Osservatorio
di Politica internazionale

Senato
della Repubblica

Camera
dei deputati

Ministero
degli Affari Esteri
e della Cooperazione
Internazionale

La difesa cibernetica in Europa
Una panoramica degli ultimi sviluppi e le opportunità per l'Italia

giugno 2020

159

Approfondimenti

A cura delll'Istituto Affari Internazionali (IAI)

APPROFONDIMENTO

La difesa cibernetica in Europa
Una panoramica degli ultimi sviluppi e le opportunità per l'Italia

di Cristian Barbieri*

a cura dell'Istituto Affari Internazionali (IAI)

giugno 2020

* Cristian Barbieri collabora con il Programma Tecnologie e Relazioni internazionali dell'Istituto Affari Internazional (IAI). Recentemente ha svolto consulenze presso la Presidenza del Consiglio dei Ministri e la Fondazione Safe. In passato è stato tirocinante presso l'Agenzia dell'Unione europea Europol, specializzandosi in protezione dei dati, *e-evidence* e privacy, presso la Missione UE in Kosovo Eulex e presso l'Ambasciata italiana in Kosovo, maturando un'esperienza relativa alla cooperazione tra le forze di polizia europee e i Balcani.

I N D I C E

Executive Summary

L'Organizzazione del Trattato del Nord Atlantico (NATO) e l'Unione europea (UE) hanno riconosciuto il campo cibernetico come teatro di possibili conflitti militari e definito lo stesso come quinto dominio di scontro, oltre a terra, aria, mare e spazio, sin dal 2016. Gli elementi unici del dominio cibernetico quali l'ubiquità, la velocità di trasmissione dei dati e l'assenza di confini geografici e politici collocano la materia tra il novero delle nuove minacce ibride, con conseguenze per l'intera Ue.

Nonostante ciò, a livello europeo la questione della difesa cibernetica appare ancora in una fase embrionale. Dal punto di vista politico-strategico vanno sottolineati due elementi di innovazione: l'istituzione da parte della Commissione a guida Ursula von der Leyen della nuova Dg Defis (*Directorate-General Defence Industry and Space*), che avrà competenze in materia di industria della difesa, compresa la difesa cibernetica, e l'aggiornamento nel novembre 2018 del *Quadro strategico dell'Ue in materia di ciberdifesa* adottato dal Segretariato generale del Consiglio dell'UE nel novembre 2014.

Dal punto di vista operativo, la Commissione europea e il Consiglio dell'Ue si affidano principalmente al lavoro dell'EDA, l'Agenzia europea per la difesa, rafforzata recentemente nella *mission* e nelle finanze. L'EDA contribuisce alla ricerca e allo sviluppo di soluzioni tecnologiche di difesa cibernetica attraverso la cooperazione strutturata permanente (PeSCo), la Revisione annuale coordinata sulla Difesa (CARD) e i progetti pilota PADR (*Preparatory Action on Defence Research*).

L'Italia aderisce a queste iniziative. Tuttavia, nello specifico delle Padr, seppur ben inserita nei primi progetti, essa non ha ancora mostrato la proattività richiesta dal campo della difesa cibernetica e necessaria per posizionarsi in maniera adeguata in questo settore crescente. Il nostro Paese potrebbe usufruire delle piattaforme di scambio di informazioni per affinare la recente messa in opera di strumenti di difesa cibernetica sul territorio nazionale, come il Comando interforze per le operazioni cibernetiche (Cioc), traendo spunto da quegli Stati membri che hanno una cultura più sensibile nei confronti delle problematiche della difesa *cyber* e strutture più avanzate. Inoltre, contribuendo ai progetti europei, l'Italia potrebbe influenzare le strategie e dottrine europee in ambito cibernetico-militare.

La difesa cibernetica: un nuovo dominio di scontro

Il campo cibernetico è riconosciuto, dal 2016, sia dall'Organizzazione del Trattato del Nord Atlantico che dall'Unione europea, come teatro di possibili conflitti militari e definito come quinto dominio di scontro, oltre a terra, aria, mare e spazio[1].

Il dominio cibernetico è caratterizzato da elementi unici quali l'ubiquità, la velocità di trasmissione dei dati e l'assenza di confini geografici e politici. Gli Stati membri dell'UE non sono immuni da possibili attacchi ad opera di gruppi sponsorizzati da stati esteri o da comandi cibernetici esterni all'Unione. Gli eserciti nazionali stanno sviluppando una fortezza dimensione cibernetica e molti tra gli Stati membri hanno adottato una strategia di difesa cibernetica talvolta anche attraverso l'istituzione di veri e propri comandi *cyber*[2].

Osservare il tema della difesa cibernetica sul piano europeo significa analizzarlo alla luce di caratteristiche multilaterali e multilivello. Occorre riconoscere che l'accostamento di tre concetti come cibernetica, difesa e Unione europea può risultare arduo per tre ordini di problemi, uno per ognuno dei termini proposti.

In primis, si può partire dal lemma cibernetico. Lo studio della materia cibernetica è ancora parzialmente inesplorato dalla ricerca accademica e risulta complicato per la generalità del termine stesso che afferisce a campi diversi della conoscenza. Una prima doverosa distinzione che permette di restringere il campo di analisi è quella tra i concetti di *sicurezza cibernetica* e di *difesa cibernetica*. Con la prima si intende più in generale la sicurezza delle infrastrutture cibernetiche, siano esse private o pubbliche, di interesse nazionale e non, oggetto di attacchi e intrusioni esterni o soggetti a incidenti, e principalmente con riferimento agli attori civili dello Stato.

L'UE ha regolato questa materia attraverso il *Cybersecurity Act*[3], regolamento che prevede tra l'altro il rafforzamento dell'agenzia preposta alla sicurezza cibernetica, l'Agenzia europea per la Sicurezza delle reti e dell'informazione (*European Network and Information Security Agency*, ENISA), e dei centri tecnici nazionali, i *Computer Emergency Response Team* (CERT)[4]. Altro documento fondamentale nel campo della sicurezza cibernetica è la direttiva NIS[5], recepita in Italia con il decreto legislativo del 18 maggio 2018, n. 65[6].

---

1 NATO, *Cyber Defence*, aggiornato 17 marzo 2020, https://www.nato.int/cps/en/natohq/topics_78170.htm.

2 L'Italia ha costituito il Comando interforze per le operazioni cibernetiche (Cioc) nel 2017. Vedi intervista al Capo di Stato maggiore della Difesa Claudio Graziano: "Cyber Defence - Nasce il Comando Interforze per le Operazioni Cibernetiche", in *Informazioni della Difesa*, n. 3/2017, p. 6-16, https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/cyber_defence.pdf. Dall'ottobre 2019 il Generale di Brigata Giorgio Cipolloni è al comando del Cioc.

3 Sito della Commissione europea: *The EU Cybersecurity Act*, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

4 I CERT sono team di lavoro preposti ad una rapida risposta ad incidenti informatici. In Italia il responsabile per la pronta risposta ad incidenti informatici per la pubblica amministrazione è il CERT-PA operante all'interno dell'Agenzia per l'Italia digitale (Agid): https://www.cert-pa.it.

5 Direttiva (UE) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, OJ L 194, 19 luglio 2016, p. 1-30, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:32016L1148.

6 Decreto legislativo 18 maggio 2018, n. 65: Attuazione della direttiva (UE) 2016/1148…, https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg.

Per difesa cibernetica, invece, si intende lo spettro delle competenze di natura puramente militare dello Stato, e quindi, la tutela e salvaguardia di ciò che possa arrecare danno alla nazione. Qui si pone quindi una prima difficoltà di interpretazione, non facilmente risolvibile, riguardante l'ibridazione della difesa con la sicurezza.

Difatti, se in altri domini militari la natura militare è facilmente distinguibile da quella civile, si pensi al dominio marittimo ad esempio e alla distinzione tra navi militari e navi civili, nel nuovo quinto dominio cibernetico tale divisione, vista la natura duale delle tecnologie, non è facilmente rintracciabile. È necessario quindi operare alcune scelte interpretative.

La difesa cibernetica è intesa, in questo Approfondimento, come difesa *tout court* del territorio nazionale da possibili intrusioni estere o attacchi a porzioni fisiche del territorio. Essa può risultare decisiva nella protezione delle infrastrutture critiche, siano essi ospedali, reti di approvvigionamento energetico, reti di funzionamento dei trasporti. In aggiunta a ciò, la difesa cibernetica può e deve essere intesa come la difesa dell'apparato tecnologico, sia operativo che strategico, delle strutture militari operanti in territorio italiano. Si parla quindi in questo caso delle componenti cibernetiche nell'apparato difesa.

Bisogna distinguere tra *cyber* come dominio, cioè campo di azione e di potenziale battaglia, attraverso attacchi informatici capaci di bloccare intere città o funzioni vitali di un paese, e *cyber* come mezzo e infrastruttura, cioè come semplice strumento di trasmissione di informazioni per mezzo della rete. In ultima istanza, resta ancora lontana tra gli esperti e gli studiosi un'esaustiva definizione di guerra cibernetica; basti pensare anche solo alla mancanza di coerenza nell'utilizzo dei termini inglesi, *cyber warfare*, cyber war e *cyber terrorism*[7].

Il secondo punto che necessita di essere chiarito riguarda il termine difesa. In ambito europeo la competenza in tal senso è tra le più discusse e si rifà al concetto di sovranità. Storicamente, la mancata formazione di un esercito europeo, rappresentata dal fallimento della Comunità europea di difesa (CED), ha insegnato che la rinuncia degli Stati membri ad una parte di competenza così delicata come la sovranità militare è lontana dall'essere attuabile in un contesto comunitario che tende ad un preoccupante riemergere di istanze sovraniste.

La Politica di sicurezza e di difesa comune (PSDC) dell'UE resta fortemente influenzata da decisioni intergovernative. Questo rende più difficilmente attuabile, in un prossimo futuro, l'autonomia strategica sul piano militare ambìta e necessaria all'Unione per competere in contesti internazionali.

Di contrasto, è da tenere in conto la frammentazione delle spese nell'ambito della difesa degli Stati membri, risultante in una deficienza nell'interoperabilità a livello europeo delle molte soluzioni nazionali e alla dipendenza da aziende esterne all'UE per strumenti chiave della difesa nazionale. Per questa ragione l'Unione sta tentando negli

---

[7] Sulla questione della mancanza di una definizione condivisa si veda: Cristian Barbieri, Jean-Pierre Darnis, Carolina Polito, "Non-proliferation Regime for Cyber Weapons. A Tentative Study", in *Documenti IAI*, n. 18|03 (marzo 2018), https://www.iai.it/it/node/8870.

ultimi anni una convergenza verso, se non una difesa comune europea, una politica di *pooling and sharing* (messa in comune e condivisione) delle risorse a livello nazionale[8].

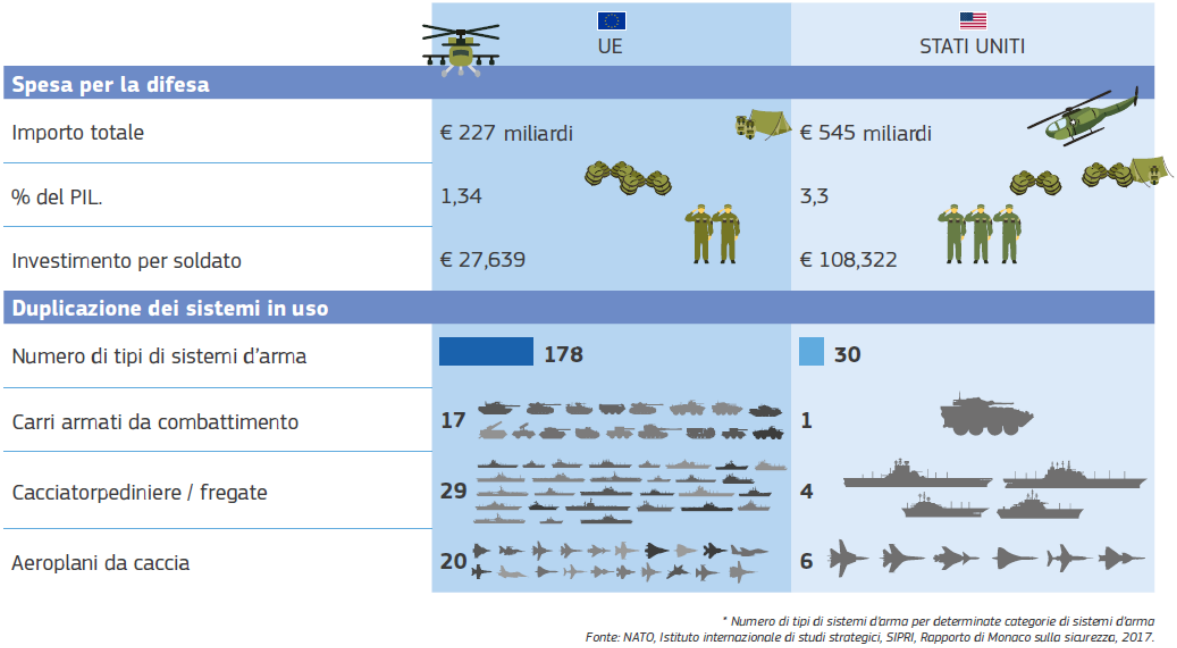

Figura 1 - Il costo della frammentazione e delle inefficienze attuali – Fonte: Commissione europea, *Verso un'Unione europea della difesa*, maggio 2019, https://doi.org/10.2775/60537.

Questo passaggio ci porta all'ultimo termine cardine: l'UE stessa. Senza divagare sui possibili futuri sviluppi dell'Unione, è fondamentale sottolineare che quanto a competenza militare nell'ambito della difesa cibernetica in Europa lo scenario appare tutt'ora frastagliato e non ben definito. I fondi dell'Unione per attività di ricerca e sviluppo in ambito di difesa sono stati attivati solo a partire dal 2017[9].

Da un punto di vista strategico, gli ultimi documenti prodotti in ambito europeo, che verranno analizzati nel prossimo paragrafo, sono formulati dal Parlamento Europeo e dalla Commissione Europea, mentre sul piano operativo, numerose sono le agenzie e gli organi dell'UE che annoverano all'interno del proprio mandato una competenza cibernetica. Tra queste, le più importanti in materia di difesa cibernetica sono: l'Agenzia europea per la difesa (EDA)[10], ENISA[11] e l'Accademia europea per la sicurezza e la difesa (AESD)[12].

---

8 Rosalie Parent, *Pooling & sharing: Member States' engagement and the support by the EU*, Bruxelles, Parlamento europeo, 2015, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/534994/EXPO_IDA(2015)534994_EN.pdf.

9 Parlamento europeo, *L'Unione europea sostiene gli investimenti militari congiunti*, 3 luglio 2018, https://www.europarl.europa.eu/news/it/headlines/security/20180122STO92206/l-unione-europea-sostiene-gli-investimenti-militari-congiunti.

10 Sito EDA: https://www.eda.europa.eu.

11 Sito ENISA: https://www.enisa.europa.eu.

12 Sito AESD: https://esdc.europa.eu.

In conclusione, la complessità nel definire l'ambito di azione della difesa cibernetica è amplificata nel contesto europeo multilaterale in cui coesistono azioni comunitarie ed intergovernative.

La strategia europea in ambito cibernetico e i fondi per la difesa cibernetica

Da un punto di vista strategico sono pochi i documenti ufficiali degli organi UE che concorrono a stabilire una strategia europea di difesa cibernetica. Al contrario della strategia di sicurezza cibernetica, adottata nel 2017 con il *cybersecurity act*[13], sono assenti iniziative legislative del Parlamento europeo in ambito di difesa cibernetica.

Già da una rapida lettura del *Libro bianco sul futuro dell'Europa*[14] e del *Documento di riflessione sul futuro della difesa europea*[15], entrambi prodotti dalla Commissione europea nel 2017, si nota che il tema della difesa cibernetica è poco più che un'apparizione estemporanea lasciata alla volontà di cooperazione intergovernativa degli Stati membri e alla cooperazione in ambito Nato.

Il documento strategico più utile a comprendere gli sviluppi nel contesto europeo della difesa cibernetica è il *Quadro strategico dell'UE in materia di cyberdifesa* adottato dal Consiglio dell'UE nel novembre 2014 e il cui ultimo aggiornamento è del 19 novembre 2018[16].

Tale documento, già dalla premessa, conferma la definizione Nato del ciberspazio come quinto dominio operativo a sé stante, e si pone come obiettivo di sviluppare ulteriormente la politica di difesa cibernetica dell'UE attraverso sei priorità: il sostegno alle capacità di sviluppo della difesa cibernetica; il rafforzamento della sicurezza dei canali di informazione e comunicazione della Politica di sicurezza e di difesa comune; la promozione della cooperazione civile-militare; lo sviluppo di ricerca e tecnologie; il miglioramento delle opportunità di formazione, istruzione ed esercitazione; e infine il potenziamento della cooperazione con altri partner internazionali, in particolare con la NATO.

a) Sostegno alle capacità di sviluppo della difesa cibernetica

Il Consiglio sottolinea la necessità di una visione comune in merito al campo di applicazione della difesa cibernetica. In questo modo, il Consiglio intende invitare gli Stati membri, su base volontaria, a migliorare la cooperazione tra i CERT militari nazionali e il CERT-EU, allo scopo di rendere più efficace la prevenzione e il trattamento degli incidenti, ad utilizzare i fondi in ambito di Cooperazione strutturata permanente (*Permanent Structured Cooperation*, PeSCo)[17] ed a sfruttare il Fondo

---

[13] Sito Commissione europea: *Cybersecurity*, aggiornato 8 marzo 2020, https://ec.europa.eu/digital-single-market/en/cyber-security.

[14] Commissione europea, *Libro bianco sul futuro dell'Europa. Riflessioni e scenari per l'UE a 27 verso il 2025* (COM/2017/2025), 1 marzo 2017, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52017DC2025.

[15] Commissione europea, *Documento di riflessione sul futuro della difesa europea* (COM/2017/315), 7 giugno 2017, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52017DC0315.

[16] Consiglio dell'Unione europea, *Quadro strategico dell'UE in materia di ciberdifesa*, 19 novembre 2018, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/it/pdf.

[17] Sito PeSCo: https://pesco.europa.eu.

europeo per la difesa (*European Defence Fund*, EDF)[18] per sviluppare congiuntamente capacità di difesa cibernetica.

Una forte spinta, perlomeno a livello simbolico, verso una maggiore integrazione europea in ambito militare, e conseguentemente in ottica di difesa cibernetica, è stata recentemente prodotta dalla Commissione guidata da Ursula von der Leyen con la decisione, unica nella storia dell'UE, di istituire una Direzione generale (Dg) Industria della difesa e spazio (*Directorate-General Defence Industry and Space*, Dg Defis)[19].

La Dg Defis tuttavia, per le già citate ritrosie di alcuni Stati membri nell'accettare una competenza così delicata in seno alla Commissione, si concentra principalmente su due pilastri: l'industria della difesa e lo spazio. Installatasi a pieno regime il 25 febbraio del 2020, la struttura non ha ancora prodotto effetti concreti, se si escludono le nomine dei capi unità e la decisione di ereditare dalla Dg Mercato interno la gestione del cruciale EDF. Va sottolineato, in questo caso, la totale assenza di funzionari italiani in posti chiave dell'industria della difesa, occupata da funzionari di nazionalità francese e tedesca[20]. L'EDF è stato istituito dalla commissione guidata da Jean-Claude Juncker nel 2017, con il chiaro obiettivo di raggiungere un'autonomia strategica europea nel campo della difesa, che risultava essere esageratamente duplicata (si pensi solo alle 17 differenti tipologie di carri armati presenti nell'UE).

L'EDF ha due sezioni, una dedicata alla ricerca (*research window*), la cui gestione è affidata all'EDA attraverso il programma Azione preparatoria per la ricerca nel settore della difesa (*Preparatory Action on Defence Research*, PADR), e una di sviluppo delle capacità che è gestita dalla Dg Defis attraverso il Programma europeo di sviluppo del settore industriale della difesa (*European Defence Industrial Development Programme*, EDIDP). L'UE ha stanziato per questo fondo 500 milioni di euro in co-finanziamento per gli Stati membri per il biennio 2019-2020[21], come descritto dalla figura 2.

---

[18] Sito Commissione europea: *European defence fund*, https://ec.europa.eu/growth/sectors/defence/european-defence-fund_en.

[19] Sito Commissione europea: *Defence Industry and Space*, https://ec.europa.eu/info/departments/defence-industry-and-space_en.

[20] Ibid.: *DG Defis – Organigramme*, https://ec.europa.eu/info/sites/info/files/organisation_charts/dg-defis-organigramme_en.pdf

[21] Sui fondi europei si veda anche: Alessandro Marrone, Paola Sartori, "Recenti sviluppi verso la difesa europea: opportunità e sfide per l'Italia", in *Approfondimenti dell'Osservatorio di politica internazionale*, n. 148 (gennaio 2019), http://www.parlamento.it/documenti/repository/affariinternazionali/osservatorio/approfondimenti/PI0148.pdf

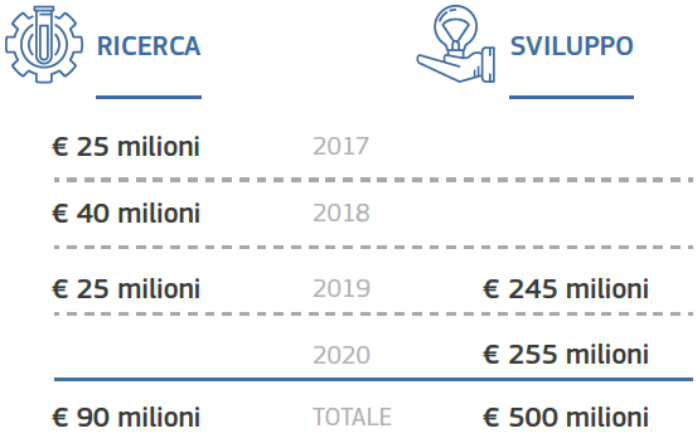

Figura 2 – Bilancio dell'Ue per l'industria della difesa 2017-2020 – Fonte: Commissione europea, *Verso un'Unione europea della difesa*, cit.

La decisione di creare un'industria europea della difesa attraverso questo fondo ha forti ripercussioni anche sul piano della difesa cibernetica, visto che un totale di circa 32 milioni di euro è disponibile per progetti relativi alle capacità di difesa cibernetica (figura 3). Questi sono suddivisi equamente per la progettazione del 2019 e per quella del 2020, aspirando a colmare il *gap* europeo nella sicurezza delle infrastrutture militari.

Intelligence, secured communication & Cyber		
Categories	Budget per category	
	2019	2020
Cyber situational awareness and defence capabilities, military networks and technologies for secure communication and information sharing	€ 17.7 million	€ 14.3 million
Space Situational Awareness (SSA) and early warning capabilities		€ 22.5 million
Positioning, Navigation and Timing (PNT) and satellite communication capabilities	€ 44.1 million	
Maritime surveillance capabilities		€ 20 million
European Command and Control (C2) system from strategic to tactical level	€ 20 million	

Figura 3 - I fondi EDIDP per la difesa cibernetica in Europa – Fonte: Commissione europea, *Stepping up the EU's role as a security and defence provider*, marzo 2019, https://ec.europa.eu/docsroom/documents/34509

In generale, sarà interessante comprendere, nel corso del 2020, se la nuova Commissione attraverso Dg Defis riuscirà ad ottenere una maggiore partecipazione degli Stati al fondo o se la strada verso l'autonomia strategica dell'UE sarà percorsa solo da una minima parte della totalità degli Stati membri. In questo ultimo caso, sarebbe opportuno che l'Italia facesse parte della coalizione di volenterosi per poter influenzare lo sviluppo dell'industria europea della difesa.

b) Rafforzamento della comunicazione e informazione della PSDC

Questa priorità è soprattutto di natura operativa ed organizzativa interna all'UE per la PSDC e non si rivolge agli Stati membri. È chiara la necessita di rendere sicuri i canali operativi delle missioni PSDC e viene quindi richiesto ad ogni documento programmatico delle missioni (*Concept of Operations*) di aggiungere un capitolo riguardante la sicurezza e la difesa delle reti da eventuali attacchi esterni.

L'azione principale è volta a sviluppare il concetto di difesa strategica per le missioni e operazioni militari in ambito PSDC ed attuate internamente al Servizio europeo per l'azione esterna (SEAE) congiuntamente alle sue divisioni (*European Union Military Staff*, EUMS; *Military Planning and Conduct Capability*, MPCC; *Crisis Management and Planning Directorate*, CMPD; *Civilian Planning and Conduct Capability*, CPCC).

c) Promozione e cooperazione civile-militare

La terza priorità del Consiglio in ambito di difesa cibernetica affronta il tema della cooperazione civile-militare, cruciale per l'efficacia degli strumenti di difesa dello spazio cibernetico. Allo stesso tempo, tale strumento, è uno dei più difficili da sviluppare proprio a causa della natura riservata delle operazioni militari. Conscio di ciò, il Consiglio sollecita la cooperazione intra-europea tra le agenzie dell'Unione, siano esse a carattere militare, come l'EDA, o a carattere civile come ENISA e EUROPOL.

Gli ostacoli alla collaborazione sono legati principalmente alle classificazioni dei documenti e alla confidenzialità delle strategie di difesa cibernetica a livello nazionale. La cooperazione risulta complicata anche a livello nazionale, tanto che il Consiglio invita agli Stati membri a promuovere internamente la cooperazione civile-militare attraverso un corretto scambio di informazioni tra i CERT nazionali e gli organi preposti alla sicurezza cibernetica individuati dalla direttiva NIS. Per quanto riguarda la condivisione di informazione tra gli Stati membri, il Consiglio si affida ai fondi stanziati con l'EDF e alla sua "finestra" di ricerca PADR, chiedendo agli Stati membri la maggiore inclusione possibile di soggetti civili, quali industrie e centri di ricerca europei.

d) Ricerca e tecnologia

L'obiettivo cardine del *Quadro strategico* è di raggiungere una capacità autonoma europea di difesa cibernetica; ciò è raggiungibile solo attraverso un forte investimento in ricerca e sviluppo di nuove tecnologie, con la collaborazione e cooperazione degli Stati membri. Anche in questo caso sono disponibili per gli Stati membri i fondi dell'EDF, sia sul piano della ricerca tramite le PADR sia su quello dello sviluppo delle capacità con l'EDIDP, fondi gestiti dall'EDP[22].

Il Consiglio affida inoltre alla Commissione europea il compito di promuovere una catena di approvvigionamento di tecnologia favorendo il mercato europeo delle piccole e medie imprese e istituendo un Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e una Rete dei centri nazionali di coordinamento. La

[22] Cfr. sezione III.

proposta di istituzione del Centro è al momento al vaglio del Parlamento europeo e, se attivato nel 2020, potrebbe migliorare il coordinamento delle azioni di ricerca anche sul piano della difesa cibernetica[23].

Si nota la consapevolezza da parte della Commissione europea della scarsità di strutture adeguate, quali un forte mercato europeo capace di sopperire alle richieste di sicurezza cibernetica degli Stati membri e dell'Unione stessa, e la necessità di affidarne il coordinamento alla Commissione europea stessa. In aggiunta, sul piano della ricerca e dello sviluppo di nuove tecnologie, va sottolineata la decisione dell'EDA e della Commissione europea di mettere in comune le rispettive agende di sviluppo tecnologico, punto critico negli anni precedenti in quanto fonte di duplicazione di progetti interno all'UE.

e) Miglioramento delle opportunità di formazione, istruzione ed esercitazione

Come osservato in molte ricerche, il fattore umano incide fino al 40 per cento circa sugli incidenti informatici[24]; gli individui, siano essi semplici utenti o specialisti di sicurezza cibernetica, sono la prima e ultima linea di difesa nel campo cibernetico[25]. La cosiddetta vulnerabilità informatica passa quindi anche da un singolo utente debole della catena operativa.

Consapevole di ciò, il Consiglio pone come priorità il miglioramento delle opportunità di formazione, istruzione ed esercitazione di personale Ue e degli Stati membri. Esse si svolgono sia in seno all'Unione, in particolare grazie al rafforzamento del ruolo svolto dall'AESD[26], che tra partner internazionali come per esempio gli accordi stretti tra UE e NATO.

f) Potenziamento della cooperazione con la NATO

Il Consiglio individua la necessità di incrementare la cooperazione con la NATO per lo sviluppo di capacità di difesa cibernetica efficaci e resilienti quale una delle priorità. La Nato fa del Centro di eccellenza cooperativa in difesa cibernetica (*Cooperative Cyber Defence Centre of Excellence*, CCDCOE) di Tallin in Estonia uno dei fiori all'occhiello dell'organizzazione.

Il CCDCOE è stato fondato nel 2007 in risposta all'attacco ai sistemi estoni, sponsorizzato dalla Russia, che bloccò il paese baltico per due settimane[27]. Grazie

---

[23] Commissione europea, *Proposta di Regolamento che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento* (COM/2018/630), 12 settembre 2018, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52018PC0630.

[24] ENISA, *Cyber Security Culture in organisations*, novembre 2017, https://doi.org/10.2824/10543; IBM, *2019 Cost of a Data Breach Report*, https://www.ibm.com/security/data-breach.

[25] Wolfgang Röhrig, Rob Smeaton, "Cyber security and cyber defence in the European Union. Opportunities, synergies and challenges", in *Cyber Security Review*, Summer 2014, p. 23-27, https://www.cybersecurity-review.com/?p=1071.

[26] Cfr. sezione III.

[27] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", in Dan Remenyi (a cura di), *Proceedings of the 7th European Conference on Information Warfare and Security*, Reading, Academic Publishing, 2008, p. 163-168, https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective.

all'esperienza maturata e ad una forte struttura organizzativa, il CCDCOE ha una rapida capacità di risposta ad incidenti informatici e organizza annuali esercitazioni di eccellenza mondiale, il *Cyber Coalition Exercise,* alla cui ultima sessione erano presenti anche rappresentanti dell'UE[28].

La collaborazione in materia cibernetica è svolta sulla base della dichiarazione di Varsavia, firmata l'8 luglio del 2016[29]. Tale dichiarazione consente lo scambio di concetti e dottrine militari, la partecipazione congiunta a esercizi cibernetici, la formazione e lo scambio di informazioni tecniche tra CERT-EU, CERT nazionali e il *NATO Computer Incident Response Capability* (NCIRC). Quest'ultimo punto in particolare è di cruciale importanza, se si pensa che nel solo 2019 lo scambio di informazioni NATO-UE ha riguardato ben 41 eventi critici[30]. La collaborazione è stata a più riprese confermata ad alto livello – l'ultimo incontro risale al dicembre 2019 – sottolineando l'esistenza di interessi strategici e la volontà di aumentare le occasioni di scambio.

Tuttavia, occorre anche sottolineare due punti critici di tale collaborazione. *In primis* riguardo l'ambivalenza generale del rapporto UE-NATO, dovuta alla presenza di membri esterni all'UE come Stati Uniti, Turchia e Regno Unito che rende più difficile il già delicato equilibrio decisionale europeo sia su un piano politico sia su un piano operativo. Tale presenza rende infatti le superiori dotazioni Nato in termini di difesa cibernetica, non direttamente fruibili dalla totalità degli Stati membri venendo a mancare il requisito dell'interoperabilità delle strutture all'interno del sistema UE, vista anche l'assenza di sei Stati membri UE nel Patto atlantico.

In secondo luogo, per essere davvero efficace, la collaborazione deve andare oltre l'attuale mero scambio di informazioni tecniche e partecipazione a esercitazioni congiunte. Da un punto di vista politico, una coerenza interpretativa di UE e NATO sul diritto internazionale del ciberspazio, come ad esempio sulle sanzioni da adottare per comportamenti statali illegali, potrebbe risultare in una codificazione più efficace dello stesso.

Sul piano operativo, la creazione di un esercizio annuale di difesa cibernetica congiunto, al posto di semplici, e talvolta incostanti nel tempo, partecipazioni di Stati membri UE a esercizi Nato e viceversa, potrebbe migliorare la *situational awareness* nelle due organizzazioni e facilitare lo scambio di informazioni tra civile e militare.[31]

La cooperazione con la NATO non può quindi, in ultima istanza, sostituire uno sviluppo autonomo della difesa cibernetica dell'UE e deve essere perseguita come un corollario della strategia di difesa cibernetica dell'UE stessa.

---

28 Sito CCDCOE: *Exercises*, https://ccdcoe.org/exercises.

29 SEAE, *Collaborazione UE-NATO – Factsheet*, 11 giugno 2019, https://europa.eu/!nd78hD.

30 UE-NATO, *Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017*, 17 giugno 2019, p. 6, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf.

31 Bruno Lété e Piret Pernik, *EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*, German Marshall Fund, Washington, dicembre 2017.

Il contributo alla difesa cibernetica delle agenzie dell'Unione europea

Lo sviluppo autonomo delle capacità di difesa cibernetica in Europa è affidato principalmente all'EDA, un'agenzia del Consiglio dell'UE con funzionamento intergovernativo, istituita nel 2004 e fortemente rafforzata nel 2017, divenendo anche segretariato della PeSCo. L'approccio intergovernativo crea tuttavia notevoli difficoltà operative al lavoro dell'agenzia.

Se infatti la *mission* dell'Agenzia è quella di "aiutare il Consiglio e gli Stati Membri nello sforzo di migliorare le capacità di difesa dell'UE"[32], nel dettaglio tale supporto è attuato con un approccio "*à la carte*", lasciando ampio potere decisionale di cooperazione agli Stati membri.

Nell'orizzonte comunitario, l'Eda è anche la titolare dell'agenda più ampia di collaborazione in materia cibernetica tra gli Stati membri, agenda che essa attua attraverso tre recentissimi strumenti: la PeSCo, stabilita nel dicembre 2017, la Revisione annuale coordinata sulla difesa (*Coordinated Annual Review on Defence*, CARD), lanciata nel maggio 2017 e collegata con il Piano di sviluppo delle capacità militari (*Capability Development Plan*, CDP) e le PADR del giugno 2017, gestite per conto della Dg Defis[33].

Nel quadro dei progetti PeSCo, al 2020 risultano attivi otto progetti sotto la categoria *Cyber-C4ISR* (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*). Di questi, solo quattro però sono strettamente rivolti ad aumentare le capacità di difesa cibernetica dell'Unione, mentre gli altri quattro sono relativi alla protezione delle comunicazioni cibernetiche di piattaforme di comando e controllo[34].

Nel dettaglio, i quattro progetti sulla difesa cibernetica hanno scopi molto simili e mirano alla cooperazione tra gli Stati membri che ne fanno parte, tramite la creazione di *team* o piattaforme di risposta rapida (*Cyber Rapid Response Team* a guida lituana *e Cyber Threats and Incident Response Information Sharing Platform* coordinato dalla Grecia) o la creazione di vere e proprie accademie e centri di risposta volti anche alla formazione del personale (*EU Cyber Academia and Innovation Hub* guidato dal Portogallo *e Cyber Info Domain Coordination Center* coordinato dalla Germania).

Purtroppo anche in questo caso occorre sottolineare la mancanza di coesione nelle proposte progettuali degli Stati membri. Si ritrova infatti non solo una duplicazione dei progetti sia tra Stati membri che tra questi ultimi e l'UE (ad esempio con l'AESD), ma anche una forte frammentazione tra gli sforzi degli Stati membri, si pensi che il progetto a guida portoghese conta solo un altro membro, la Spagna. L'Italia è presente, nello specifico ambito della difesa cibernetica, solo nel progetto "*Cyber Threats and Incident Response Information Sharing Platform*" a guida ellenica, progetto che punta a sviluppare misure di difesa cibernetica attive, e quindi non solo di difesa, ma anche di

---

[32] Consiglio dell'Unione europea, *Azione comune 2004/551/PESC del Consiglio, del 12 luglio 2004, relativa alla creazione dell'Agenzia europea per la difesa*, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32004E0551.

[33] EDA, *Factsheet: Cyber Defence*, 5 novembre 2018, https://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-cyber-defence.

[34] Sito EDA: *Current list of PESCO projects*, https://www.eda.europa.eu/what-we-do/our-current-priorities/permanent-structured-cooperation-(PESCO)/current-list-of-pesco-projects.

risposta ad attacchi esterni[35]. Il tutto è svolto di concerto con Portogallo, Austria, Cipro, Spagna e Ungheria, con lo scopo di creare un *network* di condivisione di *intelligence*. Il progetto, finanziato attraverso l'EDF, ha un costo totale di 2,2 milioni di euro e dovrebbe terminare nel 2020.

Altro strumento in seno all'EDA è il CDP che definisce le capacità militari da sviluppare all'interno dell'UE, dando orientamenti di lungo periodo sulle necessità di sviluppo tecnologico dell'UE. Il CDP è strutturato sulla base delle indicazioni fornite dagli Stati membri e sul lavoro di EDA, MPCC e EUMS. La sua ultima versione è stata approvata il 28 giugno 2018 dai ministri della difesa dei Paesi UE[36]. Questo documento indica di quali equipaggiamenti necessitano le forze armate europee, in un orizzonte decennale, per assicurare la sicurezza e difesa dell'Europa. Nell'ultima revisione, il CDP ha inserito le capacità di risposta ad attacchi *cyber* come una delle 11 priorità future dell'Unione.

Il documento si sofferma principalmente sulla necessità di dar vita a un sistema di infrastrutture europeo per le operazioni di difesa cibernetica che abbiano un vocabolario comune e tecniche procedurali, organizzative e standard dotati di interoperabilità tra le capacità cibernetiche nazionali. Altro punto sottolineato dal CDP è la necessità di comuni attività di ricerca e sviluppo di tecnologie che permettano il miglioramento degli strumenti di *Situational awareness*. Tutto ciò al fine di consentire una risposta autonoma e di individuare minacce cibernetiche militari. Inoltre, sono necessarie all'UE capacità di sviluppo di modelli predittivi di analisi delle minacce[37]. Tale richiesta è stata reiterata nelle Conclusioni del Consiglio sulla sicurezza e la difesa dello scorso 17 giugno 2019[38].

Figura 4 - Le priorità secondo il CDP in ambito di difesa cibernetica europea - Fonte EDA: *Capability Development Plan*, cit.

Per ognuna delle 11 priorità l'EDA elabora in seguito gli "*Strategic Context Cases*" (SCC)[39] anche chiamate "vie di approccio". Sono dei documenti divisi in due parti, la

---

35 Sito PeSCo: *Cyber Threats and Incident Response Information Sharing Platform*, https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform.

36 Sito EDA: *Capability Development Plan*, https://www.eda.europa.eu/what-we-do/our-current-priorities/capability-development-plan.

37 Eda, *The EU Capability Development Priorities*, 3 dicembre 2018, https://www.eda.europa.eu/info-hub/publications/publication-details/pub/the-eu-capability-development-priorities.

38 Consiglio dell'Unione europea, *Sicurezza e difesa: il Consiglio adotta conclusioni*, 17 giugno 2019, https://europa.eu/!rr79Vy.

39 Portale EDA: *EDA Prioritisation Tool*, https://prioritisation.eda.europa.eu.

prima che contiene una fotografia dello stato dell'arte attuale nella capacità analizzata (es. difesa cibernetica) e la seconda che delinea le idee e i possibili progetti futuri in termini di ricerca e sviluppo (es. difesa attiva).

La difesa cibernetica ha un documento apposito, non consultabile pubblicamente ma richiedibile al Punto di contatto nazionale EDA. Ogni documento è preparato da un *team* formato da rappresentanti degli Stati membri, istituzioni europee e rappresentanti delle aziende. Questo meccanismo è volto ad agevolare l'individuazione di *gaps and needs* dell'UE e degli Stati membri in specifiche tematiche per permettere l'elaborazione di *roadmaps* concertate tra tutti gli attori interessati[40].

Le "vie di approccio" confluiscono poi in una piattaforma di condivisione ad accesso riservato sul sito EDA[41], dove gli Stati membri identificano attività chiave strategiche per la loro implementazione attraverso i fondi europei[42] al fine di realizzare l'autonomia strategica dell'UE.

Altre iniziative di rilievo per il supporto alla difesa cibernetica svolte dall'Eda sono le *CapTech*[43], gruppi di lavoro di esperti con il compito di mappare le aree di ricerca tecnologica al fine di rispondere alla *Overarching Strategic Research Agenda* (OSRA)[44]. Ogni *CapTech* lavora su *Tecnology Building Blocks* (aree tecnico-scientifiche di potenziale collaborazione europea) e produce documenti strategici per ogni tecnologia o dominio militare di impiego.

Ogni Stato ha un referente nazionale per i gruppi *CapTech* e il tema della difesa cibernetica è gestito in un gruppo guidato da un funzionario dell'Eda e da un *rapporteur* rappresentante dell'industria; per l'Italia, un esempio di partecipante ai *CapTech* è il Consiglio nazionale delle ricerche (CNR) tramite il Dipartimento di Ingegneria, ICT e Tecnologie per l'Energia e i Trasporti con 10 ricercatori[45]. I fondi in questo caso sono stanziati esclusivamente dagli Stati membri[46].

Da segnalare, per quanto riguarda la condivisione di *policy* con la Commissione europea, che l'Eda ha istituito un gruppo di ricerca che stila annualmente una *Strategic Research Agenda* (SRA) sulla difesa cibernetica[47]. La SRA è parte della OSRA e fornisce indicazioni sui campi da sviluppare per una efficace difesa cibernetica europea. Nell'ultimo aggiornamento del 2019 la SRA ha individuato i seguenti elementi tecnici che dovranno essere necessariamente di dominio autonomo dell'Ue nel prossimo futuro:

1) la necessità di sviluppare un sistema di crittografia condivisa;

---

[40] EDA, *Factsheet: Strategic Context Cases (SCCs)*, 25 ottobre 2019, https://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-strategic-context-cases-(sccs).

[41] Portale Eda: *EDA Prioritisation Tool*, https://prioritisation.eda.europa.eu.

[42] EDA, KSA Presentation, gennaio 2018, https://eda.europa.eu/docs/default-source/documents/ksa-presentation.pdf.

[43] Sito EDA: *Capability Technology Areas*, https://www.eda.europa.eu/Aboutus/how-we-work/expert-teams/capability-technology-areas.

[44] EDA, *Factsheet: Overarching Strategic Research Agenda (OSRA)*, 25 marzo 2019, https://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-overarching-strategic-research-agenda-(osra).

[45] Si veda il sito del Dipartimento: *Attività internazionale*, http://www.diitet.cnr.it/attivita-internazionale.

[46] EDA, *Factsheet: Cyber Defence*, cit.

[47] *Ibid.*

2) lo sviluppo di sistemi integrati sicuri;

3) la capacità di rapida individuazione di *software* di minaccia;

4) lo sviluppo di tecniche di simulazione e visualizzazione;

5) la protezione di reti e sistemi di comunicazione;

6) l'aggiornamento di tecnologie di identificazione ed autenticazione.

Infine, l'EDA gestisce le PADR che, finanziate attraverso l'EDF, ne costituiscono la prima "finestra" di ricerca. Esse hanno l'obiettivo di formare un mercato unico europeo della difesa, attraverso una forte spinta alla ricerca e allo sviluppo di soluzioni europee. Attualmente nessuno dei progetti PADR già assegnati ha obiettivi specificamente di difesa cibernetica, mentre nei bandi del 2019 era prevista una *call* specifica sull'utilizzo dell'intelligenza artificiale come tecnologia rivoluzionaria in ambito di difesa cibernetica[48]. Tra le proposte ricevute dall'EDA sette sono state selezionate a marzo 2020[49].

Una particolare posizione nell'universo delle agenzie europee in materia cibernetica è quella di ENISA, titolare del portafoglio di sicurezza *cyber* dell'UE in ambito prettamente civile. Il vincolo appare chiaro anche nello statuto dell'Agenzia, tanto che il termine difesa appare solo tre volte e a indicare chiaramente il perimetro dove si ferma il lavoro dell'Agenzia.

Tuttavia, come già discusso, la natura ibrida della minaccia cibernetica fa sì che nello sviluppo operativo ENISA abbia iniziato già dal 2017 a cooperare con l'EDA non solo nello scambio di buone pratiche ma anche nell'organizzazione di esercizi di addestramento congiunto, cooperazione confermata poi dal memorandum d'intesa firmato nel maggio 2018 con l'Eda, EUROPOL e il CERT-EU[50].

Va sottolineato che Enisa è il braccio operativo dell'UE per quanto riguarda la protezione del mondo cibernetico, con un mandato specifico di tutela delle infrastrutture europee. Questo ha permesso all'Agenzia di sviluppare negli ultimi anni importanti conoscenze per quel che concerne i rischi derivanti dal campo cibernetico che ogni anno sono raccolti nel "*Threat Landscape*".

L'ultima versione del documento, datata gennaio 2019[51], rafforza ancora di più il legame tra civile e militare mutuando dalle strategie britanniche[52] il concetto di difesa attiva. Con tale locuzione si intende una strategia proattiva di risposta a minacce esterne che non si ferma all'individuazione dell'intrusione nel sistema e alla sua eliminazione

---

[48] EDA, *Preparatory Action on Defence Research. 2019 Calls for proposals and General Annexes*, marzo 2019, https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/wp-call/pa-call-document-padr-fss-19-call-text_en.pdf.

[49] Commissione europea, *2019 Preparatory Action on Defence Research (Padr) Calls – Description of Selected Proposals*, marzo 2020, https://eda.europa.eu/docs/default-source/documents/padr-calls-factsheet-v2.pdf.

[50] Il testo del memorandumdel 23 maggio 2018 è disponibile nel sito Eda: https://www.eda.europa.eu/docs/default-source/documents/mou---eda-enisa-cert-eu-ec3---23-05-18.pdf.

[51] ENISA, *ENISA Threat Landscape Report 2018*, gennaio 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[52] Ian Levy, *Active Cyber Defence – One Year On*, Londra, National Cyber Security Centre, 5 febbraio 2018, https://www.ncsc.gov.uk/information/active-cyber-defence---one-year-on.

ma si estende alla ricerca dell'autore e, in *extrema ratio*, alla risposta cibernetica a un attacco. Tale strategia va legata al concetto di intelligence per le minacce *cyber*.

Anche in questo caso si noti l'ibridazione tra civile e militare, intesa come capacità di uno Stato di dotare i propri servizi di intelligence di professionisti capaci di difendere le infrastrutture in modo proattivo al fine di contrastare lo spionaggio cibernetico. Tale tipo di attacco è reputato dallo studio di ENISA come uno dei 15 rischi più incombenti per le infrastrutture europee.

Per tale ragione viene richiamata la necessità di stabilire a livello europeo una Unità di difesa cibernetica comune, come già proposto dalla Commissione Affari esteri del Parlamento europeo nella risoluzione del 13 dicembre 2017[53]. In caso di attacchi sponsorizzati da entità statali, un'unità di difesa cibernetica comune permetterebbe una difesa attiva efficace in grado di interrompere e individuare i perpetratori dello stesso[54].

Infine, merita una menzione, se non altro in termini di possibile sviluppo futuro, l'AESD, organo integrato nel SEAE[55], che ha in forza 168 istruttori di difesa cibernetica provenienti da tutta Europa.

Nato nel 2016, l'AESD è stata incaricata dal Consiglio di creare una piattaforma informatica in materia di istruzione, formazione, valutazione ed esercitazioni (*Education, Training, Evaluation and Exercise*, ETEE). Tale piattaforma, attiva dal 2019, dovrebbe diventare al più presto il punto di riferimento dell'UE per la formazione e l'addestramento di esperti di difesa cibernetica. L'AESD ha inoltre creato, all'interno del programma Erasmus militare, uno specifico modulo per favorire lo scambio di personale militare tra i Paesi membri dell'UE anche in ambito informatico.

Conclusioni: quali opportunità per l'Italia?

L'UE sta affrontando la nuova sfida, rappresentata dalla difesa cibernetica, tramite numerosi strumenti di coordinamento e supporto agli Stati membri, con l'obiettivo dichiarato di raggiungere un'autonomia di difesa europea che comprenda anche la difesa cibernetica.

Seppur mancando un piano strategico condiviso da tutte le istituzioni europee, che esiste invece nel campo della sicurezza cibernetica, il *Quadro strategico dell'Ue in materia di ciberdifesa* approntato dal Consiglio è un primo strumento di valutazione delle politiche europee. L'UE sta coordinando e promuovendo gli impegni degli Stati membri attraverso l'Eda, grazie all'attivazione di ingenti fondi con capitoli dedicati al *cyber*, come l'Edf, con la presenza di specifici bandi per lo sviluppo di tecnologie di difesa cibernetica all'interno della PADR, e con l'istituzione della AESD.

---

[53] Parlamento europeo, *Risoluzione del 13 dicembre 2017 sulla relazione annuale sull'attuazione della politica di sicurezza e di difesa comune*, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0492_IT.html.

[54] Giuseppe Del Giudice, "Cyber warfare: tecniche, obiettivi e strategie dietro gli attacchi 'state-sponsored'", in *Agenda digitale*, 7 gennaio 2020, https://www.agendadigitale.eu/sicurezza/cyber-warfare-tecniche-obiettivi-e-strategie-dietro-gli-attacchi-state-sponsored.

[55] Consiglio dell'Unione europea, *Decisione (PESC) 2016/2382 del 21 dicembre 2016, che istituisce l'Accademia europea per la sicurezza e la difesa (AESD)…*, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016D2382.

Si tratta certamente di iniziative recentissime che avranno modo di esser migliorate e calibrate in futuro, ma è necessario ricordare che recentissima è anche la materia trattata. Il lavoro dell'UE verso l'autonomia strategica in materia di difesa appare chiaro e coerente, tuttavia essendo la difesa una materia intergovernativa non può progredire speditamente senza il supporto di tutti gli Stati membri.

L'Italia, dal canto suo, seppur ben inserita nei primi progetti PADR[56], non ha ancora mostrato la necessaria proattività richiesta nello specifico dal campo della difesa cibernetica. Maggiore partecipazione e reattività nella partecipazione a progetti europei porterebbero tre importanti benefici al Sistema Paese.

In primis, l'Italia potrebbe usufruire delle piattaforme di scambio di informazioni per affinare la recente messa in opera di strumenti di difesa cibernetica sul territorio nazionale, come il CIOC, traendo spunto da quegli Stati membri che hanno una cultura più sensibile nei confronti delle problematiche della difesa *cyber* e strutture più avanzate. Uno scambio continuo e coordinato di buone pratiche con stati come la Francia dove già è operativo dal 2017 il Comcyber, il comando cibernetico francese, o con la Germania, che con il Cyber- und Informationsraum, operativo anch'esso dal 2017 ha inaugurato la stagione dei comandi *cyber* europei, potrebbe contribuire all'accelerazione della operatività del giovane comando cibernetico italiano. L'Italia dovrebbe quindi puntare ad inserire il CIOC all'interno di progetti Edf, possibilmente creando un asse con la Francia e la Germania.

In aggiunta, inserendosi in numerosi progetti europei, l'Italia sarebbe capace di influenzare le strategie e dottrine europee in ambito cibernetico-militare, settore, come visto, ancora in fase embrionale. Questo permetterebbe al nostro Paese di avere un ruolo di primo piano in quel quinto dominio di scontro che potrebbe risultare decisivo in caso di possibili futuri conflitti internazionali sia di natura cibernetica sia di natura tradizionale.

Infine, una partecipazione italiana maggiore all'EDF, sia nella finestra PADR che nell'EDIDP, favorirebbe l'inserimento di aziende italiane nel nascente mercato europeo della difesa cibernetica. Questo gioverebbe sia all'industria interna italiana, che troverebbe ampi spazi ancora incontaminati di opportunità produttive e di mercato, sia all'intero Sistema Paese, che potrebbe ancora una volta esercitare le capacità di innovazione e creatività già manifestate in passato nel settore aerospaziale.

In conclusione, l'Italia non deve perdere l'occasione di contribuire alla creazione di una dottrina militare cibernetica europea, di inserire propri *asset* strategici in un mercato in crescita e in continua evoluzione, e di utilizzare fondi europei per il miglioramento delle nascenti strutture cibernetiche nazionali. Se ben intercettata, difatti, la possibile minaccia cibernetica può tramutarsi in un'opportunità di primato, non solo europeo ma anche internazionale, per il comparto di difesa italiano.

---

[56] Si veda il progetto Ocean2020 a guida Leonardo e con partecipazione del Ministero della Difesa: https://ocean2020.eu.

Osservatorio di Politica internazionale

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

L'Osservatorio realizza:

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

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

Approfondimenti
Studi monografici su temi complessi dell'attualità internazionale

Note
Brevi schede informative su temi legati all'agenda internazionale

www.parlamento.it/osservatoriointernazionale

Senato della Repubblica

Camera dei Deputati

Ministero degli Affari Esteri
e della Cooperazione
Internazionale

Coordinamento redazionale:

Camera dei deputati
Servizio Studi
Tel. 06 67604172
email st_affari_esteri@camera.it