond Benjamin ha sostenuto che, nonostante l'organizzazione non abbia ricevuto finora notizia di eventi catastrofici legati alla sicurezza cibernetica, vi è piena consapevolezza che "terroristi, criminali e hacktivisti sono generalmente pronti a sfruttare le vulnerabilità della società civile"[68].

Secondo queste istituzioni nell'ambito della sicurezza cibernetica le minacce più dirette all'aviazione civile sarebbero quelle provenienti da entità non statuali, ossia da organizzazioni terroristiche, hacktivisti e criminali cibernetici. Sulla base di questa valutazione, la presente ricerca esclude l'analisi delle minacce legate a un possibile attacco informatico condotto da entità statuali, o para-statuali e alle operazioni di guerra elettronica. Ciononostante è bene sottolineare che, in virtù della combinazione di risorse e capacità tecnologiche, sono proprio gli stati a rappresentare il pericolo maggiore per le infrastrutture critiche di paesi terzi[69]. Analogamente, non si farà un diretto cenno ai possibili rischi derivanti dalle azioni di dipendenti infedeli o soggetti appartenenti a fornitori e subfornitori, che vengono considerati implicitamente quali possibili strumenti operativi della minaccia.

Nella sezione seguente si cercherà di comprendere secondo quale logica si muovono gli attori non statuali quando operano nello spazio cibernetico. Successivamente, si svolgerà un'analisi dettagliata del loro modus operandi, cercando di individuare se esistono delle regolarità tanto nelle tecniche impiegate quanto negli obiettivi. Nell'ultima parte si riassumerà quanto evidenziato dall'analisi e si fornirà una prima valutazione sullo stato della minaccia cibernetica nei confronti di infrastrutture critiche come i sistemi Atm/Atc.

3.1 Attaccare oppure no? Due prospettive a confronto

Cosa spinge i terroristi o altre tipologie di attori a condurre attacchi informatici contro le infrastrutture critiche di un paese?[70] Due sono gli approcci principali con cui si è affrontato tale quesito. Secondo uno schema d'analisi di costi e benefici, ad un terrorista non conviene pianificare e condurre operazioni complesse nello spazio cibernetico perché economicamente troppo dispendiose e perché i risultati ottenibili non avrebbero lo stesso impatto mediatico di una bomba detonata nel centro di una città. Da un punto di vista "tecnologico", invece, un terrorista può

[68] Raymond Benjamin, *Opening Remarks to the Conference on Civil Aviation Cyber Security*, cit.

[69] Secondo alcune valutazioni per i prossimi 5-10 anni solo i governi nazionali disporranno degli strumenti tecnologici e finanziari atti a sviluppare le capacità necessarie per attaccare le infrastrutture critiche di un paese. Si veda: Ics-Cert, *Cyber Threat Source Descriptions*, https://ics-cert.us-cert.gov/node/18.

[70] Questa sezione non intende descrivere vulnerabilità specifiche di infrastrutture critiche come gli Atm, considerando che nel mondo Atc, nel caso italiano in particolare, non vi sono sistemi Scada. Questa sezione ha lo scopo di evidenziare come alla base delle scelte delle organizzazione terroristiche, dei gruppi di hacktivisti o dei criminali cibernetici, vi sia una sottintesa analisi dei costi e benefici che rende la probabilità di certe azioni maggiore o minore. In questa sezione si fa riferimento prevalentemente alla logica d'azione delle organizzazioni terroristiche.

ISSN 2280-6164

puntare alle infrastrutture critiche di un paese semplicemente perché ciò è fattibile, ovvero perché i sistemi su cui si reggono queste strutture non sono e non saranno mai completamente sicuri, come tutti i sistemi fondati sull'It.

Partendo dal lavoro di Giampiero Giacomello[71], Maura Conway sostiene che almeno quattro fattori possono spingere un'organizzazione terroristica ad utilizzare tattiche e strumenti diversi da quelli informatici: costo, complessità, fattore distruzione e impatto mediatico[72]. L'autrice utilizza gli esempi di Stuxnet e di un ordigno esplosivo improvvisato (improvised explosive device, Ied) per spiegare la propria teoria. Stuxnet è un worm[73] creato probabilmente da una o più autorità statuali con l'intenzione di rallentare e/o fermare il programma nucleare iraniano. Il worm venne scoperto nel 2010 quando gli ingegneri iraniani si resero conto che un quinto delle centrifughe della centrale nucleare erano state danneggiate. In base alle fonti disponibili, ad oggi si tratta dell'unico attacco cibernetico che ha prodotto un effetto fisico. Seppur limitato al danneggiamento delle sole centrifughe, questo risultato ha richiesto una notevole expertise tecnica e ingenti risorse finanziarie. Secondo alcune analisi Stuxnet è il prodotto di circa 10.000 ore di lavoro di sviluppo da parte di una o più squadre di esperti informatici e ingegneri, con un costo complessivo variabile da qualche milione a decine di milioni di dollari[74]. Al contrario, costruire uno Ied è particolarmente semplice per la facilità di reperire il materiale necessario a un costo non proibitivo e la relativa facilità di assemblarlo. Nonostante ciò un attacco con Ied è in grado di causare danni materiali di notevole entità, di certo più ingenti di quelli causati da Stuxnet. Il grado di distruzione diventa quindi un fattore determinante anche nella considerazione dell'ultimo elemento da considerare: l'impatto mediatico. Secondo Conway, attacchi cibernetici come quelli a cui possono aspirare attualmente le varie organizzazioni terroristiche non hanno la stessa risonanza mediatica ottenibile con l'esplosione di una bomba che provoca decine di vittime tra la popolazione civile. L'insieme di questi quattro fattori (costo, complessità, livello di distruzione e impatto mediatico) rende pertanto le attività di terrorismo cibernetico possibili, ma fortemente improbabili[75].

[71] Giampiero Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism", in *Studies in Conflict and Terrorism*, Vol. 27, No. 5 (2004), p. 387-408.

[72] Maura Conway, "Reality Check: Assessing the (Un)likelihood of Cyberterrorism", in Thomas M. Chen, Lee Jarvis, Stuart Macdonald (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, Springer, 2014, p. 103-122.

[73] "Particolare categoria di malware capace di autoreplicarsi ma che, a differenza di un virus, non ha bisogno di legarsi ad un eseguibile per diffondersi in quanto modifica direttamente il sistema operativo del computer che lo ospita ed utilizza le connessioni internet". Si veda la voce "worm" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#w.

[74] Per un'analisi più approfondita si veda: US Senate Committee on the Judiciary, *Virtual Threat, Real Terror: Cyberterrorism in the 21st Century*, Hearing before the Subcommittee on Terrorism, Technology, and Homeland Security, 24 February 2004, http://www.gpo.gov/fdsys/pkg/CHRG-108shrg94639.

[75] Maura Conway, "Reality Check: Assessing the (Un)likelihood of Cyberterrorism", cit. Per una visione opposta si veda: Gabriel Weimann, *Terrorism in Cyberspace. The Next Generation*, Washington, Woodrow Wilson Center Press / New York, Columbia University Press, 2015, p. 152-153.

ISSN 2280-6164

Da un punto di vista "tecnologico", Clay Wilson argomenta invece che lo spazio cibernetico può presentare delle vulnerabilità facilmente sfruttabili dai terroristi. Innanzitutto l'aggiornamento dei software che fanno funzionare e regolano le infrastrutture critiche non avviene regolarmente, o abbastanza velocemente rispetto a quando vengono rilasciati gli aggiornamenti delle "patch" di sicurezza[76]. In alcuni casi il software di tali sistemi può essere proprietario, non standard, o datato, e quindi il venditore può decidere di non eseguire più gli aggiornamenti di sicurezza anche in presenza di nuove criticità. E questo è fortemente rischioso se si è consapevoli che i software di sicurezza non aggiornati sono facilmente visibili attraverso motori di ricerca pubblici come Shodan. L'aggiornamento di una patch può risultare dispendioso e difficile da gestire anche nel caso di software non obsoleti. Installare un aggiornamento di una componente dell'infrastruttura critica può comportare la sospensione del servizio e quindi rendere difficile un suo aggiornamento costante. Similmente, oggi molte infrastrutture critiche sono connesse e gestite da network controllati in remoto dai quartieri generali dei sistemi Scada e Industrial Control Systems (Ics) per la generazione di report utili alla gestione dei sistemi stessi[77]. Con l'allacciamento della rete all'esterno queste infrastrutture possono essere soggette ad attacchi e, se non protette adeguatamente, possono essere infettate da malware in grado poi di espandersi in tutta la rete Ics o Scada. Tecniche di spionaggio informatico possono essere utilizzate per scoprire le vulnerabilità di un sistema e creare precise istruzioni per la programmazione di malware da iniettare nel sistema vittima. Infine, potenziali terroristi potrebbero essere già in possesso di malware potenti che possono essere riprogrammati per sfruttare le vulnerabilità di più sistemi. Flame[78] e Stuxnet sono due esempi di malware che una volta scoperti sono stati analizzati da varie organizzazioni e poi modificati per essere riutilizzati in diverse circostanze. Sono passati alla storia per la presenza di molteplici "zero-day-exploits"[79]. Non esistono contromisure per attacchi di questo genere proprio perché si tratta di vulnerabilità non conosciute. In questo contesto, sembra che questi exploit, una volta prerogativa dei soli attori statuali e delle relative agenzie, siano oggi a disposizione anche di altre entità[80].

[76] Componente software espressamente sviluppata per aggiornare un programma allo scopo di correggerne errori, rimuoverne vulnerabilità di sicurezza e/o migliorarne l'usabilità e l'efficienza. Si veda la voce "Patch (computing)" in Wikipedia, https://en.wikipedia.org/wiki/Patch_(computing).

[77] I sistemi Scada e Ics sono sistemi automatizzati utilizzati per controllare i processi industriali, come ad esempio la regolamentazione della trasmissione della corrente elettrica. Si veda: Democratic Policy & Communication Center, *Glossary of Cyber Related Terms*, July 2012, http://www.dpc.senate.gov/docs/fs-112-2-183.pdf.

[78] Per una descrizione di Flame e dei suoi effetti si veda: Kaspersky Lab, *What is Flame Malware?*, http://www.kaspersky.com/flame.

[79] "Una minaccia informatica che sfrutta vulnerabilità di applicazioni software non ancora divulgate o per le quali non è ancora stata distribuita una patch". Si veda la voce "zero-day" nel glossario del Cert nazionale Italia.

[80] Clay Wilson, "Cyber Threats to Critical Information Infrastructure"; in Thomas M. Chen, Lee Jarvis, Stuart Macdonald (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, Springer, 2014, p. 123-137.

© 2015 IAI ISSN 2280-6164 DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

ISSN 2280-6164

Le due prospettive offrono degli spunti interessanti sulla possibilità che vari attori possano decidere di attaccare infrastrutture critiche come i sistemi Atm/Atc. Da un punto di vista "tecnologico", come argomentato da Wilson, puntare a compromettere i sistemi informatici di queste infrastrutture è fattibile perché questi sistemi non saranno mai sicuri. Può essere fondata l'ipotesi che un attacco cibernetico in grado di bloccare delle centrifughe risulti meno mediatico di una bomba che fa decine di morti, ma ciò dipende e dipenderà dall'entità dell'attacco informatico. Se in futuro un'organizzazione terroristica sarà effettivamente in grado di bloccare un sistema Atm e di causare la morte di civili su larga scala, tale attacco non risulterà certo "meno mediatico" di una bomba detonata in una piazza. Tuttavia la possibilità che esistano falle tali da permettere un attacco a strutture informatizzate complesse non implica che terroristi, hacktivisti e criminali cibernetici decidano di farlo o ne abbiano le capacità. Come evidenziato da Conway, condurre un attacco con effetti simili a quelli provocati dal worm Stuxnet è un'attività al momento estremamente complessa che richiede risorse finanziarie e tecniche ingenti e, come si vedrà nel prosieguo della ricerca, non è chiaro se attori non statuali siano per ora in grado di esprimere tali risorse.

3.2 Attori, obiettivi e modus operandi

Questa sezione presenta un'analisi dei mezzi e degli obiettivi di quegli attori che sono stati identificati come possibili minacce dalle autorità dell'aviazione civile, ovvero organizzazioni terroristiche, hacktivitsi e criminali cibernetici. Si intende presentare una panoramica delle attività nello spazio cibernetico di questi attori, e quindi determinare le loro reali capacità e intenzioni.

Organizzazioni terroristiche (Isis e Al-Qaeda)[81]

Lo Stato islamico dell'Iraq e della Siria (Islamic State of Iraq and Syria, Isis) è un gruppo militante jihadista proclamatosi califfato nel giugno del 2014. Attualmente controlla vaste porzioni di territorio fra la Siria e l'Iraq, anche grazie all'appoggio di decine di migliaia di combattenti e seguaci giunti da varie parti del mondo[82]. In quanto califfato, rivendica l'autorità su tutta la comunità musulmana e si prefigge come obiettivo l'estensione della propria giurisdizione su tutto il pianeta. Diverse organizzazioni internazionali e stati nazionali l'hanno designato come organizzazione terroristica. Oltre ai successi militari sul terreno e alla brutalità delle

[81] Questo studio analizza l'utilizzo dello spazio cibernetico da parte delle sole Isis e Al-Qaeda, nonostante anche altre organizzazioni terroristiche facciano uso della rete per promuovere i loro obiettivi. Queste due organizzazioni terroristiche sono state scelte perché costituiscono un pericolo maggiore per l'Italia, il caso studio che viene analizzato nel capitolo successivo. Per una disamina sull'utilizzo della dimensione cibernetica da parte di altre organizzazioni terroristiche si veda:"Terror Goes Cyber: The Cyber Strategies and Capabilities of Al Qaeda, ISIS, Al Shabaab, and BokoHaram", in *Bat Blue Special Reports*, April 2015, http://www.batblue.com/?p=6166.

[82] Tobias Feakin and Benedict Wilkinson, "The Future of Jihad: What Next for ISIL and al-Qaeda?", in *ASPI Strategic Insights*, June 2015, https://www.aspi.org.au/publications/the-future-of-jihad-what-next-for-isil-and-al-qaeda.

sue pratiche, l'Isis ha attirato l'attenzione di studiosi ed esperti per il proprio utilizzo dello spazio cibernetico. L'Isis opera sia nel cosiddetto "deep" e "dark" web[83], sia nella parte della rete "in superficie", dove cerca di dare la più ampia visibilità alle proprie azioni. L'organizzazione terroristica utilizza lo spazio cibernetico principalmente per attività di propaganda e reclutamento[84], trasferimento di expertise in ambito informatico e finanziamento[85].

Un'altra dimensione emergente è quella riconducibile ad attività volte ad ottenere l'accesso non autorizzato a sistemi informatici (hacking[86]) o l'interruzione di servizi informatici (tramite ad esempio DoS), portate avanti forse da esponenti dell'Isis, o più probabilmente da gruppi di hacker direttamente affiliati. Nel marzo 2015 militanti pro-Isis hanno sfruttato una serie di vulnerabilità della piattaforma WordPress e compromesso circa 200 siti web. In aprile hacker affiliati all'Isis hanno preso il controllo dell'account Twitter del cantante egiziano Nugoum e inviato un elevato numero di messaggi di propaganda a favore dell'organizzazione terroristica. In agosto il gruppo affiliato Al-Battar Media ha pubblicato un video della durata di nove minuti contente informazioni (nome, email, indirizzo, numero telefonico, indirizzo IP e stato di provenienza) relative a personale militare americano, inglese, francese ed italiano, dichiarando di averle raccolte dopo aver penetrato "un sito militare britannico". In aggiunta, degne di nota sono le azioni condotte dall'Isis "Cyber Army" tra il 19 e il 29 marzo 2015. In quel lasso di tempo i jihadisti cibernetici si sono resi protagonisti di cinque web defacement ai danni di tre siti egiziani, uno

[83] Il "dark web" è un concetto distinto dal "deep web". Il deep web è una estesa sezione della rete costituita da siti web, network e contenuti digitali che non viene indicizzata dai normali motori di ricerca come Google. Il dark web è quella parte del deep web composta da siti i cui indirizzi IP sono nascosti, ma accessibili attraverso il browser Tor se si è a conoscenza dell'esatta Url. Si veda: Pierluigi Paganini, "The Dark web – Why the hidden part of the web is even more dangerous?", in *Security Affairs*, 11 October 2015, http://securityaffairs.co/wordpress/40933. Il browser Tor è stato appositamente progettato per preservare l'anonimato degli utenti in rete. Per i dettagli si rinvia alla pagina del progetto: https://www.torproject.org.

[84] La propaganda è realizzata attraverso social media, video, forum, pubblicazioni, giochi online e oggetti di merchandising. Twitter e Facebook vengono sfruttati come "diari" in cui si testimonia ciò che accade sul campo di battaglia, offrendone una copertura quasi in tempo reale. L'organizzazione è arrivata al punto di creare una applicazione ("Dawn of Glad Tidings") in grado di mandare costanti aggiornamenti e inviare tweet automatici. Quanto al reclutamento, si stima che a gennaio 2015 circa 30.000 individui da oltre 80 stati si sarebbero trasferiti in Siria e Iraq per arruolarsi fra le file dell'Isis, di cui tremila provenienti dall'Europa. Servizi online come Kik o Skype offrono ai jihadisti la possibilità di comunicare in tempo reale e di coordinare la propria attività di reclutamento e/o di comando e controllo. Ibid. Beatrice Berton and Patryk Pawlak, "Cyber jihadists and their web", in *EUISS Briefs*, No. 2/2015, http://www.iss.europa.eu/publications/detail/article/cyber-jihadists-and-their-web.

[85] L'Isis spiega ai propri adepti come rimanere anonimi online: sul sito JustPaste.it si possono trovare dei manuali prodotti dall'organizzazione terroristica su come usare Vpn (Virtual Private Network) o più in generale su come rendere la navigazione online più sicura, sia via browser sia con un cellulare. Quanto al finanziamento, l'Isis sarebbe in grado di trasferire somme di denaro ai militanti che operano in Occidente e viceversa attraverso servizi quali PayPal e Bitcoin. Numerosi attacchi informatici dell'Isis sono condotti sono volti a ottenere dati bancari o gli account di carte di credito. I jihadisti utilizzano attacchi phishing oppure comprano online dati di carte di credito rubate. Ibid.

[86] Democratic Policy & Communication Center, *Glossary of Cyber Related Terms*, cit.

ISSN 2280-6164

francese e uno russo. A luglio sono circolate su Twitter immagini contenenti dati personali di soldati Nato ottenuti, secondo gli hacker, dopo aver violato uno dei siti dell'Alleanza atlantica[87]. A maggio hacker affiliati con l'Isis sarebbero stati inoltre in grado di violare le caselle di posta elettronica di alcuni rappresentanti del governo britannico, tra cui il ministro dell'Interno Theresa May. Non è ancora chiaro a quali informazioni gli hacker abbiano avuto accesso: le autorità competenti hanno escluso che ci sia stata un'esfiltrazione di dati, richiedendo però una modifica delle password utilizzate dai vari utenti e una revisione delle procedure di sicurezza[88].

Sebbene natura e affiliazione con l'Isis non siano ancora del tutto chiare, l'Islamic State Hacking Division (Ishd) e il Cyber Caliphate sono altri due gruppi di hacker che hanno condotto operazioni informatiche a sostegno dell'organizzazione terroristica. Ad oggi, le analisi più accreditate inducono a pensare che si tratti di gruppi (in gergo "crew") spontanei che l'Isis non controlla direttamente[89]. Per via del loro seguito mediatico, si è ritenuto opportuno analizzare le attività di questi due collettivi nel corso del 2015.

A marzo su alcuni forum jihadisti sono circolate le foto e gli indirizzi di 100 militari statunitensi. Nel messaggio di introduzione, l'Ishd sosteneva di averle ottenute dopo aver penetrato molteplici server, banche dati e servizi di posta elettronica militari protetti. L'obiettivo della diffusione delle informazioni personali era fare in modo che "i nostri fratelli residenti in America possano occuparsi di voi"[90]. Ad agosto l'Ishd ha pubblicato nomi, email e altre informazioni sensibili – 1.351 indirizzi – di personale militare e governativo statunitense. Fino ad allora si ritiene che l'Ishd fosse guidato dal ventunenne Junaid Hussain[91], in arte Abu Hussain Al-Britani, il quale si suppone stesse insegnando tecniche di penetrazione di sistemi informatici ad altre reclute dell'Isis, prima di venire ucciso il 25 agosto in un raid americano.

Un altro gruppo responsabile di attività di hacking a favore dell'Isis è il Cyber Caliphate, comparso per la prima volta sulla scena nel dicembre 2014 con un attacco all'Albuquerque Journal. Tra il 10 e il 16 gennaio 2015, a seguito delle vicende di Charlie Hebdo, il Cyber Caliphate ha lanciato l'operazione #OpFrance contro migliaia di siti web francesi con il supporto di altri gruppi islamisti. A condurre le operazioni nello spazio cibernetico, oltre al Cyber Caliphate, è stata una rete informale di gruppi di hacker e singoli che volevano manifestare il proprio malcontento per la reazione occidentale agli attentati in Francia[92]. Secondo le

[87] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", in *MEMRI Inquiry & Analysis Series*, No. 1183 (21 August 2015), http://www.memri.org/report/en/0/0/0/0/0/857/8714.htm.

[88] Claire Newell et al., "Cabinet ministers' email hacked by Isil spies", in *The Guardian*, 11 September 2015, http://t.co/8gLdpIHwGa.

[89] Interviste, ottobre 2015.

[90] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.

[91] Ibid.

[92] Tra i nomi principali della campagna si ricordano gli AnonGhost, i Fallaga Team, gli Izzah

© 2015 IAI ISSN 2280-6164 DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

autorità francesi, gli attacchi hanno colpito circa 1.300 siti, ma con conseguenze trascurabili (prevalentemente web defacement)[93]. Secondo altre fonti una parte degli attacchi sarebbero stati di tipo DDoS[94]. Sempre a gennaio il Cyber Caliphate è riuscito ad ottenere l'accesso agli account Twitter e YouTube di US Centcom, diffondendo messaggi a favore dell'Isis, nonché informazioni sul personale Centcom ottenute, secondo il gruppo jihadista, grazie alla penetrazione di reti classificate. Lo stesso mese un collettivo con il nome "Official Cyber Caliphate" afferma di aver violato il sito della compagnia di bandiera Malaysia Airlines. Al di là del web defacement ai danni del proprio sito online, la compagnia aerea afferma però che nessun estraneo è riuscito ad accedere ai server[95]. A febbraio lo stesso gruppo ha avuto accesso all'account Twitter di Newsweek, utilizzato poi per diffondere propaganda Isis e "materiale classificato". In aprile il Cyber Caliphate ha compromesso i sistemi informatici di TV5 Monde, interrompendone la diretta televisiva e il funzionamento del sito web ed eseguendo un defacement della pagina Facebook[96]. In ottobre il gruppo di hacker ha ottenuto l'accesso a circa 54 mila account Twitter, che ha utilizzato nuovamente per la diffusione di messaggi di sostegno all'Isis. La maggior parte delle vittime, che hanno visto pubblicate in rete le proprie informazioni personali, risiede in Arabia Saudita. Gli hacker islamisti hanno reso inoltre pubblici i dati personali dei capi di Cia, Fbi e National Security Agency (Nsa)[97].

Al-Qaeda ("La base") è un'organizzazione terroristica fondata nel 1988 dal multimilionario saudita Osama Bin Laden, e responsabile di una serie di attacchi terroristici di ampia portata come quelli di New York nel 2001, di Bali nel 2002 e Madrid nel 2004. Le successive operazioni militari statunitensi in Afghanistan, Iraq, Pakistan e Yemen si crede abbiano notevolmente indebolito la leadership dell'organizzazione, anche se i gruppi regionali che ad essa si ispirano continuano a costituire un pericolo serio alla sicurezza occidentale e non[98].

Hackers e gruppi islamisti veri e propri come la Middle East Cyber Army e la United Islamic Cyber Force.

93 Carola Frediani, "Isis, al Qaeda e la sfida del cyber terrorismo", in *l'Espresso*, 4 febbraio 2015, http://espresso.repubblica.it/plus/articoli/2015/02/02/news/isis-al-qaeda-e-la-sfida-del-terrorismo-informatico-1.197769; Radware, "ISIS Cyber Attacks" in *ERT Threat Alert*, April 2015, http://security.radware.com/uploadedFiles/Resources_and_Content/Threat/ERT%20Threat%20Alert%20-%20ISIS%20Cyber%20Attacks.pdf.

94 Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.; Radware, "ISIS Cyber Attacks", cit.

95 Al-Zaquan Amer Hamzah, "Malaysia Airlines website targeted by hacker group 'Cyber Caliphate', in *Reuters*, 26 January 2015, http://reut.rs/1z0irG4.

96 Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.; Radware, "ISIS cyber attacks", cit.

97 Swati Khandelwal, "ISIS Supporter Hacks 54,000 Twitter Accounts and Posts Details of Heads of the CIA and FBI", in *The Hacker News*, 8 November 2015, http://thehackernews.com/2015/11/hacking-twitter-account.html.

98 Mark Hosenball, "U.S. says al Qaeda core weak, but affiliates still threaten", in *Reuters*, 30 April 2014, http://reut.rs/1hTuTjC.

ISSN 2280-6164

Al-Qaeda dimostrò il suo interesse per lo spazio cibernetico già vent'anni fa quando creò il suo primo sito, Azzam.com. Secondo il testo "I 39 principi della Jihad", pubblicato nel 2003, la jihad elettronica è un dovere fondamentale e sacro per tutti i musulmani[99]. Esso rientra nel più ampio quadro strategico fornito dal testo "44 Ways to Support Jihad" (44 modi per supportare la Jihad), in cui la rete è concepita come un importante mezzo per diffondere la "guerra santa" e seguirne le notizie. L'utilizzo di internet da parte di Al-Qaeda può essere meglio compreso se letto in funzione di "Al-Qaeda 20 years strategy", in cui si dimostra come la jihad online sia finalizzata alla propaganda, a radicalizzare la comunità islamica e a reclutare nuovi martiri[100].

Verso la metà degli anni 2000 erano presenti sei gruppi associabili alla "ciber jihad" di Al-Qaeda: Ansar Al-Jihad Lil-Jihad Al-Electroni, Munazamat Fursan Al-Jihad Al-Electroni, Majmu'at Al-Jihad Al-Electroni, Majma' Al-Haker Al-Muslim, Inhiyar Al-Dolar e Hackboy. Nel corso degli anni Al-Qaeda ha dichiarato di aver avuto successo nell'esecuzione di alcune operazioni cibernetiche, anche se non è generalmente verificabile l'autenticità di queste affermazioni[101]. Nel marzo 2013 l'Al-Qaeda Electronic Army e la Tunisian Cyber Army hanno dichiarato di aver violato i siti web del Pentagono e del dipartimento di stato americani, notizia poi riportata anche dal sito web ehackingnews.com. Un mese dopo, un utente del forum jihadista Shumouk Al-Islam discuteva della scoperta da parte dell'esperto spagnolo Hugo Teso della possibilità di dirottare areoplani attraverso l'uso di uno smartphone Android[102]. Nel corso del 2015 sembra che l'attività dell'Al-Qaeda Electronic Army si sia concentrata prevalentemente in attività di web defacement contro siti occidentali[103].

Secondo alcuni rapporti, Al-Qaeda e le sue "legioni" cibernetiche discutono continuamente nei vari forum in rete della possibilità di condurre attacchi informatici[104]. Fra gli obiettivi di Al-Qaeda figurerano anche le funzioni di comando e controllo dei sistemi Scada, anche se non è dato sapere se l'organizzazione sia effettivamente in possesso delle capacità tecniche e delle risorse necessarie per condurre operazioni di questo tipo. Su un sito associato con Al-Qaeda erano invece riportate informazioni riguardanti l'esecuzione di attacchi DDoS[105].

[99] Beatrice Berton and Patryk Pawlak, "Cyber jihadists and their web", cit.

[100] Vito Morisco, "Network jihadisti tra virtuale e reale", in *Il mondo dell'intelligence. Approfondimenti*, maggio 2015, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/network-jihadisti-tra-virtuale-e-reale.html.

[101] Steven Stalinsky and R. Sosnow, "From Al-Qaeda to the Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad", in *MEMRI Inquiry & Analysis*, 5 December 2014, http://cjlab.memri.org/wp-content/uploads/2014/12/cyber-jihad-2.pdf.

[102] Ibid.

[103] Site Inteligence Group, "Al-Qaeda Electronic", in *Dark Web & Cyber Security*, https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=656&Itemid=1355.

[104] Steven Stalinsky and R. Sosnow, "From Al-Qaeda to the Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad", cit.

[105] Ibid.

DOCUMENTI IAI 15 | 23 - DICEMBRE 2015 ISSN 2280-6164

Hacktivisti

Il termine hacktivism deriva dalla combinazione dei termini hacker e actvism e si riferisce all'utilizzo dello spazio cibernetico a sostegno di una causa politica, promuovendo la libertà di parola e i diritti umani[106]. Nel corso degli anni le capacità tecniche degli hacktivisti sono aumentate esponenzialmente. Da operazioni di web defacement contro siti non particolarmente protetti si è passati ad attività complesse, che hanno mostrato l'impiego di tecniche del tutto simili a quelle dei criminali cibernetici e degli hacker ingaggiati dai governi[107]. Ad oggi sembra che questi attori non abbiano condotto attacchi di particolare rilevanza contro le infrastrutture critiche di un paese, anche se un rapporto dell'Ics-Cert[108] statunitense ha attribuito alla categoria degli hacktivisti una serie di attacchi alle strutture Ics/Scada statunitensi nel corso del 2014[109].

Tra i collettivi hacktivisti più famosi vi è senza dubbio Anonymous, un gruppo di hacker formatosi all'inizio degli anni 2000, con l'obiettivo di rendere gratuita l'informazione online. Dopo l'arresto di uno dei suoi "leader", l'americano Hector Monsegur, e di altre importanti figure del movimento nel febbraio 2012, l'azione di Anonymous sembra essersi scissa tra una componente globale e una regionale. La componente globale porta avanti campagne di attacco solo raramente e perlopiù in reazione ad un evento o un incidente. Le versioni locali di Anonymous sono invece proattive, ovvero conducono spesso attacchi informatici non necessariamente in risposta ad un evento[110]. Tra le tecniche maggiormente impiegate figurano i web defacement, DoS contro siti web governativi e/o altre importanti istituzioni e gli Sql-injection[111]. Il modus operandi di Anonymous si articola solitamente in tre fasi[112]:

106 Pierluigi Paganini, "Hacktivism: Means and Motivations ... What Else?", in *InfoSec Resources*, 2 October 2013, http://resources.infosecinstitute.com/?p=21557. Ics-Cert, *Cyber Threat Source Descriptions*, cit.

Rob Rachwald, "The Evolving Nature of Hacktivism", in *Imperva Cyber Security Blog*, 8 August 2012, http://blog.imperva.com/2012/08/the-evolving-nature-of-hacktivism.html.

107 Pierluigi Paganini, "Hacktivism: Means and Motivations ... What Else?", cit.

108 Industrial Control Systems Cyber Emergency Response Team. Per il rapporto si veda: Ics-Cert, *ICS-CERT Monitor*, September 2014-February 2015, https://ics-cert.us-cert.gov/monitors/ICS-MM201502.

109 Pierluigi Paganini, "Hacktivism: Means and Motivations ... What Else?", cit. In un messaggio al Wall Street Journal Anonymous definiva ridicola l'idea di chi gli attribbuiva l'intento di attaccare la rete elettrica.

110 Rob Rachwald, "The Evolving Nature of Hacktivism", in *Imperva Cyber Security Blog*, 8 August 2012, http://blog.imperva.com/2012/08/the-evolving-nature-of-hacktivism.html.

111 "Sql-injection (spesso abbreviato in Sqli) è una tecnica mediante la quale utenti malintenzionati possono iniettare comandi Sql arbitrari in una query verso un database, sfruttando tipicamente come veicolo d'attacco errori nella convalida lato server dei dati inviati ad una pagina Web. Comandi Sql iniettati in questo modo possono compromettere seriamente la sicurezza di un'applicazione Web, consentendo ad un attaccante di ottenere privilegi di accesso elevati ad un Dbms o ad un sito e di visualizzare od alterare i dati in esso contenuti". Si veda la voce "Sql injection" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#ss.

112 Imperva, "The Anatomy of an Anonymous Attack", in *Hacker Intelligence Reports*, February 2012, http://www.imperva.com/download.asp?id=312.

ISSN 2280-6164

durante la prima fase, alcuni hacktivisti cercano di radunare più persone sui social media quali Facebook e Twitter e siti come YouTube. Nella seconda fase, gli hacker più competenti iniziano il processo di ricognizione con strumenti quali Nikto e Acunetix per individuare vulnerabilità nel sistema da attaccare[113]. Durante l'attacco, gli hacker utilizzano software disegnati specificatamente per l'esfiltrazione di dati, come ad esempio Havij[114]. Nella terza fase, nel caso l'esfiltrazione dei dati fallisca, gli hacker più competenti chiedono supporto alla base reclutata in precedenza per lanciare un attacco DDoS. L'attacco avviene per mezzo di software convenzionali, reperibili sul mercato nero del web, oppure tramite siti web creati appositamente per l'attacco[115].

Riguardo alle attività di Anonymous nel corso del 2015 non vi è da segnalare nessuna particolare cesura o cambiamento rispetto all'azione degli anni precedenti, a parte le iniziative contro i sostenitori e gli affiliati dell'Isis. Ad aprile hacker di Anonymous hanno sferrato una serie di attacchi contro siti web israeliani per vendicare "i crimini commessi nei territori palestinesi". Sebbene il Computer Emergency Response Team (Cert) israeliano abbia affermato che nessuno dei siti governativi sia stato violato, Anonymous ha rilasciato dati diversi sull'impatto dell'operazione, dichiarando di aver sottratto almeno 150.000 informazioni personali (numeri telefonici e account di Facebook, Gmail, Hotmail). Le agenzie di stampa israeliane hanno confermato la compromissione di alcuni siti web governativi[116]. A giugno gli hacker mascherati sono stati responsabili di un attacco DDoS contro il sistema informatico del governo canadese, in reazione all'approvazione della nuova legge antiterrorismo[117]. A luglio il collettivo di hacker è riuscito ad ottenere dati appartenenti allo US Census Bureau, in risposta alla negoziazione di accordi quali il Transatlantic Trade and Investment Partnership (Ttip) e il Trans Pacific Partnership (Tpp) che, secondo gli hacker, minacciano di estendere misure restrittive sulla proprietà intellettuale ai paesi dell'Asia orientale[118]. Infine è stata di particolare interesse la reazione di Anonymous all'attentato terroristico che ha portato alla morte di due giornalisti della testata francese Charlie Hebdo. In seguito alla settimana di attacchi informatici compiuta da simpatizzanti e sostenitori dell'Isis, il collettivo di hacker ha annunciato una rappresaglia contro coloro che supportano una forma violenta di jihad[119]. Da gennaio fino a luglio 2015, secondo fonti pubbliche, il gruppo di

[113] Nikto è un web scanner utilizzato per testare le vulnerabilità dei server web per file pericolosi, sofware non aggiornati e altri tipi di problemi. Acunetix è uno scanner "black box" impiegato per scansionare le vulnerabilità di siti e applicazioni web.

[114] Havij è uno strumento che rileva le vulnerabilità Sql-injection di una pagina web.

[115] Imperva, "The Anatomy of an Anonymous Attack", cit.

[116] Pierluigi Paganini, "Anonymous collective hit Israel as part of opIsrael", in *Security Affairs*, 8 July 2015, http://securityaffairs.co/wordpress/35776.

[117] L'attacco è stato confermato dalle autorità canadesi. Si veda: Pierluigi Paganini, "#OpC51 Anonymous hit systems at Canadian Government", in *Security Affairs*, 18 June 2015, http://securityaffairs.co/wordpress/37883.

[118] Paganini Pierluigi, "Anonymous Hacks US Census Bureau against TPP/TTIP", in *Security Affairs*, 25 July 2015, http://securityaffairs.co/wordpress/38817.

[119] Pierluigi Paganini, "Update Charlie Hebdo Tango Down – Anonymous promises to avenge the massacre", in *Security Affairs*, 11 January 2015, http://securityaffairs.co/wordpress/32006.

ISSN 2280-6164

hacker pare abbia collaborato con la Fbi nell'indagine relativa alla compromissione dell'account Twitter di US Centcom, ed abbia attaccato gli account dei social media utilizzati da Isis per la diffusione della propria propaganda e pubblicato una lista di siti web che si ritiene sponsorizzino la causa jihadista[120]. Un gruppo affiliato ad Anonymous, GhostSec, sembra abbia collaborato con l'intelligence e le forze di polizia americane per sventare attentati terroristici pianificati dall'Isis in Tunisia e a New York[121].

Criminali cibernetici e crimine organizzato

Il crimine online si è sviluppato in questi anni grazie alla facilità di comunicazione, la possibilità di rimanere anonimi e di reperire facilmente gli strumenti necessari ad attività illegali nello spazio virtuale. Tutto questo ha contribuito a rendere il crimine online uno dei settori più proficui dell'economia mondiale. Già da anni sono emerse reti di criminali che operano quasi esclusivamente nella realtà virtuale. Il fulcro del crimine online è incentrato attorno a gruppi di individui che si incontrano prevalentemente sul web e raramente di persona. Queste organizzazioni criminali sono solitamente gestite da hacker esperti che di rado commettono il reato in prima persona, ma agiscono perlopiù come coordinatori[122]. Le vulnerabilità dei vari sistemi sono sfruttate attraverso malware quali virus, trojan, keylogger[123] e botnet[124].

Il crimine organizzato ha tra le sue attività lo spionaggio industriale a scopo di profitto. Disponendo di ingenti risorse economiche è in grado di assumere hacker competenti e di altro profilo per portare avanti i propri obiettivi. Le infrastrutture critiche possono divenire l'obiettivo di attacchi volti a favorire i concorrenti nel medesimo settore, sottrarre segreti industriali o informazioni riservate[125].

Il 2015 ha visto una continua evoluzione del mondo del crimine informatico, con l'uso di tattiche di attacco più efficienti e in grado di garantire sempre maggiori profitti.

[120] Pierluigi Paganini, "Anonymous supports FBI investigation of US CENTCOM hack", in *Security Affairs*, 19 January 2015, http://securityaffairs.co/wordpress/32403; Pierluigi Paganini, "Anonymous vigilantes are fighting against the ISIS propaganda", in *Security Affairs*, 30 March 2015, http://securityaffairs.co/wordpress/35486.

[121] Pierluigi Paganini, "Anonymous's team GhostSec thwarts Isis terror", in *Security Affairs*, 26 July 2015, http://securityaffairs.co/wordpress/38860.

[122] Tatiana Tropina, "Cyber Crime and Organized Crime", in *Freedom from Fear*, No. 7 (July 2010), p. 16-17, http://f3magazine.unicri.it/?p=310.

[123] "Strumento (hardware o, più diffusamente, software) che realizza uno sniffing monitorando e/o registrando quello che un utente digita sulla tastiera del computer. Può essere utilizzato per l'assistenza tecnica o come malware per sottrarre credenziali di accesso, numeri di carte di credito o altri dati sensibili". Si veda la voce "keylogger" nel glossario del Cert nazionale Italia, https://www.certnazionale.it/glossario/#k.

[124] "Rete di computer compromessi (bot o zombie) collegati tramite Internet e controllati da un entità detta botmaster attraverso vari canali di comunicazione, tra cui Irc (Internet Relay Chat) e le reti P2P (peer-to-peer)". Si veda la voce "botnet" nel glossario del Cert nazionale Italia, https://www.certnazionale.it/glossario/#b.

[125] Ics-Cert, *Cyber Threat Source Descriptions*, cit.

ISSN 2280-6164

La competizione fra i vari venditori di malware ha alzato il livello dell'innovazione, in alcuni casi giungendo fino all'adozione di tecniche utilizzate dai più complessi attori statali. Allo stesso tempo gli interessi dei criminali cibernetici sembrano essersi orientati prevalentemente verso istituzioni commerciali e finanziarie. Tuttavia secondo il Cert statunitense tra gli attori che nel 2014 hanno tentato di attaccare i sistemi Ics/Scada delle infrastrutture critiche americane ci sarebbero anche i criminali cibernetici[126].

3.3 Stato della minaccia cibernetica verso i sistemi Atm/Atc

Se si analizzano le azioni condotte nello spazio cibernetico da Isis e Al-Qaeda si evince che la loro entità non sia stata tale da rappresentare un pericolo imminente per infrastrutture critiche come i sistemi Atm/Atc. Il livello di sofisticazione delle operazioni condotte nello spazio cibernetico si è rivelato ben più basso del livello di promozione mediatica ricevuto.

Nel caso dell'accesso all'account di Twitter dell'US Centcom da parte del Cyber Caliphate, vari analisti hanno sottolineato come per "violare" gli account del famoso social media sia necessario indovinare, o ottenere, le credenziali di accesso di un utente (password più username / email / numero di telefono), ma questo non significa essere in grado di penetrare le ben più protette reti militari, sia quelle classificate (come NiprNet) che non classificate (SiprNet)[127]. Per quel che riguarda la presunta diffusione di materiale classificato, il Central Command ha confermato che nessun sistema è stato alterato, e che l'episodio va considerato "un atto di puro vandalismo"[128]. In merito al presunto furto di dati avvenuto nell'agosto 2015 da parte dell'Ishd, fonti ufficiali avevano già confermato subito dopo la pubblicazione dei dati che nessuna lista di nominativi e informazioni era stata ottenuta attraverso un attacco informatico[129]. A conferma di ciò, nell'ottobre 2015 il cittadino kosovaro Ardit Ferizi è stato arrestato in Malesia per aver fornito a Junaid Hussain i dati personali appartenenti ai 1.351 soldati americani, ossia le informazioni successivamente pubblicate su Twitter dall'esperto informatico dell'Isis[130]. Secondo il Dipartimento di Giustizia americano, Ferizi ha ottenuto queste informazioni penetrando il sistema informatico di un'azienda americana, e non reti militari protette[131]. Anche

[126] EMC, "Cybercrime 2015. An Inside Look at the Changing Threat Landscape", in *RSA White Papers*, April 2015, http://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf; Ics-Cert, *ICS-CERT Monitor*, September 2014-February 2015, cit.

[127] David C. Gompert and Martin C. Libicki, "Decoding the Breach: The Truth about the CENTCOM Hack", in *The Rand Blog*, 3 February 2015, http://www.rand.org/blog/2015/02/decoding-the-breach-the-truth-about-the-centcom-hack.html.

[128] Emma Graham-Harrison, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?", in *The Guardian*, 12 April 2015, http://gu.com/p/47at3/stw.

[129] "US military data stolen by Daesh's 'Hacking Division'", in *PressTV*, 13 August 2015, http://www.presstv.com/Detail/2015/08/13/424575/ISIL-Hack-US-Military.

[130] US Department of Justice, *ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges*, 15 October 2015, http://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges.

[131] Ibid.

ISSN 2280-6164

in altri casi (l'attacco a TV5 Monde), in cui sembrava che il Cyber Caliphate fosse riuscito a dimostrare un livello di sofisticazione più elevato del normale web defacement, alcuni analisti hanno suggerito che l'attacco si era verificato perché le password di alcuni account di TV5 erano state mandate in onda per errore durante le riprese negli studi della Tv[132]. È quasi superfluo sottolineare come questi attacchi non abbiano nulla a che vedere con attacchi verso sistemi Atm/Atc, pertanto saper violare alcuni sistemi o servizi web non dimostra affatto che si disponga di una capacità tecnica elevata, indispensabile per penetrare sistemi con svariati livelli di protezione come quelli di diverse infrastrutture critiche. Queste violazioni al massimo fanno notare quale effetto, anche mediatico, un danno reputazionale possa apportare agli interessi di una singola entità o di un "sistema paese".

Nel caso di Isis quindi, in nessuno dei casi analizzati (che sono, in base alle fonti disponibili, quelli più rilevanti) l'organizzazione terroristica ha dimostrato una maturità tecnica tale da farci concludere che sia in grado di attaccare con successo sistemi caratterizzati da politiche di sicurezza ben più stringenti di un network televisivo o di un account Twitter. Lo stesso ragionamento può essere fatto per Al-Qaeda, la quale ha mostrato, almeno nel corso del 2015, un attivismo minore dell'Isis nello spazio cibernetico. Per concludere, le organizzazioni terroristiche hanno finora sfruttato lo spazio cibernetico prevalentemente per incrementare l'efficacia delle proprie operazioni di comando e controllo, per la diffusione della propria propaganda, per attività di finanziamento e reclutamento. Prima di essere in grado di sferrare un attacco in grado di produrre effetti di una certa rilevanza è ipotizzabile vi siano dei segnali che indichino un significativo aumento della sofisticazione delle abilità tecnologiche degli attaccanti. Sebbene sia ormai acclarato che le infrastrutture critiche informatizzate di un paese facciano parte degli obiettivi sensibili delle organizzazioni terroristiche, non risulta che queste ultime abbiano manifestato l'intenzione di colpire i sistemi Atm di un paese. Questo non esclude tuttavia che ci sia interesse ad attaccare il settore dell'aviazione civile in generale.

Le analisi e le valutazioni di autorità istituzionali ed esperti confermano la disamina di cui sopra. Nel 2012 il capo dell'intelligence americana James Clapper sosteneva di aver "rilevato che alcune organizzazioni terroristiche hanno accresciuto il proprio interesse nello sviluppo di capacità cibernetiche offensive, ma saranno probabilmente limitate dalle loro risorse, limiti organizzativi e diverse priorità"[133]. Nel 2015 il giudizio non sembra essere cambiato e la minaccia non sembra essere aumentata: "Gruppi terroristici continueranno a sperimentare tecniche di hacking, che potrebbero essere alla base dello sviluppo di capacità più avanzate. I simpatizzanti di gruppi terroristi condurranno probabilmente attacchi informatici

[132] "Des mots de passe de TV5 Monde sous les images de France 2 et BFM TV", in *Télé Satellite et Numérique*, 10 avril 2015, http://www.telesatellite.com/actu/45271-des-mots-de-passe-de-tv5-monde-sur-les-images-de.html.

[133] James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, 31 January 2012, https://www.hsdl.org/?abstract&did=699575.

ISSN 2280-6164

di basso livello per conto di quest'ultimi e per attrarre l'attenzione dei media, i quali amplificheranno le capacità e la minaccia proveniente da questi attori"[134]. Anche secondo il Cert statunitense, noti gruppi terroristi hanno capacità informatiche meno sviluppate rispetto ad altri attori, così come è meno sviluppata la loro propensione ad utilizzare lo spazio cibernetico rispetto a diversi tipi di strumenti per raggiungere i loro obiettivi. Pertanto il livello di minaccia posto da questi attori è considerato basso[135]. La valutazione delle autorità americane è condivisa da molti altri analisti[136].

Tenendo conto dei differenti intenti e obiettivi rispetto agli attori di matrice terroristica, gli hacktivisti hanno confermato un livello tecnico più elevato rispetto a quello delle organizzazioni sopra analizzate. Ad operazioni di web defacement, che di per sé non dimostrano un grado di sofisticazione particolarmente alto, si sono affiancati attacchi DoS/DDoS contro siti web istituzionali e la sottrazione di informazioni da domini più complessi rispetto agli account Twitter di US Centcom e di Newseek. Più in generale si continua ad osservare un incremento costante del livello tecnico di questi attori. Nonostante l'Ics-Cert abbia dichiarato che nel corso del 2014 alcuni hacktivisti hanno attaccato le infrastrutture critiche americane, non vi sono informazioni che confermino che i sistemi di Atm/Atc aereo abbiano rappresentato un obiettivo specifico. Soprattutto per quel che riguarda il caso studio di Anonymous, secondo le fonti disponibili, non sembra sia manifesta l'intenzione di colpire obiettivi che potrebbero mettere a repentaglio la vita di essere umani, ma piuttosto quella di continuare a colpire istituzioni e/o personalità non in linea con le loro campagne ideologiche.

In generale, secondo le autorità americane gli hackivisti rappresentano una minaccia di livello medio, soprattutto per la capacità di condurre isolati, anche se dannosi, attacchi contro le infrastrutture critiche. Singoli o limitati gruppi di hacker invece non sembrano poter costituire una minaccia critica, sebbene il livello di pericolo aumenti considerevolmente se si considera la comunità hacker nel suo insieme[137].

[134] James R. Clapper, *Worldwide Cyber Threats, Statement for the Record, House Permanent Select Committee on Intelligence*, 10 September 2015, https://t.co/xpI06A09rD.

[135] Ics-Cert, *Cyber Threat Source Descriptions*, cit.

[136] Anche secondo Tobias Feakin, Isis e affiliati non sono in grado di lanciare complessi attacchi contro network vitali. Si veda: Tobias Feakin, "A Deadly Mistake: Don't Underestimate ISIS in Cyberspace", in *The Buzz Blog*, 1 June 2015, http://nationalinterest.org/node/13014. La stessa valutazione è offerta da Pano Yannakogeorgos, secondo cui i terroristi non hanno al momento le necessarie capacità per raccogliere informazioni sullo stato delle vulnerabilità e/o creare malware contro complessi sistemi informatici. Si veda: Pano A. Yannakogeorgos, "Rethinking the Threat of Cyberterrorism", in Thomas M. Chen, Lee Jarvis, Stuart Macdonald (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, Springer, 2014, p. 56. Per una visione opposta si veda l'esperto di sicurezza informatica Mikko Hyppönen: Pierluigi Paganini, "Mikko Hyppönen warns the ISIS has a credible offensive cyber capability", in *Security Affairs*, 26 October 2015, http://securityaffairs.co/wordpress/41438.

[137] Ics-Cert, *Cyber Threat Source Descriptions*, cit.

ISSN 2280-6164

Infine, anche il vasto mondo del crimine cibernetico ha continuato la sua evoluzione tecnica, come evidenziato dall'impiego di strumenti che prima erano prerogativa di attori più sofisticati. Anche se è difficile trarre delle conclusioni nette sull'operato di un numero di attori particolarmente elevato, le tecniche e gli strumenti utilizzati da criminali nello spazio cibernetico riflettono il loro obiettivo primario, ovvero il profitto. Seguendo questa logica, l'interruzione dei servizi di gestione e controllo del traffico aereo non sembra uno scenario corrispondente ai loro fini principali. Attaccare questi sistemi li esporrebbe ad una visibilità indesiderata.

Ciononostante, per la loro capacità di condurre attività di spionaggio industriale e le possibilità economiche a disposizione per il reclutamento di hacker competenti, criminali cibernetici e crimine organizzato rappresentano una minaccia di medio livello[138].

4. Il caso studio italiano

Il presente capitolo cerca di rispondere alle domande poste nell'introduzione di questa ricerca. Nella prima sezione si descrive il ruolo di Enav, la società che fornisce i servizi Atm/Atc in Italia, nonché, nei limiti della riservatezza imposta dalla legge sulle tecnologie in uso nelle infrastrutture critiche, le architetture e i sistemi impiegati dalla società. Sulla base di quanto analizzato nel capitolo precedente, la seconda sezione affronta il tema della minaccia cibernetica verso l'Italia. Nella terza sezione, sintetizzando i principali punti delle due precedenti, si valuta in quale misura i sistemi Atm/Atc di Enav siano vulnerabili e fino a che punto gli attori non statali presi in considerazione dispongano delle capacità tecniche per attaccarli.

4.1 Enav e la gestione del traffico aereo in Italia

A livello europeo opera Eurocontrol, organizzazione intergovernativa civile cui partecipano 41 stati europei e tre paesi limitrofi (Turchia, Armenia, Georgia) e il cui scopo principale è sviluppare e mantenere un efficiente sistema di gestione del traffico aereo a livello europeo, affiancando in questo impegno comune le autorità nazionali dell'aviazione civile (in Italia l'Enac[139]), gli enti ed i soggetti fornitori dei

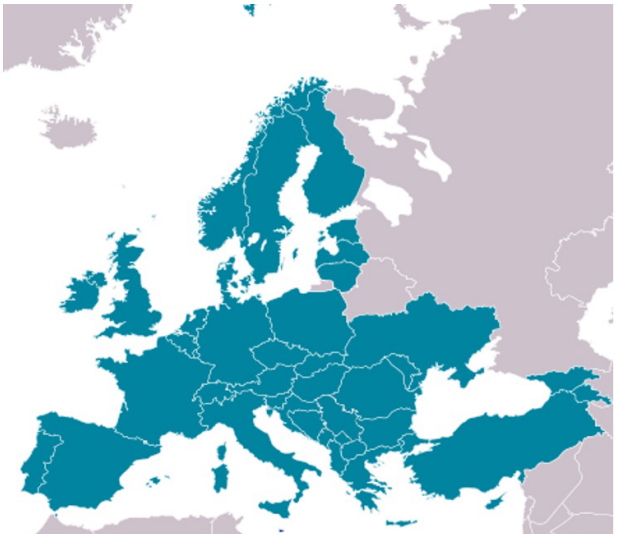
[138] Ibid. In generale, se si considera invece nello specifico il settore dell'aviazione civile, il gruppo di lavoro "Threat and Risk" dell'Icao ha concluso come anche per il 2015 il rischio cibernetico nel settore dell'aviazione civile risulti basso.

[139] In Italia l'ente regolatore per l'aviazione civile è l'Ente nazionale per l'aviazione civile (Enac), autorità di regolamentazione tecnica, certificazione e vigilanza nel settore dell'aviazione civile sottoposta al controllo del Ministero delle Infrastrutture e dei trasporti. In particolare, le principali competenze dell'Enac sono: 1) regolamentazione tecnica, attività ispettiva, e tenuta dei registri/albi; 2) razionalizzazione e modifica delle procedure attinenti ai servizi aeroportuali; 3) coordinamento con Enav e con Am; 4) rapporti con enti, società ed organismi nazionali ed internazionali che operano nel settore dell'aviazione civile; 5) istruttoria atti concernenti tariffe, tasse e diritti aeroportuali; 6) definizione e controllo dei parametri di qualità dei servizi aeroportuali e di trasporto aereo; 7) regolamentazione e valutazione dei piani regolatori, di intervento e di

ISSN 2280-6164

servizi Atm/Atc (in Italia Enav e l'Aeronautica Militare), gli utenti dello spazio aereo civile e militare, il settore industriale, le organizzazioni professionali e le competenti istituzioni europee[140].

Figura 4 | Stati partecipanti ad Eurocontrol



Spettano a Eurocontrol funzioni di studio, analisi propositive per la sicurezza della fornitura dei servizi della navigazione aerea nonché gestionali. In particolare Eurocontrol, su delega della Commissione europea, gestisce il Network Manager Operations Centre (Nmoc), unità finalizzata ad armonizzare e ottimizzare i piani di volo che riguardano l'Europa e il Central Route Charges Office (Crco), che integra la fatturazione dei servizi dei singoli operatori nazionali alle compagnie aeree. Una convenzione tra gli stati membri ha creato una commissione indipendente, la Safety Regulation Commission (Src) per produrre rapporti ed avvisi per migliorare la sicurezza del controllo del traffico aereo e per proporre l'adozione di regolamenti sulla base di requisiti denominati Eurocontrol Safety Regulatory Requirements (Esarr).

In Italia, gli Ats sono forniti prevalentemente da Enav[141], che si occupa in generale del traffico aereo civile, del traffico aereo militare non operativo e di Stato nello spazio aereo nazionale e delegato per circa 751.000 kmq, nonché negli aeroporti di competenza.

investimento aeroportuali. Il Codice della Navigazione stabilisce anche che Enac agisca come unica autorità di regolazione tecnica, certificazione e vigilanza nel settore dell'aviazione civile.

[140] Eurocontrol nasce con la Eurocontrol Convention del 13 dicembre 1960. Dati ricavati dal sito: http://www.eurocontrol.int.

[141] In aeroporti minori, per esempio Aosta e Tortolì, i servizi Ats sono erogati localmente dalle società di gestione aeroportuale.

ISSN 2280-6164

Enav gestisce quattro Acc, situati presso l'aeroporto di Milano-Linate, Padova/Abano Terme, Roma-Ciampino e Brindisi-Casale. Lo spazio aereo è suddiviso verticalmente in spazio aereo inferiore e superiore. Lo spazio aereo inferiore è suddiviso nei tre Fir di Brindisi, Roma e Milano. Mentre i primi due sono gestiti dai rispettivi Acc (Brindisi-Casale e Roma-Ciampino), il Fir di Milano è gestito da Milano-Linate nella sua parte occidentale e da Padova/Abano Terme nella sua parte orientale[142]. La suddivisione orizzontale delle Fir comporta una simile suddivisione nello spazio aereo superiore[143].

Figura 5 | Suddivisione dello spazio aereo fra Acc

Sistemi Atm/Atc

Enav fornisce a piloti e operatori aeronautici il servizio informazioni aeronautiche, le cui notizie sono elaborate per mezzo dell'Aeronautical Operational Information System (Aois). Tale sistema nazionale online è costituito da una banca dati centrale di proprietà di Enav che gestisce tutte le informazioni aeronautiche essenziali per la sicurezza e la fluidità della navigazione aerea (piani di volo, Notices To Air Men (Notam), slot Atfm, bollettini meteo). Il Centro elaborazione dati Aois assicura il servizio tramite la rete aziendale, con backup su rete satellitare. La rete Aois mette le informazioni a disposizione dei quattro Centri di controllo d'area e dei 42 aeroporti in cui Enav gestisce i servizi per la navigazione aerea. Le informazioni Aois sono messe a disposizione di tutta la comunità aeronautica (Aeronautica Militare, operatori aeronautici, società di gestione aeroportuale, autorità aeronautiche) telematicamente oppure presso gli uffici Aro (Air Traffic Services Reporting Office)

[142] L'Italia ha adottato la classificazione Icao, pur non classificando alcuna porzione di spazio aereo come B o F: classe G per i tre Fir, classi C e G per i tre Uir e classi A, D ed E per le Tma.

[143] Le Uir italiane sono ulteriormente suddivise verticalmente in due porzioni.

ISSN 2280-6164

di Enav presenti a Milano-Linate e Roma-Fiumicino, dove vengono ricevuti i dati relativi ai servizi di traffico aereo ed i piani di volo presentati prima della partenza[144].

Lo standard Amhs (Ats Message Handling Service) nasce da un'iniziativa a livello europeo per l'ammodernamento del sistema di scambio messaggi Ats (Notam, piani di volo, bollettini meteo, allarmi ecc.) nell'ambito del servizio fisso di telecomunicazioni aeronautiche, oggi basato sugli standard Aftn (Aeronautical Fixed Telecommunication Network) e Cidin (Common Icao Data Interchange Network). La situazione mondiale vede il sistema Amhs affiancarsi alla rete Aftn/Cidin anche se quest'ultima verrà progressivamente abbandonata, secondo disposizioni Icao, fino alla sua completa sostituzione entro il 2020[145]. L'Amhs è definito nei manuali e nelle Sarps Atn[146] dell'Icao come l'implementazione dello standard di comunicazione basato sul protocollo X.400[147] usato per lo scambio dei messaggi Ats su rete Atn in modalità store-and-forward. L'impiego di sistemi Amhs è stato avviato già da anni da parte dei vari Ansp europei, utilizzando, per la connessione dei vari centri, un'infrastruttura di rete basata su protocollo Tcp/Ip. Oltre ai vantaggi di natura tecnologica rispetto a Aftn/Cidin, Amhs fornisce maggiori funzioni consentendo un maggior numero di scambi di messaggi, lo scambio di dati binari, o di messaggi dai meccanismi di autenticazione[148].

Architetture sistemi Atm/Atc

La connettività del sistema di telecomunicazioni di Enav è assicurata da una nuova rete integrata per le comunicazioni operative denominata E-Net, in via di completamento. Il programma di copertura implementato da Enav in questi ultimi anni prevede la connessione di tutti gli Acc, degli aeroporti dei centri radio Torre-Bordo-Torre (Tbt) e dei centri radar attraverso un sistema di telecomunicazioni modulare per sito e per servizio con lo scopo finale di innalzare l'affidabilità e la disponibilità delle infrastrutture trasmissive nelle loro componenti locali di sito, di accesso alla rete geografica e di trasporto nazionale.

Il livello logico delle componenti di accesso è progettato per garantire maggiore resilienza, differenziando per modalità di trasporto su tecnologia Ip (Internet Protocol) per alcuni servizi (tra cui Aftn, Aois, Meteo, Oldi, Radar, ecc.) e su pura tecnologia Atm (Asynchronous Transfer Mode) per altri (fonia operativa, radio Tbt

144 Nota Vitrociset, luglio 2015.

145 Ibid.

146 Standards and Recommended Practices (Sarps) Aeronautical Telecommunication Network (Atn).

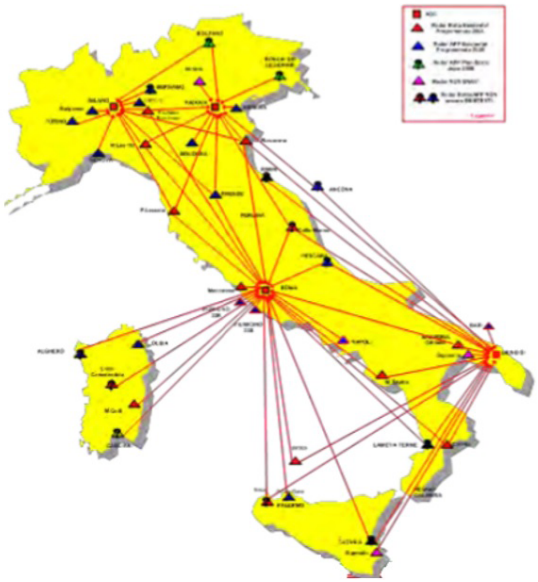
147 X.400 è una serie di raccomandazioni del Telecommunication Standardisation Sector della International Telecommunication Union (Itu-T) per la definizione di un sistema standard di scambio messaggi (Message Handling Systems), analogo alla Internet email.

148 Enav ha stipulato un accordo con Vitrociset che prevede il passaggio evolutivo dal sistema Aftn/Cidin (già fornito da Vitrociset) al nuovo Amhs. Vitrociset, *Vitrociset fornirà all'ENAV il sistema AMHS*, 26 gennaio 2010, http://www.vitrociset.it/dett_editoriale.php?id_editoriale=71.

ISSN 2280-6164

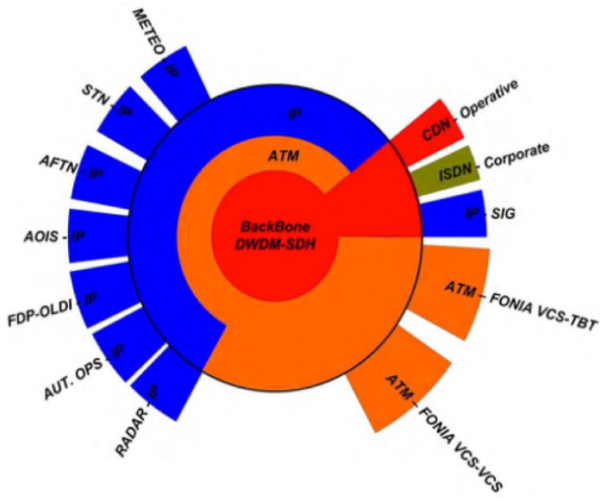
ecc)[149].

Figura 6 | Rete E-Net in Italia



Fonte: Enav.

Figura 7 | E-Net protocolli di rete e associazione con i servizi operativi



Fonte: Vitrociset.

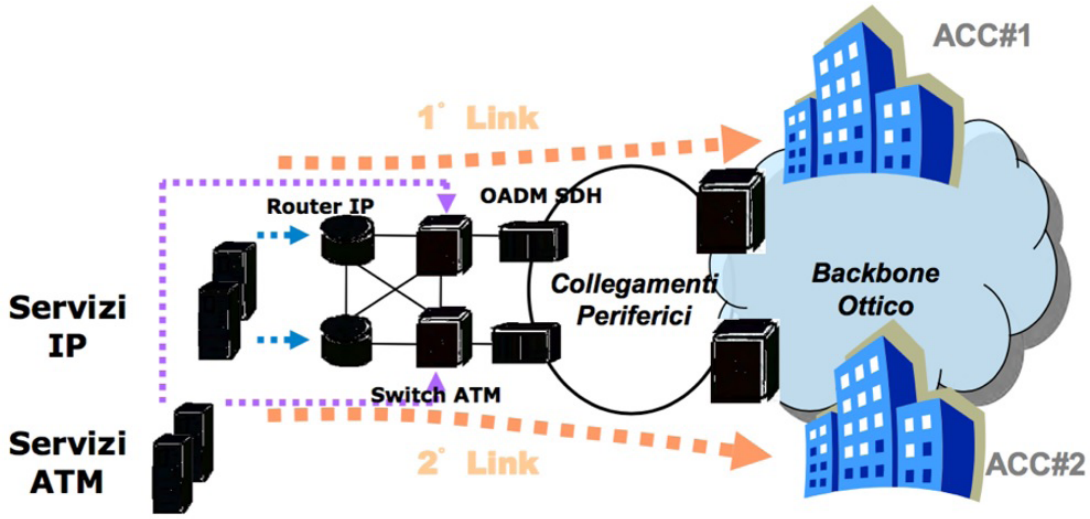
E-Net è contraddistinta da una "spina dorsale" (o "backbone") nazionale costituita da collegamenti protetti ad alta capacità tra Acc e sistemi aeroportuali per l'assistenza al volo, nonché da collegamenti terrestri tra gli aeroporti, i centri radar, i centri

[149] Ibid.

ISSN 2280-6164

radio Tbt ed i siti del backbone.

Figura 8 | Schema collegamenti terrestri e-net fra aeroporti, centri radar, centri radar, centri radio Tbt e siti del backbone



La nuova architettura di rete permette ad Enav di accedere alla rete integrata europea per le comunicazioni operative Ground-Ground denominata Pens (Pan European Network Services) usata per connettere le diverse sedi Eurocontrol e i diversi siti dei vari Ansp europei[150].

E-Net persegue i seguenti obiettivi[151]:

- realizzazione di una rete nazionale integrata per le comunicazioni operative di Enav;
- eliminazione dei "single point of failure"[152] oggi presenti nelle infrastrutture di telecomunicazione;
- duplicazione della tipologia di supporto trasmissiva ("protezione") per le applicazioni maggiormente critiche (Voice/Tbt e dati radar);
- garanzia della qualità del servizio mediante specifici "service level agreement" dedicati per ciascuna applicazione ("service oriented");
- soddisfazione dei requisiti Eurocontrol e nazionali in termini di "safety e security", nello scenario "Gate-to-Gate" e "Single Sky", ed in ottemperanza alla "Eatmp Communications Strategy";
- sviluppo di modalità cooperative con altri attori del sistema aeronautico (cd. collaborative decision-making), in particolare con aeroporti, in anticipazione

[150] Eurocontrol, *Pan-European Network Services (PENS)*, http://www.eurocontrol.int/node/1514.

[151] Enav, "Nel programma E-Net le soluzioni abilitanti per le applicazioni aeronautiche del futuro di Enav", in *Cleared*, a. VI, n. 9 (ottobre 2009), p. 4-5, http://www.enav.it/ec5/enav/it/pdf/cleared/CLEARED_5_09.pdf.

[152] Singole componenti (hardware o software, in generale) che in caso di malfunzionamento o anomalia causano disfunzione dell'intero sistema.

ISSN 2280-6164

della logica System-Wide Information Management (Swim) dei sistemi di nuova generazione.

La logica di Enav è tenere separata la rete operativa interna rispetto a quella gestionale, segnando tra le due entità un chiaro confine fisico e logico. Per le esigenze di relazione su rete pubblica, finalizzate allo scambio istituzionale, sono stati istituiti due "Point of Presence" (PoP)[153], denominati "Ire – Interconnessione reti esterne". I due PoP forniscono sia un servizio di interconnessione e trasporto del traffico tra la rete E-Net e ciascuna delle infrastrutture di ogni singola terza parte collegata, sia un servizio di protezione perimetrale della rete E-Net. I due PoP oltre a garantire una maggiore flessibilità di interconnessione garantiscono anche, per alcuni servizi, una ridondanza geografica in caso di caduta di uno dei due nodi. Su entrambi i Moduli di sicurezza (Ms) Ire oltre allo stato di firewalling[154] con spiccata granularità analitica di traffico sono stati installati Intrusion Detection System (Ids)[155] avanzati, per effettuare analisi del traffico a livello applicativo. L'accesso è permesso esclusivamente alle entità verificate ("trusted") secondo configurazioni di responsabilità/autorizzazione e con stringenti politiche di traffico. Gli eventi di quanto registrato dai Ms Ire e dagli Ids vengono ricevuti e analizzati dai sistemi del Security Operation Centre (Soc) di Enav alla ricerca di attività anomale o malevole, con una verifica comportamentale ("behavioural")[156], secondo schemi precodificati e con soglie di allarme crescenti[157].

Il servizio Aois consiste nel mettere a disposizione degli utenti informazioni aeronautiche per la navigazione aerea. Tali informazioni sono contenute in una banca dati basata su tecnologia Web/Linux J2EE con database Oracle collocata nell'Acc di Ciampino verso la quale hanno accesso vari terminali presenti negli aeroporti. Il flusso di dati avviene tramite protocollo Tcp/Ip[158].

Per il servizio Aois vanno distinte tre tipologie di infrastrutture:
- Acc di Ciampino che ospita il mainframe[159] Aois e terminali Aois;
- Acc remoti (Brindisi, Padova, Milano);
- aeroporti di tipo C/M e aeroporti di tipo S che sono la periferia.

[153] I PoP sono accessi di interconnessione.

[154] I firewall sono dispositivi che analizzano il traffico dati tra una rete interna e l'esterno in base a definite regole di sicurezza, bloccando le comunicazioni che violano le regole.

[155] Intrusion Detection System è un presidio tecnologico utilizzato per rilevare i tentativi di attacco intrusivo in un sistema (Host Ids) o rete (Network Ids).

[156] I cosiddetti behaviour-based Ids tentano di rilevare le intrusioni sulla base di comportamenti anomali da parte dei sistemi o degli utenti, o comunque comportamenti differenti da quelli attesi.

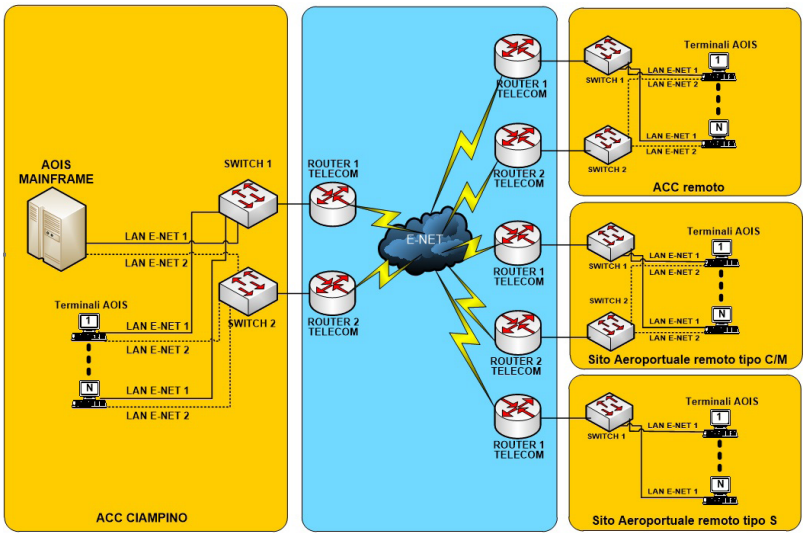
[157] Interviste, novembre 2015.

[158] Nota Vitrociset, cit.

[159] Si tratta di computer, tipicamente di notevoli dimensioni e capacità computazionali, usati da grandi organizzazioni per attività critiche ed elaborazioni massive, cui gli utenti si collegano da terminali remoti. Il nome deriva dall'aspetto dei primi mainframe, che assomigliavano a grandi armadi.

ISSN 2280-6164

Figura 9 | Servizio Aois su E-Net



Nota: Non è presente nella grafica il presidio di sicurezza, esistente su ogni interconnessione di sito in modalità ridondata.

L'infrastruttura di rete prevede una Local Area Network (Lan) nell'Acc di Ciampino sulla quale si attestano sia il mainframe Aois (in dismissione) che i terminali Aois presenti. Tale sistema distribuisce le informazioni sulla rete E-Net e, in alternativa, anche su rete pubblica in caso di emergenza, con appropriate predisposizioni di sicurezza e segmentazione su Internet dedicata. Per i collegamenti remoti sono previsti dei router e una serie di switch[160] presidiati da moduli di sicurezza basati su firewall di ultima generazione, centralmente gestiti e monitorati dal Soc.

Il centro elaborazione dati Aois assicura il servizio tramite E-Net e una rete satellitare[161] con funzioni di backup. La rete Aois mette le informazioni a disposizione dei quattro Acc e dei 42 aeroporti (43 dal 10 dicembre, con l'assunzione del servizio Atc presso l'aeroporto già militare di Brindisi-Casale) in cui Enav gestisce i servizi per la navigazione aerea. Le informazioni Aois sono messe a disposizione di tutta la comunità aeronautica (Aeronautica Militare, operatori aeronautici, società di gestione aeroportuale, autorità aeronautiche) telematicamente oppure presso gli uffici Aro di Enav. Tramite un collegamento ad alta velocità con il Centro internazionale di comunicazioni (Icc), Enav è fonte ed interfaccia nazionale della rete mondiale di telecomunicazioni aeronautiche, nota anche come Aftn. Nella rete mondiale transitano tutti i messaggi Ats (piani di volo, Notam, bollettini meteorologici e messaggi di slot). Il sistema Aois, in particolare, tratta

[160] Ibid. Router e switch sono dispositivi usati per collegare reti. I router sono tipicamente impiegati per interfacciare una rete locale con un'altra rete che fornisce connettività esterna. Gli switch sono invece utilizzati per segmentare e articolare reti locali ad alta velocità.

[161] Rete di telecomunicazione digitale, parzialmente obsoleta, che fornisce servizi di telefonia, telefax, teleconferenza, servizi addizionali (identità del chiamante, trasferimento di chiamata, multinumero) e trasmissione dati a bassa velocità (due canali bidirezionali a 64kb/s e un altro a 16kb/s).

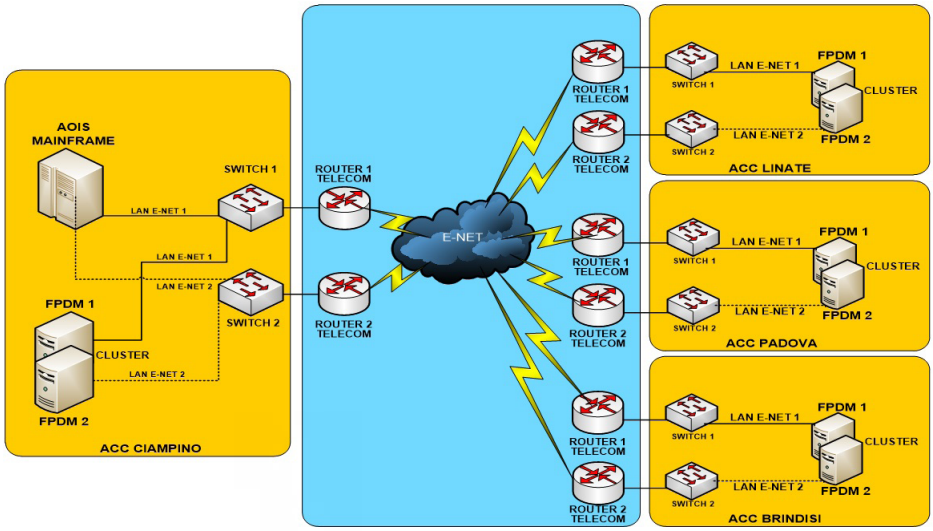
© 2015 IAI
ISSN 2280-6164
DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

quotidianamente circa 50.000 messaggi in ricezione e circa 7.000 in trasmissione[162].

Grazie alle funzioni del sistema Aois è possibile:

- presentare direttamente i piani di volo per la relativa validazione da parte di Eurocontrol;
- disporre in tempo reale delle informazioni necessarie alla sicurezza del volo (Notam, avvisi per il personale interessato alle operazioni di volo);
- visualizzare, in caso di voli soggetti a regolazione di flusso, le finestre orarie (slot Atfm) assegnate agli aeromobili in partenza;
- consultare previsioni meteorologiche di rilevanza aeronautica (bollettini meteo)[163].

Figura 10 | Servizio Aois Fpdm



Nota: La figura omette, anche se esistente, lo strato di sicurezza attraverso moduli ridondati centralmente gestiti.

L'infrastruttura di rete è costituita da circuiti ad alta affidabilità e sistemi provvisti delle opportune ridondanze al fine di assicurare al massimo grado la continuità operativa, l'immunità da interferenze e la capacità di ridurre al minimo le interruzioni di servizio dovute anche ad avarie gravi, attraverso logiche stringenti di backup, di disaster recovery e di configuration management estese a tutti i centri Atc.

Il sistema centrale integrato Aftn-Cidin-Amhs dell'Icc di Roma Ciampino, operante su piattaforma Linux, consente lo scambio di messaggi Amhs sia per gli utenti nazionali che quelli internazionali e garantisce l'interoperabilità con la rete Aftn/

[162] Enav, *Informazioni Aeronautiche*, http://www.enav.it/portal/page/portale/PortaleENAV/Home/ServiziEAttivita?CurrentPath=/enav/it/servizi_attivita/informazioni_aeronautiche.

[163] Ibid.

ISSN 2280-6164

Amhs nazionale e internazionale[164].

Il sistema centrale integrato Aftn-Cidin-Amhs consente la connessione tra i seguenti sistemi Atm/Atc:

- sistema centrale integrato Aftn-Cidin-Amhs di Fiumicino tramite doppia connessione Wide Area Network (Wan) su rete E-Net;
- postazioni User Agent (terminali Amhs presso gli Aro degli aeroporti) della periferia nazionale tramite rete E-Net;
- sistema Aois dell'Icc di Roma Ciampino;
- sistema Fdp Roma;
- sistema Fdp Milano;
- sistema Fdp Brindisi;
- sistema Aftn di Aeronautica Militare presso ReSIA;
- centro meteo Cnmca[165] di Aeronautica Militare;
- sistema Setinet per la connessione della parte Amhs al sistema Amhs di Ginevra;
- rete Pens europea, per il collegamento della rete Amhs Europa;
- sistema Amhs di Bangkok tramite circuito dedicato messo a disposizione dall'Enav presso l'Icc di Roma Ciampino (connessione Tcp/Ip)[166].

A proposito delle informazioni di volo si rileva che Enav mette a disposizione un servizio di "Self Briefing", denominato "The New Generation of Pre-Flight Information Systems". Una modalità semplice e innovativa per gli utenti aeronautici, piloti e organizzazioni per accedere alle informazioni pre-volo attraverso un portale dedicato via internet. In pochi passaggi l'utente può accedere e confezionare le informazioni aeronautiche e la documentazione pre-volo in piena autonomia[167].

Figura 11 | The New Generation of Pre-Flight Information Systems

164 Ibid.

165 Centro nazionale di meteorologia e climatologia aeronautica.

166 Enav, *Informazioni Aeronautiche*, cit.

167 Enav pubblica sulla pagina preliminare all'accesso al servizio il seguente disclaimer: "Durante le fasi di validazione e test, Enav si esonera dalla responsabilità per la correttezza, completezza e accuratezza delle informazioni fornite attraverso il portale web Self Briefing. In aggiunta nessuna responsabilità di alcun tipo, implicita o esplicita, viene assunta da Enav S.p.A."

ISSN 2280-6164

Il servizio si presenta come una applicazione web che ammette il login tramite collegamento sicuro basato su Transport Layer Security (Tls)[168], in modo da assicurare la privatezza delle comunicazioni, l'integrità dei dati scambiati, l'identità del server. L'identità dell'utente è provata attraverso un sistema tradizionale di autenticazione a singolo fattore basato su nome utente e password. Il sistema non si riferisce ai piani di volo presentati dalle compagnie aeree, bensì a quelli presentati dall'utenza preposta ed ha misure interne di verifica dei dati, su campi statici, conformi agli standard internazionali previsti dagli annessi tecnici della Convenzione di Chicago.

Poiché accetta input dall'utente (almeno per l'inserimento delle credenziali) e utilizza il linguaggio Javascript, l'applicazione web è potenzialmente soggetta ad attacchi a livello applicativo, basati su (D)DoS, Sql-injection, cross-site scripting, cookie hijacking, ed altre forme di command injection[169], che potrebbero comportare conseguenze che spaziano dall'abbattimento temporaneo dell'operatività dell'applicazione alla sua compromissione, inclusa quella della base dati a supporto dell'applicazione, fino a prevedere attacchi contro i browser degli utenti che vengono indotti a collegarsi all'applicazione. Le verifiche condotte mediante penetration test secondo le linee guida Osstm[170] e Owasp[171] hanno permesso di accertare l'assenza di vulnerabilità note, secondo i livelli di sicurezza stabiliti da Enav[172].

[168] Definito negli Rfc 2246, 4346, 5246 e 6176 della Internet Engineering Task Force (Ietf).

[169] L'attacco Sql-injection è basato sulla somministrazione, lato utente, di input malevoli all'applicazione web. Se questa non verifica accuratamente la correttezza degli input ricevuti, tali input malevoli determinano accessi impropri alla base dati sui cui è poggiata l'applicazione, consentendo all'attaccante sia di accedere ai servizi in assenza di credenziali di accesso, sia di manipolare la base dati per inserire/cancellare/modificare i dati in essa gestiti. Il cross-site scripting (Xss) è un attacco contro il browser ed è anch'esso basato sul limitato controllo che le applicazioni web hanno sugli input utente. L'attacco sfrutta una applicazione web per veicolare contenuti nocivi ai browser che visitano l'applicazione utilizzando un link appositamente preparato (Xss riflesso) o che eseguono script malevoli memorizzati dall'attaccante nei contenuti della pagina web visitata (Xss permanente). Gli attacchi basati sull'invio di dati invalidi all'applicazione web, o anche di comandi maligni, appartengono all'ampia categoria dei command injection e l'Sql-injection e l'Xss ne sono due classici esempi. Il cookie-hijacking, noto anche come furto di cookie, è un particolare tipo di furto di identità basato sull'accesso ad informazioni riservate gestite del browser, che contengono la prova che il browser si è autenticato presso un servizio web; il possesso dei dati prova appunto che l'autenticazione è già avvenuta con successo. Tali informazioni sono necessarie per evitare che gli utenti di un servizio, ad ogni interazione, debbano autenticarsi di nuovo. Il furto di tali dati consente all'attaccante di ottenere il servizio per il quale il browser ha fatto l'autenticazione senza doversi autenticare (e senza conoscere le credenziali di accesso): il risultato ottenuto è noto come session hijacking.

[170] L'Open Source Security Testing Methodology, dell'Institute for Security and Open Methodologies, organizzazione non-profit registrata in Spagna: http://www.isecom.org/research/osstmm.html.

[171] L'Open Web Application Security Project è la più nota comunità sul tema della sicurezza applicativa nel web: https://www.owasp.org.

[172] Interviste, novembre 2015.

ISSN 2280-6164

Sistemi Atc

Vengono di seguito illustrati i sistemi Atc, inclusi i sistemi di controllo, comunicazione e sorveglianza, utilizzati durante le varie fasi di controllo del traffico aereo dai controllori di volo.

Il Fdp è il sistema Atc che elabora i dati dei piani di volo per differenti finalità ovvero è in grado di fornire ai controllori del traffico aereo un vasto insieme di informazioni contenute nel piano di volo. Di fatto il sistema Fdp fornisce una predizione della situazione del traffico aereo a 30/60 minuti, tale da consentire rilevazioni anticipate delle situazioni di pericolo, rendendo possibili efficaci decisioni di pianificazione del traffico[173].

La Control Working Position (Cwp) è la postazione operativa per il controllo del traffico aereo che consente la visualizzazione della situazione corrente del traffico aereo tramite l'integrazione di dati tattici che derivano dai sistemi radar e dal sistema Fdp. Essa integra in maniera ergonomica molteplici sistemi necessari al controllore per le sue attività: schermo radar, carte e mappe aeronautiche, display delle strip elettroniche, condizioni meteo, traffico di superficie dell'aerodromo, sistemi di comunicazione, sistemi di previsione su possibili conflitti tra traiettorie di volo a medio e breve termine, quest'ultimi in grado di aiutare il controllore nella risoluzione di problematiche legate alla separazione dei velivoli[174].

Particolare cura viene attribuita da Enav alle telecomunicazioni terra-bordo-terra, che costituiscono lo strumento fondamentale di gestione del traffico aereo e il cui dispiegamento, sul territorio nazionale, avviene utilizzando la rete E-Net e con approccio basato su ridondanza fisica e logica[175].

Tutti gli aeromobili sono equipaggiati con apparati ricetrasmittenti che consentono ai piloti di effettuare le comunicazioni terra-bordo-terra, utilizzando sistemi di comunicazione analogici operanti su varie frequenze Vhf/Uhf. Per consentire il miglioramento del servizio e ridurre la congestione di comunicazione voce in banda Vhf, la tendenza è quella di utilizzare il sistema Controller Pilot Data-Link Communication (Cpdlc), che permette lo scambio dei messaggi in modo digitalizzato[176].

[173] Nota Vitrociset, cit.

[174] Ibid.

[175] Il controllo delle frequenze è assicurato dal Ministero dello Sviluppo economico attraverso le sue articolazioni centrali e territoriali. Enav ha inoltre stipulato una convenzione con il Dipartimento della Pubblica sicurezza che prevede, attraverso il Servizio Polizia postale e delle Comunicazioni, un intervento tempestivo della forza di polizia, anche per i fenomeni di interferenza radioelettrica. Si ricorda che esiste una legge speciale, la Legge n. 110 dell'8 aprile 1983 "Protezione delle radiocomunicazioni relative all'assistenza ed alla sicurezza del volo", che permette attivazioni supplementari, anche amministrative oltre che giudiziarie, per l'interdizione delle interferenze sulle reti radio del controllo del traffico aereo.

[176] Nota Vitrociset, cit.

ISSN 2280-6164

Il controllo radar del traffico aereo avviene grazie all'integrazione e combinazione dei contributi di diversi sensori radar e di sistemi di elaborazione dei dati acquisiti che li rendono disponibili alle consolle in uso ai controllori del traffico aereo. Il controllo radar si sviluppa lungo tutto il percorso di rotta fino alla localizzazione a terra del velivolo in aeroporto[177]. L'attività di sorveglianza degli aeromobili è un settore in rapida espansione e sono in corso, a livello mondiale, iniziative intese allo sviluppo di sistemi collaborativi basati su costellazioni di satelliti geostazionari, che permetteranno la ricognizione degli aeromobili in maniera precisa e resiliente (Galileo-Egnos, Aireon, Glonass, tra le diverse iniziative). Su tali sistemi sono aperti diversi tavoli di analisi, che contemplano anche gli aspetti di sicurezza, nei quali Enav ha una posizione di rilievo. La società partecipa direttamente a due programmi, Galileo-Egnos, attraverso il consorzio Essp (European Satellite Services Provider)[178] ed Aireon[179], di cui detiene partecipazioni azionarie[180].

L'Advanced Surface Movement Guidance and Control System (Asmgcs) è il sistema di sorveglianza di terra basato sull'acquisizione ed integrazione (data fusion) di dati provenienti da diversi sottosistemi di sorveglianza[181].

L'Atm Surveillance Tracker and Server (Artas) è un sistema progettato da Eurocontrol al fine di fornire una accurata "air situation picture" in una ben definita area geografica e di distribuire informazioni di sorveglianza rilevanti per tutta una serie di altri sistemi opportunamente interfacciati[182].

L'Atis è un sistema automatico di trasmissione delle informazioni generali utili al pilota riguardanti un aeroporto. Esso viene trasmesso continuamente su frequenze dedicate o può essere associato alla portante di un Vor[183] (nel D-Atis la trasmissione avviene via data link). Contiene informazioni meteorologiche e operative destinate ai piloti che intendono utilizzare l'aeroporto da cui viene emesso l'Atis[184].

Il Satellite Distribution System (Sadis) è il sistema satellitare utilizzato per la distribuzione aggiornata di informazioni ed immagini meteorologiche di alta qualità[185].

177 Ibid.
178 ESSP, *Company Structure and Ownership*, http://www.essp-sas.eu/company_structure.
179 Aireon, *About Aireon*, http://aireon.com/company.
180 Interviste, novembre 2015.
181 Nota Vitrociset, cit.
182 Ibid.
183 Vhf Omnidirectional Radio Range.
184 Nota Vitrociset, cit.
185 Ibid.

ISSN 2280-6164

La strategia di security di Enav

Le strategie di sicurezza di Enav vengono declinate attraverso una puntuale definizione dei principi cui l'azienda si ispira per la sicurezza delle informazioni. La fornitura dei servizi di navigazione aerea, come descritta dal contesto normativo, è un'attività di natura sostanzialmente pubblica, che è rivolta alla protezione di primari interessi del Paese, con riferimenti di rango costituzionale[186].

La regolamentazione europea è particolarmente stringente nel richiedere ai fornitori dei servizi di navigazione aerea un "sistema di gestione della sicurezza" che risponda alle caratteristiche – descritte nel paragrafo quattro dell'Allegato I del Regolamento Ue 1035/2011[187] – e che caratterizza il modo con cui Enav, come gli altri Ansp, deve dimostrare la propria conformità ai fini del mantenimento della certificazione di fornitore dei servizi di navigazione aerea[188].

Sulla base di tale principio, Enav ha deciso di sottoporsi ad un processo di certificazione, secondo la norma di standardizzazione Iso 27001:2014, per rendere oggettivo e misurabile, anche con valutazione di parti terze, l'intero ciclo di vita della sicurezza. Questa è estesa anche agli aspetti di sicurezza fisica, al fattore umano e ai processi, ed è fortemente integrata con gli altri sistemi di gestione esistenti in Enav: gestione della qualità Iso 9001 ed il "Safety Management System", riferito alla sicurezza operativa aeronautica[189].

L'intero processo di sicurezza si svolge nel rispetto del metodo di gestione noto come "ciclo di Deming", che prevede uno specifico impegno da parte del vertice aziendale ed un processo di analisi del rischio particolarmente pervasivo e trasversale. L'approccio metodologico è incardinato su principi semplici, che vogliono superare il tradizionale approccio basato su protezioni perimetrali e sicurezza multi-strato, mirando alla messa in sicurezza di reti, sistemi, software e processi, e adottando un processo di gestione del rischio articolato, ispirato allo standard Iso 31000[190], come illustrato nella figura 12.

[186] Regolamento CE 550/2004 sulla fornitura di servizi della navigazione aerea nel cielo unico europeo, 10 marzo 2004, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32004R0550.

[187] Regolamento di esecuzione (UE) n. 1035/2011 che stabilisce i requisiti comuni per la fornitura di servizi di navigazione aerea..., 17 ottobre 2011, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32011R1035.

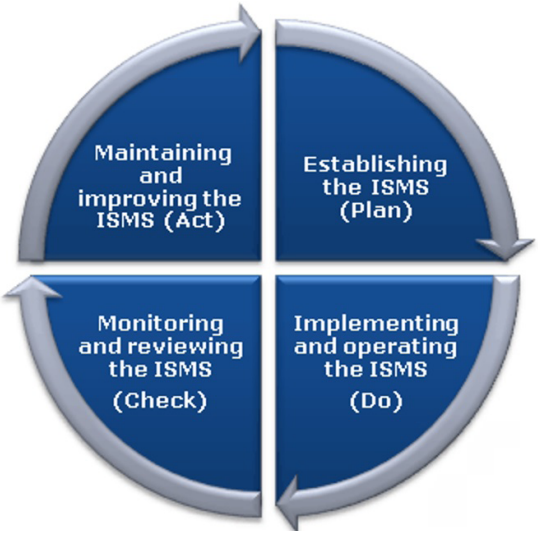
[188] Va anche tenuto presente che la posizione di garanzia evidenziata impone, in riferimento all'art. 40 del Codice penale, l'adozione di ogni misura praticabile, in quanto "non prevenire un evento, che si ha l'obbligo giuridico di prevenire, equivale a cagionarlo".

[189] Interviste, novembre 2015.

[190] ISO, *ISO 31000 - Risk management*, http://www.iso.org/iso/iso31000.

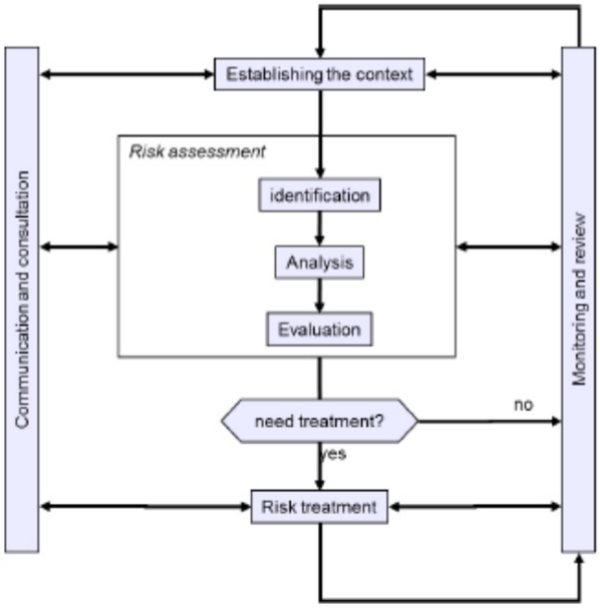
ISSN 2280-6164

Figura 12 | Ciclo di deming per l'Information Security Management System



Enav è l'unico provider certificato in Europa e questo ha consentito di mettere a punto un processo che mira a determinare le vulnerabilità in considerazione dei risultati dell'analisi del rischio, con una gestione della sicurezza che valorizzi le buone pratiche e preveda la diffusione delle stesse.

Figura 13 | Processo di gestione del rischio (Iso 31000)



Per quanto concerne la valutazione del rischio, si fa riferimento alla metodologia Magerit e all'applicazione Pilar[191], che permette un'immediata valutazione delle

[191] Magerit è una metodologia di analisi e gestione dei rischi elaborata dallo spagnolo Consejo

DOCUMENTI IAI 15 | 23 - DICEMBRE 2015
ISSN 2280-6164

relazioni tra assetti, rischi, e gestione e mitigazione del rischio, con un'attenzione particolare alle misure di "gestione della continuità operativa".

Per questo genere di attività esiste una funzione aziendale specificamente preposta alla gestione della sicurezza logica. Essa applica in maniera stringente il principio della "separazione dei compiti"[192] e si avvale di un Soc polifunzionale e integrato con i processi di sicurezza fisica, la cui organizzazione e il cui funzionamento sono stati impostati a partire dal 2009[193].

Il Soc di Enav gestisce la sicurezza in maniera centralizzata attraverso specifici processi, procedure e tecnologie e coopera con vari soggetti interni ed esterni. I domini di monitoraggio del Soc sono la sicurezza dei servizi non operativi, la sicurezza dei servizi operativi e la sicurezza della rete E-Net. Le funzioni attribuite al Soc includono la gestione centralizzata di: controllo degli accessi e rilevamento di intrusioni; allarmi e avvisi; eventi di sicurezza; coordinamento con le forze di polizia e il personale di sorveglianza delle unità Ats; supporto nella gestione di crisi; gestione degli eventi di sicurezza fisica. Svolge inoltre attività di intelligence attraverso la correlazione di eventi fisici-logici, impiegando un'architettura a più strati, con un massivo utilizzo di software a sorgente aperta ("open source") e risorse certificate, tutte interne.

L'attività del Soc è a supporto di tutte le esigenze del gruppo relative alla sicurezza delle informazioni e contribuisce, su specifico mandato della direzione aziendale, alla definizione dei requisiti di dominio e di compilazione del software sicuro nonché alla verifica della sicurezza nelle fasi di progettazione, oltre ad erogare costanti – e anche automatizzati – servizi di valutazione delle vulnerabilità ("vulnerability assessment") e monitoraggio di conformità ("compliance monitoring"). La figura 14 schematizza i servizi di supporto forniti dal Soc di Enav.

Un ulteriore elemento da menzionare è la partecipazione di Enav, integrato con gli altri attori che operano nel campo della sicurezza e difesa, nell'attuazione della strategia cibernetica nazionale[194]: attraverso una rete convenzionale estesa, Enav partecipa all'insieme della rete di sicurezza e difesa nazionale, in conformità alla natura ed alla missione dell'organizzazione[195].

superior de administración electrónica per ridurre al minimo il rischio nell'uso delle tecnologie dell'informazione, con particolare attenzione alla pubblica amministrazione. Magerit fornisce un'applicazione, Pilar, per l'analisi e gestione dei rischi di un sistema informativo.

[192] In inglese, "segregation of duties". Si tratta di un principio in base al quale l'attività di progettazione dei sistemi, l'esercizio degli stessi, la proposizione dei requisiti di sicurezza e il loro monitoraggio devono essere incardinati in capo a soggetti organizzativi diversi, al fine di ridurre se non eliminare i potenziali "conflitti di interesse".

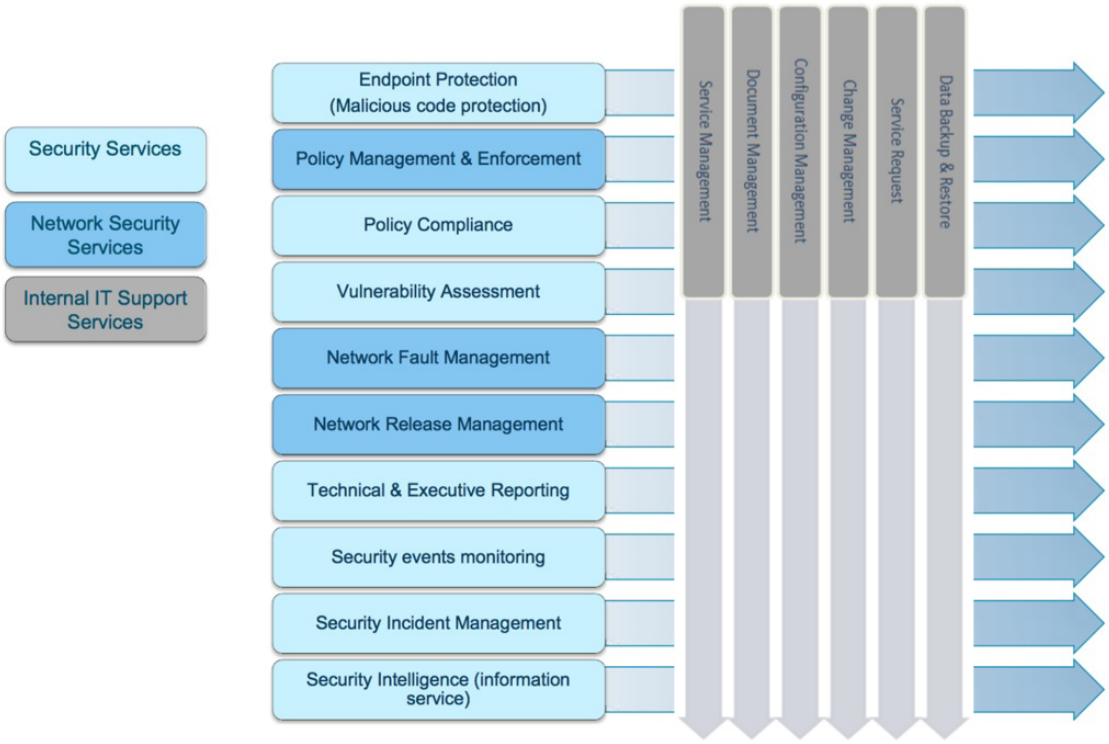
[193] Interviste, novembre 2015.

[194] Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, cit.; e *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, dicembre 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf.

[195] Polizia di Stato, *Sicurezza: rinnovato l'accordo tra Polizia di Stato ed Enav*, 22 gennaio 2015,

ISSN 2280-6164

Figura 14 | Catalogo servizi Soc Enav



4.2 Minacce cibernetiche verso l'Italia

Organizzazioni terroristiche (Isis e Al-Qaeda)

L'Isis considera l'Italia un obiettivo legittimo per via del suo ruolo nella coalizione impegnata contro l'organizzazione terroristica in Siria e Iraq e per il valore simbolico di Roma[196].

Proprio come gli altri stati che hanno partecipato alle operazioni in Medio Oriente, nel corso del 2015 anche l'Italia è stata obiettivo delle presunte attività cibernetiche dell'Isis. L'episodio più rilevante è avvenuto a maggio 2015, quando sostenitori pro-Isis hanno distribuito via Twitter un documento firmato dall'Ishd e contenente le informazioni personali di dieci militari italiani. Nel documento l'Ishd sosteneva di aver ottenuto l'accesso a "server sicuri", proprio come era avvenuto in occasione della pubblicazione di informazioni riguardanti il personale militare americano ad agosto 2015. Il documento, pubblicato sul sito Justpaste.it e poi distribuito

http://www.poliziadistato.it/articolo/view/37318; Stefania Ducci, "Moving Toward an Italian Cyber Defense and Security Strategy", in Daniel Ventre (ed.), *Cyber Conflict. Competing National Perspectives*, London, Wiley / Hoboken, Iste, 2012, p. 165-191.

196 Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, febbraio 2015, p. 31, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2015/02/relazione-2014.pdf.

© 2015 IAI
ISSN 2280-6164
DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

tramite Twitter, veniva accompagnato dall'hashtag #WeWillBurnRome[197]. Scritto in italiano, il messaggio dell'Ishd affermava:

> Conquisteremo Roma, e Aqsa, distruggeremo le vostre croci, con il benestare di Allah. I'm back altough the disbelievers dislike it. Giuriamo su allah che entreremmo [sic] e conquisteremmo [sic] roma non manca tanto... Un messaggio ai lupi solitari aspettiamo le vostre sorprese Italia ha dichiarato la guerra e noi l'abbiamo dichiarata tempo fa Aljihad Aljihad Aljihad. Allora saremo noi a portare la jihad nelle vostre terre. Hai detto che la mano dell'America è lunga e può giungere ogni dove, e allora sappi che i nostri coltelli sono affilati: tagliano mani e gole dei miscredenti[198].

Al di là di questo episodio, l'attività informatica "offensiva" (o presunta tale) dell'Isis o di suoi sostenitori e affiliati, è stata perlopiù caratterizzara da attacchi informatici di basso livello tecnico. Ne sono un esempio i web defacement dei siti web della regione Lombardia, della sezione toscana del Partito Democratico e dell'Accademia della Crusca[199]. Non è detto però che questi atti siano ascrivibili all'attività dell'Isis o che avessero come obiettivo le istituzioni italiane. È possibile, infatti, che gruppi di hacker sostenitori della causa jihadista abbiano lanciato dei programmi online che quasi automaticamente abbiano poi colpito siti web non particolarmente protetti[200].

L'attività cibernetica dell'Isis e dei suoi sostenitori si è concretizzata maggiormente sotto forma di minacce che hanno utilizzato il web come strumento di propagazione. Sempre nel corso del 2015 esempi significativi sono state le intimidazioni verso: l'Italia e l'Europa (individuate come possibili obiettivi dei "missili" dell'Isis), il ministro degli Esteri Paolo Gentiloni (definito "ministro dell'Italia crociata") e infine l'Italia in generale (in un libro disponibile online in cui si afferma che l'Isis dovrebbe allearsi con la mafia per conquistare Roma)[201]. A luglio sono stati arrestati

[197] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.; Site Intelligence Group, "'Islamic State Hacking Division' Calls for Attacks on 10 Italian Army Personnel", in *Dark Web & Cyber Security*, 1 June 2015, https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-6-1-15-ishd-calls-for-attacks-on-10-italian-army-personnel.html; Alessandro Burato, "Islamic State Hacking Division ai 'lupi' di IS: 'Colpite i soldati italiani'", in *ITSTIME*, 20 July 2015, http://www.itstime.it/w/?p=1962.

[198] Alessandro Burato, "Islamic State Hacking Division ai 'lupi' di IS: 'Colpite i soldati italiani'", cit.

[199] "Hacker pro Isis su sito web Lombardia", in *Ansa Cronaca*, 2 febbraio 2015, http://www.ansa.it/sito/notizie/cronaca/2015/02/02/hacker-pro-isis-su-sito-web-lombardia_7035dab0-d8de-4c8c-84ab-6c28ccc2d5c6.html; "Hacker su sito Pd Toscana, sigla Isis", in *Ansa Toscana*, 7 marzo 2015, http://www.ansa.it/toscana/notizie/2015/03/07/hacker-su-sito-pd-toscana-sigla-isis_afb49349-360d-4dd8-9d5e-89893b96983f.html; "Hackerato sito Crusca, simboli", in *Ansa Toscana*, 9 agosto 2015, http://www.ansa.it/toscana/notizie/2015/08/09/hackerato-sito-crusca-simboli-isis_1042b667-394e-4fba-99b7-0c8828df693c.html.

[200] "Hackerato sito Crusca, simboli", cit.

[201] "Terrorismo: ancora minacce web, 'missili sull'Italia'", in *Ansa Cronaca*, 3 febbraio 2015, http://www.ansa.it/sito/notizie/politica/2015/02/02/terrorismo-ancora-minacce-web-missili-sullitalia_90b0483d-6617-4127-9618-9993f953e334.html; "Isis,Gentiloni"ministro Italia crociata", in *Ansa Cronaca*, 14 febbraio 2015, http://www.ansa.it/sito/notizie/topnews/2015/02/14/

ISSN 2280-6164

un tunisino e un pachistano, i quali, secondo le autorità, rappresentavano "un serissimo pericolo di attentati alla pubblica incolumità con finalità di terrorismo"[202]. I due avevano utilizzato Twitter per diffondere immagini in cui, davanti a luoghi simbolo come il Duomo di Milano e il Colosseo, mostravano dei biglietti con scritte che minacciavano possibili attacchi contro quei monumenti. I due avevano anche espresso il desiderio di colpire la base militare di Ghedi. Di particolare rilievo è stato un documento di 64 pagine circolato in aprile, attribuibile all'Isis e scritto in italiano fluente, dal titolo "Lo Stato Islamico, una realtà che ti vorrebbe comunicare"[203].

Per quello che riguarda Al-Qaeda, il gruppo terroristico ha cercato attraverso la sua strategia cibernetica da un lato di sopperire alle perdite del suo nucleo storico e dall'altro lato di non cadere nella penombra delle primavere arabe e dell'Isis. L'attività del gruppo terrorista si è concentrata nel campo della messaggistica e nella reiterazione di una propaganda più marcatamente anti-occidentale. I messaggi diffusi nelle chat e nei forum hanno continuato ad essere il primo veicolo di radicalizzazione sia nei paesi islamici che nei paesi occidentali. Da questo punto di vista, il pericolo maggiore sembra essere rappresentato dal terrorismo cibernetico solitario. A riprova di ciò, nel 2012 la polizia giudiziaria italiana ha messo sotto indagine due individui (un italiano di origini nordafricane e un italiano convertito) per attività di propaganda e addestramento "operativo" sul web. Il tipo di attività online di Al-Qaeda in Italia, in linea con la sua azione a livello globale, sembra comunque quantitativamente inferiore a quella dell'Isis[204].

Hacktivisti

Anonymous opera in Italia a partire dal biennio 2009-2010, anni in cui partirono i primi attacchi rivolti contro organismi statali e aziende, italiani e esteri, che secondo gli hacker mascherati sono rei di condotta "anti-democratica"[205]. Il modello di Anonymous prevede la scelta da parte della base degli obiettivi e delle modalità di attacco nei forum online e nelle chat. Questo gruppo ha assunto in Italia la funzione di "ombrello", poiché ha fatto convergere al suo interno altri gruppi simili.

isisgentiloniministro-italia-crociata_4c7e0481-7371-4aba-8025-47301deb31eb.html; Marta Serafini, "Isis: 'Per conquistare l'Italia dobbiamo allearci con la mafia'", in *Corriere.it*, 26 aprile 2015, http://www.corriere.it/esteri/15_aprile_15/isis-per-conquistare-l-italia-dobbiamo-allearci-la-mafia-91641e80-e383-11e4-8e3e-4cd376ffaba3.shtml.

202 "Terrorismo: due arresti a Brescia, sostenevano l'Isis su twitter", in *Corriere.it*, 22 luglio 2015, http://www.corriere.it/cronache/15_luglio_22/terrorismo-due-arresti-brescia-sostenevano-l-isis-f7003642-3032-11e5-8ebc-a14255a4c77f.shtml.

203 "L'Isis parla italiano, 64 pagine di propaganda sul web", in *Ansa*, 1 marzo 2015, http://www.ansa.it/sito/notizie/cronaca/2015/02/28/isis-documento-di-propaganda-in-italiano-sul-web_6e00ea79-8fef-42fb-8fd7-0b88b3739403.html. Sempre a marzo è stato arrestato l'autore del documento, un ventenne italiano di origine marocchina. Si veda: "Isis, arrestato autore documento propaganda italiano", in *Ansa Piemonte*, 25 marzo 2015, http://www.ansa.it/piemonte/notizie/2015/03/25/isis-arrestato-autore-documento-propaganda-italiano_022c59db-bbdb-4578-bd47-c9f70670ac18.html.

204 Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2011*, 28 febbraio 2012, https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

205 Ibid.

© 2015 IAI ISSN 2280-6164 DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

In quanto tale, il collettivo si è confermato il gruppo di riferimento nel panorama hacktivista italiano per via di questa sua funzione "aggregante"[206].

La spinta motivazionale principale del collettivo, originariamente la libertà d'informazione in rete, ha subito negli ultimi anni un allargamento ad altri target di particolare sensibilità, come ad esempio il settore militare[207]. A partire dal 2013 lo spazio cibernetico è stato utilizzato a scopi propagandistici e come vettore di espressione di un malessere sociale, amplificato ulteriormente dalla crisi economica. Tra novembre e dicembre 2013, il movimento hacktivista ha segnato il passaggio dalla lotta per un'informazione e una rete libera al sostegno ad altri tipi di iniziative – come il movimento "No Tav" – caratterizzatosi anche in attacchi informatici verso esponenti politici e istituzioni[208]. Le campagne online sono spesso coincise con le proteste di piazza, come nel caso degli attacchi a siti istituzionali durante le manifestazioni a Roma per il diritto alla casa e contro la crisi economica dell'ottobre 2013[209]. Questo trend si è confermato anche nel corso del 2014 quando l'adesione di alcuni esponenti del movimento a idee anarchiche si è concretizzata in attacchi verso esponenti di partito e istituzioni politiche[210].

Nel 2015 l'azione di Anonymous si è concentrata soprattutto verso due obiettivi: i siti della manifestazione Expo 2015 e vari ministeri italiani. Gli hacktivisti hanno lanciato una campagna (denominata #OpItaly) contro l'esposizione universale a partire da maggio, quando sono riusciti ad eseguire un web defacement del sito padiglioneitaliaexpo2015.com[211]. Successivamente, il collettivo di hacker è riuscito a penetrare i sistemi della società Best Union, che gestiva la compravendita dei biglietti online di Expo. Anonymous ha poi diffuso via Twitter i dati dei privati cittadini che avevano acquistato i biglietti[212]. Sempre a maggio, il collettivo ha diffuso online una serie di informazioni sottratte ad un server del sottodominio eu2014.difesa.it del Ministero della Difesa, compromesso con un attacco di tipo

[206] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit.

[207] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2012*, 28 febbraio 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

[208] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2013*, 6 marzo 2014, https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

[209] Ibid.

[210] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit.

[211] Nel comunicato online il collettivo definisce l'Expo "l'espressione disgustosa della coscienza sporca degli oppressori", criticando ferocemente gli sponsor della manifestazione: "Per capire come dietro i dolci ipocriti discorsi sulla alimentazione, sui diritti e sul rispetto dell'ambiente si nascondono le mani usurpatrici e luride di sangue dei potenti dell'industria". Si veda: Andreina Baccaro, "Expo, i 7 informatici di Best Union in guerra contro Anonymous", in *Corriere di Bologna*, 5 maggio 2015, http://corrieredibologna.corriere.it/bologna/notizie/cronaca/2015/5-maggio-2015/expo-7-informatici-best-union-guerra-contro-anonymous-2301345920346.shtml.

[212] Pierluigi Paganini, "Expo 2015 – Anonymous has stolen 1TB data from Best Union ticketing service", in *Security Affairs*, 18 May 2015, http://securityaffairs.co/wordpress/36907.

ISSN 2280-6164

Sql-injection, secondo quanto riportato dalla stampa. I dati esfiltrati contenevano nomi, indirizzi email e in alcuni casi i numeri di telefono di personale della difesa e aziende in affari con le Forze armate. Con questa azione Anonymous voleva colpire il "complesso militare-industriale" e l'industria della difesa cibernetica[213]. In seguito all'arresto di due figure di rilievo del gruppo, Fabio Meier e Valerio Camici – conosciuti online con i soprannomi Otherwise e Aken – Anonymous ha dichiarato "guerra" al governo italiano. Finora si sono registrati attacchi verso il sito infomercatiesteri.it, partner del sito del Ministero degli Affari esteri e della Cooperazione internazionale, e alcuni altri siti (ferrovie.it, statoregioni.it e mobilita.gov.it[214]). Un'altra operazione (denominata "Summum ius, summa iniuria") condotta in ritorsione agli arresti, avrebbe portato alla sottrazione di dati e al web defacement di siti legati ai Ministeri dell'Interno e della Giustizia (siap-polizia.org, giustizia.lazio.it, caltanisetta.giustizia.it, sap-nazionale.org, assopolizia.it, carabinieri-unione.it e uilpolizia.it[215]). Questa operazione sarebbe stata compiuta da gruppi emergenti all'interno della galassia Anonymous Italia e avrebbe sfruttato delle vulnerabilità "storiche" di questi siti, tra cui password non cifrate[216]. Vale la pena di ricordare che anche Enav fu oggetto di tentativi (infruttuosi) di defacement del sito istituzionale, che portarono ad indagini e al successivo rinvio a giudizio per gli autori[217].

Negli ultimi anni il gruppo ha diminuito la sua azione in termini quantitativi, anche se non in termini qualitativi, come dimostra il costante incremento tecnico degli attacchi. In merito alle tecniche impiegate, si è notato lo sviluppo di malware specifici la cui azione è stata favorita dall'assenza sul mercato di specifici prodotti di contrasto. Si è fatto anche ricorso a nuove tecniche di anonimizzazione per il lancio di attacchi attraverso social network che, attraverso la formazione di botnet, hanno permesso di celare i veri responsabili delle operazioni[218]. Si è potuto osservare al contempo il passaggio da attacchi DoS e web defacement a Sql-injection, nonché worm e tecniche di spear phishing per il furto di informazioni sensibili. Nondimeno, queste attività hanno evidenziato che solo una parta minoritaria del movimento ha capacità informatiche di un certo rilievo, mentre i simpatizzanti sembrano disporre di competenze tecniche limitate[219].

[213] Carola Frediani, "Anonymous colpisce il ministero della Difesa", in *La Stampa*, 19 maggio 2015, http://www.lastampa.it/2015/05/19/italia/cronache/anonymous-colpisce-il-ministero-della-difesa-qlFNgswyvu20wnQiNYK1kL/pagina.html.

[214] Site Intelligence Group, "Partner of the Italian Ministry of Foreign Affairs Targeted as Part of "Operation Italy", in *Dark Web & Cyber Security*, 9 June 2015, http://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-6-9-15-partner-of-the-italian-ministry-of-foreign-affairs-targeted-as-part-of-opitaly.html; Marta Serafini, "Anonymous attacca siti del governo per vendicare I compagni arrestati", in *6gradi*, 4 agosto 2015, http://seigradi.corriere.it/?p=10142.

[215] La notizia è stata riportata dal blog di Anonymous. Interviste, novembre 2015.

[216] Interviste, ottobre 2015.

[217] Interviste, novembre 2015. Si veda inoltre: "Anonymous, tutti i dettagli dell'operazione Tango Down", in *Zeus News*, 17 maggio 2015, http://www.zeusnews.it/n.php?c=19252.

[218] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2012*, cit.

[219] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica*

ISSN 2280-6164

Criminali cibernetici e crimine organizzato

Se si considerano gli obiettivi e le tattiche impiegate dal crimine online, il livello di pericolo proveniente da criminali cibernetici e dal crimine organizzato riguarda soprattutto gli aspetti di sicurezza economica, piuttosto che quelli di sicurezza e difesa nazionali[220]. Il facile accesso a malware, ransomware[221], trojan (ecc.) nel deep web ha permesso il loro utilizzo anche a quelle organizzazioni criminali che prima non vi facevano ricorso[222]. Tra le tecniche di anonimizzazione più utilizzate figurano i Virtual Private Network (Vpn)[223] e la rete Tor[224]. La criminalità organizzata partecipa soprattutto a campagne di spionaggio industriale che non si esclude possano essere ordinate da aziende in lotta per fette di mercato nello stesso settore[225]. In tale contesto sono stati segnalati degli attacchi contro dispositivi mobili come cellulari e servizi di "mobile banking". Anche gli ultimi sviluppi sembrano confermare che il crimine organizzato continui ad essere una minaccia più per gli aspetti economici che per quelli di sicurezza, come dimostra l'arruolamento di hacker competenti da parte di boss mafiosi in attività di clonazione di carte di credito[226].

4.3. Quale pericolo per i sistemi Atm/Atc in Italia?

4.3.1 Valutazione di breve periodo

Il fattore tecnologico

L'elevata componente tecnologica di Enav, considerata anche la molteplicità di sistemi, taluni legacy e altri commercial-off-the-shelf (Cots)[227], può costituire

dell'informazione per la sicurezza 2013, cit.

220 Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit.

221 "Malware che limita l'accesso al sistema informatico infettato e richiede il pagamento di un riscatto per la rimozione del blocco. Alcune forme di questo malware crittografano i file sul disco del sistema mentre altre bloccano il sistema visualizzando messaggi che inducono l'utente a pagare". Si veda la voce "ransomware" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#r.

222 Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit.

223 Ibid.

224 "Consiste in una rete di router, gestiti da volontari, che consentono l'anonimato e la criptazione delle comunicazioni poiché il pacchetto dati inviato, prima di giungere al server di destinazione, passa attraverso dei router intermedi che reindirizzano i dati costituendo un circuito crittografico a strati (da cui il termine onion). Tale strumento consente altresì di erogare 'servizi nascosti', costituenti un vero e proprio mercato nero, ospitati su server che, facendo parte della stessa rete Tor, non sarebbero localizzabili". Ibid, p. 87.

225 Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2013*, cit.

226 Salvo Palazzolo, "I boss reclutano una banda di hacker e clonano migliaia di carte di credito", in *Repubblica.it*, 29 settembre 2015, http://palermo.repubblica.it/cronaca/2015/09/29/news/i_boss_reclutano_una_banda_di_hacker_e_clonano_migliaia_di_carte_di_credito-123895964.

227 Definiamo come prodotto legacy il software scritto da un dato produttore per rispondere ad

ISSN 2280-6164

un fattore di complessità nel quale si possono celare vulnerabilità, che possono incidere sulla disponibilità ed integrità delle informazioni e quindi pregiudicare i servizi della navigazione aerea.

L'analisi tecnologica a campione, svolta sulla parte del network e in particolare sulla rete E-Net e su alcuni applicativi destinati all'esercizio del controllo del traffico aereo, ed i cui dettagli per evidenti esigenze di riservatezza non possono trovare esplicita divulgazione nel presente studio, hanno permesso di definire alcuni aspetti:

- la disponibilità del network fisico della rete E-Net è attualmente assicurata da una primaria società di telecomunicazioni con la quale Enav ha specifici accordi di monitoraggio tecnico per il funzionamento ordinario e la misura delle performance;
- il coordinamento tra i due Soc e processi di "escalation" in caso di in incidente, sin dai primi segnali, nonché consistenti livelli di servizio ("service level agreement" a livello contrattuale);
- le interconnessioni verso l'esterno sono fortemente presidiate a livello di conduzione dei moduli di sicurezza, di implementazione di politiche di traffico particolarmente restrittive, di verifica di parti terze e di regolarità nel traffico, con l'utilizzo delle capacità elaborative e di coordinamento offerte dal software di analisi dati Splunk e da specifiche applicazioni open source che Enav ha scritto per il controllo dinamico dei comportamenti degli utenti e delle applicazioni, nella logica di Security Information and Event Management (Siem) avanzato;
- in particolare, l'utilizzo di Ids layer 7 e Proxy layer 7[228] determina un effettivo consolidamento del perimetro, con una significativa riduzione della superficie di attacco;
- un severo controllo del patching dei sistemi Cots, supportato da un'attività di intelligence per la verifica di emergenti vettori di minaccia, sia attraverso analisi verticali di prodotto e di dominio sia attraverso il flusso informativo proveniente da fonti qualificate nazionali ed estere[229].
- la considerazione dei due PoP Ire di Milano e Roma come elementi di massima attenzione e con gestione delle porte ammissibili fondata su criteri di eccezionalità e sul principio del privilegio minimo[230] ("least privileage") permette di limitare per tipologia, natura e riconoscibilità il traffico ammesso sulle porte dei relativi firewall.

esigenze specifiche e non suscettibile di diffusione di mercato. I Cots sono i prodotti commerciali che non consentono personalizzazioni ma sono venduti in massa dal produttore che ne consente di massima solo le configurazioni.

[228] Qui "layer 7" si riferisce allo strato applicativo del modello Iso/Osi (Open Systems Interconnection) per le architetture di rete (standard Iso 7498).

[229] Con particolare riguardo al supporto preventivo svolto dalle organizzazioni nazionali nel quadro della strategia cibernetica ed in particolare Cnaipic, Dis e Cert nazionale.

[230] Il principio del privilegio minimo è quello di attribuire ad una persona le autorizzazioni necessarie e sufficienti per svolgere il proprio lavoro, consentendogli però l'accesso esclusivamente alle informazioni che ha interesse, titolo e ragione di conoscere. Tale principio ha come corollario la necessità che, a un cambio di ruolo delle autorizzazioni, queste ultime siano immediatamente riviste. In caso di cessazione dal servizio, invece, esse devono essere immediatamente revocate.

© 2015 IAI ISSN 2280-6164 DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

- i test periodici di resilienza, in modalità "black box", permettono di saggiare l'effettivo mantenimento dei livelli di sicurezza attesi.

Si è poi proceduto ad analizzare il portale sperimentale Self Briefing che, sebbene sarà a breve sostituito da diversa applicazione, è utile per descrivere come Enav disponga di propri assetti tecnologici su reti pubbliche. Va premesso che il portale non si trova su rete operativa e non è direttamente interconnesso ad altri sistemi operativi.

Come ogni applicazione web, il portale Self Briefing potrebbe essere attaccato ricorrendo a numerose possibili tecniche, fra le quali è doveroso rammentare (D) DoS, Sql-injection, cross-site scripting, cookie hijacking ed altre forme di command injection.

Nel caso di successo di attacchi (D)DoS, le conseguenze appaiono abbastanza limitate. L'applicazione diviene irraggiungibile per la grande maggioranza degli utenti legittimi, situazione a cui si sopperisce con i metodi in uso in altri Paesi del mondo e sanciti dal piano di contingenza di Enav. Anche l'eventuale completa indisponibilità dell'applicazione non sembra delineare scenari realmente problematici. Ben più grave sarebbe la situazione in cui l'attacco (D)DoS avesse successo sull'intero sistema Fdp, impedendo di fatto l'immissione, l'elaborazione e la visualizzazione dei piani di volo. Questa è la ragione che ha spinto Enav, oltre a rafforzare le difese di perimetro con consistenti "demilitarised zones"[231] e firewall, alla netta separazione della rete E-Net dalle reti non operative, come quella di Self Briefing o quelle utilizzate per i servizi gestionali più tradizionali (una Mpls commerciale). In particolare il Self Briefing non è direttamente collegato al Fdp, in quanto i piani di volo provengono dall'ufficio di accettazione di Eurocontrol Network Manager[232].

Gli attacchi Sql-injection rappresentano, in piena evidenza, una minaccia tra le più temibili, poiché diventano possibili scenari in cui l'attaccante riesce ad autenticarsi e ad accedere alle funzioni dell'applicazione pur non essendo un legittimo utente, essendo perciò abilitato a operare anche con credenziali di amministrazione. Consentendo il sistema l'immissione di piani di volo, l'utente legittimo è abilitato ad accedere al database in scrittura, per cui quello illegittimo (che può apparire legittimo tramite Sql-injection) potrebbe essere in grado di scrivere informazioni accuratamente artefatte, o addirittura di effettuare operazioni di cancellazione/

[231] Quando si tratta di dare accesso dall'esterno ad alcuni server o servizi che si trovano sulla rete interna, è necessario creare uno strato di sicurezza per far sì che le applicazioni che si trovano nelle "demilitarised zone" non permettano poi l'accesso ad un attaccante che penetri verso la rete interna. Tale isolamento permette, perciò, di consentire l'accesso autorizzato esclusivamente ai servizi esposti nella "demilitarised zone", mentre agli altri servizi ogni accesso non "trusted" è precluso. I server esposti, perciò, diventano dei "bastioni",costituendo degli "avamposti" della rete dell'organizzazione che, per necessità, devono essere esposti verso l'esterno e andranno comunque protetti.

[232] Interviste, novembre 2015.

ISSN 2280-6164

modifica su dati di cui non è proprietario. Il sistema Self Briefing è tuttavia monitorato da una sonda Ids abilitata alla rilevazione di tali attacchi e, in aggiunta, il sistema non accetta indistintamente informazioni contenute in un qualsiasi piano di volo, ma ogni piano è soggetto a una validazione operativa a più livelli, in accordo con gli standard internazionali degli annessi tecnici della Convenzione di Chicago[233].

La minaccia del cross-site scripting, in base alle informazioni disponibili, dovrebbe essere limitata alla modalità riflessa che, spesso indotta dal social engineering[234], porta l'attaccato a ricevere sollecitazioni nocive sul proprio browser, verosimilmente lasciando inalterato il sistema di Self Briefing. Le conseguenze possibili per il computer attaccato includono l'installazione di malware, l'esfiltrazione di dati e l'arruolamento in una botnet. Se ciò accadesse, avrebbe però un impatto irrilevante sui servizi Atm/Atc e sarebbe comunque visibile attraverso i sistemi di monitoraggio del traffico e degli schemi comportamentali[235].

Il cross-site scripting diviene più pericoloso se associato ad un'operazione di cookie hijacking. Come è noto, una vota completata l'autenticazione di un utente legittimo, questi potrebbe ricevere sul proprio browser un cookie di sessione, magari contenente un token di autenticazione[236]. L'uso del cross-site scripting, assieme a un completo rispetto della Same Origin Policy (Sop)[237], potrebbe permettere a un'applicazione aperta su altro pannello dello stesso browser di impossessarsi del cookie e mostrarne quindi il contenuto al server per dimostrare di avere già effettuato l'autenticazione. Tale applicazione opererebbe in questo modo un vero e proprio furto di credenziali, consentendo a terzi di sostituirsi all'utente legittimo. Altre forme di command-injection potrebbero consentire all'attaccante di conseguire risultati similari (autenticazione, accesso alla base dati, furto di credenziali). Le attività di penetration test (sia in modalità "black box" che in modalità "white box"[238], in particolare quelle parti effettuate da parti terze esterne) hanno al momento escluso esposizioni al rischio, con il catalogo di vulnerabilità note e strumentazione evoluta – attraverso il tool Metasploit e con la suite completa Burp, dedicata specificamente all'analisi delle applicazioni web.

[233] Interviste, novembre 2015.

[234] "Letteralmente indica lo studio del comportamento di un individuo con l'obiettivo finale di ricavarne informazioni utili per perpetrare un successivo attacco nei suoi confronti. Il termine viene comunemente usato per indicare l'attacco stesso, ovvero le tecniche per ottenere i dati personali della vittima mediante opportuni inganni mirati, tipicamente appartenenti alla categoria del phishing". Si veda la voce "social engineering" nel glossario del Cert nazionale Italia: https://www.certnazionale.it/glossario/#ss.

[235] Interviste, novembre 2015.

[236] Numero casuale generato dal server e consegnato al browser, spesso attraverso un cookie, da esibire successivamente come prova di autenticazione già avvenuta.

[237] Criterio di sicurezza impiegato nelle pagine web, secondo il quale uno script proveniente da una pagina web non può far riferimento ad altri siti web.

[238] Ossia conoscendo esattamente dall'interno architettura, codici di compilazione e strutture del software.

ISSN 2280-6164

Ancora in relazione al fattore tecnologico, va rammentato come le attività Atc dipendano fortemente dalla disponibilità di dati corretti e continuamente aggiornati. A livello del tutto teorico si rileva la possibile eventualità che un ben orchestrato attacco DoS sia in grado di interrompere il flusso di informazioni che alimenta le attività di Atc. Questa situazione è nondimeno prevista nel piano di contingenza e prevede l'immissione dei dati di volo con modalità alternative, con impatti limitati sulle attività Atc.

Non ci si può peraltro esimere dal considerare le problematiche connesse al già menzionato progetto Amhs che, con l'introduzione delle tecnologie digitali nella comunicazione, richiede la messa in opera di misure volte a preservare e garantire la sicurezza delle informazioni, con particolare riguardo all'integrità e all'autenticità dei dati, all'identificazione del partner di comunicazione e alle eventuali necessità di confidenzialità e di controllo degli accessi. A tal proposito si raccomanda l'identificazione e la considerazione dei requisiti di sicurezza sin dalla fase di progettazione.

È pertanto da ritenersi che nel breve periodo – sebbene gli accessi alla rete pubblica debbano comunque considerarsi con grande attenzione come potenziali obiettivi, anche in considerazione dei livelli di capacità delle forze non statuali considerate – la probabilità di attacco debba considerarsi limitata in funzione del consistente dispiegamento delle contromisure presentate.

Il fattore umano

Lo studio ha confermato che il fattore umano è l'elemento critico e la chiave di volta a protezione dei sistemi Enav[239]. Il fattore umano è estremamente delicato proprio nell'approccio ad un ambiente ad elevatissima componente tecnologica, come quella dei servizi della navigazione aerea e che richiede, uno sforzo sempre crescente, non limitato alla dimensione della sola "consapevolezza", ma soprattutto alla piena adesione alle politiche di protezione, che avviene attraverso reiterati costanti processi di promozione della cultura della sicurezza[240]. A questo proposito, sono apparse coerenti le iniziative contenute nel set di procedure e nei processi di Enav, in attuazione dei principi della norma Iso 27001.

La ricerca ha inoltre consentito di rilevare la presenza di procedure di identificazione per i controllori in procinto di entrare nella sala di controllo, ove possono accedere alle varie consolle, ricevere informazioni e assistere gli aeromobili. Il tutto viene svolto nel rispetto delle misure volte a ridondare le risorse che garantiscono il corretto comportamento di un sistema avionico.

[239] Lo evidenzia la targa presente all'interno del Soc di Enav: "non è stato ancora inventato il firewall contro gli stupidi".

[240] A questo proposito, si ipotizza che il malware Stuxnet possa essere stato introdotto non attraverso la rete ma con l'impiego inappropriato di supporti removibili (penne Usb). Farhad Manjoo, "Don't Stick It In. The dangers of USB drives", in *Slate*, 5 October 2010, http://www.slate.com/articles/technology/technology/2010/10/dont_stick_it_in.html.

ISSN 2280-6164

In effetti, un controllore del traffico aereo che decidesse di fornire a un aeromobile informazioni "avvelenate", o comunque contraffatte, avrebbe in pratica difficoltà a celare il proprio operato al controllore a lui abbinato[241]. Inoltre, anche nell'ipotesi che ciò sia fattibile, non si evidenziano possibili risultati potenzialmente pericolosi, in quanto le informazioni contraffatte avrebbero come effetto estremo quello di inviare l'aeromobile su rotte sbagliate, evento che successivamente, al passaggio a un altro Acc, sarebbe risolto da altro controllore del traffico aereo. Non appare altresì convincente l'azione di un ipotetico terrorista che, attraverso opportune pressioni sul controllore, tenti di far schiantare l'aeromobile contro un ostacolo o di farlo viaggiare su rotte improbabili fino all'esaurimento del carburante. Il pilota infatti, che ha la decisione finale sulla sicurezza dell'aeromobile, sarà comunque in grado di reagire appropriatamente, modificando ancora la rotta, magari sulla base di un contatto radio con altro Acc o con una torre di controllo.

Altra ipotesi che si può prendere in considerazione è quella di azioni multiple coordinate che, se opportunamente veicolate dai controllori, potrebbero creare situazioni complesse, come ad esempio situazioni in cui la separazione fra aeromobili è ridotta ai minimi termini e risulta insufficiente lo spazio di manovra. Si tratta chiaramente di un caso limite. Come potrebbero molti controllori essere indotti a fornire informazioni alterate ai piloti? Gli standard operativi impongono ai controllori l'impiego della sola strumentazione preposta all'Atc, escludendo categoricamente l'utilizzo di smartphone o altri dispositivi personali. Diverrebbe dunque problematico per l'attaccante cibernetico impiegare il social engineering per convincere i controllori del verificarsi di situazioni irrealistiche, nelle quali si sentirebbero obbligati a mandare agli aeromobili informazioni differenti da quelle attese. Infatti, le politiche di sicurezza interna all'Enav impediscono la pratica nota come Bring-Your-Own-Device (Byod), che rappresenta oggi un fattore di rischio in molte organizzazioni con elevate esigenze di sicurezza[242]. In generale, il Byod consente di introdurre sul luogo di lavoro dispositivi non messi in sicurezza, sui quali è molto più facile veicolare messaggi con mittente falsificato (spoofed), grazie al gran numero di applicazioni insicure che normalmente girano sugli smartphone più diffusi.

In considerazione del tema del fattore umano, pur tenendo conto delle politiche già in atto da parte di Enav, si raccomanda di tenere alto il livello di tensione sull'aspetto di gestione, promozione e valorizzazione dei processi culturali, in ogni partecipe dell'organizzazione e anche nei soggetti partner, dell'imprescindibile necessità di presidiare la sicurezza come "valore".

[241] I controllori di volo operano sempre in coppia.

[242] Il Byod è oggi argomento piuttosto controverso, poiché i suoi sostenitori si appellano all'incremento di produttività che esso può generare. Nel caso tuttavia di infrastrutture critiche dovrebbe essere solo il processo di analisi del rischio a determinare la decisione di rinunciare al Byod.

DOCUMENTI IAI 15 | 23 - DICEMBRE 2015 ISSN 2280-6164

La necessità di presidiare anche il personale di parte terza e l'auspicabile collaborazione delle forze di polizia e dell'intelligence nella verifica da parte del personale dell'affidabilità dei fornitori e dei manutentori potrebbe rappresentare un oggettivo miglioramento nel quadro delle azioni della strategia cibernetica nazionale.

La minaccia cibernetica

Il caso studio presentato nel capitolo quattro dimostra che l'Italia non è esente dalla minaccia cibernetica proveniente da organizzazioni terroristiche di matrice jihadista. Sebbene il pericolo di Al-Qaeda sembri essersi affievolito, l'attivismo online dell'Isis deve far suonare qualche campanello d'allarme. L'episodio più significativo è quello avvenuto a maggio 2015, quando l'Ishd ha affermato di essere riuscita a penetrare i sistemi informatici della Difesa e a ricavarne indirizzi e foto di militari italiani. Nelle intenzioni questa azione è del tutto simile alla presunta esfiltrazione di dati che avrebbe permesso all'Ishd di pubblicare nomi, indirizzi email e altri dati di personale militare americano, atto poi risultato falso. Anche nel caso italiano si nutrono dei fortissimi dubbi sulla veridicità dell'operazione contro le Forze Armate. Infatti, si può desumere con una ragionevole dose di certezza che l'atto sia stato compiuto da un individuo (o più) che ha condotto un'attività di profilazione del personale militare italiano da fonti aperte e poi abbia consegnato il materiale reperito all'Ishd, emulando l'azione di Ardit Ferizi. L'esfiltrazione di dati da reti protette si ritiene dunque molto improbabile[243]. Tuttavia questo episodio in particolare certifica, se mai ce ne fosse stato il bisogno, che anche l'Italia, proprio come gli altri paesi impegnati nella campagna anti-Isis in Iraq e Siria, è un obiettivo dell'organizzazione terroristica. Questo significa che, proprio come per Stati Uniti, Regno Unito e altri paesi occidentali, l'intenzione, probabilmente più futura che attuale, di colpire le infrastrutture critiche informatizzate italiane sia reale. Come rilevato nel terzo capitolo, però, anche nel caso italiano non vi sono indicazioni che fanno presagire un imminente attacco verso l'aviazione civile e le sue infrastrutture. Escludendo il presunto attacco ai danni della Difesa, anche per l'Italia l'attività cibernetica dell'Isis si è articolata soprattutto in attività di propaganda e reclutamento, e non ha fatto intravedere una sofisticazione tecnica elevata. Per quello che si è potuto osservare finora, organizzazioni terroristiche quali l'Isis e Al-Qaeda non sembra abbiano sviluppato dei malware particolari per colpire obiettivi specifici in Italia, né sembra siano in grado di farlo, tanto da far presumere che si stiano affidando quasi esclusivamente ad hacker esterni per condurre le proprie azioni nello spazio cibernetico.

Infine, e per quanto possa sembrare paradossale, anche la recente "attività di polizia" condotta da Anonymous verso gli affiliati e i sostenitori dell'Isis aggiunge un ulteriore elemento di difficoltà alla pianificazione e all'esecuzione delle operazione cibernetiche di Isis e Al-Qaeda, sebbene taluni osservatori abbiano sottolineato come le azioni del colletivo possano interferire con le azioni delle agenzie di

[243] Interviste, ottobre, 2015.

ISSN 2280-6164

intelligence o di polizia[244].

In linea con quanto espresso nel terzo capitolo, il caso italiano attesta le maggiori capacità tecniche degli hacktivisti rispetto alle organizzazioni terroristiche di matrice islamista, come dimostrano gli attacchi Sql-injection ai danni della Difesa. Maggiori capacità tecniche, nondimeno, non equivalgono alla certezza di poter violare sistemi informatici complessi che richiedono, oltre ad una certa expertise tecnica, una buona capacità di raccolta delle informazioni che, nel caso di strutture legate alla sicurezza nazionale, non sono facili da ottenere. Un ulteriore elemento che non va dimenticato riguarda le motivazioni alla base degli attacchi hacktivisti. In particolare, il movimento di Anonymous nasce da una spinta ideologica verso la libertà di informazione. Sebbene nel caso di Anonymous Italia si sia potuto osservare un allargamento degli obiettivi contro diverse istituzioni governative (in particolare la Difesa) e non (No Tav, Expo ecc.), la possibilità che questi attori rivolgano i propri attacchi verso strutture informatizzate come i sistemi Atm – attacchi suscettibili di mettere a rischio vite umane – appare contraria alla logica d'azione del collettivo di hacker. E anche se il livello di pericolo posto da questi attori può essere valutato come "concreto, attuale e con una proiezione di medio-lungo periodo"[245] per altri tipi di obiettivi, come espresso dall'esperta di hacktivismo Gabriella Coleman, "buttare giù un sito non è terrorismo [...]. Attaccare una rete elettrica sì, ma non è mai successo. Se gli anons (Anonymous) lo facessero, sarebbero spacciati come attivisti politici"[246].

Quanto espresso per gli hacktivisti sembra rilevante anche per criminali cibernetici e crimine organizzato. La necessità di assicurarsi fette del mercato nero digitale ha dato una spinta innovativa importante nella creazione e sviluppo di nuovi malware. Questa dinamica ha elevato il livello tecnico dei criminali cibernetici a tal punto da permettere loro di padroneggiare strumenti che prima erano di utilizzo quasi esclusivo di realtà statuali. Ciononostante, sebbene la minaccia derivante dal crimine cibernetico in associazione al crimine organizzato possa essere giudicata alta per le sue ingenti capacità tecniche dovute all'arruolamento di hacker competenti[247], è improbabile che criminali cibernetici costituiscano un pericolo per il sistema Atm di Enav. L'attacco rischierebbe di compromettere la loro necessità di rimanere nella penombra e di "far saltare la copertura" a operazioni più profittevoli e meno rischiose.

[244] Larry Greenemeier, "Anonymous's Cyber War with ISIS Could Compromise Terrorism Intelligence", in *Scientific American*, 19 November 2015, http://bit.ly/1I1bCql.

[245] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 85.

[246] Carola Frediani, "Vi racconto le mille facce di Anonymous", in *l'Espresso*, 12 novembre 2014, http://espresso.repubblica.it/visioni/tecnologia/2014/11/10/news/vi-spiego-le-mille-facce-di-anonymous-1.187319.

[247] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 86.

ISSN 2280-6164

In un'ottica olistica di valutazione delle vulnerabilità dei sistemi Atm e della minaccia a essi rivolta, non va dimenticato il ruolo di autorità statali, su tutti la Polizia postale e delle Comunicazioni e il Dipartimento delle Informazioni per la sicurezza (Dis), nelle attività di prevenzione e contrasto a potenziali fenomeni di terrorismo cibernetico.

La Polizia postale e delle Comunicazioni – e al suo interno in particolare il Cnaipic – è preposta alla prevenzione e alla lotta alla criminalità informatica ordinaria, organizzata e di matrice terroristica verso le infrastrutture critiche informatizzate nazionali. Per quello che riguarda le aree di intervento della polizia postale vi sono sia il contrasto alle attività di diffusione di messaggi di propaganda e reclutamento, sia ad attività illecite di danneggiamento, compromissione e sfruttamento della rete[248]. L'attività di costante monitoraggio della rete risale al 2007 e continua oggi più che mai con un'apposita task force composta da più di 20 operatori attivi 24 ore al giorno, sette giorni su sette, con l'ulteriore supporto del Dis e della Polizia di Prevenzione[249].

Tabella 1. Attività della polizia postale a contrasto dell'azione cibernetica dell'Isis (gennaio-ottobre 2015)

Spazi web	Numero	Monitorati	Oscurati
Siti	20	19	1
Forum	32	10	22
Blog	6	6	/
Media	18	18	/
Twitter	10.939	350	6.386
Facebook	275	85	/
Segnalati all'A.G	10		
Totale	11.300	488	6.409

Fonte: Ministero dell'Interno.

Queste attività di monitoraggio avvengono in collaborazione con le altre realtà internazionali, su tutte Interpol ed Europol, con le quali è posto in essere uno scambio di informazioni in tempo reale, arricchito ulteriormente dalla presenza di una banca dati gestita da Europol, all'interno della quale i vari paesi aderenti possono inserire i risultati della propria attività[250]. Anche se non è possibile dare un giudizio organico sull'efficacia del Cnaipic, le oltre duecento indagini per attacchi informatici contro enti pubblici e nei confronti di imprese e le 114 persone deferite

[248] Associazione italiana per la sicurezza informatica, *Rapporto Clusit 2015 sulla sicurezza Ict in Italia*, cit.

[249] Roberto Di Legami, "La minaccia corre sul Web", in *Poliziamoderna*, febbraio 2015, p. 12-17, http://www.poliziamoderna.it/articolo.php?cod_art=3757.

[250] Ibid.

ISSN 2280-6164

presso l'autorità giudiziaria segnalano il livello di attività dell'organo di polizia. Nel caso specifico di questa ricerca, l'arresto nel 2015 di un cittadino tunisino e di un cittadino pakistano, entrambi accusati di fare propaganda online a favore dell'Isis, testimonia l'operato della polizia postale, il cui ruolo è stato ulteriormente rafforzato con l'ultimo decreto anti terrorismo[251].

Anche il Dis ha un ruolo fondamentale nella prevenzione e nell'acquisizione di informazioni inerenti alla minaccia cibernetica, sia per il settore pubblico che per le industrie e l'entità di importanza strategica del settore privato. Recentemente è stato redatto un protocollo d'intesa, ancora in fase di finalizzazione, tra il comparto intelligence e il Cnaipic con l'obiettivo di consolidare sia l'attività di contenimento delle possibili minacce, sia l'attività di intelligence. Per di più, il Dis ha costituito un'apposita "Piattaforma di Cyber Collaboration" con i responsabili dei principali servizi pubblici e delle infrastrutture critiche nazionali, tra cui Enav, per permettere una condivisione di informazioni e dati tecnici per il miglioramento della loro sicurezza cibernetica[252].

In questo contesto, le convenzioni che Enav ha in corso sin dal 2008 sulla base del Decreto Pisanu, con il Cnaipic[253] ed analogamente con il Dis, in forza dell'art. 13-bis della Legge 124/2007 sono un ulteriore elemento di protezione ai sistemi in uso dalla società pubblica[254].

Per concludere, le misure messe in campo da Enav, le limitate risorse tecniche a disposizione dell'Isis, i differenti obiettivi di hacktivisti e criminali cibernetici e la funzione di prevenzione delle autorità italiane, ci consentono di affermare che il livello di pericolo al quale i sistemi italiani di Atm/Atc sono sottoposti sia basso, per lo meno nel breve termine.

4.3.2 Valutazione di medio e lungo periodo

I sistemi di gestione del traffico aereo dell'aviazione civile affronteranno un lungo processo di trasformazione che li porrà di fronte, in un futuro non troppo remoto, a problematiche rilevanti per quel che riguarda la propria sicurezza cibernetica.

Il Next Generation Air Transportation System (NextGen) è il nuovo sistema di gestione del traffico aereo che dovrebbe essere implementato negli anni a venire negli Stati Uniti e che prevede il passaggio da un sistema di navigazione basato su radar a terra a un sistema di navigazione satellitare, il passaggio da comunicazioni

[251] Decreto legge n. 7 del 18 febbraio 2015, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2015-02-18;7; Enzo Quarantino, "Polizia Postale, così scoviamo jihadisti su web", in *Ansa Cronaca*, 22 luglio 2015, http://t.co/HkCAiv2tz5.

[252] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 107.

[253] Polizia di Stato, Sicurezza: rinnovato l'accordo tra Polizia di Stato ed Enav, cit.

[254] Stefania Ducci, "Moving Toward an Italian Cyber Defense and Security Strategy", cit.

ISSN 2280-6164

vocali a digitali, e la creazione di un sistema di gestione altamente integrato[255]. L'utilizzo di queste nuove tecnologie, come sostenuto dal Gao in un rapporto pubblicato nell'aprile 2015, rischia però di esporre il sistema Atm a dei pericoli che saranno intrinseci al tipo di tecnologie impiegate. Secondo l'autorità americana, se la Faa non sarà in grado di sviluppare un modello di sicurezza adeguato, ciò comporterà dei seri rischi. Allo stesso modo, la crescente interconnessione degli aeromobili moderni con la rete internet aumenterà le possibilità che vi siano accessi remoti non autorizzati all'avionica di un aeroplano[256].

Similmente, la Commissione europea ha lanciato nel 2004 il programma Single European Sky (Ses), che ha come obiettivo la riforma dell'intera struttura Atm europea[257]. All'interno del Ses si è così sviluppato il Single European Sky Atm Research (Sesar), che dovrebbe portare alla luce un nuovo sistema Atm in grado di gestire un traffico aereo in costante aumento, e a costi minori[258]. Il programma mira a superare la frammentazione nazionale esistente e a convogliare gli sforzi di ricerca e di sviluppo del settore verso sistemi di controllo di traffico aereo omogenei e moderni, in grado di garantire una capacità di traffico tre volte superiore a quella attuale, con costi unitari di rotta dimezzati, coefficienti di sicurezza dieci volte maggiori e ricadute ambientali dieci volte minori[259]. La nuova tecnologia permetterà un maggiore scambio di informazioni non solo tra i controllori di volo e l'aeroplano, ma anche con altre entità e attori[260]. Tuttavia il nuovo sistema, che dovrebbe essere implementato entro il 2020, comporterà dei rischi per una serie di fattori che ne aumenteranno l'efficienza, ma anche le vulnerabilità, proprio come per il NextGen americano[261].

Pertanto, da questa breve disamina si intuisce che il futuro dell'aviazione e dei sistemi Atm in particolare non sarà esente dal rischio. Tanto in America quanto in Europa, attraverso l'adozione di nuovi sistemi Atm si tenterà di diminuire i costi e di migliorare l'efficienza della gestione di un traffico aereo destinato a crescere annualmente del 5 per cento nei prossimi vent'anni[262]. Il passaggio da un tipo di

[255] Faa, *Fact Sheet: NextGen*, 19 August 2015, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=19375.

[256] Gao, *FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*, April 2015, http://www.gao.gov/assets/670/669627.pdf.

[257] Sesar Joint Undertaking, *Background on Single European Sky*, http://www.sesarju.eu/node/37.

[258] Enav è fortemente presente sin dall'origine del programma e partecipa attivamente ad iniziative significative proprio sul versante security, tra le quali merita particolare rilievo la cooperazione tra Eurocontrol e i fornitori dei servizi della navigazione aerea per la creazione di un Cert Atc europeo, strettamente connesso con quelli dei Paesi non europei.

[259] Enav, *Sesar*, http://www.enav.it/portal/page/portal/PortaleENAV/Home/ChiSiamo?CurrentPath=/enav/it/servizi_attivita/AttivitaInternazionali/principali_progeprog/sesar_it.

[260] Sesar, *SESAR: The future of flying*, July 2010, http://ec.europa.eu/transport/modes/air/sesar/doc/2010_the_future_of_flying_en.pdf.

[261] Sesar Joint Undertaking, *Study launched to address cyber-security in SESAR*, 22 May 2015, http://www.sesarju.eu/node/1821.

[262] Airbus, *Global Market Forecast 2015-2034*, http://www.airbus.com/company/market/forecast.

© 2015 IAI ISSN 2280-6164 DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

comunicazioni all'altro, così come le maggiori interconnessioni fra le varie parti del sistema, farà crescere il numero di vulnerabilità sfruttabili da attori con intenzioni criminose. Un'evoluzione di questa natura renderà il rapporto fra aviazione civile e sicurezza cibernetica ancora più stretto, con quest'ultima che giocherà un ruolo sempre più rilevante nell'ambito della protezione dei cittadini e della sicurezza nazionale.

In tema di entità della minaccia, il pericolo per le infrastrutture critiche potrebbe crescere nel medio e lungo periodo. Alcuni degli stati più avanzati stanno investendo massicciamente in sicurezza informatica nel tentativo di rendere più sicuri i propri sistemi, sia nel settore pubblico che nel privato. In occidente basta pensare a paesi come Stati Uniti e Gran Bretagna, i quali stanno allocando importanti risorse nella formazione universitaria per aumentare il livello di expertise onde far fronte ad una domanda in continuo aumento[263]. Altri paesi non necessariamente nell'emisfero occidentale, come ad esempio l'India, contano già su un livello di alfabetizzazione informatica piuttosto elevato. Maggiore sarà l'esigenza di protezione, più elevata sarà probabilmente la presenza di esperti con titoli di studio specialistici con le caratteristiche tecniche in grado di assicurarla. All'incremento della sofisticazione tecnica si associerà un aumento dell'interdipendenza mano a mano che più dispositivi saranno connessi e che la maggior parte dei servizi verranno forniti e gestititi in rete. Se questo è vero, impedire che il crescente numero di attori con elevate competenze tecniche non si associ a gruppi con finalità terroristiche o criminali, sarà una delle priorità fondamentali per le autorità nazionali preposte alla protezione dello spazio cibernetico. Il caso di Junaid Hussain, cittadino britannico di Birmingham esperto di informatica poi arruolatosi nelle file dell'Isis, è in questo senso emblematico.

Benché la minaccia proveniente da attori come Isis o Al-Qaeda non sia in questo momento elevata, il suo livello potrebbe aumentare nel medio e lungo termine. Già nel 2005 uno dei leader di Al-Qaeda, Omar Bakri Muhammad, sosteneva che ci fossero migliaia di simpatizzanti di Al-Qaeda che stavano studiando informatica per dare un contributo alla "guerra santa"[264]. Centri di ricerca specializzati confermano che le attività cibernetiche di Al-Qaeda diventeranno giornaliere[265]. Anche per l'Isis, un incremento del livello di expertise tecnica potrebbe registrarsi abbastanza rapidamente, a maggior ragione se nuove generazioni con un'educazione informatica avanzata decidessero di sposarne la causa e di arruolarsi, come tra l'altro hanno già fatto in migliaia, anche provenienti dall'Occidente[266]. Si ritiene

[263] White House, *The Comprehensive National Cybersecurity Initiative*, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative; Gareth Halfacree, "UK government pledges funds for cyber security education", in *bit-tech*, 23 September 2015, http://www.bit-tech.net/news/bits/2015/09/23/cyber-security-education/1.

[264] Roland Heickerö, "Cyber Terrorism: Electronic Jihad", cit., p. 558.

[265] Steven Stalinsky and R. Sosnow, "From Al-Qaeda to the Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad", cit.

[266] Ics-Cert, *Cyber Threat Source Descriptions*, cit; Aaron Y. Zelin et al., "Up to 11,000 foreign fighters in Syria; steep rise among Western Europeans", in *ICSR Insights*, 17 December 2013, http://

ISSN 2280-6164

molto probabile che l'Isis possa far maturare tattiche e mezzi che hanno portato ad importanti successi nello spazio cibernetico – per ora più che altro mediatici – oppure possa chiedere ai suoi simpatizzanti online di condurre attacchi per suo conto[267]. Secondo il direttore dell'Fbi James Comey, l'Isis si "starebbe svegliando" all'idea di sferrare attacchi a infrastrutture critiche attraverso malware complessi[268]. Nell'ottobre 2015 un esponente di rilievo del Dipartimento della Sicurezza interna statunitense ha rivelato in una conferenza i tentativi dell'Isis di attaccare le industrie del settore elettrico americane, seppur sottolinenando che i tentativi sono risultati poco credibili per le capacità tecniche espresse finora[269]. Un'ulteriore evoluzione potrebbe essere determinata dalla stabilizzazione dell'Isis quale stato vero e proprio. In questo momento l'organizzazione terroristica potrebbe non avere tra le sue priorità quella di estendere le proprie capacità informatiche in maniera significativa, visto il forte coinvolgimento in operazioni militari in Siria e Iraq[270]. Nel caso riuscisse a consolidarsi come entità statuale potrebbe verosimilmente pensare di istituire un commando di guerrieri cibernetici proprio come hanno fatto altri stati. Allo stato attuale una simile evoluzione risulta però difficile da prevedere. Resta infine da valutare l'impatto che l'uccisione nell'agosto 2015 del presunto capo dell'Ishd Junaid Hussain potrà avere nell'evoluzione delle capacità tecniche dell'Isis. Secondo fonti statunitensi, Hussain avrebbe aiutato l'Isis ad alzare le sue protezioni contro la sorveglianza elettronica occidentale e assemblato malware per penetrare sistemi informatici. Egli avrebbe sostenuto l'adozione di tecnologie per la criptazione delle comunicazioni fra i membri dell'Isis, promosso il reclutamento di esperti informatici, tra cui hacker e programmatori, e formato altri membri dell'Isis in questo settore. In un'interazione online avrebbe anche discusso della possibilità di ottenere uno zero-day exploit[271]. In poche parole, Hussain avrebbe consolidato e istituzionalizzato l'interesse dell'Isis per il mondo cibernetico. Queste informazioni nondimeno non ci dicono se sia stato proprio Hussain ad ordinare le presunte operazioni cibernetiche dell'Isis o a condurle in prima persona. Per alcuni il nativo di Birmingham si sarebbe occupato principalmente dell'attività di propaganda e di reclutamento, e avrebbe lasciato ad altre "crew", non sotto il diretto controllo dell'Isis, l'esecuzione di operazioni di hacking[272]. Se Hussain è effettivamente stato il personaggio chiave delle campagne online dell'Isis, è possibile che la sua morte possa rallentare il processo di evoluzione tecnica dell'organizzazione terroristica, anche se per valutare ciò sarà necessario attendere i prossimi mesi; diversamente,

icsr.archivestud.io/2013/12/icsr-insight-11000-foreign-fighters-syria-steep-rise-among-western-europeans.

267 Cory Bennett and Elise Viebeck, "ISIS preps for cyber war", in *The Hill*, 17 May 2015, http://thehill.com/node/242280.

268 Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.

269 "ISIS is attacking the U.S. energy grid (and failing)", in *CNN Money*, 16 October 2015, http://cnnmon.ie/1PjyZmf.

270 Emma Graham-Harrison, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?", cit.

271 Margaret Coker, Danny Yadron, Damian Paletta, "Hacker Killed by Drone Was Islamic State's 'Secret Weapon'", in *The Wall Street Journal*, 27 August 2015, http://on.wsj.com/1WVAfhO.

272 Interviste, ottobre, 2015.

ISSN 2280-6164

se le operazioni targate Isis sono state invece compiute da hacker affiliati è probabile che continuino nei mesi a venire.

Capire le prospettive future dell'hacktivismo italiano in questo particolare momento storico non è compito semplice. Anonymous Italia ha subito due grosse perdite con gli arresti di Fabio Meier e Valerio Camici, che secondo gli inquirenti rappresentavano figure di una certa rilevanza del mondo hacktivista nazionale ed internazionale. I due sarebbero stati i responsabili delle recenti operazioni contro i siti web dell'Expo e della Difesa[273]. Se sono vere le supposizioni secondo cui il movimento di Anonymous Italia è composto da una nicchia di hacker esperti e una base meno dotata tecnicamente è possibile che il colpo inferto dalle autorità italiane abbia dei contraccolpi importanti. Anonymous ha già dichiarato guerra al governo italiano per la detenzione dei due hacker e chiesto supporto al resto del collettivo. Se il movimento globale reagirà alla detenzione dei due membri del collettivo è probabile che si registreranno delle campagne di una certa rilevanza contro i siti istituzionali italiani, anche se per ora non sembra vi sia stata una particolare risposta dalla componente internazionale[274]. Per quel che riguarda il giudizio, in ottica previsionale, che le elevate capacità acquisite dagli attivisti digitali siano "idonee a rendere gli stessi oggetto di potenziale manipolazione ed etero-direzione da parte di entità strutturate, per il conseguimento di obiettivi diversi dalla protesta on-line"[275] è difficile prevedere se questo si possa concretizzare in un attacco verso le infrastrutture critiche come i sistemi Atm.

È probabile che criminali cibernetici continuino la loro evoluzione tecnica mentre il crimine organizzato continuerà ad affidarsi sempre di più ad hacker per le sue operazioni illecite nella realtà virtuale. Se il trend di questi ultimi anni si confermerà, la minaccia proveniente da questo tipo di attori continuerà ad aumentare sia per la quantità di dispositivi connessi in futuro, sia perché il mercato dei malware diventerà sempre più competitivo. Da tenere in considerazione anche la possibilità che criminali cibernetici entrino in possesso di strumenti particolarmente sofisticati come quelli diffusi online dopo che la società milanese Hacking Team, specializzata in software per la sorveglianza, ha subito un attacco informatico cui è seguita la diffusione in rete di prodotti venduti solitamente alle agenzie di polizia e intelligence[276]. Detto questo, il pericolo proveniente da questi attori verso i sistemi del traffico aereo resterà probabilmente non troppo elevato anche in futuro.

[273] Polizia di Stato, Polizia delle Telecomunicazioni, "Comunicato Stampa: Operazione Unmask", in *Valtellina News*, 19 maggio 2015, http://www.valtellinanews.it/assets/Uploads/Comunicato-stampa-UNMASK-Finale-20-maggio-2015-1.pdf.

[274] Interviste, ottobre 2015.

[275] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 85.

[276] A questo proposito sembra che gruppi cinesi di hacker abbiano già cominciato ad adottare alcuni strumenti della società per la raccolta di informazioni. Si veda: James Griffiths, "Chinese hackers used tools leaked after attack on Italian cybersecurity firm Hacking Team", in *South China Morning Post*, 20 July 2015, http://www.scmp.com/node/1838426.

ISSN 2280-6164

Infine, una prospettiva che si dovrà cercare di evitare a tutti i costi sarà la combinazione delle opzioni possibili, finora comunque mai verificatesi. In sostanza le agenzie di polizia e di intelligence dovranno assicurarsi che chi ha intenzione di colpire infrastrutture critiche non si doti delle capacità di farlo, e che chi ne ha le capacità non maturi le ragioni per farlo. Ad oggi non sembra si sia stretto nessun sodalizio fra hacker dotati di una certa expertise e organizzazioni terroristiche o potenti bande di criminali che hanno come obiettivo le infrastrutture critiche di un paese. Se ciò avvenisse, si realizzerebbe un connubio pericoloso di capacità e risorse che metterebbe in serio pericolo le infrastrutture informatizzate nazionali ed internazionali.

Conclusioni

Questa ricerca si è posta l'obiettivo di rispondere a una domanda tanto semplice nella sua formulazione quanto complessa nella sua verifica: i sistemi Atm/Atc di Enav sono sicuri dalla minaccia cibernetica? Una risposta ovvia a un simile quesito sarebbe che un sistema non è a rischio solamente quando è spento, se un hacker non è riuscito a penetrarlo in precedenza. Anche un sistema che si ritiene sicuro e protetto può essere violato attraverso un attacco basato su uno zero-day. L'idea che non si potrà mai essere protetti completamente, però, non significa che non ci siano – o non si possano costruire – diversi livelli di protezione che rendano tale minaccia meno incombente.

In una scala di valori che comprenda un livello basso, medio e alto, questa ricerca sostiene che, nel breve periodo, la possibilità che i sistemi Atm/Atc di Enav siano attaccati con successo da parte di attori non statuali risulta bassa. Lo si può sostenere per una serie di fattori.

Innanzitutto, da un punto di vista tecnologico, Enav si è dotata delle metodologie e degli strumenti necessari per far fronte a questo tipo di minacce. E anche se il sistema rimane "in pericolo", a causa dell'impossibilità di ottenere la sicurezza totale, la ricerca non ha riscontrato delle particolari vulnerabilità in grado di far suonare significativi campanelli d'allarme. Per converso tale esito deve tenere in conto la necessità di presidiare con costante e anzi crescente attenzione gli aspetti tecnologici, di processo e di sistema degli interessi nazionali. Questo dovrebbe realizzarsi in una logica di continua verifica dei livelli di rischio e delle mutevoli vulnerabilità, soprattutto data la sempre maggiore apertura e interoperabilità con altri sistemi.

Il sistema di difesa, dunque, non deve essere l'unica variabile presa in considerazione, in quanto un'analisi completa deve passare anche per la valutazione delle capacità tecniche dei possibili attaccanti. Le autorità dell'aviazione civile hanno individuato nelle organizzazioni terroristiche, negli hacktivisti e nei criminali cibernetici le maggiori minacce rivolte al settore dell'aviazione civile. Attualmente, tuttavia, nessuno di questi attori costituisce una seria minaccia ai sistemi Atm/Atc di

ISSN 2280-6164

nessun paese, compresa l'Italia. Organizzazioni terroristiche come Isis e Al-Qaeda hanno mostrato per ora capacità di hacking limitate, anche se le loro azioni hanno riscosso un particolare successo mediatico. L'expertise tecnica di Anonymous è decisamente più elevata, e potrebbe costituire una minaccia per l'aviazione. Tuttavia è improbabile che il collettivo di hacker sia interessato a compromettere sistemi informatici il cui danneggiamento potrebbe comportare dei seri rischi alla vita delle persone. Criminali cibernetici e crimine organizzato potrebbero essere interessati a colpire il settore dell'aviazione civile, ma soprattutto la sua parte commerciale e finanziaria. Infine, va ricordato il ruolo preventivo e di contrasto svolto da istituzioni quali il Cnaipic e il Dis, la cui funzione costituisce un ulteriore ostacolo a possibili attacchi contro le infrastrutture critiche informatizzate.

Se queste valutazioni hanno una valenza per il breve periodo, questo non significa che rimarranno immutabili in futuro. Per questo la ricerca tenta di offrire alcuni spunti di riflessione e di guardare anche al medio-lungo termine.

In un futuro non troppo lontano i sistemi Atm/Atc sia europei che americani affronteranno una profonda trasformazione tecnologica che li renderà più efficienti, ma anche più interconnessi e potenzialmente più vulnerabili. Questo innalzerà inevitabilmente il pericolo, richiedendo un necessario rafforzamento delle difese a protezione di questi sistemi.

Nel medio-lungo periodo è plausibile pensare che il sistema educativo reagirà alla domanda del mercato Ict sfornando un crescente numero di specialisti di sicurezza informatica. In un'ottica di sicurezza nazionale, sarà fondamentale assicurarsi che questi futuri specialisti non abbiano motivo di radicalizzarsi e non manifestino intenzioni di supportare ideologie estremiste o radicali. Il caso di Junaid Hussain, che abbiamo trattato in questa ricerca, è emblematico. Altri possibili casi di radicalizzazione interna dovranno essere evitati in futuro, tenendo conto di tutte le difficoltà che si incontrano nell'individuare e arginare fenomeni che avvengono spesso a livello individuale, e sono perciò difficilmente controllabili.

Non si può escludere a priori che nel medio periodo l'Isis non sviluppi la sua expertise tecnica e diventi un pericolo serio alle infrastrutture critiche di un paese. Questo dipenderà da molte variabili, tra cui la sua capacità di stabilizzarsi come "stato", di attrarre individui con un'educazione elevata o di farsi sostenere da un numero crescente di hacker localizzati nelle regioni più disparate del mondo. Ovviamente tutti questi fattori non sono scontanti, ed anche se qualcuno può ritenere che queste condizioni non si verificheranno facilmente, le autorità preposte alla prevenzione e al contrasto di attività online illecite dovranno comunque monitorare quegli spazi virtuali dove si potrebbero manifestare i primi segnali allarmanti.

Il futuro di Anonymous Italia è incerto dopo l'arresto di due fra gli esponenti di spicco del panorama hacktivista italiano. È difficile prevedere come, pur non avendo gerarchie, il collettivo si potrà riassestare dopo che sono stati messi fuori gioco due individui che assicuravano una certa leadership, quantomeno tecnica. Benché il livello di hacking potrà variare, e forse diminuire, quello che molto probabilmente

ISSN 2280-6164

non cambierà sono le intenzioni degli hacktivisti nei confronti di infrastrutture critiche come i sistemi Atm/Atc, che si ritiene (e si spera) continueranno a non costituire un loro obiettivo operativo.

Il livello tecnico dei criminali cibernetici continuerà ad aumentare negli anni a venire, se non altro perché la competizione fra venditori di malware e un mercato nero online in continua espansione li spingerà a sviluppare strumenti sempre più sofisticati. Sebbene il livello di expertise tecnica imponga di tenere sotto attento scrutinio questi attori, anche in futuro è improbabile che criminali cibernetici possano concentrarsi su obiettivi sensibili come i sistemi di gestione e controllo del traffico aereo, e si distolgano da obiettivi molto più remunerativi e meno rischiosi come i settori commerciali e finanziari dell'aviazione civile.

Questa ricerca non esaurisce certamente tutti i possibili argomenti che varrebbe la pena approfondire nell'ambito del rapporto fra sicurezza cibernetica e aviazione civile. Il presente rapporto è partito da una prospettiva ampia ed ha evidenziato come vi siano più elementi del settore che sono vulnerabili, come ad esempio i sistemi informatici interni degli aeroporti e i sistemi a bordo degli aeromobili. Future ricerche nel settore dovranno presumibilmente investigare anche questi aspetti per avere un quadro più ampio dei rischi informatici dell'aviazione civile.

Sforzi di analisi futuri dovranno anche tenere in considerazione l'evenienza che non solo attori non-statuali, ma anche attori statuali o para-statuali costituiscano una possibile minaccia alle infrastrutture critiche di un paese. Quantunque questa possibilità possa apparire attualmente remota, i recenti conflitti in Georgia e Ucraina e le schermaglie diplomatiche nel Mar Cinese Meridionale hanno permesso di ravvisare quale uso potrebbe essere fatto dello spazio e delle armi cibernetiche in situazioni di conflitto[277]. Dal momento che sono gli attori statuali quelli che, per risorse e obiettivi di sicurezza nazionale, spingeranno l'innovazione in campo cibernetico negli anni a venire, gli esperti informatici a protezione di infrastrutture critiche dovranno inevitabilmente tenere conto del grado di sofisticazione di questi attori per cercare di rendere più sicuri possibili i loro sistemi. Questo dovrà avvenire cercando di mantenere sempre elevato il livello qualitativo dei processi di sicurezza, abbinando sicurezza logica, fisica e di processo, e allineandosi ai migliori standard di settore.

Aggiornato 4 dicembre 2015

[277] CrowdStrike, "Rhetoric Foreshadows Cyber Activity in the South China Sea", in *CrowdStrike Blog*, 1 June 2015, http://t.co/Ifl4L5xDr7; Kenneth Geers, "Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises", in *FireEye Threat Research Blog*, 28 May 2014, http://ow.ly/xlq1T; David Hollis, "Cyberwar Case Study: Georgia 2008", in *Small Wars Journal*, 6 January 2011, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

DOCUMENTI IAI 15 | 23 - DICEMBRE 2015
ISSN 2280-6164

Ringraziamenti

Gli autori intendono ringraziare quanti hanno permesso di portare a compimento questo studio, e in particolare:

Aeronautica Militare
Ente nazionale per l'assistenza al volo (Enav)
Ente nazionale per l'aviazione civile (Enac)
Ministero dell'Interno
Ministero dei Trasporti
Presidenza del Consiglio dei Ministri

Un ringraziamento speciale va a:
Francesca Bosco, Project Officer, United Nations Interregional Crime and Justice Research Institute (Unicri)
Jean Pierre Darnis, Vicedirettore Programma Sicurezza e Difesa dell'Istituto Affari Internazionali (IAI)
Pierluigi Paganini, Chief Information Security Officer presso Bit4Id e membro del Treat Landscape Stakeholder Group dell'Enisa (European Union Agency for Network and Information Security)
Stefano Silvestri, Direttore di AffariInternazionali e Consigliere scientifico dello IAI

A questa ricerca hanno contribuito anche Daniele Fattibene, Francesca Monaco, Nicolò Sartori e Alessandra Scalia del Programma Sicurezza e Difesa dello IAI.

Questa ricerca è stata realizzata con il sostegno di Vitrociset.

ISSN 2280-6164

ISSN 2280-6164

DOCUMENTI IAI 15 | 23 - DICEMBRE 2015

Istituto Affari Internazionali (IAI)

L'Istituto Affari Internazionali (IAI), fondato nel 1965 su iniziativa di Altiero Spinelli, svolge studi nel campo della politica estera, dell'economia e della sicurezza internazionali. Ente senza scopo di lucro, lo IAI mira a promuovere la conoscenza dei problemi attraverso ricerche, conferenze e pubblicazioni. A questo scopo collabora con istituti, università, fondazioni di altri paesi, partecipando a diverse reti internazionali. I principali settori di ricerca sono le istituzioni e le politiche dell'Unione europea, la politica estera taliana, le tendenze dell'economia globale e i processi di internazionalizzazione dell'Italia, il Mediterraneo e il Medio Oriente, l'economia e la politica della difesa, i rapporti transatlantici. Lo IAI pubblica una rivista trimestrale in lingua inglese (The International Spectator), una online in italiano (AffarInternazionali), due collane monografiche (Quaderni IAI e IAI Research Papers) e altre collane di paper legati alla ricerca dell'istituto.

Via Angelo Brunetti, 9 - I-00186 Roma
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Ultimi DOCUMENTI IAI

15 | 23 Tommaso De Zan, Fabrizio d'Amore e Federica Di Camillo, *Protezione del traffico aereo civile dalla minaccia cibernetica*

15 | 22 Eleonora Poli and Maria Elena Sandalli, *Financing SMEs in Asia and Europe*

15 | 21 Anna Gervasoni, *Alternative Funding Sources for Growth: The Role of Private Equity, Venture Capital and Private Debt*

15 | 20 Umberto Marengo, *Italian Exports and the Transatlantic Trade and Investment Partnership*

15 | 19 Irene Fellin, *The Role of Women and Gender Policies in Addressing the Military Conflict in Ukraine*

15 | 18 Nicoletta Pirozzi e Lorenzo Vai, *Proposte di riforma della Politica europea di vicinato*

15 | 17 Pier Domenico Tortola and Lorenzo Vai, *What Government for the European Union? Five Themes for Reflection and Action*

15 | 16 Silvia Colombo, *La crisi libica e il ruolo dell'Europa*

15 | 15 Serena Giusti, *La Politica europea di vicinato e la crisi in Ucraina*

15 | 14 Fabrizio Saccomanni, *The Report of the Five Presidents: A Missed Opportunity*