4.2 Regno Unito

Dopo aver creato la National Cyber Force (Ncf) nel 2020 per condurre anche operazioni cibernetiche offensive mirate, il Regno Unito ha deciso di assumere una posizione ancora più chiara sul ruolo che intende giocare in ambito cibernetico sulla scena internazionale[95].

La *Integrated Review of Security, Defence, Development and Foreign Policy* del marzo 2021 anticipa l'adozione di una nuova strategia cibernetica per dotare il Regno Unito dello spettro completo delle capacità necessarie a rilevare, dissuadere e fermare gli avversari anche in questo dominio[96]. Sebbene l'aggiornamento della strategia cibernetica non sia ancora stato pubblicato, la *Integrated Review* offre degli spunti di riflessione rilevanti. Ad esempio, fa esplicito riferimento alla possibilità di impiegare armi cibernetiche e qualsiasi altro tipo di sistema d'arma[97] in risposta a un attacco che rientri nell'ambito di applicazione dell'art. 5 della Nato, così come alla possibilità di utilizzo dell'Active Cyber Defence (Acd) in caso di necessità[98]. In questo contesto, la "difesa attiva" britannica coincide in buona parte con la difesa avanzata statunitense.

Le operazioni cibernetiche offensive saranno portate a termine dalla Ncf, che vede confluire in un unico organo personale appartenente al Ministero della Difesa, al Government Communication Headquarters (Gchq) e ai servizi di intelligence, dato l'elevato numero di attacchi che vengono condotti nel dominio cibernetico e considerata la necessità di attuare una risposta coordinata[99]. A causa dell'accresciuta minaccia, a partire dal 2016 il Paese ha incrementato l'allocazione di fondi disponibili per il dominio cibernetico e ha creato un fondo per l'innovazione di difesa e cyber di 165 milioni di sterline per il quinquennio 2016-2021[100]. Sempre per sostenere

[95] Londra ha avviato una serie di iniziative per incrementare la resilienza cibernetica delle proprie Forze Armate. Un esempio è fornito dal programma Land Cyber che mira a fornire protezione cibernetica al personale dispiegato e agli equipaggiamenti impiegati in zone con campi elettromagnetici ostili. Maggiori informazioni sul programma possono essere consultate qui: Governo britannico, *Land Cyber Programme Guidance*, aggiornato al 23 febbraio 2021, https://www.gov.uk/guidance/land-cyber-programme.

[96] Governo britannico, *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, 16 marzo 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

[97] Il riferimento alle altre tipologie di armi è stato fatto ai sottomarini nucleari Trident. Si veda ad esempio: Dan Sabbagh, Jessica Elgot e Patrick Wintour, "Defence Review: UK Could Use Trident to Counter Cyber-Attack", in *The Guardian*, 16 marzo 2021, https://www.theguardian.com/p/gmkz7.

[98] Per maggiori informazioni si veda: Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit.

[99] Governo britannico, *National Cyber Force Transforms Country's Cyber Capabilities to Protect UK*, 19 novembre 2020, https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk.

[100] Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit.

DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021
ISSN 2280-6164

una difesa cibernetica all'avanguardia, è stato recentemente inaugurato un *cyber corridor* nel nord del Paese, ovvero un distretto che vedrà la partecipazione degli attori pubblici e privati coinvolti nel settore, anche al fine di creare professionisti altamente specializzati[101]. In tal modo Londra cerca di attuare l'approccio *whole-of-society* indicato nella *Integrated Review*, per rafforzare la resilienza nazionale e creare sinergie pubblico-private, anche attraverso l'impiego dei cosiddetti hacker etici che aiutano nell'individuazione delle falle di sistema[102].

4.3 Francia

La difesa cibernetica in Francia viene assicurata dal Segretariato generale della Difesa e della Sicurezza Nazionale, il quale si avvale dell'Agenzia Nazionale per la Sicurezza dei sistemi informatici (*Agence nationale de la sécurité des systèmes d'information* - Anssi)[103]. Attraverso l'Anssi, la protezione e la difesa dagli attacchi cibernetici sono assegnate a strutture separate, il cui coordinamento è assicurato dalla presenza del *Centre de coordination des crises cyber*. Ad assicurare missioni e capacità offensive sono le Forze Armate e il servizio d'informazione, mentre le missioni e capacità difensive sono prerogative dell'Agenzia[104]. L'azione dell'Anssi è supportata dal *Commandement de la cyber défense*, che non solo è l'organismo responsabile della sicurezza e difesa cyber di sistemi, infrastrutture e operazioni del Ministero della Difesa, ma è anche chiamato a intervenire in caso di attacchi cibernetici di portata nazionale[105].

A seguito degli attacchi cibernetici ai danni di due ospedali francesi[106], nel febbraio 2021 il Presidente francese, Emmanuel Macron, ha stanziato 1 miliardo di euro per la realizzazione di un piano di messa in sicurezza delle infrastrutture critiche del Paese[107]. L'investimento si aggiunge al 1,6 miliardi di euro previsti dalla Legge di programmazione militare 2019-2025 insieme all'incremento di personale di 1.000 combattenti cyber, con l'obiettivo di arrivare ad avere 4.500 unità nel 2025[108]. La

[101] Governo britannico, *International Policy Review Puts Cyber at the Centre of the UK's Security*, 14 marzo 2021, https://www.gov.uk/government/news/international-policy-review-puts-cyber-at-the-centre-of-the-uks-security.

[102] Ministero della Difesa britannico, *Ethical Hackers Collaborate with Defence to Strengthen Cyber Security*, 3 agosto 2021, https://www.gov.uk/government/news/ethical-hackers-collaborate-with-defence-to-strengthen-cyber-security.

[103] Governo francese, *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »*, 8 luglio 2009, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212.

[104] Amaelle Guiton, "Cyber à la française : l'attaque et la défense, de la 'séparation' à l' 'interaction'", in *Libération*, 30 gennaio 2020, https://www.liberation.fr/france/2020/01/30/cyber-a-la-francaise-l-attaque-et-la-defense-de-la-separation-a-l-interaction_1776147.

[105] Senato della Repubblica francese, *Délégation parlementaire au renseignement - Rapport d'activité 2019-2020 n. 506*, 11 giugno 2020, http://www.senat.fr/notice-rapport/2019/r19-506-notice.html.

[106] "Cyber Attacks Hit Two French Hospitals in One Week", in France 24, 16 febbraio 2021, https://f24.my/7NQx.

[107] Presidenza francese, *Accélération de la stratégie nationale en matière de cybersécurité*, 18 febbraio 2021, https://www.elysee.fr/emmanuel-macron/2021/02/18/strategie-nationale-cybersecurite.

[108] Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit.

ISSN 2280-6164

nuova allocazione di fondi è ricompresa nel piano di rilancio e di programmazione degli investimenti e dovrà assicurare un approccio a tutto tondo verso la difesa cibernetica. Il nuovo stanziamento permetterà maggiori investimenti in ricerca e sviluppo di tecnologie *secure by design* per una loro applicazione sia nel settore pubblico che privato e prevede un investimento nella formazione e impiego di un maggior numero di personale specializzato. A tal fine, in autunno 2021, verrà inaugurato un campus dedicato alla sicurezza cibernetica, che costituirà la sede dei principali attori del settore con l'obiettivo di creare sinergie tra le varie competenze e accrescere le capacità di reazione agli attacchi cibernetici[109]. A riprova dell'importanza data al settore, il Campus Cyber francese è partecipato al 44 per cento dallo stato francese[110].

Lo sforzo proattivo di creazione di regole condivise a livello internazionale ha portato la Francia a dare vita al cosiddetto Appello di Parigi nel 2018. Nel novembre 2021, in occasione del Paris Peace Forum 2021, la Francia presenterà i risultati raggiunti finora all'interno dei vari gruppi di lavoro che compongono l'iniziativa[111].

4.4 Germania

Il 2021 dovrebbe essere un anno di rilievo nell'ambito della difesa cibernetica in Germania. Durante quest'anno, infatti, il Comando per lo spazio informatico e cibernetico (*Kommando Cyber- und Informationsraum* - Cir) creato nel 2017, dovrebbe raggiungere la piena capacità operativa di 14.500 unità di personale[112]. Il Cir è considerato al pari degli altri comandi delle Forze Armate, ed è l'organo responsabile per la sicurezza e integrità delle infrastrutture informatiche e dei sistemi d'arma del Ministero della Difesa tedesco. In caso di attacco all'apparato di sicurezza cibernetica nazionale, il Comando fornisce il proprio supporto al *Bundesamt für Sicherheit in der Informationstechnik* (Bsi), che è l'autorità nazionale per la cybersecurity nazionale[113]. A causa di vincoli costituzionali, il supporto che il Comando può fornire è di "assistenza amministrativa" nello svolgimento quotidiano di attività di supporto. In caso di attacco cibernetico di portata nazionale che richiede il dispiegamento di personale militare, al pari delle altre Forze Armate anche il personale del dominio cibernetico necessita della

[109] Sito del Campus Cyber: https://campuscyber.fr.

[110] Campus Cyber, *Le Campus Cyber clôture sa 2ème augmentation de capital*, 28 luglio 2021, https://campuscyber.fr/?p=944.

[111] Ministero degli Esteri francese, *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, febbraio 2021, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[112] Sito del Ministero della Difesa tedesco: *FAQ: Cyber-Abwehr*, https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr.

[113] Per maggiori informazioni sulle modalità di azione del Cir nella struttura di sicurezza cibernetica nazionale si rimanda a: Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit., sezione 5.

ISSN 2280-6164

preventiva autorizzazione parlamentare[114].

Nel 2021 ci sarà anche l'aggiornamento della *Cyber-Sicherheitsstrategie*, la Strategia di sicurezza cibernetica del 2016[115]. Stanti le proposte di modifica finora avanzate[116], la struttura di difesa attuale non dovrebbe subire modifiche sostanziali, ma viene evidenziato come sia necessario aumentare la condivisione di informazioni rilevanti, sia a livello nazionale che internazionale – Ue e Nato – per accrescere le capacità di resilienza cibernetica. Inoltre, si ravvisa l'urgenza di definire la tipologia di operazioni da poter portare a compimento in risposta a un attacco cyber.

La mancanza di un quadro regolamentare a livello internazionale che determini le regole del gioco e indichi le procedure da seguire in caso di attacchi rappresenta per la Germania una grave mancanza, non solo da un punto di vista meramente normativo, ma principalmente in relazione alla possibilità e modalità di reazione a un attacco cibernetico. Con l'obiettivo di colmare questa lacuna, il governo federale ha pubblicato a marzo 2021 un *position paper* sull'applicazione del diritto internazionale dello spazio cibernetico, nel quale si riconosce il carattere di violazione della sovranità territoriale di uno stato nel caso di un'operazione cibernetica attribuibile a uno stato terzo e che causi effetti fisici e danni sul territorio dello stato attaccato[117]. Tuttavia, la stessa presa di posizione chiarisce che un singolo attacco a una parte di un'infrastruttura critica o volto a generare menomazioni funzionali non può essere considerato una violazione della sovranità territoriale, dato che non esiste al momento una definizione univoca e condivisa di quale sia la soglia necessaria a valutare un attacco cyber un attacco allo stato. Nel delineare le tipologie di contromisure applicabili, la Germania sottolinea la necessità di cautela nell'attuazione delle stesse, date le possibili ripercussioni che possono avere sugli altri settori dello stato e sulla società. In linea con il diritto internazionale, si ribadisce come l'autodifesa possa essere messa in atto con qualsiasi tipologia di risposta, purché proporzionata all'attacco. Tuttavia, si apre la strada alle "misure prese per stato di necessità", ossia a quelle risposte attive attuate in virtù della limitatezza della contromisura e in risposta ad attacchi effettuati ai danni di, o aventi come obiettivo, un interesse essenziale dello stato. In tali casi, la

[114] Ibid.

[115] Ministero degli Interni tedesco, *Cyber Security Strategy for Germany 2016*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en.

[116] Il Ministero dell'Interno ha presentato dei punti chiave che rappresentano degli spunti da cui elaborare eventuali ulteriori modifiche: Ministero dell'Interno tedesco, *Eckpunkte für die Cyber-Sicherheitsstrategie 2021*, marzo 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/03/eckpunkte-cyber-sicherheitsstrategie-2021.pdf. Ai punti chiave ha fatto seguito la posizione della Lega federale dell'industria tedesca (Bundesverband der Deutschen Industrie, Bdi), *Cyber-Sicherheitsstrategie 2021*, 14 aprile 2021, https://bdi.eu/publikation/news/cyber-sicherheitsstrategie-2021.

[117] Governo tedesco, *On the Application of International Law in Cyberspace. Position Paper*, marzo 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

ISSN 2280-6164

risposta può essere effettuata senza riguardo alla tipologia di danni che l'attacco può causare, siano essi nel mondo fisico o nello spazio cibernetico.

4.5 Spagna

La difesa dello spazio cibernetico è messa in atto in Spagna dal *Mando Conjunto del Ciber Espacio* (Mcce), creato nel 2020 e sotto la dipendenza dello Stato Maggiore della Difesa. La missione del Comando interforze è quella della direzione, controllo, coordinamento ed esecuzione delle azioni necessarie a mantenere la libertà d'azione delle Forze Armate nello spazio cibernetico e a mantenere in stato di sicurezza le infrastrutture critiche per la sicurezza nazionale e di difesa[118].

Il Comando si basa sul precedente Comando Interforze di Difesa Cibernetica (*Mando Conjunto de Ciberdefensa* - Mccd) e sul Comando dei sistemi di informazione e telecomunicazione (*Jefatura de Sistemas de Información y Telecomunicaciones* - Jcisfas), non più presenti nell'attuale struttura dello Stato Maggiore della Difesa[119]. Esso include nella sua struttura anche il team di risposta alle emergenze informatiche che avvengono nel settore militare (*Centro de Respuesta ante Incidentes del Ministerio de Defensa* - Esp-Cert-Def) e che coopera con gli altri Cert nazionali di natura civile[120].

Da un punto di vista operativo, qualora necessario è la *Fuerza de Operaciones en el Ciber Espacio* (Foce) a intervenire[121], unica forza all'interno del Mcce che opera in modo continuativo e permanente per fornire una consapevolezza situazionale quanto più completa possibile[122]. In caso di attacco, la strategia nazionale di sicurezza cibernetica del 2019, oltre alle operazioni di difesa, prevede operazioni di risposta difensiva per la neutralizzazione dell'attacco con azioni offensive proporzionate all'evento ostile subito. Ma, a differenza di altri Paesi alleati, la Spagna non contempera la possibilità di effettuare operazioni offensive in mancanza di uno scontro armato dichiarato.

La costituzione del Comando può essere ricompresa tra le azioni attuate dal governo spagnolo in risposta all'attacco cyber subito nel 2019 ai danni del Ministero della Difesa[123]. All'attacco è seguito anche un aggiornamento della strategia nazionale, con focus sulla formazione del personale dell'Amministrazione dello stato, ma che

[118] Ministero della Difesa spagnolo, *Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa*, Articolo 9, https://www.boe.es/eli/es/o/2020/07/27/def710.

[119] Sito del Ministero della Difesa spagnolo: *Mando Conjunto del Ciberespacio*, https://emad.defensa.gob.es/unidades/mcce.

[120] Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit., p. 28.

[121] Ministero della Difesa spagnolo, *Orden DEF/710/2020, de 27 de julio*, cit., comma 7.

[122] DefensaCom, *Nuestra Ciberseguridad, un bien estratégico* (video), 28 aprile 2021, https://youtu.be/o-GfMHdUrqI.

[123] Miguel González, "Una 'potencia extranjera' atacó los ordenadores de Defensa", in *El País*, 27 marzo 2019, https://elpais.com/politica/2019/03/25/actualidad/1553543912_758690.html.

© 2021 IAI
ISSN 2280-6164
DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021

dovrà essere ancora aggiornata nel corso del 2021[124].

La politica di sicurezza cibernetica spagnola conferisce un ruolo importante alla collaborazione pubblico-privata e, al fine di un migliore dialogo tra le parti, nel luglio 2020 è stato creato il Forum nazionale della sicurezza cibernetica[125]. Il forum mira ad analizzare le capacità tecnologiche nazionali che possono essere potenziate e sfruttate per soddisfare le esigenze delle Forze Armate.

ISSN 2280-6164

[124] Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit., p. 27.
[125] Sito del Foro nacional de Ciberseguridad: https://foronacionalciberseguridad.es.

5. Cyber defence: difendere l'indifendibile

di Alessandro Marrone[126]

Lo spazio cibernetico rappresenta un dominio operativo *sui generis*, al quale sono applicabili solo alcuni elementi degli approcci sviluppati negli altri domini che hanno tutti una dimensione fisica. Esso presenta perciò sfide nuove che richiedono uno sforzo creativo e adattivo da parte delle Forze Armate chiamate a operarvi, specie nelle condizioni di una "media potenza" come l'Italia, che sconta la non padronanza di un ambiente operativo strutturalmente poco difendibile.

5.1 Guerra in tempo di pace e crisi cibernetica

Nello spazio cibernetico è in corso da anni quella che può definirsi una "guerra in tempo di pace"[127], per cui il conflitto generalizzato tra diversi stati non è ufficialmente dichiarato, e non vi sono escalation tali da portare a una guerra convenzionale. Tuttavia, le parti in lotta investono sistematicamente risorse significative per infliggere danni alle strutture statuali e sociali avversarie e/o per saggiarne il livello di vulnerabilità. Tali risorse supportano la conduzione di una serie di attività aggressive che vanno dallo spionaggio all'interruzione di servizi (*Distributed Denial of Service*), dall'interferenza nei processi politici alla "presa in ostaggio" (ransomware) di mole di dati o intere infrastrutture critiche – come l'esempio dell'attacco alla statunitense Kaseya di luglio 2021 o alla Regione Lazio nell'agosto dello stesso anno.

La situazione nello spazio cibernetico ha diversi punti di contatto con quella nel mondo reale del periodo post Guerra Fredda, che ha visto una serie di operazioni militari, anche ad alta intensità e su larga scala, avvenire senza dichiarazioni di guerra – in particolare, ma non solo, in seguito agli attacchi terroristici dell'11 settembre 2001. Più di recente, il dominio cibernetico è considerato uno dei campi privilegiati della cosiddetta "guerra ibrida", condotta utilizzando senza soluzione di continuità tutte le leve a disposizione del potere statuale[128] che, dall'uso delle forze speciali alla manovra militare convenzionale, ha trovato massima espressione nell'occupazione russa della Crimea nel 2014.

Il dominio cibernetico presenta tuttavia una sfida ulteriore. Mentre il processo politico-militare dei principali Paesi Nato – e dell'Alleanza nel suo complesso – negli anni ha sostanzialmente preso le misure sia con le operazioni di contrasto

[126] L'autore ringrazia Vincenzo Camporini per i commenti ricevuti sulla prima bozza del capitolo.

[127] Sul concetto di "guerra in tempo di pace" si veda: Stefano Silvestri, "Guerre nella globalizzazione: il futuro della sicurezza europea", in *IAI Papers*, n. 20|12 (maggio 2020), https://www.iai.it/it/node/11674.

[128] Si veda al riguardo, tra gli altri: Hanna Smith, "Hybrid Threats to Allied Decision-Making", in Sonia Lucarelli, Alessandro Marrone e Francesco N. Moro (a cura di), *NATO Decision-Making in the Age of Big Data and Artificial Intelligence*, Bruxelles, NATO, marzo 2021, p. 44-56, https://www.iai.it/it/node/12844.

ISSN 2280-6164

al terrorismo che con le attività militari nei confronti della Russia, questo non è avvenuto per il caso di una crisi cibernetica di portata considerevole, che fortunatamente non si è ancora verificato. Non è quindi chiaro come si reagirebbe al riguardo, neanche in termini di attivazione dell'art. 5 del Trattato di Washington. Né è facile valutare efficacia ed efficienza della *governance* attuale, in Italia e in Europa, nell'individuare un eventuale attacco, reagire in modo tempestivo e coordinato, mitigare i danni a dati e infrastrutture critiche, attribuire la paternità dell'attacco, e compiere tutte le azioni possibili e necessarie sul continuum difesa-offesa.

5.2 La difesa avanzata di uno spazio senza confini

Essendo privo di confini tangibili al suo interno, il dominio cibernetico richiama in qualche modo quello marittimo, dove da ogni porto è in teoria raggiungibile qualsiasi altro porto sulla Terra (a eccezione ovviamente dei mari chiusi). Rispetto al campo marittimo tre sono le differenze principali. In primo luogo, le distanze si percorrono in frazioni di secondi, per cui non vi è alcuna distanza fisica a giocare a favore della difesa. Inoltre, oggi è possibile monitorare i movimenti delle flotte nemiche sul mare, mentre è molto difficile farlo nello spazio cibernetico, aumentando così l'effetto sorpresa a favore dell'attaccante. Infine, dato il livello di interconnessione raggiunto, mentre dal mare sono attaccabili solo le fasce costiere, un attacco cibernetico può colpire qualsiasi assetto del Paese, polverizzando concetti come retrovie o profondità strategica.

Date le condizioni del dominio cibernetico, specie dal punto di vista delle grandi potenze, limitarsi a rispondere a attacchi cyber equivale a cedere costantemente terreno agli avversari, vedere erodere il proprio potere militare, rischiare la compromissione dei propri sistemi informatici, e incoraggiare le potenze ostili a compiere attacchi sempre più sofisticati[129]. Metaforicamente, è come se la Marina statunitense durante la Guerra Fredda fosse rimasta nei porti americani in attesa dell'arrivo dei sottomarini e delle navi sovietiche, invece di pattugliare attivamente l'Atlantico e il Pacifico per assicurarne le rotte e contenere le attività avversarie[130].

Non a caso oggi la strategia del CyberCom statunitense riprende il concetto di "difesa avanzata", un elemento tradizionale della postura americana nei domini operativi tradizionali, in particolare aereo e marittimo, da perseguire anche in quello cibernetico[131]. L'obiettivo è "raggiungere e mantenere la superiorità nello spazio cibernetico per influenzare la condotta degli avversari, ottenere vantaggi operativi e strategici per le Forze Armate, difendere e promuovere gli

[129] Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit., p. 13.

[130] Paul M. Nakasone, "A Cyber Force for Persistent Operations", in *Joint Force Quarterly*, No. 92 (gennaio 2019), p. 10-14, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950.

[131] Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy", in *US Department of Defense Articles*, 20 settembre 2019, https://www.defense.gov/Explore/News/Article/Article/1966758.

© 2021 IAI
ISSN 2280-6164
DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021

interessi nazionali"[132]. Tale superiorità viene ottenuta tramite la "persistenza" delle operazioni, mantenendo l'iniziativa con una campagna articolata, ingaggiando costantemente gli avversari e creando incertezza sul raggiungimento dei loro obiettivi. È sostanzialmente un continuum tra azioni difensive e offensive, che punta a operare il più possibile a ridosso degli avversari, senza tregua, per negare loro un vantaggio operativo e crearne uno per le forze statunitensi[133].

Gli Stati Uniti operano in una posizione di vantaggio unica per risorse umane ed economiche, civili e militari, nonché per il ruolo delle grandi aziende private americane nella produzione della componentistica, nell'integrazione dei sistemi e nella gestione dei dati e del web. Tuttavia sia Cina e Russia, le potenze più attive nel dominio cibernetico, sia alleati Nato come Francia e Gran Bretagna, sia Israele o altri Paesi, anche piccoli, operano dichiaratamente con un approccio simile basato sulla successione continua di azioni difensive e offensive condotte in modo integrato. Azioni che possono comprendere la suddetta *threat intelligence*[134], il monitoraggio o addirittura l'uso di *Advanced Persistent Threat* (Apt)[135], attività di *reverse engeneering* su software, firmware[136] o hardware per acquisire indirettamente le competenze e la tecnologia necessarie e riprodurli autonomamente. L'insieme di tali attività, accomunate da una stessa ratio, può essere definito con una certa ambiguità anche difesa avanzata[137].

Un'ambiguità peraltro non nuova per l'Italia, dove nel 1999 si definiva la partecipazione dei cacciabombardieri Tornado alla campagna aerea Nato in Kosovo come difesa avanzata, anche per superare le resistenze interne a partecipare alle operazioni in mancanza di un'autorizzazione esplicita dell'Onu. Rispetto al continuum di operazioni difensive e offensive nello spazio cibernetico, nonostante alcuni sviluppi recenti, l'Italia sconta un certo ritardo normativo e strategico sulla difesa cibernetica che in parte inibisce i necessari sviluppi dottrinali, operativi e tecnologici. Ad esempio, non è chiaro quanto sia permessa la *Computer Network Exploitation*, ovvero la raccolta di informazioni su un determinato obiettivo accedendo ai suoi dati senza comprometterne la funzionalità[138]. Per analogia con l'esperienza trentennale nel mondo fisico, come l'Italia ha condotto decine di missioni militari all'estero anche in assenza di un conflitto dichiarato, potrebbe far condurre operazioni di difesa avanzata nello spazio cibernetico[139].

[132] US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, cit., p. 5.

[133] Ibid., p. 6.

[134] Si veda al riguardo il capitolo 2 del presente studio.

[135] Per una discussione degli Apt si veda il paragrafo su deterrenza e attribution del presente capitolo.

[136] Il firmware è un programma integrato direttamente in componente elettronico programmato.

[137] Nella letteratura rilevante per questo argomento viene usata anche la formula "difesa proattiva" (proactive defence) con un significato parzialmente sovrapponibile a quello di "difesa avanzata". Ai fini della chiarezza analitica ed espositiva, si è scelto di usare solo quest'ultimo concetto, considerato prevalente tra le fonti consultate.

[138] Intervista, 27 maggio 2021.

[139] Intervista, 4 giugno 2021.

DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021 ISSN 2280-6164

5.3 Un dominio virtuale di cui non si hanno le chiavi

Nel dominio cibernetico le leggi della fisica funzionano in modo diverse dagli altri quattro domini fisici. Non solo perché, come accennato prima, il fattore tempo cambia di svariati ordini di grandezza, misurando le operazioni in frazioni di secondo. Ma soprattutto perché tutti gli attori operano attraverso infrastrutture e infostrutture senza le quali lo stesso spazio cibernetico non esisterebbe, dotate di proprie leggi peraltro in evoluzione continua. Senza arrivare all'estremo della trilogia cinematografica di Matrix[140], nel mondo virtuale odierno chi controlla tali assetti detiene in un certo senso le chiavi della rete ed è quindi in grado di monitorarlo e intervenire ad ampio spettro tempestivamente – o preventivamente. Basti pensare agli internet provider, ai server e data center, ma anche ai produttori di sistemi quali rooter, modem, pc, fino ai singoli microprocessori, e ai software, compresi gli antivirus. Tutto ciò che rende possibile il web è anche di default un mezzo per controllarlo.

Il fatto che tali assetti siano nelle mani principalmente di grandi aziende americane, a partire da Microsoft, Intel, Cisco, Google, Apple, Facebook e Amazon, offre un vantaggio strategico agli Stati Uniti, il cui governo si trova in una posizione privilegiata unica quanto ad accesso ai dati, nonché di potenziale influenza sullo stesso uso del web. Basti pensare al fatto che l'enorme mole di dati scambiata tra tutti i dispositivi con Internet Protocol (Ip) viaggia attraverso connessioni ed è smistata tramite snodi (switch) dove possono essere appositamente inserite sonde, dall'azienda costruttrice o dal provider, volte a individuare i dati rilevanti, decrittarli, e poi far proseguire il loro spostamento nello spazio cibernetico senza che mittente e destinatario si accorgano della condivisione di informazioni con soggetti terzi[141]. Non è un caso che il principale rivale sistemico[142] di Washington, ovvero Pechino, abbia investito così massicciamente nella corsa alle Ict, alle telecomunicazioni e a tutto ciò che riguarda lo spazio cibernetico, compresa la tecnologia 5G. La Cina ha l'ambizione di sottrarsi al vantaggio strategico statunitense in questo dominio e di costruirne uno proprio con inevitabili conseguenze sui Paesi che accetteranno di utilizzare tecnologia cinese in questo campo. In gioco vi è la possibilità di inserire sistematicamente scatole nere (black box) e ingressi nascosti (backdoors) in miliardi di sistemi nel mondo, che l'utente non è nemmeno consapevole di avere[143]. Elementi così complessi e nascosti che per essere individuati necessiterebbero di un *pool* bene organizzato di conoscenze ingegneristiche e informatiche, una risorsa che solo pochi grandi attori pubblici o privati sono in grado di acquisire e mantenere nel tempo[144].

[140] The Matrix, 1999; The Matrix Reloaded, 2003; The Matrix Revolution, 2003.

[141] Intervista, 27 maggio 2021.

[142] Il termine "rivale sistemico" è utilizzato in riferimento alla Cina da diversi documenti sia Nato, compreso il rapporto del gruppo di esperti presentato dal Segretario generale Jens Stoltenberg a fine 2020, sia Ue.

[143] Intervista, 4 giugno 2021.

[144] Intervista, 27 maggio 2021.

DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021 ISSN 2280-6164

Tale situazione influenza e delimita fortemente le possibilità di difesa cibernetica di un Paese come l'Italia. Da un lato, il vantaggio strategico del principale alleato Nato offre delle garanzie in termini di difesa collettiva, deterrenza e contrasto rispetto ai rivali strategici Russia e Cina; dall'altro esso limita le ambizioni di autonomia strategica europea nelle frazioni della catena di produzione nelle quali alcuni Paesi europei hanno le competenze necessarie a ridurre il gap tecnologico già esistente, ma contenibile. Soprattutto, mentre gli Stati Uniti, e forse in prospettiva la Cina, possono in una certa misura influenzare il dominio cibernetico, per l'Italia gran parte delle condizioni in cui operare sono date.

In questo contesto, il consolidamento delle attività precedentemente assegnate al Cvcn nell'ambito del Perimetro di difesa cibernetica nazionale e ora trasferite all'Acn, ha potenzialmente una forte rilevanza per la difesa cibernetica dell'Italia. Se svolte in modo intelligente, efficace ed efficiente, con procedure snelle e risorse adeguate, le attività di validazione e certificazione possono infatti rappresentare un primo passo per verificare e comprendere più a fondo i dispositivi Ict acquisiti dalle istituzioni pubbliche e dai soggetti privati inclusi nel Perimetro. Il primo passo di un percorso che, portando a una maggiore consapevolezza di limiti e vulnerabilità degli strumenti utilizzati, aiuta la formulazione di una migliore postura difensiva, l'individuazione di fornitori più affidabili e, per quanto possibile, il supporto a fornitori nazionali per determinati elementi su cui ricercare una maggiore autonomia tecnologica.

5.4 Il problema della deterrenza e dell'attribuzione degli attacchi

Anche il principio della deterrenza affronta problemi in parte nuovi nel dominio cibernetico. Tradizionalmente, si può dissuadere un avversario dall'attaccare alterando il suo calcolo strategico in due modi: schierando una linea difensiva di forza tale da rendere quasi impossibile il suo successo (*deterrence by denial*), oppure minacciando una rappresaglia in grado di far sì che anche una vittoria temporanea si trasformi in una sconfitta disastrosa (*deterrence by punishment*). Alla luce dell'analisi svolta, la prima modalità non può essere attuata nello spazio cibernetico, in quanto la costruzione di difese cibernetiche risulta tendenzialmente più costosa, complessa, inefficace e inefficiente del tentativo stesso di penetrarle, tanto l'offesa è strutturalmente avvantaggiata sulla difesa. Inoltre, la velocità dell'avanzamento tecnologico rischia di rendere superabili delle difese cibernetiche fino a poco tempo prima ritenute inespugnabili. Il che non implica rinunciare a difendersi al meglio delle proprie possibilità: occorre anzi utilizzare tutti gli strumenti tecnologici e le modalità organizzative disponibili per proteggersi dal maggior numero di attacchi e di attori, in modo da limitare al massimo le possibilità di intrusioni, danni e crisi cibernetiche.

Tuttavia, occorre prendere atto che neanche la difesa cibernetica più avanzata può resistere a lungo a un attacco sofisticato e su larga scala, condotto da gruppi

© 2021 IAI ISSN 2280-6164 DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021

specializzati che abbiano il supporto di uno stato con risorse significative[145]. È anche per questo motivo che Stati Uniti, Francia e Regno Unito hanno intrapreso la strada della difesa avanzata, ovvero di un contrasto costante per degradare le capacità offensive avversarie.

Poiché la *deterrence by denial* non può funzionare nella totalità dei casi, specie di fronte ad attacchi sostenuti da attori statali, sia gli Stati Uniti che la Nato si stanno attrezzando per attuare la *deterrence by punishment*. Di recente Washington ha cercato di operare una distinzione tra attacchi "distruttivi" e il "normale" spionaggio condotto online, per scoraggiare il primo tollerando il secondo, così come tra obiettivi che si vorrebbe tenere off limits dagli attacchi reciproci e quelli che di fatto si accettano come terreno di scontro[146]. Fa parte di quest'approccio la proposta del Presidente Joe Biden al suo omologo Vladimir Putin avanzata durante il vertice bilaterale di giugno 2021 a Ginevra, di considerare 16 tipologie di infrastrutture critiche americane off limits da attacchi cibernetici distruttivi, dando la disponibilità di lavorare insieme a un'analoga lista di obiettivi russi. Il senso più o meno implicito di questa proposta è stabilire delle soglie da non superare nello spazio cibernetico, pena un'escalation sul terreno convenzionale.

Come discusso nel precedente capitolo, anche l'Alleanza atlantica negli ultimi anni ha elaborato una posizione ufficiale per cui la cyber defence è parte della difesa collettiva alleata. Nel 2020 il Nac ha riaffermato che i Paesi membri sono determinati a usare non solo capacità cyber ma anche terrestri, marittime o aeree per dissuadere un attacco cibernetico, difendersi da esso e contrastarlo, considerando quindi tutti i domini operativi in modo integrato ai fini della deterrenza e difesa[147]. Una dichiarazione forte, volta a scoraggiare attacchi cibernetici di gravità tale da innescare una risposta militare convenzionale – attacchi che finora sono rimasti appositamente nella zona grigia appena al di sotto dell'art. 5 da parte Nato[148].

Il problema principale con la *deterrence by punishment*, sia per gli Usa che per gli alleati Nato, è attribuire la paternità dell'attacco (*attribution*) per essere certi di colpire chi lo ha effettivamente condotto o ordinato, offrendo al contempo prove sufficienti per legittimare una rappresaglia agli occhi dell'opinione pubblica. Data l'assenza di informazioni e prove fisiche e l'estrema manovrabilità dei dati virtuali, la certezza sulla paternità di determinati attacchi è quasi impossibile da raggiungere[149]. Si punta almeno a dotarsi di capacità tecnologiche per capire se

[145] Intervista, 5 luglio 2021.

[146] Vladimir Soldatkin e Humeyra Pamuk, "Biden Tells Putin Certain Cyberattacks Should Be 'Off-Limits'", in *Reuters*, 17 giugno 2021, https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16.

[147] Alessandro Marrone, "Nato e difesa cibernetica: una risposta militare ad attacchi cyber?", in *AffarInternazionali*, 22 marzo 2021, https://www.affarinternazionali.it/?p=87347.

[148] Sul ruolo della Nato nella guerra in tempo di pace si veda: Alessandro Marrone e Karolina Muti, "Il futuro della Nato: l'Alleanza euro-atlantica nella guerra in tempo di pace", in *IAI Papers*, n. 20|28it (novembre 2020), https://www.iai.it/it/node/12251.

[149] Intervista, 27 maggio 2021.

ISSN 2280-6164

c'è un'alta probabilità che l'attacco provenga da una certa fonte[150], dopodiché serve la volontà politica per affermare una responsabilità altrui e adottare le misure conseguenti in base alla propria postura di deterrenza e difesa. Aldilà delle diverse procedure a livello nazionale, l'attribuzione di un attacco resta una decisione prettamente politica. Peraltro, la diversa distribuzione tra i Paesi delle capacità tecnologiche per verificare una determinata attribuzione rende difficile la formazione di un consenso informato tra alleati sulla paternità degli attacchi, per cui gli stati europei hanno poche possibilità di andare oltre la fiducia sugli elementi addotti dagli Usa.

È in questo contesto che si colloca la crescita di Apt, ovvero di attacchi cibernetici nei quali l'attaccante penetra un network senza suscitare allarme e rimane non identificato per lungo tempo, anche mesi, continuando la sua intrusione per raggiungere gli obiettivi fissati. Per analogia, il termine Apt è stato associato a gruppi in grado di compiere attacchi del genere in maniera sempre più sofisticata, su larga scala e sotto copertura, sia in modo autonomo, sia al servizio del miglior offerente, oppure nel quadro di rapporti più o meno indiretti con stati tra cui Cina, Russia, Iran, Corea del Nord e diversi altri. Anche tramite gli Apt le armi per la guerra cibernetica sono acquistabili in rete, rappresentando un settore estremamente redditizio che attrae gruppi sempre più organizzati di hacker[151]. Le ripetute accuse di Washington verso Mosca o Pechino, nel primo caso supportate da diversi altri Paesi Nato, scontano questa situazione che oggettivamente facilita chi vuole celare la paternità di un attacco.

Sul labile confine virtuale tra deterrenza e difesa, è diffusa la pratica del *hack-back*, ovvero di un contrattacco proporzionale nei confronti della fonte che si ritiene abbia condotto un attacco. Stante il suddetto problema di *attribution*, tra gli stati, inclusi quelli Nato, vi sono differenti interpretazioni sulla misura in cui un'attribuzione è adeguatamente certa e un *hack-back* è congruo a quanto subito[152], ma resta il fatto che bisogna attrezzarsi adeguatamente per compiere tali operazioni nel quadro della suddetta difesa avanzata. A tal proposito, gli Apt costituiscono parte del problema ma potenzialmente anche parte della soluzione: data la difficoltà di collegarli ai loro stati sponsor, possono rappresentare bersagli per azioni di *hack-back* che quindi ufficialmente non toccano nessuno stato terzo, e risultano proporzionali all'attacco ricevuto. Un po' come i mercenari durante la Guerra Fredda e i contractor in tempi più recenti, gli Apt sembrano essere tra gli assetti sacrificabili nella guerra cibernetica senza portare a ulteriori escalation.

Anche a tal riguardo, nonostante i recenti sviluppi, l'Italia sconta ancora un ritardo normativo che inibisce i necessari sviluppi dottrinali, operativi e tecnologici da parte delle forze preposte alla difesa cibernetica, e in particolare del Cor. Ad esempio, senza la garanzia funzionale definita delle istituzioni competenti, in una

150 Ibid.
151 Ibid.
152 Ibid.

ISSN 2280-6164

situazione legalmente non di conflitto la Difesa incontra limiti anche nel colpire minacce eventualmente identificate per tempo[153]. Inoltre, se la Nato decidesse una risposta collettiva a un attacco cibernetico subito da uno degli alleati, ex art. 5 del Trattato di Washington, l'Italia incontrerebbe ostacoli normativi nel contribuire allo sforzo operativo comune. A livello tattico e operativo sono stati compiuti dei passi in avanti su vari fronti, tuttavia la situazione complessiva è ancora insoddisfacente rispetto a Paesi europei paragonabili come Francia e Gran Bretagna, molto più propensi sia ad *hack-back* sia ad altre forme di difesa avanzata.

5.5 Difesa e resilienza del castello

Lo spazio cibernetico è il regno dell'intelligence, delle incursioni sotto copertura, degli attacchi a sorpresa, delle forze agili e veloci, dei ribaltamenti di fronte, tutti elementi propri dell'approccio orientale all'arte della guerra predicato a partire da Sun Tzu – e non a caso la Cina sembra muoversi molto a suo agio in questo dominio. Lo spazio cibernetico è anche il dominio in cui l'eterna e universale rincorsa tra strumenti di offesa e di difesa – nella metafora tra spada e scudo, corazza e cannone – accelera a un ritmo esponenziale, bruciando in poco tempo vantaggi tecnologici faticosamente perseguiti, specie da parte della difesa.

In questo contesto, oltre ovviamente alle tecnologie a disposizione, per la difesa cibernetica conta molto l'organizzazione della realtà da difendere, e il dominio terrestre offre una buona metafora al riguardo. La geografia è data, con le sue montagne e fiumi, come lo è per l'Italia il dominio cibernetico disegnato e costantemente sviluppato da attori non italiani. Tuttavia sta a chi deve difendersi la scelta di dove costruire un castello, se a fondovalle o in cima a un colle, e come costruirla, con quante porte d'accesso, che tipo di mura, e così via. Fuor di metafora, per la difesa cibernetica è fondamentale la visione architetturale a monte, e il conseguente sviluppo di sistemi, reti, software, applicazioni e tutto ciò che concorre a definire come un'azienda o un'istituzione si colloca nello spazio cibernetico. E attualmente il ruolo di chi disegna e sviluppa le Ict è tanto fondamentale quanto disconnesso da quello di chi si deve occupare di difendere quanto si è costruito, che spesso interviene *ex post* per "rafforzare" la difesa cibernetica. Occorre qui un cambio di paradigma per cui la sicurezza viene considerata tra i principi cardine nel disegnare qualsiasi sistema sin dalle prime fasi, *ex ante*, secondo il principio *secure by design*.

Per esempio, dotarsi di un insieme di sistemi e software provenienti dallo stesso fornitore crea una omogeneità che facilita l'attacco cibernetico una volta superata la linea di difesa esterna. Viceversa, una rete disomogenea con elementi acquisiti da diversi fornitori crea per default barriere e filtri all'incursione avversaria anche una volta che abbia superato il perimetro da proteggere. Certo, più aumentano i fornitori e più cresce il numero di black box e backdoor inserite nei sistemi usati, tuttavia anche in questo caso la parcellizzazione limita la quantità di dati

[153] Ibid.

ISSN 2280-6164

facilmente ottenibile da ogni singolo fornitore che abbia tale accesso interno, e rende più difficile raggiungere quella visione d'insieme molto più preziosa di una serie di informazioni parziali. In altre parole, "è la somma che fa il totale". Un altro esempio di *secure by design* consiste nel progettare reti i cui nodi non comunichino tutti tra di loro, ma abbiano diversi livelli di protezione, e in cui i dati siano custoditi in maniera parcellizzata e nascondendo quelli di maggior pregio. Metaforicamente, un attacco che superi il fossato e il cancello del castello, avendo poco tempo a disposizione prima di ritirarsi, dovrebbe limitarsi a saccheggiare i magazzini e non gli oggetti di pregio se questi ultimi sono custoditi in un mastio separato dalle mura, al cui interno ogni stanza ha una sola porta e ogni porta ha una chiave diversa. Anche perché, fuor di metafora, l'attenzione dell'attaccante si sta spostando sempre più dal sistema al dato, e anche la difesa cibernetica dovrebbe tenerne conto[154].

Sul lato della domanda di Ict, il problema di integrare chi gestisce le reti e chi deve difenderle tocca l'organizzazione stessa degli attori pubblici, in particolare della Difesa ma non solo. Tuttavia, anche il lato dell'offerta non ne è immune, in quanto il settore privato vede di fatto percorsi formativi e professionali diversi per chi disegna i sistemi e per chi si occupa della loro sicurezza, a danno proprio del principio *secure by design*[155]. Al riguardo, dal lato della domanda l'Italia ha fatto un importante passo in avanti con la costituzione del Cor, che ha centralizzato in un'unica catena di comando e controllo interforze la gestione della rete delle Forze Armate e la condotta di operazioni cibernetiche. Questa buona prassi dovrebbe fare da esempio per un più generale coordinamento all'interno dei Ministeri interessati, nel governo e nel Perimetro, in modo da aumentare la resilienza di tutti gli attori coinvolti e quindi le loro chance di difesa. Anche qui l'obiettivo è un cambio di paradigma: dall'intervenire dopo un incidente informatico, in modo giocoforza poco efficace, al prevenire sistematicamente il suo stesso verificarsi.

5.6 L'essere umano, tecnologia preziosa e vulnerabile

Per la difesa cibernetica è ovviamente essenziale la tecnologia ma, nonostante i progressi compiuti dalle Ict e quelli in corso quanto a *Big Data* e intelligenza artificiale, le risorse umane restano uno tra gli elementi più preziosi e vulnerabili.

Per trasformare la mole di dati raccolti e correlati dai software in conoscenza utile ai fini della difesa cibernetica servono bravi analisti, e ne servono abbastanza per schierare un team di difesa cibernetica attivo in modo adeguato 24 ore su 24 e 7 giorni su 7 – a maggior ragione se si intendono condurre operazioni più ampie nel quadro della difesa avanzata[156]. Così come nel settore privato serve un ingresso costante di tecnici che abbiano il profilo adeguato allo sviluppo dei vari elementi

[154] Intervista, 4 giugno 2021.
[155] Intervista, 5 luglio 2021.
[156] Intervista, 27 maggio 2021.

ISSN 2280-6164

funzionali a difesa e resilienza cibernetica[157]. Su entrambi i fronti i numeri di laureati nelle università italiane sono assolutamente insufficienti[158] e tale scarsità dell'offerta rispetto alla domanda nazionale e globale rende le risorse umane ancora più preziose e contese, come evidenziato in precedenza rispetto alle difficoltà del Cor nel dotarsi e mantenere personale adeguato.

La risorsa umana non è solo preziosa, ma è molto vulnerabile, e da diversi punti di vista. Nelle Forze Armate una scarsa comprensione dei rischi delle Ict e dell'operare nello spazio cibernetico, sia a livello individuale che come team, porta ad aprire grandi brecce nella difesa cibernetica anche tramite comportamenti banali. Inoltre, chi a vario titolo ha accesso a dati e reti è in qualche modo a guardia delle porte del castello e se la guardia non è adeguatamente selezionata, fidelizzata e controllata, la sua veglia rischia di risultare poco vigile, permettendo di penetrare anche una difesa cibernetica ben costruita.

ISSN 2280-6164

157 Intervista, 4 giugno 2021.

158 Interviste, 4 giugno, 27 maggio e 4 luglio 2021.

6. Criticità di sistema e raccomandazioni

di Alessandro Marrone e Ester Sabatino

Negli ultimi decenni il tema della difesa cibernetica ha assunto rilevanza crescente, a fronte dell'elevato numero di attacchi sia verso attori privati, sia a scapito delle strutture della pubblica amministrazione e dell'apparato di difesa sul territorio nazionale e all'estero. Il caso dell'attacco alla Regione Lazio dell'agosto 2021 è stato probabilmente il maggiore campanello d'allarme agli occhi dell'opinione pubblica italiana, anche a causa del suo legame con la campagna vaccinale contro il Covid-19.

Nel più ampio quadro della cybersecurity, la difesa cibernetica ha una sua specificità e importanza da tre punti di vista. In primo luogo, il dominio cibernetico può essere considerato un terreno di scontro ad alta intensità nel quale non è mai stato finora dichiarato un conflitto, ma in cui gli attacchi sono numerosi, vengono attuati da una pluralità di attori statali e non, e possono portare all'attivazione della clausola di difesa collettiva della Nato, con ripercussioni anche nel "mondo reale". In questo campo grandi e medie potenze mettono in campo risorse militari, e non, al servizio della politica di difesa dello stato.

In secondo luogo, di conseguenza, il dominio cibernetico vede il formarsi di comandi, agenzie e unità sia nei Ministeri della Difesa dei Paesi alleati sia a livello Nato, con i conseguenti sviluppi dottrinali e operativi analizzati nei precedenti capitoli.

Infine, la questione della cyber defence apre il campo a riflessioni strategiche nuove su cosa vuol dire difendersi e attaccare, nonché dissuadere un attacco, sia in questo dominio operativo sia negli altri quattro domini pervasi dal cyberspace. Una riflessione con fortissime implicazioni per la sicurezza nazionale, le strutture e l'operato della Difesa italiana, il ruolo della Nato e dell'Italia all'interno dell'Alleanza atlantica.

Bisogna quindi portare avanti una riflessione focalizzata sulla cyber defence per affrontare meglio minacce, rischi e sfide, e per coglierne le opportunità, tramite decisioni ponderate ma tempestive, atti concreti e finanziamenti adeguati.

L'importanza dell'approccio unificato e del dialogo intersettoriale

Riconoscere la specificità e importanza della difesa cibernetica ovviamente non vuol dire ragionare per compartimenti stagni, tutt'altro. La varietà delle tipologie di attacco e le possibili ripercussioni che si possono generare impongono un approccio unificato tra i vari attori coinvolti e una riflessione strategica a tutto tondo. Questo è quanto mai vero se si considera che attacchi ai danni di un attore privato di rilevanza nazionale o di un'infrastruttura critica possono avere effetti negativi sui sistemi infostrutturali e infrastrutturali nazionali con conseguenze sia

ISSN 2280-6164

nel dominio cibernetico, sia nel mondo reale. Per di più, dal punto di vista della Difesa, ogni dominio operativo, in aggiunta a quello specifico cyber, può essere soggetto ad attacchi informatici, sia in Italia sia all'estero.

Per quanto attiene alla presenza di un approccio unificato volto al raggiungimento di più elevati standard di sicurezza settoriale, l'Italia per alcuni aspetti ha inizialmente agito in modo pioneristico, ma ha tardato poi nello stare al passo con gli aggiornamenti imposti dalla velocità dell'avanzamento tecnologico e dalla pervasività della minaccia cibernetica. Infatti, se a livello internazionale da tempo i Paesi alleati e partner dell'Italia hanno provveduto a dotarsi di agenzie e strutture che operano un raccordo tra i vari attori coinvolti nella gestione e mantenimento della sicurezza cibernetica nazionale[159], in Italia si è dovuto attendere il 2021 per avere l'istituzione dell'Agenzia per la Cybersicurezza Nazionale.

L'Acn è l'attore primario in tema di sicurezza cibernetica nazionale. La decisione di collocare l'Agenzia alle dirette dipendenze della Presidenza del Consiglio dei Ministri e al di fuori dell'apparato di intelligence nazionale risolve alcune precedenti difficoltà d'azione e gestione. Restando indubbia l'esperienza del personale dei servizi di informazione della Repubblica, il ventaglio di attività necessarie per assicurare la sicurezza cibernetica vanno oltre quelle specifiche di intelligence e la collocazione a riporto della Presidenza assicura l'alta direzione e controllo dell'Agenzia da parte del Presidente del Consiglio dei Ministri e quindi del vertice politico dell'esecutivo.

Il senso del nuovo assetto legale e istituzionale raggiunto, e in particolare del Perimetro e dell'Agenzia, è quello di un approccio interministeriale, collegiale dell'esecutivo e della pubblica amministrazione al tema della difesa e sicurezza cibernetica, ognuno contribuendo nel proprio ruolo. Un approccio che in Italia è necessario su diversi aspetti della sicurezza nazionale, dalle missioni all'estero alle esportazioni nella difesa[160], dalla politica industriale[161] alle infrastrutture critiche[162], ma che in questo caso è reso ancora più impellente dalla trasversalità del dominio cibernetico.

[159] A titolo di esempio, in Germania la Bsi è stata creata nel 1991 e la Francia ha istituito l'Anssi nel 2009.

[160] Si vedano al riguardo: Alessandro Marrone, Michele Nones e Ester Sabatino, "La regolamentazione italiana degli accordi G2G nel settore della difesa", in *Documenti IAI*, n.20|16 (settembre 2020), https://www.iai.it/it/node/12069; Alessandro Marrone, Ottavia Credi e Michele Nones, "Controllo parlamentare sull'esportazione dei sistemi d'arma: modelli comparati", in *Approfondimenti dell'Osservatorio di politica internazionale*, n. 180 (luglio 2021), https://www.iai.it/it/node/13826.

[161] Alessandro Marrone, "Politica industriale della difesa, se il ministro ci mette la faccia", in *AffarInternazionali*, 29 luglio 2021, https://www.affarinternazionali.it/?p=89012.

[162] Si vedano tra gli altri: Paola Tessari e Karolina Muti, *Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations*, Bruxelles, Parlamento europeo, luglio 2021, https://doi.org/10.2861/179721.

DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021 ISSN 2280-6164

Il lavoro di razionalizzazione e riorganizzazione della governance della sicurezza cibernetica nazionale è uno sforzo positivo nell'ottica dell'efficientamento di sistema, nel quale però bisognerà tenere adeguatamente in considerazione le specificità e competenze delle singole amministrazioni coinvolte, operando un lavoro di raccordo e collaborazione interministeriale. Inoltre, in considerazione della pervasività degli attacchi cibernetici e della loro potenziale velocità di penetrazione e azione, è di fondamentale importanza che i vari interessi in gioco vengano contemperati rapidamente, per attuare tempestivamente la risposta più adeguata attraverso l'azione del Nucleo per la cybersicurezza, l'organo all'interno dell'Acn preposto alla risposta e gestione di crisi di natura cibernetica a livello nazionale.

L'importanza del dialogo tra i vari attori pubblici e privati sembra essere stato recepito dal decisore politico, che in fase di conversione in legge del DL n. 82/2021 ha dato maggiore rilievo ai ministeri maggiormente coinvolti, tra cui quello della Difesa che dovrà essere consultato nella partecipazione dell'Agenzia a progetti e iniziative in collaborazione con la Nato e l'Agenzia Europea per la Difesa, nella definizione di aspetti collegati alla ricerca militare e nella fase di formazione settoriale del personale grazie alle competenze altamente specializzate del personale delle Forze Armate.

Uno sviluppo positivo al riguardo potrebbe consistere in una fase di formazione collettiva per chi nei diversi ministeri e agenzie si occupa o occuperà di cybersecurity, compreso il personale militare. Come l'Istituto Superiore di Stato Maggiore Interforze Mobile (Issmi) rappresenta un importante passaggio per maturare lo spirito interforze tra i futuri vertici delle singole Forze Armate, così una Cyber Defence Academy potrebbe rappresentare quel centro di alta formazione dove le esperienze maturate nel comparto difesa potranno e dovranno coniugarsi con le competenze presenti nella pubblica amministrazione, in uno spirito di coesione all'interno del Perimetro.

Inoltre, è positivo che il Parlamento abbia deciso di istituire un Comitato tecnico-scientifico per supportare l'Agenzia con proposte e consulenza. La presenza di rappresentanti qualificati di industria, enti di ricerca, accademia e associazioni di settore che siedono attorno allo stesso tavolo del personale dell'Agenzia è un valido tentativo di incrementare il dialogo tra gli attori coinvolti, non solo per coordinare le attività da compiere, ma anche per valutare le modalità più adeguate a raggiungere migliori livelli di sicurezza cibernetica.

Maggior coinvolgimento della componente industriale

Nel dominio cibernetico è fondamentale un dialogo costante, sistematico, a vari livelli tra la Difesa e l'industria nazionale. Un dialogo che comprenda lo scambio di informazioni tempestivo sugli attacchi che avvengono con frequenza e gravità crescente. Lo scambio, ovviamente, dovrebbe tenersi ai massimi livelli di confidenzialità, coinvolgere e arricchire tutti gli attori coinvolti nel Perimetro, anche in chiave di maggiore difesa e resilienza rispetto ad attacchi futuri. Scambio

ISSN 2280-6164

ISSN 2280-6164

DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021

Istituto Affari Internazionali (IAI)
L'Istituto Affari Internazionali (IAI) è un think tank indipendente, privato e non-profit, fondato nel 1965 su iniziativa di Altiero Spinelli. Lo IAI mira a promuovere la conoscenza della politica internazionale e a contribuire all'avanzamento dell'integrazione europea e della cooperazione multilaterale. Si occupa di temi internazionali di rilevanza strategica quali: integrazione europea, sicurezza e difesa, economia internazionale e *governance* globale, energia e clima, politica estera italiana; e delle dinamiche di cooperazione e conflitto nelle principali aree geopolitiche come Mediterraneo e Medioriente, Asia, Eurasia, Africa e Americhe. Lo IAI pubblica una rivista trimestrale in lingua inglese (*The International Spectator*), una online in italiano (*AffarInternazionali*), tre collane di libri (*Global Politics and Security*, *Quaderni IAI* e *IAI Research Studies*) e varie collane di paper legati ai progetti di ricerca (*Documenti IAI*, *IAI Papers*, ecc.).

Via dei Montecatini, 17 - I-00186 Roma, Italia
T +39 06 6976831
iai@iai.it
www.iai.it

Ultimi DOCUMENTI IAI

Direttore: Alessandro Marrone (a.marrone@iai.it)

21 | 12	Alessandro Marrone, Ester Sabatino e Ottavia Credi, *L'Italia e la difesa cibernetica*
21 | 11en	Ottavia Credi and Camilla Vianini, *Space and European Digital Sovereignty*
21 | 11	Ottavia Credi e Camilla Vianini, *Spazio e sovranità digitale europea*
21 | 10	Marietta S. König and Liliya Buhela, *The OSCE Asian Partnership: Developments and Thematic Priorities*
21 | 09	Ester Sabatino (a cura di), *La collaborazione italo-britannica nel settore della difesa e sicurezza dopo la Brexit*
21 | 08	Eleonora Poli e Margherita Salvia, *Unione europea: cittadinanza e beni comuni europei*
21 | 07	Valeria Branca, *Financing Infrastructure Investments for Local Communities*
21 | 06	Alessandro Marrone e Karolina Muti, *La difesa missilistica dell'Europa e l'Italia: capacità e cooperazione. Executive summary*
21 | 05	Alessandro Marrone and Karolina Muti (eds), *Europe's Missile Defence and Italy: Capabilities and Cooperation*
21 | 04	Eleonora Poli, Monika Sie Dhian Ho and Brigitte Dekker, *Van Wittel/Vanvitelli Roundtable Policy Report*