Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021

L'Italia e la difesa cibernetica

di Alessandro Marrone, Ester Sabatino e Ottavia Credi

ABSTRACT

Il tema della difesa cibernetica ha assunto rilevanza crescente in Italia, a fronte dell'elevato numero di gravi attacchi sia verso soggetti privati sia contro le Forze Armate e la pubblica amministrazione – come nel caso della Regione Lazio nel 2021. L'Italia ha affrontato il tema con l'istituzione del Comando per le Operazioni in Rete (Cor) nell'ambito della Difesa, e con una più ampia riforma della *governance* del settore che ha portato alla definizione del Perimetro di sicurezza cibernetica nazionale e alla creazione della Agenzia per la Cybersicurezza Nazionale (Acn). A livello internazionale, sia i principali alleati Nato sia l'Alleanza nel suo complesso stanno sviluppando un proprio approccio alla *cyber defence*, mentre si apre una riflessione strategica e dottrinale rispetto a un dominio operativo nuovo e dalle caratteristiche uniche. Un dominio nel quale il ruolo della tecnologia e del settore privato è dirompente, richiedendo nuove forme di dialogo e collaborazione tra le istituzioni e l'industria nazionale.

Sicurezza informatica | *Politica militare* | *Italia* | *Nato*

keywords

L'Italia e la difesa cibernetica

di Alessandro Marrone, Ester Sabatino e Ottavia Credi*

* Alessandro Marrone è responsabile del programma Difesa dell'Istituto Affari Internazionali (IAI). Ester Sabatino è stata ricercatrice nel programma Difesa dello IAI fino al 31 agosto 2021. Ottavia Credi è ricercatrice junior nei programmi Difesa e Sicurezza dello IAI.

· Questo documento è stato preparato per il seminario a porte chiuse "La cyber defence in Italia: sviluppi in rete" organizzato dallo IAI il 21 luglio 2021 con il supporto di Elettronica, ed è stato rivisto alla luce del dibattito ivi svoltosi.

ISSN 2280-6164

Introduzione

Il tema della *cyber defence* ha assunto negli ultimi anni una rilevanza crescente a livello nazionale e internazionale, a fronte di un numero in costante aumento di attacchi cibernetici. Secondo alcune stime[1], nel solo primo semestre del 2020, più di un sesto degli 850 attacchi gravi registrati a livello mondiale ha interessato strutture governative. Nello stesso periodo, gli attacchi rivolti alle infrastrutture critiche sono cresciuti dell'85 per cento rispetto allo stesso periodo dell'anno precedente. Questo secondo trend è riscontrabile anche per l'Italia, dove nel 2020 sono state registrate più di 500 denunce di attacchi alle infrastrutture di rilevanza nazionale, a fronte di un totale di circa 147 denunce nel 2019[2]. L'accelerazione nel numero di tentativi di sottrazione di dati, interruzione di servizi, compromissione delle infrastrutture tecnologiche, è ancora più allarmante se si considera che a portare a termine gli attacchi è una varietà sempre più numerosa di attori, che vede parimenti coinvolti attori statali e non-statali.

Recenti attacchi cibernetici con conseguenze di portata internazionale, come ad esempio nel caso di attacco ransomware ai danni dei software prodotti dalla statunitense Kaseya di luglio 2021, oppure nel contesto italiano il caso della Regione Lazio, pongono maggiormente in luce le potenzialità e i rischi per la sicurezza nello spazio cibernetico. Uno spazio in cui non vi è un quadro legislativo condiviso a livello internazionale e nel quale non è presente una limitazione alla proliferazione dei sistemi da poter impiegare, anche in considerazione della natura intrinsecamente duale dei dispositivi utilizzati.

Dal punto di vista della difesa, il cyber rappresenta una sfida da affrontare e un'opportunità da sfruttare che non possono essere lasciate in secondo piano. In ambito militare, la difesa da potenziali attacchi cibernetici può interessare diverse strutture, dal personale dispiegato nelle missioni internazionali, ai sistemi ed equipaggiamenti in uso, alle Forze Armate sia sul suolo nazionale che all'estero, fino alla protezione delle informazioni di rilevanza strategica e alla difesa effettiva da attacchi, siano essi rivolti alle strutture militari o aventi come obiettivo più ampio la sicurezza di una nazione. Nel quadro dell'Alleanza atlantica – per la quale un attacco cibernetico può portare all'attivazione della clausola della difesa collettiva, ex art. 5, e con possibili conseguenze anche nel "mondo reale" – si lavora sulla creazione di un approccio condiviso tra i suoi stati membri. Questi ultimi tuttavia divergono per strutture e capacità nazionali preposte alla difesa cibernetica, così come per postura nazionale in relazione alle possibili operazioni di risposta.

[1] Si veda, ad esempio: Associazione Italiana per la Sicurezza Informatica, *Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia*, ottobre 2020, p. 20, https://clusit.it/wp-content/uploads/download/Rapporto-Clusit_2020_web_ottobre.pdf.

[2] Senato della Repubblica, *Convegno "Agenzia per la sicurezza nazionale. Asset strategico per l'Italia digitale"*, Roma, 6 luglio 2021 (video), https://youtu.be/jxJXK9XmlPo.

ISSN 2280-6164

È in questo contesto che si inserisce la difesa cibernetica dell'Italia. Il Comando per le Operazioni in Rete (Cor), istituito nel 2020 e a valenza interforze, è l'organo preposto al contrasto di attacchi cibernetici alle strutture della Difesa e in caso di attacchi di rilevanza nazionale. Tuttavia, così come avviene negli altri Paesi di principale interesse per l'Italia, la *cyber defence* italiana è solo un aspetto del più ampio contesto della sicurezza nello spazio cibernetico, in cui una molteplicità di attori – prima tra tutti la nuova Agenzia per la Cybersicurezza Nazionale (Acn) – è chiamata a intervenire a vario titolo, con l'obiettivo di incrementare la resilienza del Paese e le capacità e rapidità di risposta in caso di crisi cibernetiche. Il presente studio intende fornire un'analisi approfondita e ad ampio spettro della difesa cibernetica in Italia, collocandola nel contesto Nato e mettendo in luce le principali novità che derivano dal nuovo quadro istituzionale nazionale, con uno sguardo particolare all'approccio della Difesa, gli aspetti strategici di questo dominio, e i passi in avanti che il sistema-Paese può compiere per offrire una risposta coordinata e a tutto tondo alla minaccia cyber.

ISSN 2280-6164

1. Il quadro legislativo e istituzionale italiano

di Ester Sabatino

Il quadro legislativo e istituzionale italiano in materia di sicurezza cibernetica è attualmente in fase di evoluzione e si sta delineando attorno all'Acn, istituita con decreto legge (DL) n. 82 del 14 giugno 2021[3], convertito con modificazioni in legge n. 109 del 4 agosto 2021[4]. Con tale modifica, il legislatore muove i propri passi dalla crescente consapevolezza della complessità della minaccia cyber, a partire dalla stretta connessione tra la sicurezza cibernetica dello stato e la difesa nazionale[5]. Al fine di comprendere meglio la realtà attuale, il presente capitolo descrive brevemente i principali passaggi normativi che hanno delineato il quadro legislativo e istituzionale per la sicurezza cibernetica in Italia a partire dal 2013, per poi concentrarsi sull'Agenzia.

1.1 L'evoluzione normativa italiana dal 2013 al 2020

La difesa cibernetica in Italia si inserisce all'interno del più ampio quadro di sicurezza cibernetica. Sulla spinta di iniziative sia a livello dell'Unione europea (Ue) che nell'ambito dell'Alleanza atlantica, con il decreto del Presidente del Consiglio dei Ministri (Dpcm) del 24 gennaio 2013 (Decreto Monti) l'Italia si dota per la prima volta di una struttura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche[6].

Il Decreto Monti individua nel Dipartimento delle Informazioni per la Sicurezza (Dis) l'organo responsabile per la tutela della sicurezza cibernetica del Paese, nonostante i compiti derivanti dal Decreto fossero diversi rispetto a quelli attribuiti storicamente al Dis quale organo di intelligence. Il Decreto istituisce, inoltre, il Nucleo per la Sicurezza Cibernetica (Nsc) per il supporto operativo in caso di crisi cibernetiche di rilevanza per la sicurezza nazionale, e un tavolo interministeriale per la prevenzione e gestione di tali crisi. Il Decreto conferisce inoltre al Comitato Interministeriale per la Sicurezza della Repubblica (Cisr) il compito di proporre al Presidente del Consiglio dei Ministri il quadro strategico nazionale per la sicurezza dello spazio cibernetico e gli indirizzi strategici in materia di cybersecurity tramite il

[3] Italia, *Decreto-Legge 14 giugno 2021, n. 82: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg.

[4] Italia, *Legge 4 agosto 2021, n. 109: Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/sg.

[5] Senato della Repubblica, *Risoluzione approvata dalla Commissione sull'affare assegnato n. 423*, 7 aprile 2021, http://www.senato.it/japp/bgt/showdoc/18/SommComm/0/1210625/index.html?part=doc_dc-allegato_a:1.

[6] Presidenza del Consiglio dei Ministri, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, 24 gennaio 2013, https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

ISSN 2280-6164

Piano nazionale per la sicurezza dello spazio cibernetico. Tra le ulteriori attribuzioni del Cisr definite dal Decreto Monti, vi sono l'elaborazione di linee di indirizzo per eventuali collaborazioni tra enti pubblici e privati e la diffusione di buone prassi per la protezione dello spazio cibernetico, nonché la promozione di adozione di iniziative atte ad assicurare la partecipazione italiana a quadri di cooperazione a geometria variabile, compresi quelli Nato e Ue. In tutte le sue funzioni, il Cisr era affiancato da un Cisr tecnico, ovvero da un organismo collegiale di coordinamento.

L'impianto normativo e istituzionale italiano per la sicurezza cibernetica è stato poi modificato dal Dpcm del 17 febbraio 2017 (Decreto Gentiloni)[7], seguito dal Piano nazionale per la protezione cibernetica e la sicurezza informatica[8]. Una certa spinta all'evoluzione dell'architettura nazionale è stata fornita dalla necessità di razionalizzare e semplificare un panorama istituzionale complesso, con il tentativo di creare sinergie ed economie di scala nel contrasto coordinato alla minaccia cyber.

Con il Decreto Gentiloni il Dis viene investito di ulteriori compiti e diventa sia l'apparato operativo della struttura di sicurezza cibernetica, sia l'organo deputato a definire le linee d'azione per la sicurezza in questo dominio e della risposta in caso di crisi. Tra le modifiche che vanno verso un rafforzamento dei ruoli del Dipartimento, vi è lo spostamento del Nsc: precedentemente presso l'Ufficio del Consigliere militare della Presidenza del Consiglio, il Nucleo viene inserito nella struttura del Dis, che lo presiede con un proprio vice direttore generale. Tra i vari compiti dell'organo vi è quello di raccordo tra gli attori coinvolti a vario titolo nell'architettura di sicurezza cibernetica nazionale, nonché di gestione delle crisi nello spazio cibernetico.

Un'altra importante novità introdotta dal decreto attiene alla creazione, in capo al Ministero dello Sviluppo economico, di un Centro di valutazione e certificazione nazionale (Cvcn)[9] per la verifica degli standard di sicurezza dei prodotti tecnologici destinati a essere impiegati nelle infrastrutture critiche del Paese[10]. Già nel Decreto Monti appariva la consapevolezza dell'importanza dell'attore privato nella determinazione dei livelli di sicurezza cibernetica nazionale. Questa consapevolezza ha portato alla formulazione del DL n. 105 del 21 settembre 2019 per la definizione del Perimetro di sicurezza cibernetica nazionale[11], secondo le

[7] Presidenza del Consiglio dei Ministri, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, 17 febbraio 2017, https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg.

[8] Presidenza del Consiglio dei Ministri, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, marzo 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf.

[9] Il Centro è stato istituito nel 2019. Per maggiori informazioni, si veda: Ministero dello Sviluppo economico, *Istituito il Centro di valutazione e certificazione nazionale (Cvcn)*, 19 febbraio 2019, https://www.mise.gov.it/index.php/it/198-notizie-stampa/2039261.

[10] Stefano Mele, "Le tre novità che cambieranno la cyber security nazionale, con il nuovo decreto", in *Agenda Digitale*, 14 aprile 2017, https://www.agendadigitale.eu/?p=30583.

[11] Italia, *Decreto-legge 21 settembre 2019, n. 105: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*, https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg.

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

modalità di individuazione successivamente definite dal Dpcm n. 131 del 30 luglio 2020[12]. Tra i vari obblighi[13] degli operatori individuati[14] vi è anche la necessità di certificazione dei prodotti e servizi da loro utilizzati, che dovrà essere effettuata dal Cvcn secondo le modalità recentemente definite[15]. Tutte azioni che vanno nella direzione di un rafforzamento della sicurezza dell'apparato nazionale e di una maggiore resilienza degli operatori e fornitori di funzioni essenziali dello stato, grazie all'adozione di beni, prodotti e servizi di *Information and Communications Technology* (Ict) che dovrebbero essere concepiti a monte come più sicuri e resistenti rispetto alle minacce cyber, ovvero *secure by design*. Sulla base di questa breve disamina, occorre sottolineare che nel quadro legislativo delineatosi nel tempo, e in particolare con il DL 105/2019, sebbene la Difesa sia individuata come parte del "nocciolo duro" del Perimetro, non ha ricevuto un ruolo specifico. Ciò rischia di portare a una scarsa valorizzazione delle capacità peculiari delle Forze Armate nella protezione cibernetica del Paese, anche alla luce degli sviluppi in corso sia a livello Nato, sia all'interno dei principali alleati occidentali, e che hanno coinvolto anche il Ministero della Difesa con la recente costituzione del Cor.

1.2 L'attuale quadro legislativo-istituzionale e l'Agenzia per la Cybersicurezza Nazionale (Acn)

Il quadro legislativo nazionale in materia di sicurezza cibernetica è stato ulteriormente regolato dal DL 82/2021. Il decreto, emendato con legge, introduce diverse modifiche all'apparato di sicurezza cibernetica nazionale, tra cui la suddetta istituzione dell'Acn[16]. La creazione dell'Agenzia si inserisce inoltre tra gli interventi del Piano nazionale di ripresa e resilienza (Pnrr)[17], al quale la Difesa ha dichiarato voler contribuire con le sue strutture e competenze[18].

[12] Presidenza del Consiglio dei Ministri, *Decreto 30 luglio 2020, n. 131: Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*, https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg.

[13] Per maggiori informazioni si veda: Presidenza del Consiglio dei Ministri, *Decreto 14 aprile 2021, n. 81: Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza*, https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg.

[14] Il Perimetro è stato ampliato dal Presidente del Consiglio Mario Draghi il 15 giugno 2021. Per maggiori informazioni si veda: Presidenza del Consiglio dei Ministri, *Cyber: aggiornato l'elenco dei soggetti del "perimetro di sicurezza cibernetica nazionale"*, 15 giugno 2021, https://www.governo.it/it/node/17154.

[15] Presidenza della Repubblica, *Decreto 5 febbraio 2021, n. 54: Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*, https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg.

[16] Italia, Decreto-Legge 14 giugno 2021, n. 82, cit. Gli incarichi di direttore e vice direttore dell'Agenzia sono stati rispettivamente affidati a Roberto Baldoni e Nunzia Ciardi.

[17] La cybersecurity è uno dei sette investimenti della digitalizzazione della pubblica amministrazione. I circa 620 milioni di euro dedicati serviranno a creare un'infrastruttura per la cybersecurity, rafforzare le strutture operative e incrementare le capacità nazionali di difesa informatica. Per maggiori informazioni si veda: Presidenza del Consiglio dei Ministri, *Piano nazionale di ripresa e resilienza*, maggio 2021, https://www.governo.it/sites/governo.it/files/PNRR.pdf.

[18] Senato della Repubblica, *Risoluzione approvata dalla Commissione sull'affare assegnato n. 423*, cit.

ISSN 2280-6164

La legge prevede indipendenza regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria dell'Agenzia, mentre il Presidente del Consiglio dei Ministri mantiene l'alta direzione e responsabilità generale delle politiche di sicurezza cibernetica nazionale (art. 2). L'Acn è chiamata a predisporre una relazione annuale, trasmessa al Parlamento dal Presidente del Consiglio dei Ministri. Per permettere all'Agenzia di iniziare la sua attività, il decreto istituisce una dotazione finanziaria di 2 milioni di euro per il 2021 e un'allocazione cumulativa di 529 milioni di euro per il periodo 2021-2027 (art. 18). I fondi stanziati dovranno coprire anche le retribuzioni dei 300 funzionari che daranno operatività iniziale all'Agenzia e i cui stipendi saranno equiparati a quelli dei dipendenti della Banca d'Italia. In questo modo, il Governo intende limitare il problema della bassa attrattività dell'impiego pubblico rispetto alle possibilità retributive e di carriera del settore privato nel campo della cybersecurity, che interessa l'Italia al pari degli altri Paesi europei e ha importanti implicazioni anche per le Forze Armate italiane.

Tra le modifiche principali introdotte dal DL vi è lo spostamento dell'apparato di sicurezza cibernetica nazionale dal Dis all'Agenzia, sempre organo di diritto pubblico, che risponderà direttamente alla Presidenza del Consiglio dei Ministri. L'Acn, tuttavia, lavorerà a stretto contatto con il Sistema di informazione per la sicurezza della Repubblica per mezzo del Nucleo per la cybersicurezza, che sostituisce il Nsc. Il Nucleo è costituito, oltre che dal Direttore generale dell'Acn e dal suo Vice Direttore, dal Consigliere militare del Presidente del Consiglio, rappresentanti del Dis, dell'Agenzia Informazioni e Sicurezza Interna (Aisi), dell'Agenzia Informazioni e Sicurezza Esterna (Aise), di ciascuno dei Ministeri inclusi nel Cisr[19] e rappresentanti del Ministero dell'Università e della Ricerca, del Ministro delegato per l'Innovazione Tecnologica e la Transizione Digitale, e della Protezione Civile. Il Nucleo ha il compito di programmare e pianificare la risposta a situazioni di crisi cibernetica, nonché di coordinare lo svolgimento di esercitazioni interministeriali e la partecipazione italiana a esercitazioni internazionali[20]. Da notare come il Nucleo riceve le notifiche di violazione o tentativi di violazione della sicurezza delle strutture informatiche delle articolazioni dello stato e quelle provenienti dal Computer Security Incident Response Team (Csirt) Italia[21], raccogliendo così una mole considerevole di dati. Inoltre, il Nucleo valuta l'intensità e la natura degli eventi cibernetici coinvolgenti le infrastrutture nazionali e di rilevanza nazionale che necessitano di una risposta coordinata.

[19] I membri del Cisr sono: il Presidente del Consiglio dei Ministri, l'Autorità delegata, il ministro degli Esteri, il ministro dell'Interno, il ministro della Difesa, il ministro della Giustizia, il ministro dell'Economia e delle Finanze, il ministro dello Sviluppo economico, il ministro della Transizione ecologica.

[20] Si rileva che l'art. 9, comma 1(c) non specifica se tra le esercitazioni internazionali vengono incluse anche quelle di difesa.

[21] Lo Csirt Italia è la nuova denominazione dello Csirt italiano istituito con il Decreto di attuazione della Direttiva UE 2016/1148.

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

L'Agenzia si pone come attore di riferimento unico della sicurezza cibernetica, con il compito di redigere la strategia nazionale di sicurezza cibernetica e assicurare lo svolgimento di azioni comuni per il raggiungimento di più alti livelli di resilienza nazionale. Assume tutte le funzioni relative al Perimetro di sicurezza nazionale cibernetica e agisce come autorità di certificazione della cybersecurity, in ciò rilevando le competenze del Cvcn sui prodotti e servizi acquisiti dai soggetti rientranti nel Perimetro. Essa costituisce inoltre il punto di contatto nazionale richiesto dalla Direttiva Ue 2016/1148, nonché Centro nazionale di coordinamento richiesto dal Regolamento (Ue) 2021/887[22].

Importanti attribuzioni inserite dalla legge di conversione del DL che avranno ripercussioni sulla sicurezza cibernetica nazionale in generale e del Perimetro in particolare, attengono ai servizi cloud e alla crittografia. Nel primo caso, l'Acn dovrà provvedere alla qualificazione dei servizi cloud per la pubblica amministrazione, considerati attualmente non in condizioni di sicurezza[23]. Nel secondo caso invece, dovrà assumere le iniziative necessarie a valorizzare la crittografia come strumento per la sicurezza cibernetica, in ciò attuando le azioni necessarie al rafforzamento dell'autonomia industriale e tecnologica dell'Italia.

Alcune delle funzioni precedentemente attribuite al Cisr, vengono ora trasferite al Comitato Interministeriale per la Cybersicurezza (Cic). Il Cic ha rilevato i compiti di consulenza, proposta e vigilanza in materia di sicurezza cibernetica, nonché di adozione degli atti attuativi del Perimetro, e di proposta dell'elenco di soggetti inclusi nel Perimetro di sicurezza cibernetica nazionale. Tuttavia, restano in capo al Cisr le attribuzioni previste in caso di rischio grave e imminente alla sicurezza delle reti. In questo caso, secondo l'art. 5 del DL 105/2019, previa deliberazione del Cisr, il Presidente del Consiglio può decidere la disattivazione di apparati o prodotti usati nella rete che sono a grave rischio di vulnerabilità.

Nel testo del DL si evince una particolare attenzione ai privati e alla formazione, confermata nella fase di conversione in legge con appositi emendamenti. Con riferimento ai primi, l'Agenzia potrà stipulare accordi bilaterali e multilaterali che coinvolgano il settore privato, con l'obiettivo di promuovere lo sviluppo di competenze e capacità industriali e tecnologiche, che potrà supportare anche grazie al coinvolgimento del sistema universitario e della ricerca. Durante la fase di conversione in legge del DL, un emendamento ha introdotto la costituzione di un Comitato tecnico-scientifico per supportare l'Agenzia con proposte e consulenza anche nell'espletamento delle funzioni e nella conduzione di attività che coinvolgono il settore privato e sarà composto anche da rappresentanti qualificati dell'industria, enti di ricerca, università e ricerca e associazioni di settore. La loro

[22] Parlamento europeo e Consiglio dell'Unione europea, *Regolamento (UE) 2021/887 del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento*, http://data.europa.eu/eli/reg/2021/887/oj.

[23] Gabriele Carrer, "Sì della Camera all'Agenzia cyber. Le novità del disegno di legge", in *Formiche.net*, 28 luglio 2021, https://formiche.net/?p=1407072.

ISSN 2280-6164

presenza fa ben sperare in un maggior dialogo tra i molteplici attori in gioco, con il fine di coordinare le attività ai vari livelli e all'interno delle diverse realtà coinvolte nell'assicurare un grado più elevato di sicurezza cibernetica.

Nell'altro campo di attenzione, la formazione, l'Agenzia si muoverà su due direttrici. La prima, di natura generale, sarà dedicata alla sensibilizzazione e alla formazione della consapevolezza della minaccia cibernetica, per mezzo di campagne di comunicazione e con il fine di accrescere la cultura nazionale di sicurezza cibernetica. La seconda direttrice sarà rivolta, invece, all'alta formazione di personale qualificato tramite percorsi accademici dedicati e potrà autorizzare la costituzione di aree dedicate allo sviluppo dell'innovazione tramite la formazione e il reclutamento di personale. Al pari di quanto accade nei principali Paesi europei e alleati[24], la scarsa formazione, sia della popolazione per quanto riguarda il riconoscimento della minaccia cibernetica, sia degli esperti di settore per le loro competenze tecnico-professionali, può rappresentare un problema rilevante nella prevenzione e risposta rispetto ad attacchi di natura cibernetica.

Nell'attuale configurazione, in caso di attacco, a intervenire sarà il Nucleo per la cybersicurezza in una composizione che include i rappresentanti dei ministeri rilevanti, con il fine di assicurare il concerto tra le azioni di risposta. Vista l'indeterminatezza dei confini nel campo cibernetico, in caso di crisi il Nucleo assicura i collegamenti necessari alla loro gestione con gli omologhi internazionali, inclusa la Nato e le altre organizzazioni internazionali di cui l'Italia fa parte[25].

Con specifico riferimento a quest'ultimo aspetto, è rilevante sottolineare che, nel delineare i compiti dell'Agenzia e del Nucleo, il DL non riconosceva ruoli particolari al Ministero della Difesa. Mentre in materia di cooperazione internazionale sulla cybersecurity si prevedeva già nel testo del DL un raccordo con il Ministero degli Affari esteri e della Cooperazione internazionale (art. 7, comma 3(q)), nel caso delle Forze Armate e della partecipazione italiana a quadri di cooperazione e organizzazioni di sicurezza le specificità della Difesa non sembravano essere messe adeguatamente in luce. Al Ministero della Difesa veniva solamente riconosciuta la competenza specifica di ente abilitato al rilascio del certificato europeo di sicurezza cibernetica, ossia della certificazione di prodotti Ict a livello di affidabilità, come da regolamento (Ue) 2019/881 (art. 7). Grazie all'introduzione di emendamenti nella fase di conversione in legge, le specificità di settore sembrano essere prese maggiormente in considerazione. La legge di conversione esplicita la necessità di un raccordo con il Ministero della Difesa in diversi ambiti d'azione, a partire proprio dalla partecipazione italiana a progetti e iniziative in collaborazione con la Nato e l'Agenzia Europea per la Difesa, per includere gli aspetti collegati alla ricerca militare e la contribuzione alla formazione settoriale grazie alle competenze altamente specializzate delle Forze Armate.

[24] Per maggiori informazioni si rimanda al capitolo 5 del presente studio.

[25] Italia, *Decreto-Legge 14 giugno 2021, n. 82*, cit., art. 10.

ISSN 2280-6164

2. Il Comando per le Operazioni in Rete (Cor)

di Alessandro Marrone e Ottavia Credi

In generale, la Difesa ha un suo ruolo e mandato chiaro nel tutelare l'interesse nazionale anche fuori dal territorio del Paese – come avviene d'altronde nel mondo reale con le missioni all'estero. Inoltre, il Ministero della Difesa ha la necessità permanente di proteggere i propri assetti infostrutturali e infrastrutturali, a partire dalla propria rete.

In questo contesto, e rispetto al quadro normativo e istituzionale delineato dal primo capitolo, tra i soggetti più rilevanti per la difesa cibernetica del Paese vi è certamente il Cor, di natura interforze e posto sotto la diretta catena di comando dello Stato Maggiore della Difesa (Smd). Inaugurato nel febbraio 2020, il Cor è incaricato di coordinare le attività di sicurezza e difesa cibernetica delle Forze Armate e del Ministero della Difesa[26].

2.1 Origine e presupposti

Tra i motivi che hanno portato all'istituzione del Cor, due sono particolarmente importanti. In primo luogo, la creazione di questa struttura è derivata dalla necessità di avere un unico comando che comprendesse competenze necessarie a operare nello spazio cibernetico, incluse le Ict, le capacità di comando, controllo, telecomunicazioni e informatica (*Command, control, communication, and computers*, C4) e di intelligence, sorveglianza e ricognizione. Ciò è di particolare rilievo per mettere insieme, in un comando con una visione unitaria e una impostazione più operativa, competenze e responsabilità in precedenza frammentate, soprattutto per le unità che si occupano delle componenti Ict e C4 della Difesa, e per quelle incaricate di condurre operazioni nel dominio cibernetico, come discusso più nel dettaglio nel prossimo paragrafo.

In secondo luogo, la creazione del Cor è stata diretta conseguenza della volontà di raggiungere un più alto livello di efficienza e razionalizzazione della struttura tecnico-operativa della Difesa, anche in funzione di una collaborazione tra le diverse Forze Armate sempre più sinergica e consolidata. In questo senso, si inserisce in quel lungo e difficile percorso verso un rafforzamento del livello interforze, che metta a sistema le competenze delle Forze Armate con una catena di comando più efficace ed efficiente. La logica interforze è ancora più importante di fronte all'affermarsi, nella riflessione sia alleata che di competitori strategici, di operazioni "multi-dominio" in cui lo spazio cibernetico è considerato un dominio operativo al pari degli altri e necessita quindi di un comando unico che sia a tutti gli effetti responsabile delle operazioni cibernetiche.

[26] Per maggiori informazioni, si veda il sito del Ministero della Difesa: *Comando per le Operazioni in Rete (COR)*, https://www.difesa.it/SMD_/COR. L'incarico di Comandante del Cor è stato affidato all'Ammiraglio di Squadra Ruggiero Di Biase.

ISSN 2280-6164

ISSN 2280-6164

Oltre a porre l'accento sulla necessità di un incremento di operazioni interforze e multi-dominio, il Concetto Strategico del Capo di Stato Maggiore della Difesa (Casmd) fornisce alcune linee guida per l'approccio che le Forze Armate dovrebbero adottare nel condurre operazioni nello spazio cibernetico[27]. In particolare, il Casmd identifica sette pilastri fondamentali che caratterizzano questa dimensione: l'individuazione delle vulnerabilità; il consolidamento della resilienza; l'integrazione degli attori che operano nello spazio cibernetico sia all'interno del territorio nazionale che all'estero; la deterrenza, intesa sia come capacità che come volontà di condurre operazioni nello spazio cibernetico; la capacità di reagire in maniera rapida ad attacchi cibernetici; lo sviluppo tecnologico, tramite investimenti in ricerca e sviluppo e possibilmente attraverso il coinvolgimento di start-up e piccole e medie imprese; l'acquisizione di una *cyber awareness* funzionale alla costituzione di un approccio informato verso il dominio cibernetico e all'ottenimento di informazioni e competenze specifiche sulle quali basare lo sviluppo di nuove capacità.

Partendo da questi presupposti, un'opportuna pianificazione a lungo termine sostenuta da un conseguente investimento ha portato all'istituzione del Comando.

2.2 Organigramma e compiti specifici

Il Cor è posto sotto la supervisione del Casmd e lavora in sinergia con le unità di Esercito, Marina e Aeronautica che si occupano di difesa e sicurezza cibernetica.

Il Comando si compone di tre reparti: il Reparto C4, il Reparto Sicurezza e Cyber Defence, e il Reparto Cyber Operations[28].

Il Reparto C4 ha, di fatto, assunto le competenze prima garantite dal Comando interforze C4 Difesa (C4d), assicurando la direzione della Rete della difesa (Difenet) oltre che la gestione delle capacità Ict di tutti gli Stati maggiori. Ciò è reso possibile dall'integrazione delle competenze del Security Operations Center (Soc), Network Operations Center (Noc) e Infrastructure Operations Center (Ioc) in un'unica struttura, ovvero l'Ufficio Operatività Ict. Presso il Reparto C4 è inoltre collocato l'Ufficio Reti e Data Center, che svolge le funzioni necessarie per garantire la continuità di attività della Difesa – quello che in gergo aziendale si chiama *business continuity* – e di ripresa in caso di grave incidente – il cosiddetto *disaster recovery*. Attualmente, il Reparto può contare sia sui 12.000 chilometri di Rete Interforze in Fibra Ottica Nazionale (Rifon), che sui 10.000 chilometri di ponti radio che costituiscono la Rete Numerica Interforze (Rni) e la Metropolitan Area Network (Man) della Capitale. Oltre a garantire efficienza, monitoraggio e assistenza costante

[27] Stato Maggiore della Difesa, *Il Concetto Strategico del Capo di Stato Maggiore della Difesa*, gennaio 2020, https://www.difesa.it/SMD_/CaSMD/concetto_strategico_casmd.

[28] Si veda il sito del Ministero della Difesa: *Reparto C4*, https://www.difesa.it/SMD_/COR/Pagine/reparti.aspx.

dei servizi C4, il Reparto è impegnato in attività di progettazione, sviluppo e attuazione dei sistemi, portate avanti dall'Ufficio Sistemi e Applicativi Centralizzati.

Il Reparto Sicurezza e Cyber Defence è deputato allo sviluppo di un'architettura nazionale di difesa cibernetica e di sistemi preposti alla protezione dell'infrastruttura Ict. A tal fine, il Reparto porta avanti tre filoni di attività: l'identificazione di capacità che rafforzino la sopracitata architettura nazionale di difesa cibernetica; il monitoraggio sistematico delle attività rilevanti che avvengono entro lo spazio cibernetico, valutando il grado di vulnerabilità dello stesso; e l'elaborazione di strategie per la prevenzione di eventuali minacce nello spazio cibernetico. Nel Reparto Sicurezza e Cyber Defence continua a operare l'Ufficio Computer Emergency Response Team (Cert), attivo 24 ore al giorno, sette giorni alla settimana. Negli anni, questo organo ha aumentato sensibilmente le proprie capacità e svolge oggi anche attività preventive quali lo sviluppo di competenze di *threat intelligence* per le Forze Armate, ovvero la raccolta e l'analisi di informazioni relative a minacce cibernetiche che colpiscono o potrebbero colpire queste strutture.

Il Reparto comprende anche l'Ufficio Infrastrutture di Sicurezza, incaricato di sviluppare sistemi di sicurezza che siano ideati, progettati e realizzati tenendo in considerazione fin dall'inizio le esigenze di sicurezza e difesa cibernetica, secondo il principio di *security by design*. Si tratta di un elemento particolarmente importante, in quanto la stragrande maggioranza degli odierni dispositivi Ict, e lo stesso web, non è costruito secondo questo principio, lasciando piuttosto che le esigenze di sicurezza siano per quanto possibile prese in considerazione solo *ex post* con un rafforzamento delle capacità difensive di determinati elementi. L'Ufficio Infrastrutture di Sicurezza si occupa anche di effettuare una valutazione dei rischi cibernetici e provvedere ai diversi processi di certificazione, una competenza potenzialmente molto importante anche in relazione al compito di certificazione di sicurezza affidato dall'attuale quadro normativo alla Difesa, nonché alle attività del Cvcn rilevate dalla Acn. Infine, sempre nel quadro del Reparto, l'Ufficio Sistemi Classificati ha il compito di irrobustire e consolidare i servizi C4 classificati.

Il Reparto Operazioni Cibernetiche rappresenta infine l'integrazione nel Cor dell'ex-Comando Interforze per le Operazioni Cibernetiche (Cioc)[29]. Ad esso spetta l'intero ventaglio di attività militari che si svolgono nello spazio cibernetico, mirate alla protezione di sistemi e servizi della Difesa da minacce cibernetiche, in relazione non solo al territorio nazionale, ma anche ai vari teatri operativi. È in questo contesto che lavorano le Cellule Operative Cibernetiche (Coc), inizialmente istituite all'interno del Cioc e poi confluite nel Reparto Operazioni Cibernetiche del Cor[30]. Le Coc consistono in team di specialisti interforze in grado di condurre

[29] Il Cioc, istituito nel 2017 dal Piano nazionale per la protezione cibernetica e la sicurezza informatica, era preposto alla protezione dei sistemi e delle reti del Ministero della Difesa da minacce cibernetiche.

[30] Camera dei Deputati Commissione Difesa, "Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico", in *Resoconti stenografici*, 20 dicembre 2017, p. 32, http://documenti.camera.it/leg17/resoconti/commissioni/bollettini/pdf/2017/12/20/leg.17.bol0935.data20171220.com04.pdf.

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

operazioni difensive e offensive, lavorando per ridurre il livello di vulnerabilità cui sono soggette sia le infrastrutture cibernetiche in Italia sia i contingenti dispiegati all'estero nell'ambito delle missioni internazionali. Un esempio è offerto dalla Cellula schierata a Peja, in Kosovo, incaricata di difendere le reti non classificate usate dal contingente nazionale per condurre operazioni cibernetiche difensive[31]. Anche grazie alla loro presenza sul campo, infatti, le Coc possono essere impiegate in scenari di crisi, fornendo così una risposta più mirata e immediata[32].

Così come l'ex-Cioc[33], il nuovo Reparto si occupa di formazione e reclutamento di personale, oltre che di attività per l'analisi delle minacce e la protezione delle infrastrutture informatiche, l'innovazione della Difesa in ambito cibernetico e il *procurement* tecnologico. Anche in questo caso, il Reparto è strutturato in tre diversi Uffici. Tra i compiti dell'Ufficio Operazioni e dell'Ufficio Attività Cibernetiche rientra la conduzione dei cosiddetti *penetration tests*, ovvero simulazioni di intrusioni cibernetiche per la valutazione del livello di resilienza dei sistemi informatici della Difesa. I due Uffici sono inoltre impegnati in contatti e collaborazioni sia con Paesi partner sia con il mondo accademico nazionale. Infine, l'Ufficio Addestramento Esercito & Lessons Learned lavora per preparare il personale esterno al Cor a operare entro il dominio cibernetico[34].

Alla luce della rilevanza crescente dell'elemento umano in un ambito innovativo come quello cibernetico, la formazione delle risorse rappresenta un fattore di cruciale importanza[35]. È in questo contesto che si inserisce la recente proposta di creare, all'interno dello Smd, una Cyber Defence Academy: un sistema formativo federato nel quale potrebbero confluire centri di formazione di Dicasteri diversi al fine di integrare, strutturare e armonizzare le attività di formazione nel campo cibernetico[36]. È inoltre in corso di scrutinio da parte del Ministero della Difesa un Concept Paper elaborato dal Cor che esamina le modalità di reclutamento

[31] La Coc in questione è stata dispiegata in Kosovo nel contesto dell'Operazione Kfor, all'interno della più ampia missione Joint Enterprise della Nato. Per maggiori informazioni, si veda il sito del Ministero della Difesa: Kosovo - KFOR - Joint Enterprise, https://www.difesa.it/OperazioniMilitari/op_intern_corso/KFOR.

[32] Intervista, 21 luglio 2021.

[33] Per una spiegazione delle attività dell'ex-Cioc si veda l'intervista al Capo di Stato Maggiore della Difesa: "Cyber Defence. Nasce il Comando Interforze per le Operazioni Cibernetiche", in *Informazioni della Difesa*, n. 3/2017 (marzo 2017), p. 8-10, https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf.

[34] Al fine di aumentare la preparazione di queste risorse, nel 2016 è stato istituito il Cyber Range, attualmente in fase di perfezionamento. Il Cyber Range è un perimetro virtuale della Difesa in grado di simulare scenari di attacchi cibernetici in modo da effettuare una valutazione delle capacità di difesa del Paese nello spazio cibernetico. Per maggiori informazioni sulla Cyber Range, si veda: Alessandro Armando, "Cyber Range. Attacco e difesa in ambiente simulato", in *Gnosis*, n. 2 (febbraio 2016), p. 67-73, http://gnosis.aisi.gov.it/gnosis/Rivista47.nsf/ServNavig/47-26.pdf/$File/47-26.pdf.

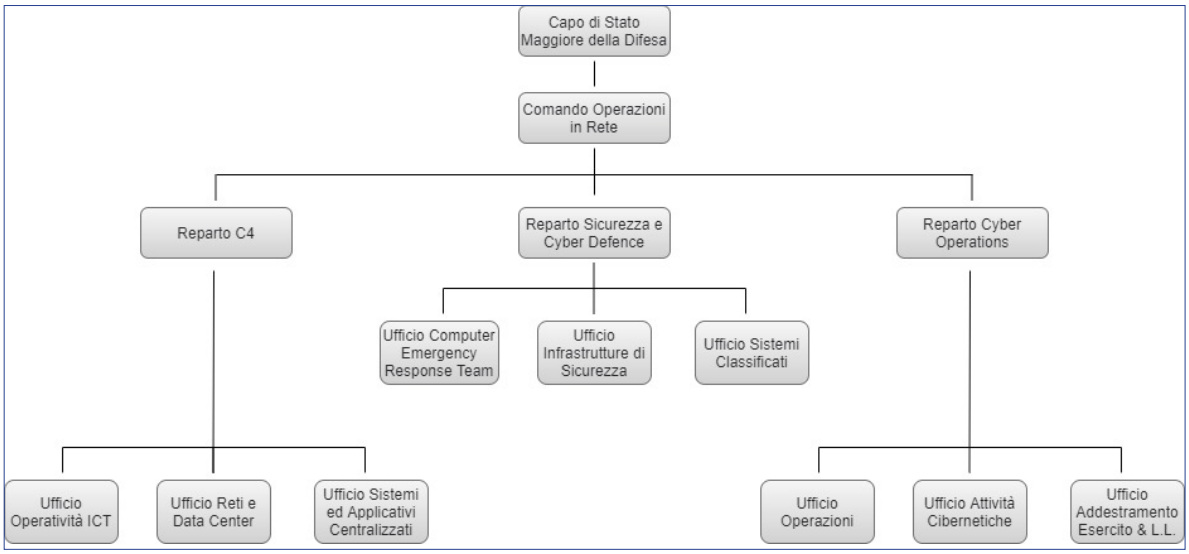
[35] Generale Enzo Vecciarelli durante il convegno "Agenzia per la sicurezza nazionale. Asset strategico per l'Italia digitale", cit.

[36] Ministero della Difesa, *Il Sottosegretario Mulè al webinar dedicato alla Cybersecurity*, 17 maggio 2021, https://www.difesa.it/Primo_Piano/Pagine/Il-Sottosegretario-Mule-al-webinar-dedicato-alla-Cybersecurity.aspx.

ISSN 2280-6164

del personale all'interno del Comando[37]. Ai temi di assunzione e formazione, è importante giustapporre quello dell'informazione: considerata la preponderanza del dominio cibernetico nella società moderna, sarebbe opportuno diffondere una conoscenza generalizzata sul mondo cibernetico, senza limitarla alla sfera degli addetti ai lavori, con il fine di rafforzare il livello complessivo di resilienza e difesa cibernetica.

Figura 1 | Organigramma del Cor



2.3 Vantaggi, potenzialità e questioni aperte

L'istituzione del Cor ha portato numerosi vantaggi rispetto alla capacità delle Forze Armate di assicurare livelli crescenti di difesa cibernetica. In primo luogo il Cor garantisce allo Smd, al Comando operativo di vertice interforze (Coi) e al Comando interforze per le operazioni delle forze speciali (Cofs) un più facile accesso alle informazioni nel e sullo spazio cibernetico. In particolare, il Cor è di fatto la principale componente cyber del Coi[38], in linea con la tendenza a portare sotto un più alto comando interforze le operazioni in tutti e cinque i domini operativi.

In secondo luogo, l'azione del Cor nello sviluppo di capacità tecnologiche e in termini di risorse umane in seno alla Difesa promette un miglioramento e potenziamento delle competenze militari italiane nello spazio cibernetico. Grazie a capacità di informatica forense, ad esempio, il Cor porterà vantaggi significativi ai fini dell'attribuzione della paternità degli attacchi subiti, con risvolti positivi anche nella prevenzione e repressione dei reati informatici e nella realizzazione

[37] Intervista, 21 luglio 2021.

[38] Sito del Ministero della Difesa: *Il Comando Operativo di Vertice Interforze (COVI)*, https://www.difesa.it/SMD_/COI.

ISSN 2280-6164

di un'effettiva deterrenza in campo cibernetico[39]. Come dimostrato dalle funzioni affidate alle Coc[40], oltre agli sviluppi in chiave difensiva – parte delle cosiddette *preventive cyber operations* – il Cor si propone di rafforzare le proprie capacità al fine di condurre anche operazioni offensive[41].

Sia l'aspetto operativo che quello di sviluppo capacitivo beneficiano dalle esercitazioni organizzate dal Cor, che hanno il vantaggio di testare *expertise* e procedure, contribuendo al miglioramento di entrambi alla luce proprio dell'esperienza nell'esercitazione.

Considerato il ruolo limitato che l'attuale quadro normativo che regola la sicurezza cibernetica del Paese riserva alla Difesa[42], per quest'ultima la creazione del Cor rappresenta un'opportunità per instaurare una maggiore sinergia con l'architettura nazionale di sicurezza cibernetica, offrendo un punto di contatto interforze per l'Acn e gli altri attori coinvolti. Tuttavia, lo sfruttamento di questa potenzialità dipenderà molto dall'approccio che adotterà l'Agenzia, dai rapporti che si instaureranno nel Nucleo, e in generale dall'assestamento del Perimetro nazionale di sicurezza cibernetica.

Attraverso le attività portate avanti dal Comando, la Difesa ha inoltre maggiori opportunità di interfacciarsi con rappresentanti del mondo accademico e delle realtà industriali. Si tratta di interlocutori fondamentali per assicurare una costante crescita e aggiornamento delle competenze del Cor stesso, e quindi per estensione della Difesa. Data la natura dello spazio cibernetico, infatti, tale processo può avvenire solo in osmosi con le realtà civili maggiormente innovative e all'avanguardia, ed è necessario incoraggiare un potenziamento della difesa e sicurezza cibernetica a tutti i livelli e in maniera uniforme[43]. Anche in questo caso, la concreta realizzazione delle potenzialità del Cor dipenderà in parte dal ruolo che giocherà l'Acn e dalle sinergie che si potranno attuare tra l'Agenzia e il Comando.

Prendendo infine in considerazione il rapporto tra Italia e Nato, il Cor ha rappresentato fino a ora il principale referente per la definizione di standard in materia di difesa cibernetica, e la stessa istituzione del Comando ha permesso alla Difesa di allinearsi con le linee guida condivise nel quadro dell'Alleanza e di dialogare con il Cyber Operation Command (Cyoc) e gli altri soggetti Nato[44]. Vi

[39] Generale Enzo Vecciarelli durante il convegno "Agenzia per la sicurezza nazionale. Asset strategico per l'Italia digitale", cit. L'informatica forense consiste nel trattamento di dati digitali con lo scopo di rilevare prove informatiche utili all'attività investigativa. Per maggiori informazioni sull'attribution, si veda capitolo 3.

[40] Camera dei Deputati Commissione Difesa, "Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico", cit.

[41] Per una breve panoramica sul tipo di operazioni che si possono condurre in Italia si rimanda al capitolo 5.

[42] Si veda il capitolo 1.

[43] Intervista, 4 giugno 2021.

[44] L'architettura Nato sarà trattata nel capitolo 3.

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

è qui una questione aperta dal mandato dell'Acn che, indicando l'Agenzia come unico punto di riferimento internazionale, sembra comprendere anche i rapporti con la Nato oltre che quelli con l'Ue.

Altra questione aperta riguarda il personale impiegato e impiegabile nel Cor ora e nel medio periodo, da due punti di vista. I ritardi nel raggiungimento della *Full Operational Capability* (Foc) rispetto ai piani iniziali testimonia una difficoltà nel reperire le risorse umane adeguate rispetto al dominio cibernetico nel personale militare attualmente in servizio. Affinché il Comando possa assicurare un elevato livello di preparazione del proprio personale, esso dovrà continuare a investire in attività formative sui temi della difesa e sicurezza cibernetica, sia per i dipendenti che per i dirigenti, possibilmente in rete con altre realtà esistenti[45]. La qualità del personale assegnato è fondamentale, perché con il Cor la Difesa può acquisire una maggiore libertà di azione nel dominio cibernetico, diventando potenzialmente sempre più in grado di condurre operazioni cibernetiche di diversa natura in maniera autonoma.

Il Cor dovrà quindi assicurare nel tempo sia un adeguato afflusso di risorse umane, sia il loro mantenimento per un tempo congruo ad assicurare continuità e crescita delle competenze collettive, sia infine un certo ricambio per sfruttare la naturale propensione verso la tecnologia e lo spazio cibernetico delle reclute più giovani. A fronte di un settore privato altamente remunerativo e competitivo quando si tratta di Ict, nonché di una relativa carenza di laureati italiani nelle discipline scientifiche, tecnologiche, di ingegneria e matematica[46], il Cor e in generale le Forze Armate dovranno sforzarsi di mettere in campo adeguati incentivi economici, stimoli e possibilità di crescita professionale[47]. In altre parole, il Cor dovrà dimostrarsi in grado di affrontare – o perlomeno mitigare – i problemi strutturali che caratterizzano il processo di reclutamento e mantenimento del personale addetto alla difesa cibernetica del Paese.

2.4 La questione dell'integrazione interforze

A livello interforze, l'integrazione nel dominio cibernetico ha compiuto negli ultimi anni grandi passi in avanti, riscontrabili ad esempio, negli sviluppi tecnologici della Rifon[48]. La centralizzazione interforze in definitiva avvantaggia tutte le singole Forze Armate perché una volta definita la *governance* della condivisione delle informazioni, con le relative pertinenze, si creano le condizioni operative e il clima di fiducia per la costruzione di una *picture* condivisa, che risulta essere

[45] Esempi di attività formative già in corso sui temi della difesa cibernetica per il personale militare consistono nella Scuola Telecomunicazioni Forze Armate (Stelmilit) con sede a Chiavari e il Laboratorio Addestrativo per la Difesa Cibernetica (Ladc) all'interno della Scuola delle trasmissioni dell'Esercito, la cui creazione ha rappresentato il primo passo per l'istituzione del Reparto di Sicurezza Cibernetica (Rsc) nell'Esercito stesso.

[46] Intervista, 5 luglio 2021.

[47] Intervista, 26 maggio 2021.

[48] Intervista, 21 maggio 2021.

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

molto più utile delle *picture* parziali raggiungibili a livello di Forza Armata.

Permangono tuttavia alcune questioni aperte, a partire da livelli non soddisfacenti di condivisione dei dati e di cooperazione tra le singole strutture. Il processo di standardizzazione su diversi fronti è ancora incompleto, e il suo completamento è particolarmente importante perché, tramite la condivisione di standard, è possibile ottenere una maggiore integrazione operativa con effetti positivi anche a livello strategico[49]. Le attività di *threat intelligence* non hanno ancora raggiunto un ottimale livello interforze[50]. Inoltre, nonostante la fusione di strutture e competenze avvenuta all'interno del Cor, i Cert delle singole Forze Armate continuano a operare, e si pone la questione di come assicurare la massima cooperazione, efficacia ed efficienza nel quadro della difesa cibernetica nazionale. Da questo punto di vista è positivo che i Cert di Aeronautica, Esercito e Marina utilizzino gli stessi sistemi per rilevare anomalie nella rete dando l'allarme su eventuali attacchi cyber in corso – i dispositivi *Security Information and Event Management* (Siem) – assicurando concretamente lo scambio di dati per il raggiungimento di una *picture* comune[51]. Il panorama resta comunque ancora variegato, e un rischio da evitare è la frammentazione e duplicazione di investimenti tra le singole Forze Armate[52]. Infine, l'ultimo Documento programmatico pluriennale (Dpp) presentato dal Ministero della Difesa[53] ha esortato a creare un sistema di difesa cibernetica coerente e interoperabile con il modello sviluppato dall'Alleanza atlantica.

L'integrazione interforze è condizione necessaria a tal fine, in quanto assicura un vertice unitario italiano in grado di rapportarsi con gli interlocutori nei Paesi alleati e a livello di strutture Nato. Ma non è condizione sufficiente, in quanto serve una maggiore comprensione degli sviluppi in corso nel quadro dell'Alleanza atlantica.

[49] Interviste 21 e 27 maggio 2021.
[50] Intervista, 27 maggio 2021.
[51] Intervista, 21 maggio 2021.
[52] Ibid.
[53] Ministero della Difesa, *Documento Programmatico Pluriennale della Difesa per il Triennio 2020-2022*, 2020, p. 44, https://www.difesa.it/Content/Documents/DPP/DPP%202020-2022.pdf.

ISSN 2280-6164

3. Gli sviluppi a livello Nato

di Ottavia Credi

La Nato è impegnata nello sviluppo di un approccio condiviso e sinergico tra i suoi membri, e con i comandi e le agenzie dell'Alleanza stessa, mirato a un progressivo miglioramento delle capacità di difesa cibernetica. Avendo riconosciuto lo spazio cibernetico come dominio operativo, l'Alleanza si pone l'obiettivo di integrare le operazioni cibernetiche a supporto delle attività militari alleate, ma anche di elevare gli standard di sicurezza dei suoi membri, avviare cooperazioni con Paesi partner, e contribuire a uno sviluppo della normativa internazionale riguardante il settore.

3.1 L'evoluzione dell'approccio alleato

Il focus della Nato sulla difesa cibernetica è aumentato in seguito agli attacchi contro alcuni obiettivi privati e istituzionali estoni nel 2007. Nel vertice del 2008 la Nato ha inaugurato la sua prima politica sulla difesa cibernetica, la *Policy on Cyber Defence*, incentrata sulla protezione delle reti dell'Alleanza e sui requisiti che i network dei Paesi membri sono chiamati a soddisfare al fine di assicurare un'adeguata difesa collettiva e capacità di gestione delle crisi[54].

Con il vertice del Galles del 2014 si è assistito a uno dei principali sviluppi dell'Alleanza nel settore, l'adozione della *Enhanced Policy on Cyber Defence*. Essa prescrive un consolidamento del rapporto con l'industria – inaugurando la Nato Industry Cyber Partnership[55] – e uno scambio di informazioni e assistenza tra Alleati più rapido e strutturato. La *Enhanced Policy* ha anche confermato l'intenzione della Nato di osservare i principi del diritto internazionale nello spazio cibernetico[56]: "la Nato ha chiarito che un grave attacco cyber può portare all'invocazione dell'articolo 5 del Trattato di Washington"[57].

Durante il vertice di Varsavia del 2016, anche in considerazione di un incremento degli attacchi cibernetici contro le infostrutture Nato del 60 per cento rispetto

[54] Susan Davis, "NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence" (148 STC 19 E rev. 1), in *NATO Parliamentary Assembly STC General Reports*, ottobre 2019, p. 1, https://www.nato-pa.int/node/56441. Il conflitto del 2008 tra Russia e Georgia ha dimostrato il potere distruttivo degli attacchi informatici. Un gruppo di hacker russi ha condotto una serie di attacchi informatici contro siti governativi e istituzionali georgiani, inclusi quelli del Ministero degli Esteri, del Ministero della Difesa e del Presidente della Repubblica. Questi attacchi sono considerati tra i primi casi storici di un attacco coordinato in maniera sincronizzata tra i domini diversi.

[55] Sito Ncia: *NATO Industry Cyber Partnership*, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html.

[56] Nato, *NATO Cyber Defence. Factsheet*, luglio 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf.

[57] Nato, *The Secretary General's Annual Report 2020*, 16 marzo 2021, https://www.nato.int/cps/en/natohq/opinions_182236.htm.

ISSN 2280-6164

al 2015, con una media di circa 500 al mese[58], l'Alleanza ha innalzato lo spazio cibernetico a dominio operativo[59] e inaugurato il *Cyber Defence Pledge*[60], una presa di impegno degli Alleati di sviluppare migliori capacità nazionali di difesa cibernetica, oltre che uno strumento utile per effettuare una valutazione autonoma dei propri progressi nel settore[61].

Il successivo vertice di Bruxelles del 2018 ha visto i membri dell'Alleanza decidere la creazione del Cyoc, all'interno dell'Allied Command Operations (Aco)[62]. Il Cyoc è l'organo responsabile delle attività cibernetiche condotte dall'Alleanza: esso deve garantire una corretta *situational awareness* dello spazio cibernetico, programmare le missioni e operazioni alleate e affrontare eventuali problemi operativi.

La dottrina che regola le operazioni alleate nello spazio cibernetico è esposta nella *Allied Joint Doctrine for Cyberspace Operations*, pubblicata all'inizio del 2020[63]. Il documento si pone tre obiettivi principali: offrire al personale alleato linee guida per l'esecuzione di attività cibernetiche; fornire indicazioni a stati membri, Paesi partner e altre nazioni e organizzazioni; fungere da riferimento per soggetti sia civili che militari interni alla Nato.

Nel più ampio contesto delle minacce ibride, che usano ampiamente lo spazio cibernetico, l'Alleanza ha sviluppato una stretta cooperazione con i propri partner – prima fra tutte l'Ue, con la quale la Nato collabora nel contrasto a minacce cibernetiche[64].

[58] Nato, *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers*, 15 febbraio 2017, https://www.nato.int/cps/en/natohq/opinions_141108.htm.

[59] Nato, *Warsaw Summit Communiqué*, 9 luglio 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

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

[61] Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO: modelli a confronto", in *Approfondimenti dell'Osservatorio di politica internazionale*, n. 164 (dicembre 2020), p. 9, https://www.iai.it/it/node/12562.

[62] Laura Brent, "NATO's role in cyberspace", in *NATO Review*, 12 febbraio 2019, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

[63] Nato Standardization Office, *Allied Joint Doctrine for Cyberspace Operations* (AJP-3.20), gennaio 2020, https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320.

[64] Sito della Nato: *NATO's response to hybrid threats*, aggiornato al 16 marzo 2021, https://www.nato.int/cps/en/natohq/topics_156338.htm. La collaborazione tra Nato e Ue in materia di difesa cibernetica è esplicitata nella Dichiarazione congiunta Nato-Ue e nel Technical Arrangement on Cyber Defence, entrambi firmati nel 2016. Si vedano: Consiglio dell'Unione europea, *Vertice NATO, Varsavia, Polonia, 8 e 9 luglio 2016*, 8 luglio 2016, http://europa.eu/!mG83HF; Nato, *NATO and the European Union enhance cyber defence cooperation*, 10 febbraio 2016, https://www.nato.int/cps/en/natohq/news_127836.htm.

ISSN 2280-6164

La dedizione dell'Alleanza al rafforzamento della propria difesa cibernetica è riflessa anche dalle dichiarazioni dei suoi vertici. In occasione del vertice di Londra del 2019, il Segretario generale della Nato Jens Stoltenberg ha definito lo spazio cibernetico un *new battleground*[65]. L'anno successivo il suo Vice, Mircea Geoană, ha dichiarato che non è possibile vincere le guerre del futuro con gli strumenti del passato e, nell'ambito della più recente *Nato Cyber Defence Pledge Conference* 2021, ha rimarcato l'impegno assunto dall'Alleanza nell'incrementare la propria resilienza e investire nelle nuove tecnologie, anche attraverso la collaborazione con i propri partner[66].

Tale impegno è manifestato anche dall'iniziativa Nato 2030[67]. Nel quadro dell'iniziativa volta a ridisegnare l'agenda dell'Alleanza per il prossimo decennio, e a scrivere un nuovo Concetto Strategico, il rapporto del gruppo di esperti presentato dallo stesso Stoltenberg sottolinea l'importanza di corroborare le capacità alleate di difesa cibernetica, migliorare i processi di finanziamento, reclutamento e addestramento interni all'Alleanza, e assicurare che essa disponga di apparati politici e legali adeguati a far fronte a minacce in questo dominio[68]. Il rapporto sottolinea il ruolo assunto dalle cosiddette *Emerging and Disruptive Technologies* (Edt) – anche in quanto terreno di confronto tra Cina e Russia – incoraggiando gli Alleati a potenziare le proprie capacità tecnologiche, con particolare riferimento all'intelligenza artificiale[69].

Per poter attivare la difesa collettiva è ovviamente necessario identificare il perpetratore di un attacco. Anche nello spazio cibernetico l'attribuzione della paternità di un'azione offensiva è fondamentale per una reazione adeguata, ma è estremamente difficile[70] e questa difficoltà continua a rappresentare un limite significativo ai fini dell'attivazione della difesa collettiva da parte Nato.

3.2 Le principali strutture Nato

Oltre al sopracitato Cyoc, che agisce a livello operativo, tra le altre strutture alleate atte alla prevenzione, gestione e analisi delle minacce cibernetiche figura, ad esempio, il Cyber Defence Management Board (Cdmb), all'interno della Emerging

[65] Jens Stoltenberg, "NATO Will Defend Itself", in "Cyber Resilience", supplemento a *Prospect*, ottobre 2019, p. 4-6, https://www.prospectmagazine.co.uk/?p=85581.

[66] Nato, *Deputy Secretary General Mircea Geoană said that NATO's DNA is values and foresight*, 11 dicembre 2020, https://www.nato.int/cps/en/natohq/news_180071.htm; Nato, *Deputy Secretary General participates in NATO Cyber Defence Pledge Conference*, 15 aprile 2021, https://www.nato.int/cps/en/natohq/news_183128.htm.

[67] Per maggiori informazioni, si veda il sito della Nato: *NATO 2030*, https://www.nato.int/nato2030.

[68] Thomas de Maizière e A. Wess Mitchell (a cura di), *NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General*, 25 novembre 2020, https://www.nato.int/cps/en/natohq/news_179730.htm.

[69] Ibid., p. 29-30; Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit., p. 7.

[70] Come discusso più nel dettaglio nel capitolo 5.

ISSN 2280-6164

Security Challenges Division. Il Cdbm rappresenta un forum all'interno del quale gli specialisti di cyber defence delle varie agenzie Nato possono confrontarsi riguardo la programmazione strategica e la direzione esecutiva delle reti alleate.

Sempre sul piano politico-strategico, il Consiglio del Nord Atlantico (North Atlantic Council - Nac) – il corpo dell'Alleanza responsabile del processo decisionale a livello politico – è supportato in materia di difesa cibernetica dal Cyber Defence Committee (Cdc). È il Nac che, nel 2020, ha stabilito che la Nato può ricorrere all'impiego di mezzi appartenenti a qualsiasi dominio operativo (non solo cyber) per il contrasto a minacce cibernetiche[71].

Prendendo invece in considerazione il livello tecnico, il Nato Cyber Security Center (Ncsc) e la Nato Computer Incident Response Capability (Ncirc) sono rispettivamente impegnati nel fornire servizi per la prevenzione, rilevazione e ripresa da attacchi informatici, e nella tutela delle reti alleate mediante analisi sistematiche delle minacce cibernetiche. Entrambe queste strutture operano all'interno della Nato Communications and Information Agency (Ncia), che si occupa del *procurement* di capacità necessarie all'Alleanza per condurre operazioni cibernetiche.

Infine, un ruolo di particolare rilievo per lo studio e l'analisi delle minacce cibernetiche è ricoperto dal Cooperative Cyber Defence Center of Excellence (Ccdcoe), con base a Tallinn. Il Ccdcoe è attualmente impegnato nel completamento e promozione della terza versione del *Manuale di Tallinn*, che mira a offrire un'interpretazione il più possibile oggettiva delle normative che si possono applicare allo spazio cibernetico[72].

Nel panorama in rapido sviluppo degli attori Nato rilevanti per la difesa cibernetica, 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[73].

Inoltre, affinché tutte le strutture appena descritte possano lavorare in maniera complementare, con l'obiettivo ultimo di irrobustire la difesa cibernetica alleata, è necessario che vi sia tra esse un più efficace scambio di informazioni. Il livello di *info-sharing* tra questi organismi non ha infatti ancora raggiunto livelli soddisfacenti e resta delicato, complicato e politicamente sensibile, in modo simile a quanto accade con l'intelligence[74]. 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 on Cyber Defence* con le autorità di ciascuno stato membro.

[71] 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.

[72] Sito Ccdcoe: *The Tallinn Manual*, https://ccdcoe.org/research/tallinn-manual.

[73] Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit., p. 7.

[74] Ibid., p. 8-9.

ISSN 2280-6164

3.3 Attività con stati membri e Paesi partner

L'Alleanza porta avanti diverse attività di formazione sul tema della difesa e sicurezza cibernetica. A titolo esemplificativo, nei primi mesi del 2021 si sono tenuti il Corso Cyber Wargaming presso il Modelling & Simulation Centre of Excellence di Roma, e una conferenza virtuale sulle operazioni cibernetiche e la sicurezza delle infrastrutture critiche organizzata dal Nato Rapid Deployable Corps Italy[75].

Tale impegno si rispecchia anche nella collaborazione della Nato con il settore privato e il mondo accademico, dimostrato ad esempio dall'organizzazione di un workshop sul tema della sicurezza nelle reti militari 5G della Nato, coordinato dal Nato Allied Command Transformation (Act) e il Ccdcoe[76].

Le attività della Nato in materia di difesa cibernetica si estendono anche alla cooperazione con i Paesi partner. Ad esempio, a gennaio 2021 l'Alleanza ha concluso un progetto mirato al consolidamento delle capacità di difesa cibernetica della Mongolia[77] e inaugurato un Cyber Response Capability Center in Moldavia a beneficio delle competenze di difesa cibernetica delle Forze Armate nazionali[78].

A riprova del perseguimento di un approccio omnicomprensivo e cooperativo alla sicurezza cibernetica, Stoltenberg ha recentemente sottolineato l'urgenza di stabilire norme condivise sul divieto di azioni offensive nello spazio cibernetico, avanzando l'idea di elaborare un trattato internazionale che governi lo spazio cibernetico a livello globale[79].

3.4 Impegno italiano

L'Italia partecipa a numerose iniziative mirate al rafforzamento della difesa cibernetica dell'Alleanza. Un esempio è offerto dall'esercitazione Cyber Coalition, un'opportunità di addestramento per la difesa dello spazio cibernetico alleato anche tramite simulazioni di attacchi a reti informatiche e infrastrutture critiche[80].

[75] Ministero della Difesa, *NATO M&S COE: 1ª edizione del Corso Cyber Wargaming*, 22 gennaio 2021, https://www.difesa.it/SMD_/Eventi/Pagine/NATO_M_S_COE_1_Edizione_del_Corso_Cyber_Wargaming.aspx; Ministero della Difesa, *NATO: NRDC-ITA il Webinar sulle operazioni cibernetiche*, 9 marzo 2021, https://www.difesa.it/SMD_/Eventi/Pagine/NDRC_IT_webinar_sulle_operazioni_cibernetiche.aspx.

[76] Ccdcoe, *First joint 5G military security workshop hosted by ACT and CCDCOE*, 5 febbraio 2021, https://ccdcoe.org/news/2021/first-joint-5g-security-workshop-hosted-by-act-and-ccdcoe.

[77] Nato, *NATO helps to strengthen Mongolia's cyber defence capacity*, 18 gennaio 2021, https://www.nato.int/cps/en/natohq/news_180697.htm.

[78] Gregorio Baggiani, "The New NATO Cyber Incident Response Center in Moldova", in *Nato Defense College Foundation Articles*, 25 giugno 2021, https://www.natofoundation.org/?p=29468.

[79] Nato, *Speech by NATO Secretary General Jens Stoltenberg followed with questions and answers at the at the 3rd German Ecumenical Church Days*, 15 maggio 2021, https://www.nato.int/cps/en/natohq/opinions_183679.htm.

[80] Sito Nato Act: *Cyber Coalition*, https://www.act.nato.int/cyber-coalition.

ISSN 2280-6164

In qualità di *Sponsoring Nation*, l'Italia supporta il Ccdcoe. Tale partecipazione rappresenta una preziosa occasione di collaborazione internazionale nel campo della difesa cibernetica, resa possibile in particolare da due esercitazioni annuali: la Crossed Swords[81] e la Locked Shields[82].

Ulteriore opportunità per l'Italia è rappresentata dalla possibilità di prendere parte a iniziative di singoli Alleati. Un esempio è offerto dall'esercitazione Cetatea[83], condotta dall'Esercito rumeno con l'obiettivo di verificare l'interoperabilità dei sistemi di comunicazione e informazione dei partecipanti.

Se l'Italia intende continuare a partecipare a pieno titolo alle operazioni alleate nello spazio cibernetico, incluse attività ed esercitazioni che comprendono operazioni offensive per il contrasto a minacce cibernetiche, sarà necessario che la normativa nazionale permetta al Paese di agire in linea con il ventaglio di possibilità offerte dall'Alleanza, come discusso nel capitolo 5.

[81] Sito Ccdcoe: *Crossed Swords*, https://ccdcoe.org/exercises/crossed-swords.

[82] Sito Ccdcoe: *Locked Shields*, https://ccdcoe.org/locked-shields.

[83] Nato Modelling & Simulations Centre of Excellence, *Exercise Cetatea 2019*, https://www.mscoe.org/?p=2514.

ISSN 2280-6164

4. La cyber defence nei principali Paesi Nato

di Ester Sabatino

La difesa cibernetica nei principali Paesi Nato viene attuata per mezzo di strategie e strutture di difesa nazionali che riflettono l'approccio del singolo Paese alla minaccia cyber. Sebbene non esista un modello unico di organizzazione delle strutture di difesa cibernetiche, possono essere tuttavia individuati dei punti di contatto e di divergenza[84], i più peculiari dei quali fanno riferimento alla possibilità di condurre solamente operazioni difensive o anche operazioni offensive sia in risposta a un attacco, sia per scopi di "difesa avanzata" e deterrenza.

4.1 Stati Uniti

Il contrasto alle minacce cibernetiche rappresenta un settore di particolare attenzione dell'amministrazione statunitense, sia da un punto di vista operativo, sia per la formazione di una dottrina e approccio condivisi in termini di cyber defence a livello internazionale.

L'organismo preposto alla difesa cibernetica della nazione è lo US Cyber Command (CyberCom) che dirige, sincronizza e coordina le operazioni e la pianificazione nello spazio cibernetico, per proteggere e promuovere gli interessi della nazione[85] attraverso il raggiungimento e il mantenimento della superiorità nel dominio cibernetico[86]. Nell'espletamento delle sue funzioni, il CyberCom è alle dipendenze del sistema di informazioni del Dipartimento della Difesa, e il suo Comandante ha il doppio cappello di Comandante anche della National Security Agency (Nsa). Il CyberCom, che comprende i rappresentanti degli altri comandi cibernetici in capo alle quattro Forze Armate, supporta le singole Forze Armate e il Comando interforze attraverso 133 gruppi operativi che è stato possibile costituire nel 2018 anche grazie all'investimento di 600 milioni di dollari[87].

La strategicità del dominio cibernetico è stata ulteriormente riconosciuta nella *Interim National Security Strategic Guidance* presentata a marzo 2021 dal Presidente Joe Biden[88]. La sicurezza cibernetica è considerata di massima priorità dall'attuale amministrazione e lo sviluppo e rafforzamento delle capacità cyber

[84] Per una panoramica delle principali esigenze comuni ai Paesi caso-studio qui riportati, si rimanda a: Alessandro Marrone e Ester Sabatino, "La difesa cibernetica nei Paesi NATO", cit.

[85] Sito US Cyber Command, *Our Mission and Vision*, https://www.cybercom.mil/About/Mission-and-Vision.

[86] US 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.

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

[88] Presidenza Usa, *Interim National Security Strategic Guidance*, marzo 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance.

ISSN 2280-6164

rappresentano il fulcro della politica corrente. Le risposte alle azioni cibernetiche vengono condotte in modo attivo e sottostanno al concetto di difesa avanzata, ossia di impegno continuo nel dominio cibernetico, per dirottare le capacità dell'avversario dall'attacco alla difesa, mantenendo in tal modo il vantaggio operativo[89]. Tra le attività ricomprese nell'ambito della difesa avanzata, lo US Cyber Command ha reso nota la conduzione di operazioni di "caccia avanzata", la cosiddetta *hunt forward*: operazioni volte a raccogliere informazioni su potenziali avversari, condividerle con i Paesi alleati e partner e danneggiare e/o contrastare attività cibernetiche malevole[90].

A seguito dell'attacco cibernetico ai danni della rete dell'oleodotto Colonial Pipeline nel 2021[91], il Presidente americano ha firmato un ordine esecutivo per assicurare migliori standard di sicurezza cibernetica anche tra gli attori privati del Paese, in base al quale le Agenzie federali e i relativi fornitori di software dovranno soddisfare degli standard qualitativi più elevati[92]. L'ordine presidenziale getta inoltre le basi per la realizzazione del Cyber Safety Review Board, un tavolo di consultazioni pubblico-privato da tenersi a seguito di attacchi cibernetici significativi, per valutare le azioni intraprese e quelle da attuare. Il rafforzamento della resilienza dei sistemi e delle infrastrutture tecnologiche in uso negli Usa sarà inoltre oggetto di una partnership pubblico-privata con le principali industrie tecnologiche nazionali, che si sono impegnate a stanziare fondi aggiuntivi per aumentare la resilienza e sicurezza dei propri prodotti[93].

Gli Usa rappresentano un attore di primo piano nella conduzione di operazioni nello spazio cibernetico e possono avere un peso determinante nella definizione di norme condivise a livello internazionale. Le linee strategiche presentate da Biden sottolineano la necessità di concordare modalità per la definizione dell'attribuzione degli attacchi cibernetici. Tale definizione permetterebbe di rispondere in modo proporzionato all'attacco e di osservare l'applicazione del diritto internazionale. Al momento in fase di discussione, il *Cyber Diplomacy Act 2021*[94] mira a creare il Bureau of International Cyberspace Policy all'interno del Dipartimento di Stato, con l'esplicito compito di consigliarlo sulle politiche da attuare nello spazio cibernetico e su questioni legate agli sforzi diplomatici internazionali in corso d'opera.

[89] Sito US Cyber Command: *Our History*, https://www.cybercom.mil/About/History.

[90] US Cyber Command Public Affairs, *US Cyber Command, DHS-CISA Release Russian Malware Samples Tied to SolarWinds Compromise*, 15 aprile 2021, https://www.cybercom.mil/Media/News/Article/2574011.

[91] Stephanie Kelly e Jessica Resnick-ault, "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators", in *Reuters*, 9 giugno 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08.

[92] Gabriele Carrer, "Perimetro cyber, dopo l'Italia gli Usa. La rivoluzione targata Biden", in *Formiche.net*, 13 maggio 2021, https://formiche.net/?p=1388957.

[93] Andrea Shalal, "U.S. to Work with Big Tech, Finance Sector on New Cybersecurity Guidelines", in *Reuters*, 26 agosto 2021, https://www.reuters.com/world/us/cyber-threats-top-agenda-white-house-meeting-with-big-tech-finance-executives-2021-08-25.

[94] Congresso Usa, *H.R.1251 - Cyber Diplomacy Act of 2021*, 23 febbraio 2021, https://www.congress.gov/bill/117th-congress/house-bill/1251.

ISSN 2280-6164

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.

DOCUMENTI IAI 21 | 12 - SETTEMBRE 2021 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.

ISSN 2280-6164

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.

ISSN 2280-6164

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.

[157] Intervista, 4 giugno 2021.

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

ISSN 2280-6164

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

che deve essere biunivoco tra le aziende parte del Perimetro, chiamate a fornire i dati e l'istituzione che, oltre a raccoglierli, dovrebbe poi condividerli nella maniera più opportuna, per creare maggiore *shared situational awareness*.

Altrettanto importante è il dialogo sull'andamento delle minacce, tra gli enti all'interno del Perimetro, così come sulle tecnologie e i correlati trend di mercato. Il coinvolgimento della componente industriale ai tavoli di consultazione istituzionale è particolarmente rilevante nel cyberspace, settore nel quale chi detiene le competenze tecnologiche è anche il detentore delle chiavi crittografiche e della conoscenza del funzionamento dei propri sistemi, nonché della mole di dati che viene trasmessa e scambiata quotidianamente. Nei dispositivi con Ip i dati viaggiano attraverso connessioni e vengono smistati tramite switch dove possono essere appositamente inserite sonde per individuare e decrittare i dati rilevanti, senza che mittente e destinatario si accorgano della condivisione delle informazioni con soggetti terzi. Per mitigare questo problema, senza coltivare l'utopia di avere le competenze necessarie per coprire tutta la catena tecnologica necessaria per un ecosistema di rete, l'Italia potrebbe puntare ad avere alcuni switch e/o software di produzione nazionale, per limitare la dipendenza da fornitori esteri e incrementare le capacità di resilienza nazionale.

Il comparto industriale italiano dovrebbe quindi essere maggiormente valorizzato, attraverso due linee d'azione. La prima consiste nel proseguimento dell'utilizzo del Golden Power, ove necessario, per assicurare il mantenimento della sovranità tecnologica nazionale in quei settori nicchia di competenza nazionale appetibili per investitori stranieri. Oltre a proteggere da tentativi di acquisto esteri ritenuti inopportuni se non ostili, l'Italia potrebbe essere maggiormente attiva nell'individuazione e valorizzazione di tutte le competenze sulle quali è ragionevole pensare alla costruzione di una autonoma capacità industriale e tecnologica nazionale nell'ottica della produzione *secure by design* di prodotti, infrastrutture, sistemi cibernetici e di gestione dati. Una produzione così delineata fornirebbe anche un contributo alla difesa dello stato. La prima linea di difesa è data infatti da un elevato livello generale di resilienza di prodotti, infrastrutture e sistemi in dotazione nel Paese. Il decreto di conversione in legge del DL 82/2021 esplicita la necessità di valorizzare la crittografia come strumento di sicurezza cibernetica e conferisce all'Agenzia il compito di qualificazione dei servizi cloud. Questi due settori, insieme a quelli della produzione di software e chip, nei quali le competenze nazionali possono in alcuni casi competere con attori stranieri, potrebbero essere tra i settori da potenziare e supportare con apposite iniziative e investimenti. Tuttavia, per arrivare a un'applicazione funzionale del principio *secure by design*, è fondamentale il suddetto dialogo tra la Difesa e l'industria nazionale, per creare, mantenere e sviluppare un quadro condiviso delle eccellenze tecnologiche nazionali in questo ambito.

ISSN 2280-6164

La prima Direttiva per la politica industriale della Difesa[163] recentemente emanata pone particolare attenzione sulla necessità di instaurare un partenariato Difesa-industria, nonché sulla necessità di volgere attenzione e risorse alla capacità di sviluppo industriale, tecnologico e di programmi. Un simile approccio è quanto mai importante anche nel settore cibernetico che, con un valore in Italia di circa 1,4 miliardi di euro, è composto da una pluralità di piccole e medie imprese e start-up capaci di apportare un valore aggiunto alle competenze d'innovazione e tecnologia italiane. Le caratteristiche del comparto, della tecnologia e del mercato tendono a frammentazione, dinamismo e fluidità, rendendo più difficile una politica industriale pubblica. Tuttavia è necessario uno sforzo istituzionale per fornire quel supporto mirato, efficace ed efficiente, parte di una seria partnership pubblico-privato, che è visto da molti interlocutori come necessario dato il carattere strategico delle tecnologie in gioco e l'aggressività di competitor e avversari internazionali. In questo contesto dovrebbe inserirsi un'attenzione prioritaria a start-up e piccole e medie imprese, portatrici di innovazione tecnologica potenzialmente molto importante, ma che, se non adeguatamente sostenute e integrate in un ecosistema con attori più consolidati, diventerebbero facile preda di investimenti stranieri volti a carpire competenze e know how.

Partendo da queste considerazioni e sulla falsa riga di altri Paesi europei, l'Italia potrebbe anche creare delle zone economiche speciali, in cui ubicare le aziende che operano nel dominio cyber affinché facciano sistema e, attraverso forme di incentivazione e agevolazioni, supportare il loro lavoro. Il veloce e costante avanzamento tecnologico che caratterizza il settore cibernetico impone la necessità di investimenti costanti e mirati. In questo sforzo, si dovrebbero tenere in considerazione le opportunità offerte dall'Unione Europea attraverso la Permanent Structured Cooperation e il Fondo Europeo di Difesa. Quest'ultimo aggiunge anche la leva del finanziamento e del co-finanziamento, e le Edt – in cui in cyber è compreso – sono un settore che gode di un'attenzione particolare e sul quale si concentrano una parte dei finanziamenti europei[164].

Rafforzamento del livello interforze e difesa avanzata

L'adozione di sistemi, strutture e software *secure by design* e alla frontiera tecnologica, sebbene fondamentale, non è sufficiente ad assicurare la difesa, che deve essere portata a termine tenendo conto della pervasività della minaccia, delle tipologie e dell'intensità degli attacchi cibernetici nonché dei loro obiettivi. In modo più spiccato che negli altri domini operativi, quello cibernetico necessita di una risposta interforze, sia per la protezione delle reti della Difesa, sia per essere in grado di intervenire nel *continuum* della dimensione civile e militare entrambe

[163] Ministero della Difesa, *Direttiva per la politica industriale della Difesa, Edizione 2021*, https://www.difesa.it/Documents/Direttiva_Ministro_Guerini2907.pdf.

[164] Su Edt e iniziative Ue si veda: Ester Sabatino e Alessandro Marrone, "Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy?", in *IAI Commentaries*, n. 21|31 (giugno 2021), https://www.iai.it/it/node/13569.

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

coinvolte negli attacchi cibernetici, soprattutto nel caso di obiettivi civili di rilevanza strategica per lo stato.

A protezione delle infrastrutture, dei sistemi di comunicazione e infostrutturali della Difesa opera il Cor a carattere interforze. Lo sforzo di "interforzizzazione" del comando, operativo dal 2020, potrebbe essere ulteriormente migliorato, con effetti positivi per quanto attiene alla concentrazione della domanda, l'eliminazione di inefficienze e duplicazioni, lo sfruttamento di economie di scala e l'incremento dell'interoperabilità dei sistemi utilizzati, da raggiungere a valle di un processo di integrazione degli aspetti operativi con quelli di sviluppo tecnologico. Il tutto, a vantaggio sia delle istituzioni pubbliche che delle industrie italiane del settore.

Passando alle possibili operazioni che possono essere condotte in linea con il quadro normativo italiano, l'approccio delle Forze Armate si differenzia da quello dei principali attori Nato di riferimento. Nel paragone con le operazioni che vengono condotte in Usa, Francia e Regno Unito, l'Italia si differenzia per l'impossibilità di portare a termine operazioni offensive in senso stretto in assenza di un attacco. Il Cor conduce operazioni con un certo vantaggio in termini di mantenimento dell'iniziativa rispetto agli avversari, sia in Italia sia nei teatri operativi all'estero, ma l'approccio di "difesa avanzata" portato avanti in vario modo da altri Paesi Nato non risulta essere attualmente contemplato in Italia. La difesa avanzata apporta vantaggi in termini di deterrenza e resilienza, ma per ottenerli sono tuttavia necessarie alcune regole di ingaggio più flessibili, che autorizzino le Forze Armate all'uso e gestione di contromisure cibernetiche in reazione a un attacco cyber a infrastrutture critiche.

Inoltre, dal momento che gli strumenti impiegati per effettuare un attacco cibernetico sono in gran parte gli stessi che vengono utilizzati per il normale utilizzo delle reti, strutture, sistemi e software cibernetici, avere delle competenze nella fase di attacco equivale a conoscere le procedure necessarie a difendersi e rispondere all'evento ostile. Come l'impresa attua il *reverse engineering* per acquisire nuove competenze e conoscenze, allo stesso modo essere in grado di attaccare un avversario significa conoscere le procedure che l'attaccato porrà in essere per difendersi e i successivi passaggi necessari per portare a termine l'attacco.

In generale, le suddette opzioni e proposte richiedono livelli di investimento più elevati, certi e costanti nel tempo, se l'Italia vuole affrontare seriamente il tema della difesa cibernetica. Il tardivo raggiungimento della piena capacità operativa del Comando, evidenzia la necessità di maggiori investimenti nel settore cibernetico e in particolare nella formazione di personale altamente qualificato che sia in grado di rispondere adeguatamente agli attacchi. Le competenze acquisite dalle Forze Armate potrebbero essere messe a sistema e, nell'ottica di razionalizzazione delle risorse e dell'agire per il sistema-Paese, essere sfruttate per la formazione dei funzionari civili dello stato, a vario titolo coinvolti nel più ampio quadro della sicurezza cibernetica nazionale.

ISSN 2280-6164

Riflessione Nato e ruolo dell'Italia

Allargando infine l'orizzonte a livello globale e in termini di prospettiva storica, si può affermare che gli alleati Nato negli anni '90 e 2000 hanno perso l'occasione di avviare una riflessione condivisa sulle implicazioni di internet per la sicurezza internazionale. In un certo senso Russia e Cina le hanno comprese prima dell'Occidente e le hanno sfruttate in modo molto efficace nello scorso decennio, costringendo gli alleati a giocare sulla difensiva in questo dominio.

Certamente, come evidenziato nel capitolo precedente, gli Stati Uniti grazie al primato tecnologico ed economico del proprio settore high tech e digitale sono in una posizione privilegiata per influenzare il dominio cibernetico. Ma dai documenti americani degli ultimi anni traspare tutta la preoccupazione per la perdita di tale vantaggio nei confronti della Cina e per l'efficace aggressività online della Russia nel quadro della guerra ibrida.

In generale, l'assenza di una riflessione strategica condivisa dagli alleati su questo campo ha portato a uno sviluppo tecnologico ed economico impetuoso quanto slegato dalle priorità della sicurezza nazionale, ai danni del principio *secure by design* che oggi si cerca di recuperare e attuare.

In questo contesto, negli ultimi anni la Nato si sta attrezzando non solo per operare nel dominio cibernetico, ma anche per comprenderne appieno tutte le implicazioni di sicurezza. A questo si collega la nuova priorità data dall'Alleanza alle Edt, molte delle quali sono intrinsecamente cyber, a partire dall'intelligenza artificiale, e l'appello per dei trattati internazionali che regolino in qualche modo il cyberspace. Questa riflessione Nato è importante per l'Italia, ed è importante che Roma vi contribuisca portando un proprio punto di vista autonomo.

aggiornato 27 settembre 2021

ISSN 2280-6164

Lista degli acronimi

Acd	Active Cyber Defence
Acn	Agenzia per la Cybersicurezza nazionale
Aco	Allied Command Operations
Act	Nato Allied Command Transformation
Aise	Agenzia Informazioni e Sicurezza Esterna
Aisi	Agenzia Informazioni e Sicurezza Interna
Anssi	Agence nationale de la sécurité des systèmes d'information
Apt	Advanced Persistent Threat
Bsi	Bundesamt für Sicherheit in der Informationstechnik
C4	Command, control, communication, and computers
C4d	Comando interforze C4 Difesa
Casmd	Capo di Stato Maggiore della Difesa
Ccdcoe	Cooperative Cyber Defence Center of Excellence
Cdc	Cyber Defence Committee
Cdmb	Cyber Defence Management Board
Cert	Computer Emergency Response Team
Cic	Comitato Interministeriale per la Cybersicurezza
Cioc	Comando Interforze per le Operazioni Cibernetiche
Cir	Kommando Cyber- und Informationsraum
Cisr	Comitato Interministeriale per la Sicurezza della Repubblica
Coc	Cellule Operative Cibernetiche
Cofs	Comando interforze per le operazioni delle forze speciali
Coi	Comando Operativo di vertice Interforze
Cor	Comando per le Operazioni in Rete
Csirt	Computer Security Incident Response Team
Cvcn	Centro di Valutazione e Certificazione Nazionale
CyberCom	US Cyber Command
Cyoc	Cyber Operation Command
Difnet	Rete della Difesa
Dis	Dipartimento delle Informazioni per la Sicurezza
Dpcm	Decreto del Presidente del Consiglio dei Ministri
Dpp	Documento programmatico pluriennale
Edt	Emerging and Disruptive Technologies
Esp-Cert-Def	Centro de Respuesta ante Incidentes del Ministerio de Defensa
Foc	Full Operational Capability
Foce	Fuerza de Operaciones en el Ciber Espacio
Gchq	Government Communication Headquarters

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

Ict	Information and Communications Technology
Ioc	Infrastructure Operations Center
Ip	Internet Protocol
Issmi	Istituto Superiore di Stato Maggiore Interforze Mobile
Jcisfas	Jefatura de Sistemas de Información y Telecomunicaciones
Ladc	Laboratorio Addestrativo per la Difesa Cibernetica
Man	Metropolitan Area Network
Mccd	Mando Conjunto de Ciberdefensa
Mcce	Mando Conjunto del Ciber Espacio
Nac	North Atlantic Council
Ncf	National Cyber Force
Ncia	Nato Communications and Information Agency
Ncirc	Nato Computer Incident Response Capability
Ncsc	Nato Cyber Security Center
Noc	Network Operations Center
Nsa	National Security Agency
Nsc	Nucleo per la Sicurezza Cibernetica
Pnrr	Piano Nazionale di Ripresa e Resilienza
Rifon	Rete Interforze in Fibra Ottica Nazionale
Rni	Rete Numerica Interforze
Rsc	Reparto di Sicurezza Cibernetica
Siem	Security Information and Event Management
Smd	Stato Maggiore della Difesa
Soc	Security Operations Center
Stelmilit	Scuola Telecomunicazioni Forze Armate

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

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*