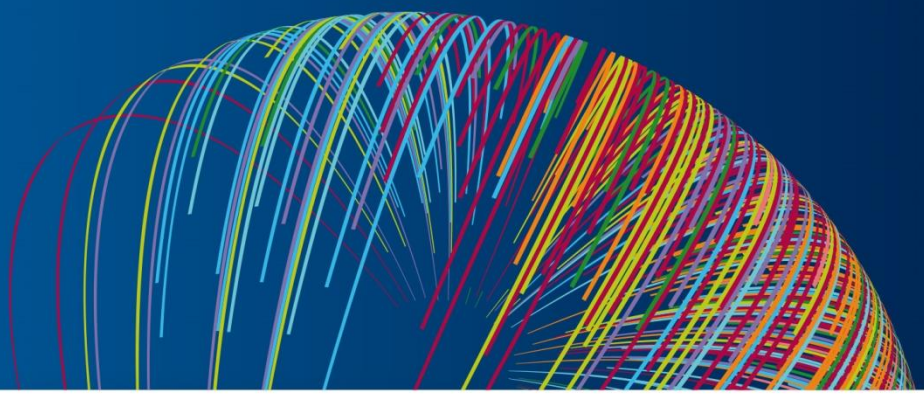
Osservatorio
di Politica internazionale



Senato
della Repubblica

Camera
dei deputati

Ministero
degli Affari Esteri
e della Cooperazione
Internazionale

La difesa cibernetica nei Paesi NATO: modelli a confronto

Dicembre 2020

164

Approfondimenti

A cura dell'Istituto Affari Internazionali

La difesa cibernetica nei Paesi NATO: modelli a confronto

Alessandro Marrone ed Ester Sabatino[1]

Sommario

[1]Alessandro Marrone è responsabile del programma Difesa dell'Istituto Affari Internazionali (IAI). Ester Sabatino è ricercatrice nel programma Difesa dello IAI.

Executive Summary

Nel più ampio perimetro della sicurezza cibernetica, il presente studio si concentra esclusivamente sulla cyber defence, analizzando l'approccio della Nato nel suo complesso ed in particolare degli stati di riferimento quanto a strategia, capacità militari e investimenti – in primis gli Stati Uniti ovviamente, ma anche Regno Unito, Francia, Germania e Spagna per fornire un solido quadro europeo.

L'approccio dell'Alleanza Atlantica verso la cyber defence si è evoluto in modo significativo negli ultimi 15 anni. Si è riconosciuto che un attacco cibernetico può arrivare a causare danni paragonabili a quelli di un attacco armato, e quindi diventare un caso di difesa collettiva ai sensi dell'articolo 5 del Trattato di Washington. La Nato ha adottato politiche e piani d'azione, istituendo comitati, agenzie e centri operativi per integrare il dominio cibernetico sia nelle operazioni che nello sviluppo delle capacità militari dei Paesi membri. Nel frattempo l'Alleanza ha sviluppato partnership con l'Unione Europea e con il settore privato sulla cyber defence.

Gli stessi Stati Uniti negli ultimi anni hanno cambiato strategia riguardo alla difesa cibernetica. Alla luce della competizione geopolitica a tutto campo con Cina e Russia, e del conseguente moltiplicarsi di attacchi cibernetici contro le istituzioni americane, Washington ha istituito un comando cyber al pari di quello aereo, terrestre o marittimo. La strategia dello US Cyber Command si basa sulla persistenza delle operazioni, mantenendo l'iniziativa tramite una campagna articolata senza soluzione di continuità tra azioni difensive e offensive. Il bilancio del comando è passato da 120 milioni di dollari nel 2010 a 600 milioni nel 2018.

Il Regno Unito ha adottato un approccio simile a quello americano, e già dal 2013 ha reso pubblico che lo sviluppo di capacità da impiegare nel dominio cibernetico a livello nazionale includeva anche quelle offensive. Tra le azioni offensive rientrano: rispondere ad attacchi cibernetici; ostacolare, degradare e disturbare le comunicazioni e i sistemi d'arma dell'avversario; attaccare sistemi e infrastrutture avversarie, con la possibilità di estendere il danno nel "mondo reale". Circa 1,9 miliardi di sterline sono stati allocati nel quinquennio 2016-2021 per la cyber defence, mentre si è perseguita una forte partnership con il settore privato.

In Francia nel 2018 il Segretariato generale della difesa e della sicurezza nazionale ha avuto il compito di elaborare una strategia di contrasto alle minacce cibernetiche. Un'apposita agenzia a carattere interministeriale, in seno al Ministero della Difesa, gestisce in modo separato sia le capacità offensive — raccolta delle informazioni e operazioni di attacco — che quelle difensive. La Francia ha previsto per il bilancio della difesa 2019-2025 un investimento di 1,6 miliardi di euro nella lotta nel dominio cibernetico, e un incremento di personale pari a circa 1.000 "combattenti cyber".

In Germania la difesa cibernetica è costituzionalmente demandata alle forze armate (*Bundeswehr*), e deve essere sottoposta alla legislazione nazionale e internazionale che regola le attività militari – con tutte le limitazioni che ne derivano. Berlino sta consolidando le infrastrutture precedentemente sviluppate a livello di singola forza armata, con l'obiettivo di arrivare ad un unico centro interforze per la difesa dei network delle istituzioni tedesche. Il Comando per lo spazio informatico e cibernetico, in fase di realizzazione, prevede un personale di ben 14.000 unità una volta raggiunta la piena capacità operativa nel 2021.

Infine, in Spagna il Comando interforze di difesa cyber, alle dirette dipendenze dello Stato maggiore della difesa, è la struttura responsabile per l'esecuzione delle azioni collegate alla protezione delle infrastrutture informatiche e dei sistemi delle forze armate. Le linee operative tengono conto della lista degli assetti prioritari in ambito cibernetico, e determinano la tipologia di risposta e la prioritizzazione degli sforzi difensivi anche in base all'entità del possibile danno di un attacco cyber.

1. Il quadro Nato

1.1 Un approccio in evoluzione e strettamente legato alla difesa collettiva

L'approccio dell'Alleanza Atlantica verso la cyber defence si è evoluto in modo significativo negli ultimi 15 anni, elevandone l'importanza quale elemento che può dare un contributo significativo a tutti e tre i "core tasks" stabiliti dall'attuale Concetto Strategico: difesa collettiva, gestione delle crisi e sicurezza cooperativa[2]. In particolare, è stato di fatto riconosciuto che un attacco cibernetico può arrivare a causare danni paragonabili a quelli di un attacco armato, e quindi diventare un caso di difesa collettiva ai sensi dell'articolo 5 del Trattato di Washington.

Già il vertice dei capi di stato e di governo del 2008 aveva adottato una prima Policy on Cyber Defence, che ha compiuto un salto in avanti nel summit del 2014 con la Enhanced Nato Policy on Cyber Defence[3]. Nel successivo vertice di Varsavia, nel 2016, i Paesi alleati hanno elevato lo spazio cibernetico a dominio, equiparandolo agli altri domini militari convenzionali. Il vertice di Varsavia ha portato anche alla firma del Cyber Defence Pledge[4] volto a istituire una piattaforma comune per migliorare le capacità nazionali di difesa e resilienza rispetto ad un attacco cibernetico. In seguito sono stati adottati diversi action plan per realizzare gli impegni presi con il Cyber Defence Pledge. L'impegno alleato si concentra sullo sviluppo di capacità in chiave difensiva, in riferimento all'articolo 3 del Trattato di Washington relativo alla capacità individuale e collettiva di resistere ad un attacco armato[5]. Si tratta di un focus in linea con l'elevata importanza attribuita agli attacchi cibernetici, giudicati sempre più frequenti, complessi e distruttivi[6], al punto da poter attivare l'articolo 5[7], tanto che nel comunicato del vertice di Bruxelles del 2018[8]viene esplicitamente affermato che la difesa cibernetica è parte della difesa collettiva Nato.

Uno dei problemi principali al riguardo è la difficoltà nel distinguere una situazione di pace da una di crisi o di conflitto, data la capacità dell'attaccante di nascondere la paternità degli attacchi condotti – o addirittura l'evento stesso. Una caratteristica purtroppo sempre più diffusa in un

[2] NATO, *Strategic Concept 2010*, 19 novembre 2010 (aggiornato al 3 febbraio 2021), https://www.nato.int/cps/en/natohq/topics_82705.htm.

[3] "Come cambia la strategia Cyber della NATO", in Analisi Difesa, 4 giugno 2019, https://www.analisidifesa.it/2019/06/come-cambia-la-strategia-cyber-della-nato/

[4] Nato, *Cyber Defence Pledge*, 8 luglio 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[5] "Allo scopo di conseguire con maggiore efficacia gli obiettivi del presente Trattato, le parti, agendo individualmente e congiuntamente, in modo continuo ed effettivo, mediante lo sviluppo delle loro risorse e prestandosi reciproca assistenza, manterranno e accresceranno la loro capacità individuale e collettiva di resistere ad un attacco armato". NATO, *Trattato Nord Atlantico*, Washington, 4 aprile 1949, https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=it.

[6] NATO, *Remarks by NATO Secretary General Jens Stoltenberg at Cyber Defence Pledge Conference, London*, 23 maggio 2019, https://www.nato.int/cps/en/natohq/opinions_166039.htm.

[7] NATO, *Deputy Secretary General at CYBERSEC: NATO is adapting to respond to cyber threats*, 28 settembre 2020, https://www.nato.int/cps/en/natohq/news_178338.htm?selectedLocale=en.

[8] NATO, *Brussels Summit Declaration*, 11 luglio 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en.

quadro strategico internazionale che vede una sorta di permanente "guerra in tempo di pace"[9]. Di fronte a questa situazione, che ha visto anche il moltiplicarsi di attacchi cibernetici durante la prima ondata di Covid-19, a giugno 2020 il North Atlantic Council ha riaffermato che i Paesi membri sono "determined to employ the full range of capabilities, including cyber, to deter, defend against and counter the full spectrum of cyber threats."[10] Da notare come la Nato si dichiari pronta ad usare non solo capacità cyber ma anche aeree, marittime o terrestri, per rispondere ad un attacco cibernetico, considerando quindi tutti i domini operativi in modo integrato ai fini della deterrenza e difesa, in linea con l'integrazione del Cyber Operation Centre nella struttura di comando Nato come deciso durante il vertice di Bruxelles. Per esercitare una efficace deterrenza è tuttavia fondamentale la capacità di attribuire la paternità degli attacchi[11], una priorità che richiede ulteriori sforzi da parte degli alleati. Riguardo al dominio cibernetico la Nato riafferma in definitiva sia la sua natura di alleanza difensiva, sia il principio che il diritto internazionale si applica anche al cyberspace[12] e deve essere rispettato[13].

Il vertice di Londra del 2019 ha dato nuovo slancio politico-strategico alle attività Nato nel campo cibernetico, assieme a quello spaziale, nella consapevolezza della competizione geopolitica a tutto campo con Cina e Russia nel quadro di un "multipolarismo aggressivo"[14]. Il Segretario Generale Jens Stoltenberg ha dichiarato che "Cyberspace is the new battleground and making Nato cyber ready—well-resourced, well-trained, and well equipped—is a top priority"[15]. Non a caso, nel 2020 il rapporto del Gruppo di Riflessione sulla Nato in prospettiva 2030 ha attribuito grande importanza alle Emerging and Disruptive Technologies (Edt) intese sia come settore sul quale investire maggiormente, sia come sfide, tra cui rientrano prioritariamente proprio quelle relative alla cyber defence, in primis l'Artificial Intelligence (Ai)[16]. Stoltenberg ha infatti sottolineato che "le minacce cyber diventeranno più pericolose con lo sviluppo di nuove tecnologie come AI e machine learning (…). Queste tecnologie stanno cambiando fondamentalmente la natura dei conflitti, tanto quanto avvenuto con la rivoluzione industriale. La Nato si sta adattando a questa nuova realtà"[17]. È quindi molto probabile che anche il nuovo Concetto Strategico su cui verosimilmente l'Alleanza

[9] Stefano Silvestri, "Guerre nella globalizzazione: il futuro della sicurezza europea", in *IAI Papers*, n. 20|12 (aprile 2020), https://www.iai.it/it/pubblicazioni/guerre-nella-globalizzazione-il-futuro-della-sicurezza-europea.
[10] NATO, *Statement by the North Atlantic Council concerning malicious cyber activities*, 3 giugno 2020, https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.
[11] NATO, *Statement by the North Atlantic Council concerning malicious cyber activities*, *cit*.
[12] Per una disamina delle principali leggi internazionali che si applicano alle operazioni cibernetiche si veda: CCDCOE, *Tallin Manual 2.0*, 2017, https://ccdcoe.org/research/tallinn-manual/.
[13] NATO, *Statement by the North Atlantic Council concerning malicious cyber activities*, *cit*.
[14] Alessandro Marrone e Karolina Muti, "Il future della Nato: l'Alleanza euro-atlantica nella guerra in tempo di pace", in *IAI Papers* n. 20|28 (novembre 2020), https://www.iai.it/it/pubblicazioni/il-futuro-della-nato-lalleanza-euro-atlantica-nella-guerra-tempo-di-pace.
[15] "NATO will defend itself", di Jens Stoltenberg, capitolo in "Cyber Resilience – How to guard against the greatest security threat of the 21st century", in *Prospect Magazine*, ottobre 2019, p.4-6 https://www.prospectmagazine.co.uk/content/uploads/2019/08/Cyber_Resilience_October2019.pdf.
[16] NATO, *NATO 2030: United for a New Era*, 25 novembre 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.
[17] NATO, *Remarks by NATO Secretary General Jens Stoltenberg at Cyber Defence Pledge Conference, cit*.

lavorerà nel 2021 porrà grande attenzione alla cyber defence, e in generale al dominio cyber e alle Edt come terreno di confronto con Cina e Russia[18].

1.2 Le strutture Nato rilevanti per la cyber defence

Già nel 2016 la Nato ha riconosciuto il cyberspace come dominio operativo, nel quale l'Alleanza deve essere in grado di operare altrettanto efficacemente che in quelli terrestre, marittimo ed aereo. Tale riconoscimento è il punto di partenza affinché i comandi delle forze alleate utilizzino il dominio e le risorse cibernetiche nelle loro operazioni, e le stesse strutture Nato si attrezzino al riguardo.

Gli alleati mantengono in ogni caso la leadership politico-militare anche nel campo cibernetico, e le strutture Nato servono, in primo luogo, come sostegno al processo decisionale. A tal fine, il North Atlantic Council è supportato dal Cyber Defence Committee, responsabile per la governance politica della difesa cibernetica Nato. Il Cyber Defence Management Board (Cdmb) all'interno della Emerging Security Challenges Division[19] riunisce invece i rappresentanti degli organi militari, diplomatici e tecnici (comandi, agenzie, ecc) responsabili per le varie attività di cyber defence Nato in un tavolo di lavoro e coordinamento permanente.

A livello operativo, nel 2019 all'interno del Allied Command Operations (Aco) di Mons è stato creato un Cyberspace Operations Centre (Cyoc) responsabile delle operazioni cyber Nato, a supporto dei comandi operativi soprattutto nel monitorare il cyberspace e coordinare le operazioni in questo dominio con quelle in campo terrestre, navale o aereo[20]. Il Cyoc potrebbe aprire la strada alla futura costituzione di un Comando Nato per le operazioni cibernetiche al pari dei comandi operanti nel domino aereo, marittimo e terrestre. Aldilà del Cyoc e della sua possibile evoluzione, già ora quasi tutti gli elementi principali del comando militare integrato Nato hanno un ruolo da giocare quanto a cyber defence, comprese ad esempio le Nato Force Integration Unit (Nfiu) dispiegate nei Paesi del fianco Est per meglio integrare le forze locali, dal Baltico alla Romania, con quelle degli altri stati membri in chiave di deterrenza e difesa nei confronti della Russia.

A livello tecnico, la Nato Communications and Information Agency (Ncia), istituita nel 2012, fornisce molte delle capacità necessarie alle strutture dell'Alleanza in termini di cyber defence. Inoltre, la Ncia gestisce direttamente alcuni dei network di sistemi informatici alleati, agendo direttamente con i Nato Cyber Security Center (Ncsc) e la Nato Computer Incident Response

[18] Alessandro Marrone, "La Nato e la rivalità sistemica con Russia e Cina", in *Affari Internazionali*, 7 dicembre 2020, https://www.affarinternazionali.it/2020/12/la-nato-e-la-rivalita-sistemica-con-russia-e-cina/.
[19] CCDCoE, "North Atlantic Treaty Organisation", in *Ccdcoe.org*, https://ccdcoe.org/organisations/nato/.
[20] La costituzione del Cyoc era stata prevista dal vertice di Bruxelles del 2018. Per maggiori informazioni si veda: Alexandra Brzozowski, "NATO sees new cyber command centre by 2023 as Europe readies for cyber threats", in *Euractiv.com*, 17 ottobre 2018, https://www.euractiv.com/section/defence-and-security/news/nato-sees-new-cyber-command-centre-by-2023-as-europe-readies-for-cyber-threats/

Capability (Ncirc). In particolare la Ncirc monitora costantemente i network dell'Alleanza, è la prima a rispondere in caso di attacchi, prepara i report al riguardo, e fornisce supporto al suddetto Cdmb. Inoltre la Ncirc, tramite un apposito centro di coordinamento, permette agli alleati di scambiare informazioni tecniche sulle minacce cyber, inclusi degli indicatori che possono fornire indizi sulla natura degli attacchi intercorsi. Di fatto, il focus operativo principale della Nato al momento è sulla protezione dei propri network. Da notare, in prospettiva italiana, che la Ncia ha rinnovato nel 2019 per ulteriori 18 mesi il contratto in vigore dal 2012 con Leonardo riguardo ai servizi di protezione informatica per l'Alleanza (Ncirc – Cyber Security Support Services). Uno staff congiunto di Leonardo e Ncia, formato da circa 200 esperti di sicurezza digitale, fornisce a personale Nato nei 30 Paesi membri servizi di rilevamento, gestione e risposta agli incidenti informatici[21]. In aggiunta, i Nato Cyber Rapid Reaction Teams sono a disposizione per essere prontamente impiegati a sostegno di Paesi membri oggetto di attacchi cyber.

Infine, al di fuori del comando militare integrato alleato, il Cooperative Cyber Defence Center of Excellence (CCDCoE),inaugurato già nel 2008 in Estonia, prepara studi e report su temi di interesse per la difesa cibernetica[22] e ospita esercitazioni periodiche come il LockedShield dal 2010. Quest'ultima esercitazione nel 2019 ha coinvolto oltre 1.000 partecipanti, tra vertici istituzionali e personale dedicato alla risposta a cyber attacks, impegnati virtualmente nel contenere una serie di attacchi alle infrastrutture critiche di un Paese durante le elezioni politiche[23]. Esercitazioni del genere sono molto importanti nel formare il personale civile e militare per i peggiori scenari di attacco cibernetico, ma la formazione deve riguardare anche abitudini nell'uso dei dispositivi informatici che indeboliscono la capacità di difesa Nato[24]. Vista l'importanza del fattore umano nella cyber defence, contribuiscono in senso lato alla capacità di difesa e resilienza Nato anche i corsi di formazione nella Communications and Information Systems School (Nciss) alleata in Portogallo e nella scuola Nato di Oberammergau in Germania, e le attività di ricerca a livello politico-militare del Nato Defence College a Roma.

Le suddette esercitazioni sono importanti anche per rafforzare le prassi di cooperazione e scambio di informazioni, come nel caso del Cyber Coalition Exercise organizzato dal Nato Allied Command Transformation (Act) per far familiarizzare i livelli apicali del processo decisionale con una situazione di attacco cyber, come avviene tramite il Crisis Management Exercise. Lo scambio di

[21] La protezione si estende dalle reti fino ai dispositivi portatili, coprendo 75 siti, tra cui il quartier generale della NATO. Il servizio ha anche operato con successo per la cyber security dei Summit NATO del 2014, 2016 e2018. "Cyber security: la NATO estende il contratto con Leonardo", in Analisi Difesa, 11 febbraio 2019, https://www.analisidifesa.it/2019/02/cyber-security-la-nato-estende-il-nuovo-contratto-con-leonardo/.

[22] Si veda ad esempio CCDCOE, "Recent Cyber Events and PossibleImplications for ArmedForces", in *CCDCOE.org*, settembre 2020, https://ccdcoe.org/uploads/2020/09/Recent-Cyber-Events-and-Possible-Implications-for-Armed-Forces-5-September-2020_Final.pdf.

[23] George Allison, "NATO takes part in international cyber security exercise", in *UK Defence Journal*, 11 aprile 2019, https://ukdefencejournal.org.uk/nato-takes-part-in-international-cyber-security-exercise/.

[24] Vivienne Machi, "Private Sector PlaysBiggerRole in NATO Cyber Strategy", in *National Defence Magazine*, 2 agosto 2017, https://www.nationaldefensemagazine.org/Articles/2017/2/8/Private%20Sector%20Plays%20Bigger%20Role%20in%20NATO%20Cyber%20Strategy.

informazioni in questo settore resta tuttavia delicato, complicato e politicamente sensibile, in modo simile a quanto accade con l'intelligence, con possibili conseguenze sulla capacità di contenimento e contrasto della minaccia. Cruciale è la costruzione nel tempo di un rapporto di fiducia tra la comunità di addetti ai lavori, anche sull'uso che si farà dell'informazione condivisa. Per favorire scambio di informazioni, la fiducia reciproca e le capacità nazionali di risposta ad attacchi cyber, dal 2015 il Cdmb è incaricato di sottoscrivere un Memorandum of Understanding (MoU) on Cyber Defence con le autorità di ciascuno stato membro[25].
Infine, occorre sottolineare come dal 2019 alcuni stati membri – tra cui Stati Uniti, Regno Unito Francia, Danimarca ed Estonia - abbiano concordato una cornice Nato nella quale integrare contributi volontari in termini di operazioni difensive e offensive[26]. Tali capacità restano in ogni caso sotto il pieno controllo e responsabilità del Paese che li detiene.

1.3 Lo sviluppo di dottrine e capacità militari

II riconoscimento Nato del dominio operativo cibernetico sta influenzando anche lo sviluppo delle dottrine e capacità militari alleate, nonché l'addestramento del personale da parte del Paesi membri in modo da aumentare la difesa e resilienza su questo fronte. Si tratta di processi complessi, lunghi e difficoltosi, necessari per integrare nel *modus operandi* militare un dominio operativo nuovo e per molti versi diverso da quelli tradizionali e fisici. Il Cyoc è l'attore chiave al riguardo, mentre l'Act considera il dominio cibernetico nel quadro più ampio della trasformazione militare e dell'innovazione tecnologica in una prospettiva di medio-lungo periodo. Nella situazione attuale, alcuni documenti alleati sulla pianificazione operativa già comprendono esplicitamente la difesa cibernetica[27], ma resta molta strada da fare per integrare pienamente la dimensione cyber nelle operazioni ed attività Nato, nonché nello sviluppo dottrinale e capacitivo su cui l'ultima parola resta agli stati membri.

Gli stati, a loro volta, utilizzano la piattaforma del Cyber Defence Pledge per valutare autonomamente nel tempo i progressi sullo sviluppo delle capacità nazionali di difesa cibernetica, anche attraverso il rapporto finale sull'attuazione degli impegni presi e per scambiarsi informazioni e buone prassi al riguardo. Un ruolo importante è giocato ovviamente anche dal Nato Defence Planning Process (Ndpp), la procedura principale, omnicomprensiva e di lungo periodo, con cui i Paesi membri concordano gli obiettivi nazionali di sviluppo delle rispettive forze armate in modo da contribuire anche agli impegni Nato di difesa collettiva e gestione delle crisi. Nel quadro del

[25] CCDCOE, "North Atlantic Treaty Organisation", *cit*.
[26] Jamie Shea, "Deterring future cyber attacks: EU, NATO and international responses", capitolo del discussion paper "Hybrid and transnational threats", in *Friends of Europe*, inverno 2018, p. 35-38, https://www.friendsofeurope.org/wp/wp-content/uploads/2019/04/FoE_SEC_PUB_Hybrid_DP_WEB.pdf.
[27] Si veda a titolo di esempio: NATO Standardization Office, *NATO Standard AJP-01 Allied Joint Doctrine*, Edizione E versione 1, febbraio 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905877/20200728-doctrine_nato_allied_joint_doctrine_ajp_01.pdf.

Ndpp, dal 2012 sono stati inseriti degli obiettivi di sviluppo di capacità di cyber defence, i cui progressi vengono valutati periodicamente.

1.4 Le partnership Nato con il settore privato e con l'UE

Per le caratteristiche intrinseche del domino cibernetico, in cui l'innovazione tecnologica è guidata principalmente da aziende private che spesso non operano nel campo militare, la cooperazione tra la Nato e la controparte industriale, compresa quella civile a vario titolo coinvolta nella gestione delle infrastrutture critiche, è estremamente importante. A tal fine già nel 2014 l'Alleanza aveva lanciato la Nato Industry Cyber Partnership (Nicp)[28], che prevede tra l'altro la partecipazione dei rappresentanti industriali al Cyber Defence Workshop annuale volto allo scambio con gli alleati di informazioni altamente tecniche sulle minacce, le vulnerabilità e le possibili soluzioni. I partner industriali inoltre aggiornano frequentemente le strutture Nato che si occupano di cyber defence sugli sviluppi e i trend che osservano in questo campo, incluse le sfide alla sicurezza associate a determinate tecnologie, contribuendo così alla riflessione alleata al riguardo.

La cyber defence è indicata dalla Dichiarazione Congiunta Nato-Ue del 2016[29] tra le sette aree prioritarie per lo sviluppo della cooperazione bilaterale. Su questa base, le istituzioni dell'Alleanza e dell'Unione hanno scambiato informazioni su strategie, politiche, standard e attività di addestramento relative alla difesa cibernetica, ed hanno partecipato alle rispettive esercitazioni – la suddetta Cyber Coalition Nato e la Cyber Europe dal lato UE. La formazione è particolarmente importante, con l'ambizioso programma di addestrare congiuntamente 10.000 effettivi nel campo della difesa cibernetica[30]. Nel 2016 le due organizzazioni hanno firmato un Technical Arrangement on Cyber Defence[31] che governa lo scambio di informazioni non classificate, a beneficio della capacità di entrambe di avere un quadro più completo della situazione e di proteggere i rispettivi network. La cooperazione Nato-Ue sulla cyber defence è oggetto di incontri regolari a livello di staff, durante i quali ci si aggiorna reciprocamente anche sulle rispettive attività settoriali e i progressi del partenariato sono stati riconosciuti nel 2019 dallo stesso Stoltenberg[32].

Al di là della stretta cooperazione con l'Ue, la Nato è aperta a cooperare con l'Onu, l'Osce, e stati terzi che condividano lo stesso approccio alleato alla cyber defence. Ad esempio, nel 2017 la

[28] NATO Communications and Information Agency, "NATO Industry Cyber Partnership", in *Ncia.nato.int*, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html.
[29] Consiglio europeo, *Joint declaration by the president of the European Council, the president of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation*, Varsavia, 8 luglio 2016, https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf.
[30] NATO Communications and Information Agency, "10,000 Cyber Defenders – Cyber education for the NATO-EU workforce", in *Ncia.nato.int*, https://www.ncia.nato.int/resources/site1/general/what%20we%20do/nci%20academy/10k_cyber_defenders_brochure.pdf.
[31] Consiglio dell'Unione europea, EU Cyber Defence Policy Framework (2018 update), Bruxelles, 19 novembre 2018 (14413/18), https://www.consilium.europa.eu/media/37024/st14413-en18.pdf.
[32] NATO, *Remarks by NATO Secretary General Jens Stoltenberg at Cyber Defence Pledge Conference, London*, *cit*.

Finlandia ha firmato un accordo con l'Alleanza, il Policy Framework Arrangement, sulla cooperazione quanto a difesa cibernetica[33].

[33] NATO, *NATO and Finland step up cyber cooperation*, 16 febbraio 2017, https://www.nato.int/cps/en/natohq/news_141464.htm.

2. Gli Stati Uniti

2.1 La strategia del Pentagono: azione persistente e difesa avanzata

L'approccio statunitense alla cyber defence è qualitativamente e quantitativamente diverso rispetto ai maggiori Paesi europei. Si tratta infatti dell'unica potenza mondiale all'interno della Nato, sempre più impegnata in una competizione geopolitica a tutto campo con la Cina — in molti ambiti un rivale quasi alla pari — con la Russia, considerata una potenza in grado di contrastare gli Stati Uniti in diversi settori. La National Security Strategy del 2017[34] prende atto di tale confronto geopolitico e indica il dominio cibernetico come uno dei principali terreni di scontro. La National Defence Strategy del 2018 mette in guardia sulle capacità degli avversari di contrastare e danneggiare le forze armate, l'economia e la società americane, anche nel cyberspace[35].

Il Dipartimento della Difesa americano aveva istituito già nel 2009 un Cyber Command (Uscybercom), all'interno dello Strategic Command, il cui comandante ha il doppio cappello di direttore della National Security Agency (Nsa) per assicurare le sinergie tra le operazioni cibernetiche e quelle di intelligence. Inizialmente il nuovo comando cyber si è concentrato solo sulla difesa dei network informatici del Pentagono, ma nel giro di pochi anni è maturata la consapevolezza che tale approccio è inadeguato per le caratteristiche intrinseche del cyberspace e per il suo essere campo di battaglia del confronto con Cina e Russia, nonché delle azioni offensive di Iran, Corea del Nord e di gruppi terroristici come il cosiddetto Stato islamico (Isis). Gli attacchi subiti nel 2016 con l'hackeraggio delle email del comitato nazionale del Partito Democratico, e poi quelli nel 2017 (WannaCry e NotPetya), hanno dimostrato una capacità offensiva degli avversari ritenuta inaccettabile per la sicurezza nazionale americana.

Di conseguenza, l'attuale concetto strategico del Uscybercom si pone l'ambizioso obiettivo di "raggiungere e mantenere la superiorità nel cyberspace per influenzare la condotta degli avversari, ottenere vantaggi operativi e strategici per le forze armate, difendere e promuovere gli interessi nazionali"[36]. Tale superiorità viene ottenuta tramite la "persistenza" delle operazioni, mantenendo l'iniziativa tramite una campagna articolata, ingaggiando costantemente gli avversari e creando incertezza sul raggiungimento dei loro obiettivi. È sostanzialmente una campagna continua tra le azioni difensive e offensive, essendo il campo di battaglia interconnesso a livello globale. In altre

[34] Governo americano, *National Security Strategy*, dicembre 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[35] Governo americano, *National Defence Strategy*, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
[36] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command*, aprile 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, p. 5.

parole, si 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[37].

In termini di dottrina militare, la strategia del Uscybercom riprende il concetto di "difesa avanzata", come dichiarato esplicitamente nel 2019 dal Segretario di Stato alla Difesa Mark Esper: un elemento tradizionale della postura americana in campo terrestre, marittimo e aereo, da realizzare anche nel dominio cibernetico[38]. L'assunto di base, comprovato dall'esperienza nei primi anni di attività del Uscybercom, è che limitarsi a rispondere ad attacchi cibernetici 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. 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 l'Atlantico e il Pacifico per assicurarne le rotte[39].

Inoltre, gli attacchi cyber contro gli Stati Uniti rimangono regolarmente al di sotto della soglia dell'aggressione armata, in modo da evitare una risposta delle forze statunitensi che mobiliti appieno il loro potenziale convenzionale. Proprio per l'impossibilità di rispondere al di fuori del cyberspace ad attacchi cibernetici di questo tipo, gli Stati Uniti hanno deciso di difendersi operando attivamente e preventivamente contro gli avversari tramite lo Uscybercom, in modo da limitare la loro capacità di azione, danneggiare le loro risorse, costringerli a concentrarsi sulla propria difesa, e in ultima analisi dissuaderli da determinate azioni offensive tramite una credibile minaccia di rappresaglia.

In questo contesto, la strategia del Uscybercom si articola in cinque imperativi[40]:
1) ottenere e mantenere la superiorità sulle capacità avversarie, anticipando i cambiamenti tecnologici e sfruttando le tecnologie emergenti più velocemente degli avversari;
2) creare un vantaggio in campo cibernetico a favore delle operazioni terrestri, marittime, aeree e spaziali, integrando il dominio cyber nella pianificazione interforze;
3) integrare le operazioni cibernetiche con quelle di intelligence e la comunicazione strategica;
4) velocizzare e rendere più agili le operazioni e i processi decisionali;
5) espandere, approfondire e rendere più operative le partnership con le altre agenzie americane, il settore privato, i Paesi alleati ed il mondo accademico.

[37] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command*, *cit.*, p. 6.
[38] Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy", in *U.S. Department of Defense*, 20 settembre 2019, https://www.defense.gov/Explore/News/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/.
[39] Paul M. Nakasone, "A Cyber Force for Persistent Operations", in *Joint Force Quarterly*, 22 gennaio 2019, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf, p. 12-13.
[40] "U.S. Cyber Command *Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command*, *cit.,* p. 8.

2.2 Lo US Cyber Command (Uscybercom)

Dal 2009 ad oggi negli Stati Uniti è avvenuto un cambio di passo non solo in termini di strategia, ma anche di mandato e dimensioni dello Uscybercom. In primo luogo, nel 2017 quest'ultimo è stato scorporato dal Comando Strategico ed elevato a comando unificato a sé stante, sullo stesso piano di quello aereo, navale o terrestre. Al tempo stesso, le sue risorse sono state fortemente potenziate: il bilancio è passato da 120 milioni di dollari nel 2010 a 600 milioni nel 2018[41]. Due anni fa lo Uscybercom è arrivato a contare su 133 gruppi operativi, il doppio del 2015[42]. Il comando è co-locato a Fort Meade con il quartier generale della Nsa, per assicurare il massimo delle sinergie tra intelligence e sicurezza interna.

I vertici dello Uscybercom comprendono rappresentanti dei comandi cyber delle quattro forze armate americane: Army Cyber Command (Arcyber), US Fleet Cyber Command 10th Fleet (FCC/C10F), US Marine CorpsForces Cyberspace (Marforcyber), 24th Air Force (Afcyber) – nonché della Guardia Costiera[43]. Tra i comandi delle singole forze armate, quello con più esperienza è l'Afcyber, istituito nel 2010 e che già nel 2015 aveva raggiunto 5.400 effettivi[44]. Con riferimento al personale, una delle sfide principali per lo Uscybercom è il reclutamento e il mantenimento in servizio dei talenti informatici che troverebbero migliori opportunità di carriera nel settore privato[45].

Nel nuovo assetto, il comando opera costantemente al di sotto della soglia dell'attacco armato, preparandosi nel frattempo ad essere una forza "letale" in caso di conflitto[46]. Nel 2016 lo Uscybercom avrebbe distrutto materiale di propaganda dell'Isis in un server locato in Germania[47]. Nel 2018 il comando sembra aver messo fuori uso la connessione internet della Internet Research Agency russa, agenzia governativa accusata da tempo di condurre attacchi hacker e interferire nel processo elettorale americano, per impedire loro di agire contro le elezioni di medio termine statunitensi[48]. Nel 2019, secondo fonti di stampa, lo Uscybercom ha posizionato malware nei software di gestione della rete elettrica russa, rispondendo a quanto avrebbe fatto la Russia con le reti energetiche americane, in modo da esercitare una certa deterrenza verso l'escalation di

[41] "A Strategic Assessment of the U.S. Cyber Command Vision", capitolo in Stanford Freeman Spogli Institute for International Studies, *Bytes, Bombs, and Spies*, 16 gennaio 2019,https://medium.com/freeman-spogli-institute-for-international-studies/bytes-bombs-and-spies-261564d51157.

[42] "A Strategic Assessment of the U.S. Cyber Command Vision", *cit*.

[43] Piret Pernik, Jesse Wojtkowiak e Alexander Verschoor-Kirss, "National Cyber Security Organisation: UNITED STATES", in *CCDCOE.org*, 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf, p. 20.

[44] Piret Pernik, Jesse Wojtkowiak e Alexander Verschoor-Kirss, "National Cyber Security Organisation: UNITED STATES", cit., p. 21.

[45] Scott Maucione, "What CYBERCOM is doing on the front lines of cyberwarfare", in *Federal News Network*, 26 ottobre 2020, https://federalnewsnetwork.com/federal-insights/2020/10/what-cybercom-is-doing-on-the-front-lines-of-cyberwarfare/.

[46] Paul M. Nakasone, "A Cyber Force for Persistent Operations", *cit*., p. 12-13.

[47] Max Smeets, "NATO Allies need to come to terms with offensive cyber operations", in *Lawfareblog.com*, 14 ottobre 2019, https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations.

[48] Jason Healey, "Taking down Russian trolls is my kind of cyber attack", in *The cipher brief*, 28 febbraio 2019, https://www.thecipherbrief.com/column/cyber-initiator/taking-down-russian-trolls-is-my-kind-of-cyber-attack.

attacchi cibernetici da parte russa[49]. Nel 2020 vi è stata la prima conferma ufficiala di un'azione importante dello Uscybercom contro il malware TrickBot di sospetta provenienza russa[50].

È tuttora in corso negli Stati Uniti un dibattito sui casi in cui le autorità americane siano autorizzate a colpire i nemici nel cyberspace[51] e non è chiaro se, quanto e come la postura più aggressiva dello Uscybercom abbia influito negli ultimi anni sulle operazioni cibernetiche degli avversari[52].

Infine, occorre notare che il Segretario alla Difesa Esper ha più volte sottolineato l'importanza dei Paesi partner degli Stati Uniti per l'efficacia della difesa cibernetica americana nei confronti della Cina[53]. Tuttavia non vi è un accordo tra i Paesi Nato sulle procedure e i limiti di un'azione offensiva nel dominio cyber, in particolare sull'accesso a sistemi e network locati in un altro Paese alleato per condurre una operazione cibernetica[54] - e il suddetto attacco dello Uscybercom contro un server in Germania ha causato non poche preoccupazioni nel governo tedesco.

[49] David E. Sanger e Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", in *The New York Times*, 15 giugno2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?auth=linked-google&login=email.

[50] Robert Chesney, "Persisently Engaging TrickBot: USCYBERCOM Takes on a Notorious Botnet", in *Lawfareblog.com*, 12 ottobre 2020, https://www.lawfareblog.com/persistently-engaging-trickbot-uscybercom-takes-notorious-botnet.

[51] Sven Herpig, Robert Morgus e Amit Sheniak, "Active Cyber Defense – A comparative study on US, Israeli and German approaches", in *Konrad Adenauer Stiftung*, marzo 2020, https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf, p. 9.

[52] Mark Pomerleau, "Two years in, how has a new strategy changed cyber operations?", in *Fifth Domain*, 11 novembre 2019, https://www.fifthdomain.com/dod/cybercom/2019/08/20/cyber-command-changed-its-approach-is-the-difference-noticeable/.

[53] Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy", *cit.*

[54] Max Smeets, "NATO Allies need to come to terms with offensive cyber operations", *cit*.

3. Regno Unito

3.1 La strategia nazionale

L'approccio del Regno Unito alle operazioni di difesa cyber è molto simile rispetto a quello statunitense, fatte salve ovviamente le debite proporzioni tra i due Paesi. Dalla prima Strategia di sicurezza cibernetica del 2009, Londra ha adottato un approccio accentrato, almeno nella formulazione di strategie e programmi e dal conseguente lancio del *National Cyber Security Programme*, ha sviluppato capacità di difesa cyber[55].

Nel 2013 il Regno Unito ha reso pubblico che lo sviluppo di capacità da impiegare nel dominio cibernetico a livello nazionale includeva anche capacità di attacco. Tuttavia, l'abilità del governo britannico di mettere in pratica operazioni offensive cyber risale almeno al 2007[56].Sempre nel 2013 è stato creato il *Joint Forces Cyber Group*— composto da due unità cibernetiche interforze supportate da una *Joint Cyber Reserve Force*[57] — operante sotto la direzione congiunta del Ministero della Difesa e del *Government Communication Headquarter* (Gchq), esterno al Ministero della Difesa, con il fine di coordinare le operazioni di *cyber warfare*.

A seguito della Strategic Defence and Security Review del 2015[58] che ha delineato la minaccia cyber tra quelle principali che il Paese deve affrontare nel futuro e alla quale l'apparato statale deve essere nelle condizioni di rispondere come se fosse un qualsiasi altro tipo di attacco convenzionale, nel 2016 è stata formulata la *National Cyber Security Strategy* incentrata su tre obiettivi principali. Il primo è assicurare la difesa e la resilienza cyber dei network britannici, nonché delle attività economiche, dei dati dei privati cittadini e delle istituzioni. Un ulteriore obiettivo è sviluppare un'industria della sicurezza cibernetica in forte crescita e con una settoriale sufficientemente elevata da assicurare lo sviluppo di sistemi di difesa cibernetica all'avanguardia. Infine, vi è una capacità di deterrenza adeguatamente sviluppata in modo da rendere il Paese un difficile obiettivo d'attacco. Per assicurare quest'ultimo obiettivo, la strategia delinea il principio di *Active Cyber Defence* (Acd)[59], ossia la capacità di rafforzare il network e il sistema di difesa

[55] Intelligence and Security Committee of Parliament, *Annual Report 2016–2017*, 2017, https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/2016-2017_ISC_AR.pdf?attachauth=ANoY7crOzLFtUORYCl8L-nwRRyDIgciKFS8G_bclsCowz4ml3LSDAf8TgiRCvk_JXiCfBj5Beoj2NDlHJQ0wVLD3Lgk4VEK5QQj4aG6WKcY06smJCurew6dGzhlcQsqLD4tXTkmziuMWEpi4WA3O4ZtzkTSim-rQHF9Ep8o-ttsbCaSD80Nu800Nn1Gn6FGCbyd2lHQfEqga-JvbDgaRMh5hBE6uhoRnLEuQ25m2hZmj8TIJvp-iqUY%3D&attredirects=0, p.35.

[56] Marcus Willett, "Why the UK's National Cyber Force is an important step forward", in *IISS Analysis*, 20 novembre 2020, https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force.

[57] UK Government, *Working for JFC*, Joint Forces Command, https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment#contents.

[58] Governo britannico, *National Security Strategy and Strategic Defence and Security Review 2015*, novembre 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf.

[59] Secondo la revisione effettuata dal National Accounting Office, l'obiettivo della ACD è tra i pochi obiettivi che al febbraio 2019 erano stati implementati, fino a quel momento, senza subire ritardi. Per maggiori informazioni si veda:

cibernetica nazionale grazie ad un'analisi costante delle minacce e ad un conseguente aggiornamento delle infrastrutture tecnologiche.

Viene intesa inoltre la possibilità di mettere in atto operazioni cyber offensive a puro scopo di deterrenza, in altre parole anche in assenza di un attacco[60], pur sempre nel rispetto della legislazione nazionale e internazionale in materia[61].

La strategia getta poi le basi per la creazione del *National Cyber Security Centre* (Ncsc)[62] che, quale organo centrale per la sicurezza cibernetica a livello nazionale, gioca un ruolo di primo piano nel coordinamento delle politiche settoriali e lavora con ministeri e agenzie per l'attuazione dei programmi di sicurezza cibernetica. Il Ncsc si avvale della collaborazione con il Gchq che, attingendo alle informazioni di sicurezza riservate, permette al centro di avere una consapevolezza della situazione completa e supportata da un'elevata expertise tecnica.

Il Ncsc, con una previsione di impiego di 950 esperti entro il 2021[63], coordina anche le azioni del *Cyber Security Operations Centre*[64], ossia il centro di difesa e risposta e ad attacchi cibernetici diretti alle infrastrutture e sistemi del Ministero della Difesa, con la possibilità di assistenza delle forze armate in caso di attacco cyber dalla portata significativa.

La strategia nazionale di sicurezza cibernetica del 2016 ha visto una successiva allocazione di 1,9 miliardi di sterline nel quinquennio 2016-2021 dal governo britannico con un incremento del 55 per cento rispetto al periodo precedente, a riconoscimento dell'accresciuta minaccia cyber.[65] Inoltre, la strategia indica il lancio di due centri di innovazione cyber, nonché la creazione di un fondo per l'innovazione di difesa e cyber di 165 milioni di sterline nel periodo 2016-2021 da impiegare in procurement innovativo e *secure-by-design.* Viene anche facilitato lo sfruttamento delle conoscenze accumulate nella *Cyber Growth Partnership* tra governo, industria e università[66]. Queste azioni sono volte ad arrivare alla completa integrazione di capacità cibernetiche negli

---

National Audit Office, *Progress of the 2016–2021 National Cyber Security Programme*, HC1988, session 2017-2019, marzo 2019, https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf, p.30.

[60] Josh Gold, "The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'", in *CCDCoE.org*, Tallinn, 2020, https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf, p. 14.

[61] Governo britannico, *National Cyber Security Strategy 2016-2021*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, p. 25.

[62] Governo britannico, *National Cyber Security Strategy 2016-2021*, *cit.*, p. 28-29.

[63] National Audit Office, *Progress of the 2016–2021 National Cyber Security Programme*, *cit.*, p. 39.

[64] Hemanth Kumar, "UK MOD announced funding for new army cyber operations centres", in *Army Technology*, 23 maggio 2019, https://www.army-technology.com/news/british-army-cyber-operations-centres/.

[65] Intelligence and Security Committee of Parliament, *Annual Report 2016–2017*, op. cit., p. 35.

[66] Governo britannico, National Cyber Security Strategy 2016-2021, *cit.*, p. 58.

equipaggiamenti militari attuali e futuri, con lo scopo finale di poter integrare la difesa cibernetica nelle fasi di pianificazione, programmazione, acquisizione e impiego delle forze armate[67].

3.2 Le *offensive cyber operations*

Come delineato nella nota condivisa 1/18 del Ministero della Difesa sulle attività cyber ed elettromagnetiche[68], l'apparato di difesa include nelle *offensive cyber operations* anche intrusioni deliberate negli apparati informatici e nel network dell'avversario, con il preciso scopo di causare danno, distruzione o malfunzionamento di sistema. Nella relazione al parlamento 2016-2017 della commissione di sicurezza[69] viene effettuata una panoramica delle operazioni offensive attuabili, le quali vengono individuate come la capacità di:

i) rispondere ad attacchi cibernetici;
ii) ostacolare, degradare e disturbare le comunicazioni e i sistemi d'arma dell'avversario;
iii) attaccare sistemi e infrastrutture più grandi, con la possibilità di estendere il danno nel "mondo reale".

Lo sviluppo di queste capacità è stato assegnato al *National Offensive Cyber Programme* già nel 2014, grazie ad una partnership tra il Ministero della Difesa e il Gchq, mentre le segnalazioni di eventuali incidenti o tentativi di intrusione nelle infrastrutture del Ministero della Difesa sono rilevate dal *MoD Computer Emergency Response Team* (Modcert)[70] che opera nell'ambito del Ncsc.

Questione di rilevanza è rappresentata dalle regole d'ingaggio delle operazioni cibernetiche offensive. Al momento, infatti, non esiste un quadro regolamentare definito e accettato a livello internazionale che indichi le modalità di impiego dell'arma cyber. A tal riguardo il Regno Unito si è fatto promotore anche di iniziative come la *Global Conference on Cyberspace,* un forum di dialogo tra governi, settore privato e società civile per promuovere lo scambio di conoscenze e discutere le norme alla base di un comportamento responsabile nello spazio cibernetico[71].

La strategia attuale sottolinea l'importanza di operare a livello internazionale nel contrasto agli attacchi, promuovendo collaborazione anche attraverso framework collaborativi ad hoc. A tal proposito, insieme ad Australia, Canada, Nuova Zelanda e Stati Uniti, Londra fa parte del *Five Eyes network* che costituisce la più stretta partnership internazionale in materia di intelligence, nella

---

[67] Ministero della Difesa del Regno Unito, *Cyber Primer (2nd Edition)*, luglio 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.

[68] Ministero della Difesa del Regno Unito, *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities*, febbraio 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

[69] Intelligence and Security Committee of Parliament, *Annual Report 2016–2017*, *cit.*, p. 43.

[70] Ministero della Difesa del Regno Unito, Cyber Primer (2nd Edition), *cit.*, p. 70. Per una panoramica delle fasi di risposta ad un attacco cyber si veda pagina 55 dello stesso documento.

[71] Intelligence and Security Committee of Parliament, *Annual Report 2016–2017*, *cit.*, p. 45.

quale gli stati membri si sono impegnati a non "spiarsi" tra di loro e a condividere i segnali di intelligence che rilevano. Londra fa parte anche delle successive estensioni del Five Eyes Network[72], ossia del *Nine Eyes* e del *Fourteen Eyes*[73] network i cui paesi partecipanti hanno mano a mano minor accesso alle informazioni condivise e, di conseguenza, possono condividerne di meno[74].

[72] I Paesi del Five Eyes network sono Australia, Canada, Nuova Zelanda, Regno Unito e Stati uniti.
[73] I Paesi del Nine Eyes network includono quelli del Five Eyes Network più Danimarca, Francia, Paesi Bassi e Norvegia. Il Fourteen Eyes Network, infine, include anche Belgio, Germania, Italia, Spagna e Svezia.
[74] Sandra Pattison, "Five Eyes, Nine Eyes and Fourteen Eyes: Is Big Brother Watching You?", in *Cloudwards*, Maggio 2020, https://www.cloudwards.net/five-eyes/.

4. Francia

4.1 La strategia e la struttura operativa cyber

Il tema della difesa cibernetica gode di particolare attenzione in Francia. Ad inizio 2018, il Primo Ministro Edouard Philippe ha affidato al Segretariato generale della difesa e della sicurezza nazionale (*Secrétariat général de la défense et de la sécurité nationale*, Sgdsn) il compito di stilare una strategia di contrasto alle minacce cibernetiche, che ha portato a quello che viene definito un Libro bianco per il contrasto della minaccia cyber[75]. Il documento, a uso interministeriale, fornisce un quadro chiaro del rischio cibernetico e sottolinea come, per assicurare una resilienza a tutto tondo, sia necessario non solo rafforzare le infrastrutture tecnologiche del Paese e avere le capacità di risposta ad un attacco di questo tipo, ma anche diffondere una cultura della sicurezza cibernetica a livello della popolazione[76].

Secondo la strategia francese, la dissuasione cibernetica presenta tre problematiche principali[77]. La prima attiene all'impossibilità di seguire una posizione pubblica chiara e credibile, ovvero di esplicitare le modalità e i sistemi attraverso i quali dovrebbe essere effettuata la dissuasione cyber. Questa difficoltà è generata dal fatto che, a differenza della deterrenza convenzionale o nucleare, conoscere le modalità di risposta implica un'evoluzione delle modalità di attacco e una conseguente inefficacia della dissuasione stessa. Il secondo limite è collegato alle conseguenze di un attacco cyber, le quali non necessariamente causano effetti distruttivi come nel caso dell'impiego dell'arma nucleare. Infine, nella dissuasione cibernetica non è possibile assicurare stabilità internazionale nella proliferazione di sistemi informatici che possono essere impiegati per scopi offensivi, da un lato perché possono essere utilizzati anche per impieghi non malevoli, dall'altro perché la tecnologia può essere detenuta anche da attori non statali, con la conseguente impossibilità di imporre un limite certo alla loro proliferazione.

Da un punto di vista operativo, il Libro bianco della difesa del 2008 ha gettato le basi per l'istituzione dell'Agenzia nazionale per la gestione degli attacchi informatici e la protezione del sistema d'informazione dello Stato (*Agence nationale de la sécurité des systèmes d'information*, Anssi)[78] in seno al Sgdsn. La creazione dell'agenzia a carattere interministeriale ha anche segnato la separazione tra le capacità offensive — raccolta delle informazioni e operazioni di attacco — e le capacità difensive — protezione e difesa degli assetti. Come si legge nella strategia, questa divisione permette una reazione agli attacchi cibernetici più veloce e un migliore coordinamento

[75] SGDSN, *Strategic review of cyber defence*, febbraio2018, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.
[76] SGDSN, Strategic review of cyber defence, *cit.*, parte 1.
[77] *Ibid.*, p. 38.
[78] Legifrance, *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 »*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212/.

con la difesa cibernetica militare[79]. Coordinamento assicurato dal *Centre de coordination des crises cyber* (C4), che riunisce i vari ministeri interessati[80] e che permette di attuare la risposta più consona in relazione all'entità dell'attacco. In caso di evento cibernetico ostile di portata nazionale o diretto verso le forze armate, sarà il Ministero della Difesa a intervenire[81].

L'agenzia coopera con il comando per la difesa cibernetica (*Commandant de la cyberdéfense*, Comcyber), istituito nel 2017 e responsabile della sicurezza e difesa cyber di sistemi, infrastrutture e operazioni del Ministero della Difesa, il quale aiuta ad acquisire un quadro completo della minaccia[82].
La costante evoluzione tecnologica in ambito cyber, così come l'elevato numero di attacchi subiti dal Ministero della Difesa[83], hanno portato ad inserire nella legge di programmazione militare (*Loi de Programmation Militaire*, Lpm) 2019-2025 un investimento di 1,6 miliardi di euro nella lotta nel dominio cibernetico e un incremento di personale pari a 1.000 "combattenti cyber", da distribuire tra il Comcyber, , la *Direction générale de la sécurité extérieure* (Dgse) e la *Direction générale de l'armement* (Dga) per arrivare al 2025 con un totale di 4.500 unità. Di questi, circa metà verrà dedicata alla protezione dei sistemi d'informazione, un quarto alla difesa cyber e la restante parte alle operazioni cibernetiche offensive[84]. Dell'allocazione totale, circa 200 milioni di euro verranno investiti nello stesso periodo di riferimento per la costruzione del cosiddetto "*temple de la cyber défense*" a Saint-Jacques de la Lande, che ospiterà una parte dei 1.000 esperti cyber aggiuntivi previsti dalla Lpm[85].

Con riferimento alla Nato, la strategia del 2018 aveva sottolineato l'importanza di portare avanti i lavori di rafforzamento della capacità cibernetiche degli alleati per mezzo di un maggior impegno all'interno del *Cyber defence Pledge*, così come attraverso una migliore integrazione delle capacità di difesa cyber[86] negli scenari operativi e nelle missioni Nato[87]. Concetto, quest'ultimo,

---

[79] Aude Géry, "La stratégie française de cyberdéfense", in *Brennus 4.0*, marzo 2020, https://www.penseemiliterre.fr/ressources/30147/14/la_strategie_francaise_de_cyberdefense.pdf.

[80] 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.

[81] Senato della Repubblica francese, *Délégation parlementaire au renseignement - Rapport d'activité 2019-2020*, dicembre 2020, http://www.senat.fr/rap/r19-506/r19-50638.html#:~:text=b)%20Le%20centre%20de%20coordination%20des%20crises%20cyber%20(C4)&text=Il%20est%20un%20m%C3%A9canisme%20permanent,minist%C3%A8res%20concern%C3%A9s%20par%20la%20crise.

[82] SGDSN, *Strategic review of cyber defence*, *cit.*, p. 47.

[83] La Ministra della Difesa Parly ha affermato che nei primi nove mesi del 2018 il Ministero ha dovuto reagire a più di 700 attacchi cyber. Per maggiori informazioni si veda: Florence Parly, *Stratégie cyber des Armées*, gennaio 2019, https://www.defense.gouv.fr/content/download/551517/9394183/20190118%20-%20Strat%C3%A9gie%20cyber%20des%20Arm%C3%A9es.pdf.

[84] Julien Nocetti, *Cyber guerre : la montée des périls*, Science&Vie, 06 giugno 2019, https://www.ifri.org/sites/default/files/atoms/files/044_051_cyberguerre-2.pdf.

[85] "Déclaration de Mme Florence Parly, ministre des armées, sur la cyberdéfense, à Rennes le 7 septembre 2020", in *Vie publique*, 7 settembre 2020, https://www.vie-publique.fr/discours/276401-florence-parly-07092020-cyberdefense.

[86] In merito alla dottrina di difesa cibernetica, la Francia ha adottato un approccio coerente con quella interalleata. Per una panoramica dell'architettura dottrinale e operativa si veda: CICDE, *Domaine 3.20 Cyberdéfense*, https://www.cicde.defense.gouv.fr/images/documentation/architectures/20190805_DOM320.pdf.

ulteriormente ribadito in più occasioni dalla Ministra della Difesa, Florence Parly, la quale ha ribadito che la Francia non esiterà ad impiegare l'arma cibernetica nelle operazioni militari[88] e che gli operatori di settore, nello svolgimento delle loro funzioni, beneficeranno delle stesse protezioni dei militari impiegati nelle operazioni all'estero[89].

4.2 Cooperazione internazionale e con l'industria

A livello regolamentare, la Francia ha assunto un approccio propositivo nella ricerca di un quadro di regolamenti condiviso internazionalmente. A tal proposito, nell'ambito del Gruppo di esperti governativi (*Group of Governmental Experts*, Gge) dell'Onu, Parigi ha proposto l'interdizione delle pratiche di *hack-back*[90] da parte di privati e l'imposizione di controlli alle esportazioni di componenti cyber che possono essere impiegate per fini malevoli, ma le proposte francesi non sono state accolte a causa della mancanza di consenso tra i rappresentanti dei 25 stati membri del Gge[91]. Queste proposte sono state parte integrante di un'altra iniziativa francese promossa sempre sotto l'egida delle Nazioni Unite e conosciuta come l'"Appello di Parigi"[92]. Per assicurare un utilizzo più sicuro dello spazio cibernetico e una maggiore sicurezza cyber a livello nazionale, la Francia ha richiesto la collaborazione degli Stati con attori privati, università e centri di ricerca, al fine di trovare una base di comprensione comune e ridurre eventi illeciti.

Inoltre, per quanto riguarda il quadro internazionale, la Francia è parte del cosiddetto *Fourteen Eyes Agreement*, conosciuto più formalmente come *Sigint Seniors Europe*. Questo accordo di condivisione interstatale di *intelligence* unisce la Francia con 13 altri Paesi in tre continenti[93].

Dal punto di vista industriale, la Francia ha prestato molta attenzione allo sviluppo nazionale ed europeo dell'industria nel dominio cibernetico, tanto da dedicare una parte della strategia del 2018 al partenariato tra le agenzie governative e le imprese del settore[94]. Nel novembre 2019, su richiesta della Ministra Parly, è stata sottoscritta una convenzione cyber tra il Ministero e le otto maggiori industrie fornitrici di sistemi d'arma in Francia, la quale prevede la creazione di specifici

---

[87] SGDSN, Strategic review of cyber defence, *cit*., p. 92.
[88] « Déclaration de Mme Florence Parly, ministre des armées, sur la cyberdéfense, à Rennes le 7 septembre 2020", *cit*.
[89] Florence Parly, *Stratégie cyber des Armées*, *cit.*
[90] Con l'espressione *hack-back* si intende tutto lo spettro di soluzioni di contrasto e non solo quelle di infiltrazione nei sistemi informatici degli avversari in risposta ad un attacco cibernetico.
[91] SGDSN, Strategic review of cyber defence, *cit.*, p. 36.
[92] France Diplomatie, *Cybersécurité : Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberespace*, https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/les-domaines-d-action-de-la-diplomatie-numerique-francaise/garantir-la-securite-internationale-du-cyberespace-a-travers-le-renforcement-de/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la.
[93] Sven Taylor, Five Eyes, Nine Eyes, 14 Eyes – Explained, in *Restore Privacy*, settembre 2020, https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/.
[94] SGDSN, Strategic review of cyber defence, *cit.*
[94] Legifrance, *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 », cit.*

gruppi di lavoro per poter meglio rispondere alle esigenze francesi di difesa cibernetica[95]. Più recentemente, tra le iniziative di rilievo portate avanti dal Ministero della Difesa all'interno del piano d'azione per le piccole e medie imprese (*Action Petites ou Moyennes Entreprises, Action PME*)[96] vi è la *diagnostic de cyberdéfense* (Diag Cyber), un sistema che permette alle imprese di verificare la resilienza cibernetica dei propri prodotti e di migliorare i propri sistemi informatici grazie alla sovvenzione del 50 per cento delle spese sostenute e per un totale di 4,5 milioni di euro per l'intero programma[97].

[95] Ministero della Difesa, Signature d'une convention cyber entre Florence Parly, ministre des Armées, et les industriels de défense, novembre 2019,https://www.defense.gouv.fr/dga/actualite/signature-d-une-convention-cyber-entre-florence-parly-ministre-des-armees-et-les-industriels-de-defense

[96] Tra le altre si veda: Ministero della Difesa, *Cyberdéfense et innovation : visite de la ministre des armées Florence Parly à Rennes*, ottobre 2019, https://www.defense.gouv.fr/dga/actualite/cyberdefense-et-innovation-visite-de-la-ministre-des-armees-florence-parly-a-rennes.

[97] "Déclaration de Mme Florence Parly, ministre des armées, sur la cyberdéfense, à Rennes le 7 septembre 2020", *cit*.

5. Germania

5.1 La divisione operativa della strategia cyber e i limiti legislativi

La Germania ha pubblicato la sua prima strategia per la sicurezza cyber nel 2011, per aggiornarla nel 2016 con un approccio interministeriale[98] che prevede un'azione da parte sia del governo federale che a livello delle singole amministrazioni dei Länder. Anche nella strategia del 2016 un'attenzione particolare è rivolta alla necessità di avere un Centro Nazionale di Risposta Cyber al quale far confluire tutte le segnalazioni di eventuali attacchi, e dal quale far partire una risposta coordinata e in linea con la legislazione nazionale e internazionale in materia.

Un'ulteriore novità introdotta con la strategia del 2016 è la menzione, per la prima volta, della possibilità di effettuare operazioni cyber offensive in risposta ad un attacco[99]. Essa indica inoltre che il Servizio di controspionaggio militare (*Militärische Abschirmdienst*, MAD) ha la responsabilità di rispondere ad eventuali eventi malevoli nel dominio cibernetico. Si prevede, nei limiti generali fissati dalla costituzione tedesca, un contributo delle forze armate (*Bundeswehr*) al raggiungimento di più alti livelli di prontezza operativa, eventualmente tramite l'azione di team di risposta agli incidenti in capo al Ministero della Difesa.

In Germania la difesa cyber è costituzionalmente demandata alla Bundeswehr, è gestita dal Ministero della Difesa e deve essere sottoposta alla legislazione nazionale e internazionale che regola le attività delle forze armate. Tuttavia, data la forte connessione tra sicurezza e difesa cyber, la Strategia nazionale del 2016 identifica un chiaro collegamento con il Libro bianco della difesa pubblicato nello stesso anno[100] e crea un nesso tra le capacità di cyber defence delle forze armate e quelle di risposta nel quadro della sicurezza cibernetica, indicando le prime come complementari alla formazione della struttura di sicurezza cibernetica nazionale, sebbene vengano gestite separatamente. Come accaduto anche in altri Paesi, la Germania è impegnata nel processo di consolidamento delle infrastrutture precedentemente sviluppate a livello di singola forza armata, con l'obiettivo di arrivare ad avere un unico centro interforze, formato da unità operative militari separate[101], che è previsto utilizzi, in futuro, anche l'intelligenza artificiale e metodi di analisi di *big data* per la formulazione di scenari quanto più completi possibile[102].

---

[98] 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.

[99] Sven Herpig, Robert Morgus e Amit Sheniak, "Active Cyber Defense - A comparative study on US, Israeli and German approaches", *cit.*, p.4.

[100] Martin Schallbruch e Isabel Marie Skierka, "The Evolution of German Cybersecurity Strategy", in *Cybersecurity in Germany*, luglio 2018, pp. 15-29, https://www.researchgate.net/publication/326511119_The_Evolution_of_German_Cybersecurity_Strategy.

[101] Cyber Security Strategy for Germany 2016, *cit.*, p. 25.

[102] Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr", *Connections QJ* 19, no. 1 (2020): 9-19 https://doi.org/10.11610/Connections.19.1.02.

Data la costante evoluzione del dominio cyber, già nel 2011 Berlino istituì un Consiglio Nazionale sulla Sicurezza Cibernetica, al quale partecipano rappresentanti dei ministeri dell'interno, difesa, esteri, affari economici ed energetici, giustizia e protezione dei consumatori, finanza, educazione e ricerca, e trasporti e infrastrutture digitali, così come rappresentanti del settore privato, con il fine di compiere i dovuti passi in avanti nell'aggiornamento della strategia cyber nazionale[103].

A livello operativo, la difesa cibernetica della Germania viene portata avanti da diversi attori, a seconda della tipologia di attacco e dell'obiettivo.

A partire dal 2009 e ancor di più a seguito della direttiva europea Network and Information Security (Nis Directive) del 2016, l'ufficio per la sicurezza nelle tecniche informative (*Bundesamt für Sicherheit in der Informationstecknik*, Bsi) si occupa dell'operatività della difesa cibernetica[104]. Per fare ciò, il Bsi monitora il network del governo federale, indaga sugli incidenti di sicurezza e attua le necessarie contromisure difensive. Da un punto di vista militare, le forze armate tedesche hanno limitate possibilità di collaborazione con gli altri organi statali a causa di limiti costituzionali che confinano il supporto delle forze armate a operazioni definite di "assistenza amministrativa"[105] — come può essere considerato il supporto al Bsi – le quali non vengono considerate delle vere e proprie operazioni. Diverso è invece il caso della risposta ad un attacco cyber che per entità[106] e magnitudine richiede il dispiegamento delle forze armate. In questo caso, anche nel dominio cibernetico, le forze armate tedesche, per poter operare sul territorio nazionale, hanno bisogno di approvazione parlamentare, che potrebbe richiedere troppo tempo in caso di attacco cyber. Nel caso invece di operazioni di difesa cibernetica all'interno di framework cooperativi, l'approvazione del Bundestag della missione è sufficiente a permettere l'impiego anche di capacità di difesa cyber.

5.2 Attenzione al personale e cooperazione internazionale

A seguito della pubblicazione del Libro bianco della difesa del 2016, venne creato un Comando per lo spazio informatico e cibernetico (*Kommando Cyber- und Informationsraum*, Cir), incaricato delle operazioni in rete e che prevede un personale di ben 14.000 unità una volta raggiunta la piena capacità operativa, pianificata per il 2021[107], e che è titolato ad intervenire nei casi di attacchi diretti verso le strutture delle forze armate o governative da parte di un altro Paese. Tuttavia, data la peculiarità della minaccia cyber, non è sempre possibile definire fin dal principio quale sia il l'autore dell'attacco, creando così la necessità di dover coordinare le varie autorità coinvolte per la

[103] Cyber Security Strategy for Germany 2016, *cit*., p. 34.
[104] Bundesamt für Sicherheit und Informationstechnik, *Cyber Sicherheit*, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/aktivitaeten_node.html.
[105] M. Schallbruche I. Skierka, "Cybersecurity in Germany", Springer Briefs, in *Cybersecurity*, p. 36, https://doi.org/10.1007/978-3-319-90014-8_4.
[106] Per l'impiego della Bundeswehr sul territorio nazionale, è necessario che l'attacco avvenga da parte di un attore statuale.
[107] Alessandro Rugolo, "Anche La Germania Ha La Sua Quarta Forza Armata", in *Difesa online*, luglio 2018, https://www.difesaonline.it/evidenza/cyber/anche-la-germania-ha-la-sua-quarta-forza-armata.

risposta[108] e regolare meglio l'eventuale cooperazione delle forze armate[109]. A tal fine, nel 2011 il governo federale istituì il Centro nazionale per la difesa cyber (*Cyber-Abwehrzentrum*, Cyber-AZ) al quale sono attribuiti esclusivamente compiti di coordinamento delle varie entità[110].

Nelle varie strategie nazionali sul cyberspace, la Germania ha sempre sottolineato la necessità di operare all'interno di quadri regolatori quanto più completi possibile e attraverso la costituzione di partnership per raggiungere maggiori livelli di sicurezza e prontezza operativa, anche nel caso di risposta ad attacchi cibernetici[111]. Da un punto di vista legale, allo stato attuale le operazioni di difesa attiva non sono esplicitamente regolate ed è in corso un dibattito a livello nazionale sull'opportunità di prevedere azioni di *hack-back*[112]. A livello internazionale, la Germania è membro del Gge[113], così come del *Fourteen Eyes network*.

Altro aspetto considerato con attenzione dal governo tedesco è la cooperazione con le industrie del settore per garantire al Paese sistemi e infrastrutture quanto più all'avanguardia possibile. A partire dal 2018, il Ministero della Difesa e quello dell'Interno hanno previsto l'istituzione di un'Agenzia per l'Innovazione nella sicurezza cibernetica con il compito di sottoscrivere contratti per progetti di ricerca ad elevato potenziale tecnologico[114]. L'agenzia è stata istituita solo nell'Agosto del 2020 e riceverà un finanziamento complessivo di 350 milioni di euro fino al 2023[115].

[108] M. Schallbruche I. Skierka, "Cybersecurity in Germany", *cit.*,p.37.
[109] Matthias Schulze, "German Military Cyber Operations are in a Legal Gray Zone", in *Lawfareblog.com*, aprile 2020, https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone.
[110] M. Schallbruche I. Skierka, *Cybersecurity in Germany*, "Cybersecurity in Germany", *cit.*, p.39.
[111] Cyber Security Strategy for Germany 2016, *cit.*, p. 21.
[112] Matthias Becker, "„Aktive Cyber-Abwehr" für Deutschland. Der geheime Krieg imNetz", in *Deutschlandfunk*, ottobre 2020, https://www.deutschlandfunk.de/aktive-cyber-abwehr-fuer-deutschland-der-geheime-krieg-im.724.de.html?dram:article_id=461140.
[113] Il Gge è composto da 25 rappresentanti di altrettanti stati. Per maggiori informazioni sulla composizione e compiti si veda: United Nations, *Group of Governmental Experts*, https://www.un.org/disarmament/group-of-governmental-experts/.
[114] Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr",*cit.*
[115] Deutsche Welle, "Germany launches cybersecurity agency to strengthen 'digital sovereignty'", in *Dw.com*, agosto 2020, https://www.dw.com/en/germany-launches-cybersecurity-agency-to-strengthen-digital-sovereignty/a-54529134.

6. Spagna

6.1 Aggiornamento strategico e ristrutturazione delle forze armate

Secondo alcune statistiche, la Spagna è tra i Paesi europei in cui avviene il maggior numero di attacchi in ambito cyber[116]. Mentre alcuni sono diretti verso settori non strategici, altri rappresentano uno spionaggio cibernetico con gravi implicazioni, come nel caso dell'attacco prolungato avvenuto durante il 2019 ai danni del Ministero della Difesa spagnolo, con il fine di reperire informazioni industriali sensibili[117].

La strategia nazionale per la sicurezza cibernetica della Spagna è stata aggiornata nel 2019[118] per tenere in considerazione le disposizioni della Strategia di sicurezza nazionale del 2017. Tuttavia, a causa del Covid-19, è stata evidenziata la necessità di aggiornare il documento strategico nel 2021, per tenere in considerazione le possibili conseguenze legate al dominio cyber di pandemie prolungate. In quest'ottica, il massiccio ricorso al lavoro da casa e un maggiore utilizzo delle piattaforme online rendono indispensabile un adeguamento dei sistemi e delle strategie pensate per contrastare attacchi cyber e rendere le strutture informatiche più resilienti, includendo in ciò anche una migliore formazione del personale e degli utenti, così come evidenziato dalla EU Security Union Strategy[119].

Nel frattempo, a maggio 2020 è stato emanato il Decreto reale n. 521/2020[120] sull'organizzazione di base delle forze armate che conferisce molto rilievo alla necessità di avere personale, strutture e sistemi di difesa adeguatamente formati e all'avanguardia tecnologica per permettere di effettuare la trasformazione digitale delle forme armate spagnole, anche in considerazione dell'accresciuta minaccia cyber.

Come negli altri Paesi Nato, la difesa cibernetica è inserita nel più ampio contesto della sicurezza cyber che comprende ma non si limita alle attività legate alle forze armate. Questo approccio è stato ulteriormente ampliato per mezzo della Direttiva sulla difesa nazionale del giugno 2020, nella quale viene affermato che l'attuale quadro di sicurezza internazionale e le minacce emergenti rendono indispensabile una migliore e più stretta collaborazione delle forze armate con

---

[116] EnigmaSoft, *Top 20 Countries Found to Have the Most Cybercrime*, https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/.

[117] Miguel Gonzales, "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.

[118] Spanish approach to cybersecurity, Decalogue CCN-CERT, giugno 2019, p.8, https://www.ccn.cni.es/index.php/en/docman/documentos-publicos/23-decalogue-spanish-approach-to-cybersecurity-2018/file.

[119] European Commission, *Communication from the commission to the european parliament, the European council, the council, the European economic and social committee and the committee of the regions on the EU Security Union Strategy*, luglio 2020, https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf.

[120] Agencia Estatal Boletín Oficial del Estado, *Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas*, 21 maggio 2020, https://www.boe.es/eli/es/rd/2020/05/19/521/con.

il sistema di sicurezza nazionale, per assicurare la protezione dei cittadini e dello stato all'interno di un quadro integrato[121]. In ambito cibernetico, già nel 2008 la Spagna aveva provveduto a costituire due centri di risposta agli attacchi cyber: l'*Istituto Nacional de Ciber seguridad Computer Emergency Response Team* (Incibe-Cert) e l'*Instituto Nacional de Ciber seguridad Computer Emergency Response Team* (Ccn-Cert). Mentre il primo è un team di risposta rapida agli attacchi cibernetici perpetrati ai danni di cittadini, imprese e altri gruppi di interesse, il Ccn-Cert è concentrato nella risposta ad attacchi diretti contro istituzioni governative[122]. In ambito militare, il Comando interforze di difesa cyber (*Mando Conjunto de Ciberdefensa de las Fuerzas Armadas*, Mccd)[123], alle dirette dipendenze dello Stato maggiore della Difesa spagnolo, è la struttura responsabile per l'esecuzione delle azioni collegate alla difesa cibernetica delle infrastrutture informatiche e dei sistemi della difesa spagnola. In particolare, l'Mccd ha il compito di attuare le azioni necessarie ad assicurare l'integrità cibernetica di tali strutture e delle capacità militari inclusi i sistemi cyber. Istituito con decreto ministeriale 10/2013[124], il comando è anche l'organismo responsabile per contribuire alla risposta appropriata in caso di attacco cibernetico ai danni della nazione. Data la vastità del dominio cibernetico, l'azione del Mccd deve osservare delle linee operative che tengano conto della cosiddetta lista degli assetti prioritari in ambito cibernetico, determinando la tipologia di risposta e la prioritizzazione dei suddetti assetti da proteggere, in base all'entità del possibile danno di un attacco cyber[125]. Il Ministero della Difesa spagnolo è dotato anche di un team di risposta alle emergenze informatiche che avvengono nel settore militare (Espcertdef) che coopera con gli altri Cert nazionali di natura civile[126].

Dal momento che il comando interforze è alle dipendenze del Capo di Stato maggiore della difesa, è presumibile pensare che le operazioni cyber, difensive o meno, siano integrate nella catena di comando anche in occasione di impiego multinazionale delle forze armate, siano esse sotto egida Nato, Eu o Onu. Ciononostante, in caso di assenza di uno scontro armato dichiarato, non è al momento prevista la possibilità di condurre operazioni offensive, a differenza di quanto avviene nel Regno Unito[127].

---

[121] Ministero della Difesa di Spagna, *Directiva de Defensa Nacional 2020*, https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2020.pdf.

[122] Bernard Meyer, "Cybersecurity in Spain", in *Cybernews*, novembre 2019, https://cybernews.com/security/cybersecurity-in-spain/.

[123] Agencia Estatal Boletín Oficial del Estado, *Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas*, *cit.*, articolo 13.

[124] Collecciòn Legislativa del Ministerio de Defensa, ano 2013, Numero 45, https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF457.pdf.

[125] Tcol. Javier Lòpez de Turiso y Sànchez, Concepto de las Operationes en el Cyberespacio, 25 maggio 2016, p.17-8, https://slideplayer.es/slide/10478974/

[126] Spanish approach to cybersecurity, *cit*., p. 13 e 19.

[127] Centro Superior de Estudios de la Defensa Nacional, *El Cyberspacio. Nuevo Escenario de Confrontaciòn, Monografias del CESEDEN*, n. 126, febbraio 2012, p. 52, https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf.

6.2 Cooperazione industriale e formazione

La strategia di sicurezza cibernetica della Spagna conferisce particolare rilevanza alla cooperazione internazionale e alla sensibilizzazione della popolazione e dei funzionari nell'uso corretto dello spazio cibernetico. Con riferimento al primo punto, a livello europeo la Spagna è alla guida di progetti rientranti nell'ambito dello *European defence industrial development programme* (Edidp) che sono connessi al raggiungimento di più elevati livelli di sicurezza cibernetica. Tra questi, Madrid coordina imprese e istituti di ricerca di quattro Paesi[128] nel progetto *European Cyber Situational Awareness Platform* (Ecysap) che mira a fornire un quadro integrato delle possibili minacce cyber che possono colpire i sistemi di difesa per permettere alle forze armate di attuare prontamente risposte, grazie anche al supporto di strumenti di decision-making[129].

Per quanto riguarda invece l'aspetto formativo, la strategia si concentra particolarmente sulla necessità di fornire training specializzato agli operatori del settore, siano essi civili o appartenenti alle forze armate. Il piano di formazione spagnolo viene rimesso al Centro Criptografico Nazionale (Ccn), ma la formazione specifica può avvenire anche per mezzo di particolari partenariati, come quello sottoscritto tra il Ministero della Difesa e l'Istituto Nazionale di Cybersecurity (Incibe) nel 2020. L'accordo prevede la realizzazione di corsi di formazione per giovani studenti, con l'obiettivo di creare maggiori possibilità di impiego dei talenti nazionali nella difesa cibernetica della Spagna[130].

[128] Commissione europea, *ECYSAP – European Cyber Situational Awareness Platform*, 2020, https://ec.europa.eu/commission/presscorner/api/files/attachment/865731/EDIDP%20-%20ECYSAP.pdf.
[129] Governo spagnolo*, Leon's Proposal, Spanish proposal to host the European Cybersecurity Industrial, Technology and Research Competence Centre*, p. 106, https://www.consilium.europa.eu/media/46697/spanish-proposal-to-host-the-european-cybersecurity-industrial-technology-and-research-competence-centre.pdf.
[130] Alfonso de Castaneda, "Defensa capacitará a 200 militares españoles en materia de ciber seguridad", in *Zona movilidad*, marzo 2020, https://www.zonamovilidad.es/defensa-formara-militares-espanoles-ciberseguridad-cybersecurity-summer-bootcamp.

Conclusioni

La minaccia cyber

Negli ultimi due decenni i casi di cyber attacks sono aumentati considerevolmente, tanto da rappresentare una vera e propria minaccia alla difesa dello stato. Per limitare l'occorrenza di attacchi cibernetici, a livello internazionale sono state portate avanti numerose iniziative volte alla regolamentazione delle azioni lecite che possono essere effettuate nello spazio cibernetico, ma con limitati risultati dovuti a divergenze di utilizzo del cyberspace, soprattutto da attori statali come Russia e Cina.

Il problema della scarsa regolamentazione viene amplificato da due ulteriori fattori. In primo luogo, se un attacco convenzionale può essere perpetrato da stati o gruppi terroristici, un attacco cibernetico può essere portato a termine da un pool di attori molto più ampio, incrementando la possibilità di occorrenza di un attacco cibernetico, la cui paternità è solitamente di difficile individuazione. In secondo luogo, la veloce innovazione tecnologica che interessa il settore impone un'attenzione e un investimento costanti nelle tecnologie dedicate al contrasto, fattore che implica l'impiego di personale tecnico altamente specializzato e di cui gli stati oggetto dell'analisi non sono sufficientemente dotati.

La risposta alleata

La potenziale pervasività degli attacchi cibernetici ha portato la Nato a dichiarare il cybespace come dominio operativo già nel 2016, di fatto compiendo un salto di qualità nell'approccio verso questo tipo di minaccia. Questi attacchi possono causare anche l'attivazione della clausola di difesa collettiva ai sensi dell'articolo 5 del Trattato dell'Atlantico del Nord, a riconoscimento del fatto che la componente cibernetica degli scontri diventerà sempre più parte integrante degli conflitti convenzionali. Allo stato attuale la difesa cibernetica è inserita a supporto dei comandi operativi terrestre, navale e aereo, ma è aperta la possibilità della creazione futura di un comando Nato per le operazioni cyber, a valle di un processo di formulazione di dottrine e sviluppo capacitivo ancora nella fase iniziale. Ciononostante, l'Ncsc e l'Ncirc della Nato forniscono supporto nel monitoraggio costante e nella risposta in caso di attacco cibernetico, mettendo a disposizione dei Paesi membri anche i Cyber Rapid Reaction Teams.

La difesa cibernetica a livello alleato non si limita alla creazione delle strutture di comando e all'impiego di personale dedicato, ma comprende anche delle partnership con attori diversi. La necessità di dotare l'Alleanza atlantica di equipaggiamenti all'avanguardia tecnologica ha portato, già nel 2014, alla costituzione di specifiche partnership con le industrie del settore cibernetico. La cooperazione Nato-Ue ha inserito già nel 2016 la dimensione cyber tra le aree prioritarie in cui collaborare.

Esigenze nazionali

L'analisi dei cinque casi studio nazionali ha portato all'individuazione di differenti approcci verso la difesa cibernetica a riprova di quanto ci sia ancora da fare nella definizione di dottrine e procedure condivise. Tra gli stati considerati vi è una sostanziale divisione tra i Paesi che prevedono la possibilità di effettuare solo azioni difensive e quelli che invece puntano sulla possibilità e capacità di portare a termine operazioni offensive anche in assenza di un attacco cyber.

Tra i primi vi sono la Germania e la Spagna, che intendono la deterrenza cibernetica come la capacità dello stato di rispondere tempestivamente e adeguatamente ad un attacco cyber, attuando quello che viene definito come *hack-back*. Ulteriori differenze tra Berlino e Madrid attengo alla possibilità di impiego delle forze armate sul territorio nazionale in caso di attacco, che nel caso della Germania ha bisogno della preventiva approvazione parlamentare. È importante sottolineare, tuttavia, come questa procedura mal si adatti alla velocità di reazione necessaria per limitare o evitare i danni di un attacco cibernetico: le tempistiche parlamentari, nei casi che richiedono azioni rapide e mirate, potrebbero causare l'incapacità dello stato di proteggere i suoi interessi primari e ostacolare di conseguenza la difesa nazionale.

Londra, Parigi e Washington hanno invece una diversa comprensione delle possibilità derivanti dall'uso attivo della cyber defence. Per le tre capitali, difesa e deterrenza cyber equivale ad assicurare non solo la capacità di reazione in caso di attacco cibernetico, ma anche la possibilità di azione preventiva ai danni di potenziali avversari, siano essi statali o meno. È secondo questa logica che, ad esempio, il Regno Unito ha portato a termine un attacco cibernetico ai danni dell'Isis già nel 2016.

Nonostante queste differenze, è possibile delineare delle esigenze condivise tra i cinque Paesi considerati che possono essere schematizzate come segue:

- Necessità di avere un quadro regolamentare e dottrinale condiviso a livello Nato, Ue e internazionale;
- Migliore integrazione della componente cyber nelle strutture di comando nazionali e alleate;
- Collaborazione più strutturata e strategica con imprese e mondo della ricerca;
- Più elevati investimenti nell'aggiornamento delle capacità cibernetiche;
- Formazione specialistica del personale militare volto alla protezione dalla minaccia cyber;
- Maggiore sensibilizzazione dei funzionari statali, dei gestori delle infrastrutture critiche e in generale della popolazione nell'utilizzo del cyberspace.

Lista degli acronimi

ACD	Active Cyber Defence
ACO	Allied Command Operations
ACT	Allied Command Transformation
Action PME	Action Petites ou Moyennes Entreprises
AFCYBER	24th Air Force
AI	Artificial Intelligence
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARCYBER	Army Cyber Command
BSI	Bundesamt für Sicherheit in der Informationstecknik
C4	Centre de coordination des crises cyber
CCDCoE	Cooperative Cyber Defence Center of Excellence
CCN	Centro criptografico nazionale
CCN-CERT	Centro Criptológico Nacional Computer Emergency Response
CDMB	Cyber Defence Management Board
CIR	Kommando Cyber - undInformationsraum
COMCYBER	Commandant de la cyberdéfense
CSSS	Cyber Security Support Services
CYBER-AZ	Cyber-Abwehrzentrum
CyOC	Cyberspace Operations Centre
DGA	Direction générale de l'armement
DGSE	Direction générale de la sécurité extérieure
DIAG CYBER	Diagnostic de cyberdéfense
ECYSAP	European Cyber Situational Awareness Platform
EDIDP	European defence industrial development programme
EDT	Emerging and Disruptive Technologies
FCC/C10F	US Fleet Cyber Command 10th Fleet
GCHQ	Government Communication Headquarter
GGE	Group of Governmental Experts
INCIBE	Istituto Nazionale di Cybersecurity
INCIBE-CERT	Instituto Nacional de Ciberseguridad Computer Emergency Response Team

LPM	Loi de Programmation Militaire
MAD	Militärische Abschirmdienst
MARFORCYBER	Marine CorpsForces Cyberspace
MCCD	Mando Conjunto de Ciberdefensa de las Fuerzas Armadas
MODCERT	Ministry of Defence Computer Emergency Response Team
MoU	Memorandum of Understanding
NCIA	Nato Communications and Information Agency
NCIRC	Nato Computer Incident Responce Capability
NCISS	Nato Communications and Information Systems School
NCSC	Nato Cyber Security Center
NCSC	National Cyber Security Centre
NDPP	Nato Defence Planning Process
NFIU	Nato Force Integration Unit
NICP	Nato Industry Cyber Partnership
NIS	Network and Information Security
NSA	National Security Agency
SGDSN	Secrétariat général de la défense et de la sécurité nationale
USCYBERCOM	US Cyber Command

Lista degli intervistati

Arteaga Felix	Ricercatore Senior, Real Instituto Elcano
Colom-Piella Guillem	Direttore Accademico dipartimento di Scienze Politiche e dell'Amministrazione, Universidad Pablo de Olavide
Fojon Enrique	Colonnello e dottore in Relazioni internazionali, già Capo Unità per la trasformazione delle Forze Armate e consigliere del Ministero della Difesa spagnolo
Giegerich Bastian	Direttore Defence and Military Analysis, International Institute for Strategic Studies (IISS)
Major Claudia	Direttore International Security Research Division, Stiftung Wissenschaft und Politik (SWP)
Maulny Jean-Pierre	Vice direttore, Institut de Relations Internationales et Stratégiques (IRIS)
Robinson Neil	Policy Officer, Nato Cyber Defence Emerging and Security Division
Smeets Max Willian	Direttore, European Cyber Conflict Research Initiative (ECCRI)
Swistek Göran	Military Officer, International Security Research Division, Stiftung Wissenschaft und Politik (SWP)

Osservatorio di Politica internazionale

Un progetto di collaborazione
tra Senato della Repubblica, Camera dei Deputati
e Ministero degli Affari Esteri e della Cooperazione Internazionale
con autorevoli contributi scientifici.

L'Osservatorio realizza:

Rapporti
Analisi di scenario, a cadenza annuale, su temi di rilievo strategico per le relazioni internazionali

Focus
Rassegne trimestrali di monitoraggio su aree geografiche e tematiche di interesse prioritario per la politica estera italiana

Approfondimenti
Studi monografici su temi complessi dell'attualità internazionale

Note
Brevi schede informative su temi legati all'agenda internazionale

www.parlamento.it/osservatoriointernazionale

Senato della Repubblica

Camera dei Deputati

Ministero degli Affari Esteri
e della Cooperazione
Internazionale

Coordinamento redazionale:

Senato della Repubblica
Servizio Affari internazionali
Tel. 06-67063666
Email: segreteriaaaii@senato.it