"IL CONTRASTO ALLA GUERRA IBRIDA: UNA STRATEGIA ATTIVA"

Non-paper

del Ministro della Difesa

Guido Crosetto

"IL CONTRASTO ALLA GUERRA IBRIDA: UNA STRATEGIA ATTIVA"

Non-paper

del Ministro della Difesa

Guido Crosetto

Edizione Novembre 2025

INDICE

"*Non-paper* sul contrasto alla guerra ibrida"

1. PREFAZIONE del Ministro della Difesa, Guido Crosetto

2. CONTESTO

2.1. Definizione di minaccia ibrida: azioni coordinate in più domini condotte da attori statuali e non-statuali, al di sotto della soglia del conflitto armato e spesso non attribuibili, mirate a danneggiare, destabilizzare o indebolire.

2.2. Gli attori principali

- Russia: secondo importanti e indipendenti analisi, attività riconducibili al suo operato includono azioni di sabotaggio, disinformazione, influenza politica, pressione su forniture strategiche, cyberattacchi, ricorso a mercenari e uso della migrazione come leva di destabilizzazione.
- Cina: secondo diversi e autorevoli osservatori, adotta una strategia multi-vettoriale, ovvero un approccio integrato che combina leve economiche, tecnologiche, informative e diplomatiche per indebolire l'UE e acquisire *know-how* strategico. Le attività includono: disinformazione sia in Italia che, ad esempio, in Africa, infiltrazioni nei sistemi bancari e nelle reti pubbliche, reclutamento in ambito cyber, e penetrazione nei settori dell'informazione, della finanza, dell'economia e dello Stato.
- Iran: secondo numerosi esperti, ricorrerebbe a *proxy* regionali (Houthi, Hezbollah, milizie sciite) e a forme di coercizione su *choke points* marittimi, oltre che ad azioni di terrorismo e attacchi cibernetici.
- Corea del Nord: utilizzo di strumenti cibernetici, finanziari e informativi come leve di pressione strategica e di autofinanziamento del regime, con operazioni spesso attribuite a gruppi statali o affiliati specializzati in attacchi *ransomware*, furti di criptovalute e operazioni di spionaggio digitale (caso "WannaCry" del 2017).

2.3. La minaccia ibrida in Italia: Vulnerabilità in energia, infrastrutture critiche ed ecosistema politico-sociale.

3. CARATTERISTICHE

3.1. Difficoltà di attribuzione e "*plausible deniability*": occultamento responsabilità dell'attore statuale.

3.2. Uso di attori non-statuali: agenti (controllo diretto) e *proxy* (nessun legame formale).

3.3. Intento destabilizzante e interferenze nei processi democratici: manipolazione di opinione pubblica, delegittimazione alleanze, campagne disinformative programmate, utilizzo spregiudicato di corruzione.

4. AMBITI DI PROTEZIONE

4.1. Protezione delle infrastrutture critiche: energia, trasporti, telecomunicazioni, sanità, finanza; nuove vulnerabilità (materie prime critiche, dipendenze da fornitori extra-UE; *choke points* marittimi come Suez/Bab el-Mandeb). Necessità di approccio integrato (*cyber* + fisico + cooperazione internazionale).

4.2. Protezione della società civile: resilienza alla disinformazione, alfabetizzazione digitale, co-regolamentazione spazio digitale.

5. STRUMENTI E DOMINI DI AZIONE

5.1. Il **cyberspazio**: dominio operativo NATO; minacce quotidiane sotto soglia a PA, sanità, energia, manifattura; casi globali ***(WannaCry, Colonial Pipeline, SolarWinds***); priorità nazionali (**Spazio *cyber* d'interesse, Arma *Cyber* civile-militare, tutele funzionali, Centro per il Contrasto alla Guerra Ibrida**).

5.2. Disinformazione e interferenza nei processi elettorali – **normativa europea:**
Foreign Information Manipulation & Interference (**FIMI**), **IA-*deepfake***, **FIMI *Toolbox***, *Hybrid Rapid Response Teams* (**HRRT**).
Linee guida UE per **piattaforme e motori di ricerca** di grandi dimensioni.

5.3. La coercizione geo-economica: *export controls* (**terre rare, semiconduttori**), acquisizioni mirate in settori strategici, uso del debito ("***debt-trap diplomacy***").

5.4. I *choke points* logistici: **Mar Rosso/Suez-Bab el-Mandeb**, vulnerabilità infrastrutture energetiche sottomarine, impatti sulle ***supply chain* globali**.

5.5. La **dimensione militare "grigia"**: sconfinamenti e posture coercitive, mercenari/*contractors*, esercitazioni provocatorie, disturbi alla navigazione/GNSS.

5.6. Sfide per le Forze Armate: capacità **multi-dominio**, ***cyber***, **IA**, protezione ***supply chain***, **formazione** anti-**minacce cognitive, *Cyber Electromagnetic Activities* (CEMA)**.

6. RISPOSTE E COOPERAZIONE INTERNAZIONALE

6.1. Ruolo della NATO, dell'UE e del G7

NATO:
- **Strategia 2025**;
- Centri di eccellenza (**Helsinki**, **Tallinn**);
- Strumenti cooperativi: *Virtual Cyber Incident Support Capability* (**VCISC**) e *Sovereign Cyber Effects Provided Voluntarily by Allies* (**SCEPVA**).
- "***NATO Approach to Countering Information Threats***" (priorità: comprensione ambiente informativo, prevenzione, contenimento/mitigazione, apprendimento.

UE:
- **Quadro normativo**: *Network and Information Security 2* (**NIS2**), ***Cybersecurity Act***, ***Cyber Resilience Act***, ***Cyber Solidarity Act***, *Digital Operational Resilience Act* (**DORA**), Direttiva Infrastrutture Critiche (**CER**), *Digital Services Act* (**DSA**), *Critical Raw Materials Act* (**CRMA**), *Anti-Coercion Instrument* (**ACI**).
- **Strutture operative**: Agenzia UE per la cybersicurezza (**ENISA**); Centro europeo di competenza per la cybersicurezza (**ECCC**); l'*Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats* (**HWP ERCHT**), *Rapid Alert System* (**RAS**); *hub* anti-disinformazione (**EDMO, EFCSN, EUvsDisinfo**).

G7:
- *Rapid Response Mechanism* (**RRM**).
- **Dichiarazioni** contro manipolazione (Vertici **Capri**, **Borgo Egnazia**, **Fiuggi**); mandato esteso a contrasto coercizione economica.

7. SCENARI DELL'EVOLUZIONE DELLA MINACCIA IBRIDA

- **Rapporto Niinistö**: resilienza, ***situational awareness, deterrence by denial/punishment,* ambiguità strategica europea.**

7.1. Evoluzione tecnologica e impiego dell'IA:
Deepfake*, microtargeting, botnet*, IA generativa per *cyber kill chain*, robotica e droni autonomi; scenari "**doppia leva**" (materie prime critiche + *choke points*).

8. *CASE STUDY* – CONFLITTO RUSSO-UCRAINO

8.1. Resistenza ucraina e suoi limiti: capacità difensiva, ma difficoltà a riconquistare territori.

8.2. Vantaggio strategico russo: risorse, economia di guerra, supporto di numerosi Paesi.

8.3. **Economia di guerra e condizioni negoziali:** produzione armamenti fuori regole di mercato, reclutamento massiccio.

8.4. Rischio per l'Europa: ritardo nelle risposte, iniziativa strategica a Mosca.

8.5-8.8. Ruolo della Russia secondo autorevoli fonti: manipolazione dell'opinione pubblica, sabotaggi, pressione migratoria, campagne di influenza in Africa, interferenze elettorali.

8.9. **Vulnerabilità occidentale nella "zona grigia":** visione binaria pace/guerra, approccio reattivo.

9. WAY-AHEAD

9.1. Principali sfide: coordinamento istituzionale, approccio ***whole-of-government,*** protezione infrastrutture e coesione sociale; necessità di sintesi stabile tra attori istituzionali **(gruppo interministeriale DIS).**

9.2. **Ruolo delle istituzioni e cooperazione:** rafforzare **resilienza democratica**, è necessario creare Centro Europeo per il Contrasto alla Guerra Ibrida; meccanismo permanente UE di monitoraggio/risposta; educazione civica e **alfabetizzazione digitale**; **partenariati** con alleati e Paesi terzi.

9.3. **Superare l'inerzia:** è necessario passare da approccio contenitivo a *difensivo* (che nel *hybrid warfare* non può che essere *proattivo*)**:** mantenersi attivi nel dominio, prevenendo azioni ostili e riducendo la libertà di manovra degli opponenti ibridi. Serve risposta multilivello (**nazionale/UE/NATO**); una strategia unitaria e continuativa, con **attenzione a teatri particolarmente a rischio** (e.g. **Balcani** e il **Sahel**), per prevenire la normalizzazione della minaccia come nuovo stato di fatto.

10. CONCLUSIONI

La guerra ibrida è **continua** e colpisce **infrastrutture critiche**, **centri decisionali**, **servizi essenziali** e la **tenuta di ogni Paese**, con rischi quotidiani e crescenti di **danni catastrofici**. Gli attacchi — condotti sul piano della **disinformazione**, della **guerra cognitiva** e nel dominio *cyber* — sfruttano la consapevolezza che "l'Occidente spesso sceglie di **non reagire**".

In sintesi, come per violazioni dello **spazio aereo**, delle **acque territoriali** o dei **confini terrestri**, anche sul piano ibrido è necessario predisporsi per **reazioni legittime e tempestive**. Occorre passare rapidamente dall'attuale **postura contenitiva** a una **postura concretamente difensiva (che in ambito *hybrid* non può che essere *proattiva*)**, sia a livello **nazionale** sia in ambito **alleanze.**

Siamo sotto attacco e le "bombe *hybrid* continuano a cadere": il tempo per agire è "**subito**".

APPENDICI

I. **Tavole sinottiche "per capire meglio": la situazione negli altri paesi occidentali**

II. **Atti di sabotaggio** a infrastrutture critiche e *asset* militari/industriali in Europa.

III. **Presenza russa in Africa/Sahel**.

IV. **Interferenze ibride sulle elezioni presidenziali romene 2024** (attacchi informatici, *deepfake*, manipolazione *social*).

V. **Interventi/obiettivi prioritari a livello UE** per contrasto alla guerra ibrida.

1. PREFAZIONE DEL MINISTRO DELLA DIFESA, GUIDO CROSETTO

Figura 1 – Il Ministro della Difesa Guido Crosetto a bordo di Nave Cavour durante l'esercitazione multidominio "Mare Aperto", scenario addestrativo che integra capacità navali, aeree, anfibie e cibernetiche per preparare il Paese a fronteggiare le moderne minacce ibride, caratterizzate da pressioni sotto-soglia e attacchi multidominio.
Fonte: Ministero della Difesa

Questo *non paper* rappresenta la mia visione relativamente a una delle più subdole minacce che ogni giorno erode in modo silente la sicurezza delle nostre società: la **minaccia ibrida**.

L'inquadramento proposto, seppur in continuo mutamento, è stato costruito integrando informazioni non classificate del comparto *intelligence* con analisi estrapolate da fonti aperte attendibili, arricchite dalle mie interlocuzioni avute con colleghi europei.

Quanto emerge è una attività malevola sotto soglia, in incessante mutamento, adattiva, multidominio e multidimensionale, volta a colpire in modo asimmetrico i centri di gravità dei nostri sistemi di *governance.*

Il **dominio *cyber*** – come ho avuto modo di condividere davanti alla **IV Commissione Difesa della Camera** a **gennaio 2025** – è il moltiplicatore che tiene insieme tutto: consente campagne di **disinformazione**, interferisce con i **processi democratici**, mette in difficoltà **infrastrutture critiche** (sanità, energia, trasporti, finanza) e rende ardua l'**attribuzione** grazie all'impiego di ***proxy*** e alla "***plausible deniability***". Nell'ambito ibrido conta più la **percezione** che la certezza: l'obiettivo non è solo colpire, ma instillare dubbio e insicurezza. La percezione pubblica di vulnerabilità, anche in assenza di prove definitive, produce effetti strategici pari – o superiori – a quelli di un attacco dichiarato.

Abbiamo organizzato le pagine seguendo un percorso lineare: **che cosa** (definizioni, attori, strumenti), **dove** (vulnerabilità e settori), **come** (risposte e linee d'azione). La sezione sulle **alleanze** (**NATO, UE, G7**) fornisce cornice, vincoli e opportunità di condivisione; il ***case study*** **sul conflitto russo-ucraino** mostra come il "sotto soglia" sia ormai uno **stato di lavoro** più che un'eccezione. In coda, un documento in appendice propone un ***benchmark*** delle organizzazioni cyber di **Germania, Regno Unito, Francia, Spagna, Stati Uniti e Canada**: non un catalogo, ma una griglia utile a capire che cosa funziona altrove e quali ***gap*** dobbiamo colmare.

Si sta consolidando, tra analisti e opinioni pubbliche, la percezione di una insufficiente deterrenza nel dominio "sotto soglia", dove la rapidità e la continuità delle operazioni ibride superano spesso la nostra capacità di reagire in modo coordinato e tempestivo.

Se devo condensare le riflessioni del mio Dicastero, quindi: **contenere non basta**. Non possiamo pensare di superare la minaccia ibrida con un approccio settoriale o monodimensionale in quanto le crisi generate saranno sempre più sistemiche e simultanee. Occorre maturare, con strumenti chiari e tempi rapidi, una capacità di azione predittiva e adattiva volta a prevenire, dissuadere e assorbire gli attacchi ibridi.

2. CONTESTO

Figura 2 – Palazzo Baracchini, Roma, sede da cui vengono coordinate le strategie nazionali di sicurezza e difesa – incluse le misure contro le minacce ibride.
Fonte: Ministero della Difesa

2.1. DEFINIZIONE DI MINACCIA IBRIDA

Partiamo dalle basi: cos'è esattamente la minaccia ibrida e chi la sta portando avanti.

Si definisce *minaccia ibrida*[1] quella portata da **attori statuali** (anche attraverso **attori non-statuali** che operano come **agenti o *proxy***) mediante una combinazione di azioni sinergiche in vari domini (diplomatico, informativo, militare, economico-finanziario e dell'*intelligence*). È oggi una delle principali sfide per le democrazie occidentali. L'obiettivo è **erodere** la **resilienza democratica**, minare la fiducia dei cittadini nelle istituzioni, dividere le società, influenzare le opinioni pubbliche con false informazioni.

La minaccia è amplificata dall'evoluzione dello spazio cibernetico e dai mutamenti dell'ambiente mediatico. Tali attività, **solitamente negabili e difficilmente attribuibili**, sono adattate alle debolezze sistemiche del Paese bersaglio o fanno leva sulle sue dipendenze, con l'intento di danneggiarlo, destabilizzarlo e/o indebolirlo. In parole povere, sfruttano ogni nostro punto debole.

Le operazioni cinetiche condotte nell'ambito di una campagna ibrida, inoltre, sono spesso coperte sotto forma di incidenti – ad esempio nel caso di danneggiamento di infrastrutture critiche. In pratica fanno passare per guasti quelli che in realtà sono attacchi mirati.

La minaccia ibrida tipicamente origina da Stati in grado di articolare rapidamente strategie **multivettoriali**, coinvolgendo tutte le articolazioni del governo per contribuire al raggiungimento degli obiettivi attraverso azioni aggressive e ad alto impatto.

Le campagne ibride comprendono azioni e strumenti in più domini volti a colpire lo Stato bersaglio su più fronti, azioni che rimangono al di sotto della soglia di un conflitto armato aperto e sono focalizzate, in termini temporali e operativi, su un unico obiettivo strategico. L'attaccante gode **di una limitata necessità di rispondere delle proprie**

[1] Sistema di informazione per la sicurezza della Repubblica, "**Glossario *intelligence***", *sicurezzanazionale.gov.it*, consultato il 5 settembre 2025, https://www.sicurezzanazionale.gov.it/comunicazione/glossario/450?utm.

azioni e sfrutta le caratteristiche delle democrazie occidentali – interpretate dall'attore ostile come vulnerabilità – a proprio vantaggio. Approfitta del fatto che noi rispettiamo le regole internazionali.

2.2. GLI ATTORI PRINCIPALI

*Figura 3 – **Vertice NATO** – discussione sulle minacce ibride – Il ministro Guido Crosetto insieme agli altri Ministri della Difesa NATO a **Bruxelles** (ottobre 2024): in questa riunione ministeriale sono state affrontate anche le minacce ibride attribuite ad attori statuali come ad esempio **Russia e Cina**. Fonte: Ministero della Difesa.*

Gli attori ibridi sono tipicamente **Stati autoritari**, in grado di orchestrare in modo agile ed efficace azioni coordinate su più domini mobilitando l'intero apparato statuale. Non è un caso: i regimi autoritari possono agire senza opposizione interna.

Secondo diverse analisi, tra i principali attori impegnati nelle attività ibride a livello globale figurano la Federazione Russa, la Repubblica Popolare Cinese, l'Iran, la Corea del Nord.

Nel 2024 a Mosca sono state attribuite numerose attività ibride ai danni dei Paesi sostenitori dell'Ucraina. Tali azioni avrebbero mirato a minare

la coesione del fronte occidentale, incidendo sulle catene di approvvigionamento e sulle fonti energetiche, e si sarebbero concretizzate in sabotaggi e cyberattacchi di intensità crescente in Europa, oltre a campagne di disinformazione e alla strumentalizzazione dei flussi migratori a fini destabilizzanti.

Nello stesso periodo, secondo autorevoli esperti, Pechino avrebbe attuato una complessa strategia multi-vettoriale a sostegno dei propri interessi strategici: penetrazione economica e tecnologica, influenza nelle infrastrutture critiche, gestione delle catene di approvvigionamento, facendo leva geo-economica sulle **materie prime** critiche (terre rare, grafite, gallio, germanio). Secondo alcune analisi, Pechino mirerebbe a un Occidente più debole e frammentato, mantenendo però il **mercato europeo stabile** e aperto così da poterlo sfruttare per la propria crescita economica e tecnologica.

In aggiunta, secondo autorevoli fonti, l'Iran **farebbe ricorso** a *proxy* regionali (come **Houthi, Hezbollah e milizie sciite**) e a strumenti cibernetici, dimostrando la capacità di minacciare snodi marittimi cruciali e destabilizzare aree strategiche. In altri termini, Teheran **tenderebbe ad avvalersi** di attori locali per colpire obiettivi in modo indiretto, mantenendo un basso profilo.

A questi si affiancano **attori non-statuali**: **gruppi terroristici**, **criminalità organizzata** transnazionale, **hacktivisti** estremisti, spesso utilizzati da Stati per garantire la c.d. *plausible deniability*[2]. In altri termini, **si ricorre ad attori terzi** per condurre attività ostili, così da celare il coinvolgimento diretto dello Stato mandante.

[2] Ministero degli Affari Esteri e della Cooperazione Internazionale, "*G7 Foreign Ministers' Meeting Communiqué – Capri, April 19, 2024: Addressing Global Challenges, Fostering Partnerships*," comunicato stampa, 19 aprile 2024, https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2024/04/g7-foreign-ministers-meeting-communique-capri-april-19-2024-addressing-global-challenges-fostering-partnerships/

2.3. LA MINACCIA IBRIDA IN ITALIA

*Figura 4 – Personale della Brigata Informazioni Tattiche dell'Esercito Italiano impegnato nell'esercitazione "**Lince Plus 1/2025**", svoltasi a maggio 2025 presso il Poligono di Cellina-Meduna (PN) e incentrata sull'impiego degli assetti di Guerra Elettronica (EW), Intelligence d'Immagine (IMINT), Human Intelligence (HUMINT), Cooperazione Civile-Militare (CIMIC), Operazioni Psicologiche (PSYOPS) e Space Support. Fonte: Esercito Italiano*

Negli ultimi anni, **l'accelerazione dei mutamenti geopolitici globali** – **dall'aggressione russa all'Ucraina sino alle tensioni nel quadrante mediorientale** – e la disarticolazione dell'assetto *post*–Guerra Fredda hanno generato una **diffusione di pratiche d'aggressione non convenzionali**, condotte **sotto–soglia** e di **difficile attribuzione.** Il mondo è diventato molto più instabile e le vecchie regole sono saltate.

La **minaccia ibrida**, pur non rappresentando uno strumento del tutto nuovo nel confronto tra Stati, ha visto un'**accelerazione** nei termini di **natura, strumenti, pervasività, velocità e magnitudine degli effetti**, rendendo necessario un **adeguamento dei dispositivi di monitoraggio, prevenzione e risposta.** In pratica le minacce ibride sono esplose e dobbiamo correre ai ripari.

L'**Italia**, per la sua postura geopolitica e il ruolo nei consessi internazionali di cui fa parte (**UE, NATO e G7**), è esposta a diversi profili di rischio, soprattutto nei seguenti ambiti:

- **energia:** il Paese è **dipendente dalle importazioni di energia**, il che lo rende vulnerabile a pressioni economiche e tentativi di destabilizzazione da parte di attori esterni;
- **infrastrutture critiche**: il territorio italiano ne **ospita numerose** (porti, aeroporti, reti elettriche, sistemi di comunicazione) che costituiscono potenziali bersagli di sabotaggi;
- **ecosistema politico-sociale**: può essere oggetto di ingerenze straniere, campagne di **disinformazione** e sfruttamento di divisioni sociali.

L'Italia è in pratica particolarmente esposta in tutti questi settori.

Alla luce di quanto esposto, appare necessario interrogarsi sugli strumenti di cui lo Stato dispone per affrontare efficacemente la minaccia ibrida.

L'*International Institute for Strategic Studies* **(IISS)**, nel 2021, ha definito il **potere cibernetico** come la *"capacità di uno Stato di proiettare potenza nel cyberspazio, al fine di conseguire obiettivi strategici ed esercitare influenza a livello globale"*. Tale definizione chiarisce come lo **Strumento militare** non solo non possa essere escluso, ma costituisca anzi un **pilastro essenziale** nella risposta agli attacchi ibridi.

Accanto ad esso, è altrettanto evidente che gli altri pilastri siano rappresentati dai **servizi di sicurezza dello Stato** e dalle **forze di polizia e di ordine pubblico**, impegnati nei diversi domini in cui la minaccia si manifesta.

Ne consegue che il paradigma più appropriato sia quello fondato sull'integrazione di **difesa e sicurezza.**

Ora che abbiamo analizzato il "**chi**" e il "**cosa**", vediamo in dettaglio "**come**" questi attori colpiscono in modo subdolo.

3. CARATTERISTICHE

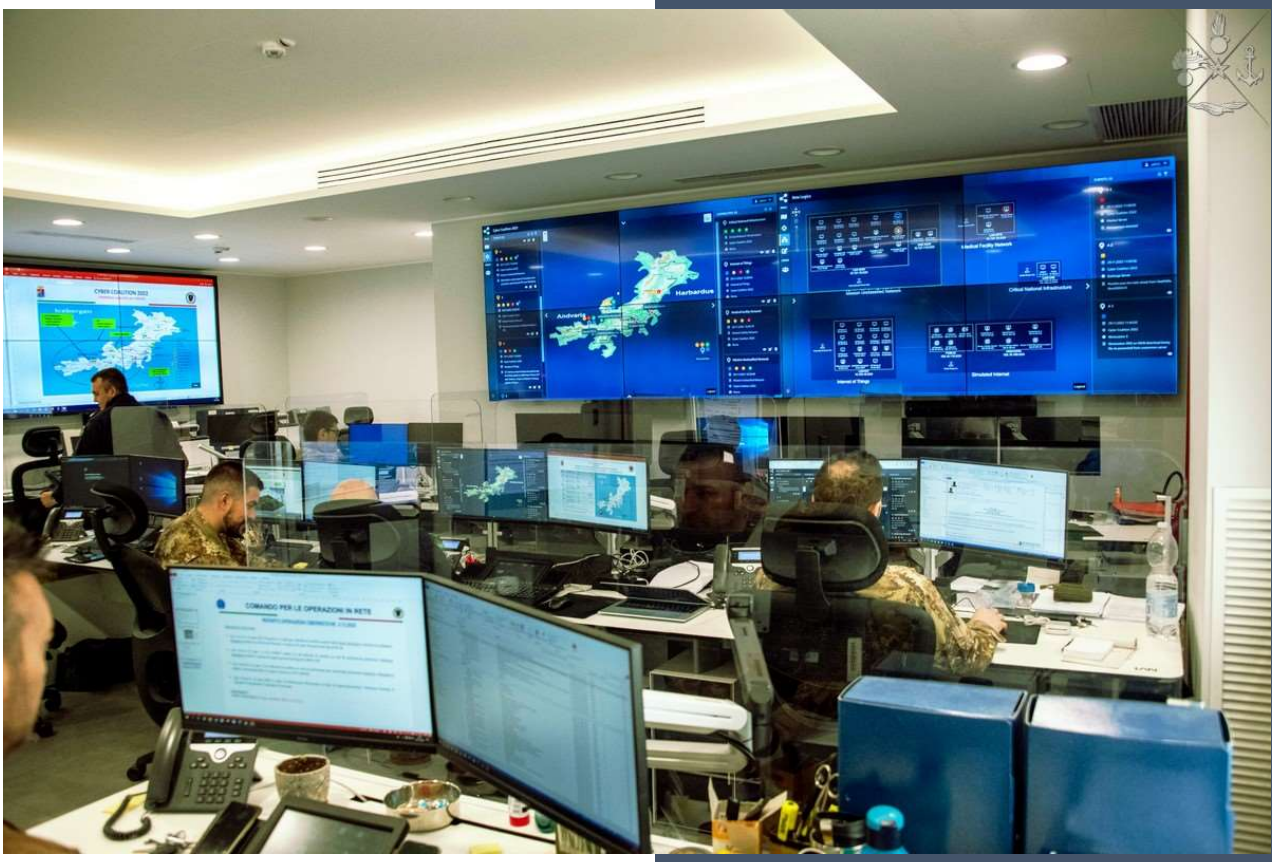


*Figura 5 – Personale Difesa al lavoro durante l'esercitazione **Cyber Coalition 2024** in Estonia.*
*Le operazioni informatiche fanno parte della guerra ibrida e spesso gli attacchi cyber non sono attribuibili con certezza a uno specifico attore statuale, permettendo la "**plausible deniability**".*
Fonte: Stato Maggiore Difesa

I principali **profili** che connotano la minaccia ibrida sono i seguenti:

- gli **attori** di natura **statuale** possono agire anche tramite soggetti terzi (*proxy*) che operano per conto, nell'interesse o in coerenza con gli obiettivi dello Stato mandante, garantendo così la "plausibile negabilità" (*plausible deniability*) del coinvolgimento statale;
- in merito alla **condotta**, l'obiettivo è intrinsecamente **destabilizzante**: le attività ibride risultano coordinate e sinergiche, coinvolgono **più domini** e impiegano una **molteplicità di strumenti.**

Chi attacca il nostro Paese e le nostre Alleanze internazionali lo fa in modo orchestrato e nascosto, per farci barcollare.

3.1. DIFFICOLTÀ DI ATTRIBUZIONE E *"PLAUSIBLE DENIABILITY"*

*Figura 6 – Due F-35B della Marina Militare durante **Mare Aperto 2025**, impegnati in operazioni congiunte dal mare e dal cielo per integrare capacità di 5ª generazione, sorveglianza avanzata e prontezza multiruolo. L'esercitazione contribuisce a rafforzare la resilienza nazionale e la capacità di risposta a scenari multidominio e a minaccia ibrida.*
Fonte: Marina Militare

La **"negabilità"** (***deniability***) si riferisce alla capacità di un attore di occultare la propria responsabilità rispetto a una determinata azione o evento, rendendo difficile o impossibile per altri attribuirne la paternità a quello specifico attore. Il colpevole, insomma, fa di tutto per non farsi scoprire.

Nel dominio ibrido, tuttavia, l'**impatto cognitivo** prevale su quello fisico: lo scopo non è soltanto **infliggere un danno**, ma **seminare incertezza, sfiducia e paura**. Anche **senza evidenze incontrovertibili**, la **sensazione collettiva di vulnerabilità** può generare **conseguenze strategiche** tanto gravi quanto — o persino più — di un attacco apertamente dichiarato.

3.2. USO DI ATTORI NON-STATUALI

*Figura 7 – Il cacciatorpediniere **Caio Duilio** della Marina Militare, dispiegato nel **Mar Rosso** nell'ambito della missione **EU Aspide 2024**. L'unità ha abbattuto **droni kamikaze lanciati dai ribelli Houthi**, esempio di minaccia ibrida condotta tramite attori non-statuali (proxy ritenuti in più sedi sostenuti dall'Iran). Fonte: Marina Militare.*

Il ricorso ad **attori non-statuali** da parte di uno Stato è finalizzato ad offuscare le responsabilità, rendendo arduo attribuire un'azione al mandante.

In particolare, nelle operazioni di **manipolazione informativa (FIMI)** e più in generale nel **dominio cibernetico**, l'attribuzione risulta ulteriormente difficoltosa data la natura **transnazionale** e spesso **anonima** dello **spazio *cyber*[3].** Lo Stato, insomma, tira i fili, ma resta dietro le quinte.

Gli attori **non-statuali** impiegati possono operare in due ruoli principali:

[3] ***European External Action Service* (EEAS).** *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI).* Ultimo accesso 5 settembre 2025. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

- **agenti**: individui o gruppi che agiscono **sotto il controllo** e il **finanziamento** diretti di uno Stato, con l'incarico di eseguire compiti specifici. Il legame tra l'agente e lo Stato è **gerarchico e formale** (sebbene possa essere dissimulato attraverso coperture), garantendo allo Stato un coordinamento centralizzato. Tuttavia, questa stretta connessione comporta un **rischio maggiore di attribuzione** diretta in caso di scoperta dell'agente;
- ***proxy***: agiscono per conto di uno Stato **senza un legame formale** o un controllo diretto da parte di quest'ultimo. L'assenza di un rapporto organico tracciabile offre allo Stato mandante un ampio margine di **impunità**, consentendogli di negare qualsiasi coinvolgimento.

Una mano invisibile muove queste pedine cercando di non lasciare tracce.

3.3. INTENTO DESTABILIZZANTE E INTERFERENZE NEI PROCESSI DEMOCRATICI

*Figura 8 – Il **Ministro della Difesa Guido Crosetto**, al **Forum Globsec 2024** di Praga, ha avvertito dell'opera di **propaganda anti-occidentale** e **disinformazione** condotta da alcuni attori nel quadro di una "guerra ibrida" mirata a influenzare opinione pubblica e istituzioni. Questo tipo di interferenze mina i processi democratici e la stabilità politica.*
Fonte: Ministero della Difesa

Gli attori della minaccia ibrida sfruttano **vulnerabilità politiche, economiche e sociali** con tattiche volte a destabilizzare i processi democratici degli Stati bersaglio. Tali tattiche includono:

- **interferenze nei processi elettorali e democratici** (ad esempio, azioni mirate a influenzare o sabotare consultazioni elettorali)[4];
- **delegittimazione dei sistemi e dei processi democratici**;
- **indebolimento** della **coesione sociale nazionale** e della **fiducia** nei confronti del **governo**;

[4] Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza, *Relazione annuale sulla politica dell'informazione per la sicurezza – 2025* (Roma, 2025), sezione "La minaccia ibrida nell'anno elettorale", infografiche.

- **destabilizzazione** dell'**ecosistema informativo** interno;
- **diffusione** di **sfiducia** nelle **alleanze e organizzazioni sovranazionali** (come UE, NATO, G7)[5].

In poche parole, seminano *caos* e sfiducia dovunque riescano.

Una volta comprese le loro tattiche, è ora di chiedersi nel prossimo capitolo: "**dove** siamo più vulnerabili?"

[5] Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza, *Relazione annuale sulla politica dell'informazione per la sicurezza – 2025* (Roma, 2025), sezione "La proiezione internazionale della Russia".

4. AMBITI DI PROTEZIONE

*Figura 9 – Esercitazione militare italiana "**Brilliant Rust**" - **giugno 2022** in scenario di guerra ibrida.*
Fonte: Esercito Italiano

4.1. LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

*Figura 10 – **Operatori cyber italiani e statunitensi** in esercitazione congiunta di difesa cibernetica (maggio 2023). Fonte: Esercito Italiano*

Le infrastrutture critiche costituiscono il **pilastro** del **funzionamento di un Paese** e rappresentano un bersaglio primario delle minacce ibride.

Se danneggiate o compromesse, esse possono avere un **impatto gravissimo sulla sicurezza nazionale**, sull'**economia** e sul **benessere** della popolazione. Rientrano in questa categoria settori quali:

- **energia** (centrali elettriche, gasdotti, rete di distribuzione elettrica);
- **trasporti** (aeroporti, ferrovie, porti, strade);
- **telecomunicazioni e IT** (reti *internet*, centrali telefoniche, *data center*);
- **sanità** (ospedali, strutture sanitarie, reti di emergenza);
- **finanza** (banche, sistemi di pagamento, mercati finanziari).

Basta colpire uno di questi settori per mettere in forte difficoltà una intera Nazione.

Inoltre, **nuove vulnerabilità** assumono un **rilievo crescente**:

- **materie prime critiche**: l'**UE** dipende **quasi totalmente** da fornitori **extraeuropei**, in particolare dalla **Cina** (**98%** per i **magneti permanenti**, **100% per le terre rare pesanti**).
  L'**Italia** presenta una **dipendenza da importazioni** di circa il **47%**, oltre il **doppio della media UE**;
- ***choke points* marittimi**: il canale di **Suez** e **Bab el-Mandeb** sono oggi strumenti di guerra ibrida. Come riportato da molte fonti, gli attacchi condotti dai ribelli Houthi nel Mar Rosso **avrebbero di fatto risparmiato** le navi russe e cinesi, costringendo molte altre imbarcazioni a circumnavigare l'Africa con costi e tempi aggiuntivi. È ormai un dato riportato anche dalla stampa che, per l'Italia, circa il **40%** del **commercio marittimo** passa da **Suez**[6].

Questi numeri parlano chiaro: dipendiamo fortemente da altri in settori cruciali.

Per **proteggere i nostri Paesi** dalla minaccia ibrida è quindi fondamentale un **approccio integrato e coordinato** che combini la **sicurezza *cyber***, la sicurezza **fisica** e la **cooperazione** internazionale.

Non possiamo ragionare a compartimenti stagni: serve una visione d'insieme e fare squadra.

4.2. LA PROTEZIONE DELLA SOCIETÀ CIVILE

Il contrasto alle minacce ibride di matrice statuale (o sostenute da attori statuali) richiede non solo misure di sicurezza tradizionali, ma il coinvolgimento di tutti i settori della società in un approccio integrato ***whole-of-society***. I pilastri della **posizione italiana** in tal senso includono:

[6] Reuters. "*Italian Ports Fear Blow to Business From Red Sea Crisis*." 17 gennaio 2024. https://www.reuters.com/world/middle-east/italian-ports-fear-blow-business-red-sea-crisis-2024-01-17/

- **costruzione di una società resiliente alla disinformazione**, attraverso iniziative di:
  - **alfabetizzazione digitale**;
  - formazione al ***fact-checking*** diffuso;
  - sviluppo del **pensiero critico**;
- **co-regolamentazione dello spazio digitale**, coinvolgendo **attori pubblici**, **privati** e **autorità** di regolazione indipendenti per definire **regole condivise**.

In pratica, serve un patto sociale: tutti coinvolti, dalla scuola ai *social media*: è prima di tutto una battaglia culturale che va combattuta da tutta la società.

Andiamo ora a vedere più da vicino **con quali "armi"** (dal *cyber* alla propaganda disinformativa) i nemici ci attaccano.

5. STRUMENTI E DOMINI DI AZIONE

*Figura 11 – **Eurofighter Typhoon** italiani in **decollo immediato** (Alpha Scramble) dalla **base NATO di Šiauliai**, in Lituania.*
Le Forze Armate devono sviluppare una capacità multi-dominio, integrando forze aeree, terrestri, navali, cyber ed elettromagnetiche (CEMA), per rispondere efficacemente alle sfide della guerra ibrida moderna.
Fonte: Aeronautica Militare

5.1. IL CYBERSPAZIO

Nel 2016 la NATO ha dichiarato quello cibernetico **dominio di operazioni**[7] a pari grado e insieme a quelli classici: terrestre, marittimo (che include la dimensione subacquea) e aero-spaziale e spazio[8].

Nel dominio *cyber*, più che negli altri domini, la sicurezza di uno Stato è continuamente, ogni giorno, messa a repentaglio da una durissima competizione, non solo tra Nazioni, ma anche tra attori non statuali, difficile da fronteggiare in quanto operante "sotto la soglia dell'attacco fisico armato". In maniera incessante, il nostro Paese riceve **decine di attacchi *cyber*** e li subisce in maniera trasversale e a qualsiasi livello. Si tratta di minacce, attacchi ripetuti ed interferenze malevole che prendono di mira sia la sfera pubblica che quella privata (economica, industriale, dei trasporti, delle comunicazioni, etc.).

Parliamo di servizi e funzioni essenziali, vitali, per ogni Stato/Nazione e per ogni organizzazione internazionale a cui abbiamo deciso di aderire e a cui, storicamente, apparteniamo (NATO, UE, ONU), ma anche per la vita stessa dei cittadini. Accade a partire dai **servizi** e funzioni fornite dalle infra- (e info-) strutture, che, proprio per le loro funzioni così delicate, giudichiamo e valutiamo come "**critiche**" per il Paese. Ma, per la natura stessa del dominio *cyber*, gli effetti non sono sempre riconducibili ad azioni palesi. Inoltre, gli attori malevoli sono raramente identificabili, comunque non con certezza, e quindi non perseguibili in accordo a norme statuali e costituzionali interne, o del Diritto Internazionale.

Quanto esposto rappresenta uno degli scenari della "**guerra ibrida**", dove il dominio *cyber* è uno dei tanti vettori: sabotaggi di sistemi o sottrazione di informazioni, oltre che campagne di **disinformazione** mirate a condizionare le percezioni e le convinzioni di cittadini e Istituzioni. Vere e proprie aggressioni che sfruttano reti e connessioni digitali. Aggressioni che avvengono o da sole o perché impiegate per

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

[8] Nel 2019, la NATO ha dichiarato inoltre anche lo Spazio quale ulteriore dominio di operazioni. *NATO – Official text: NATO's Overarching Space Policy, 27-Jun.-2019*

preparare ed accompagnare operazioni nei domini tradizionali (sul terreno, per mare o nei cieli) e che possono generare anche conseguenze concrete per la sicurezza nazionale ed europea. Non sono problemi virtuali: i danni poi si "sentono" nel mondo reale.

Gli **attacchi informatici** non colpiscono solo i sistemi militari, ma anche settori civili vitali: emblematico è stato l'attacco *ransomware* ***WannaCry*** **(2017)** che ha compromesso migliaia di ospedali e servizi pubblici, o il caso ***Colonial Pipeline*** **(2021)** che ha bloccato la distribuzione di carburante negli Stati Uniti.

Il **furto di dati sensibili** e lo **spionaggio digitale** diventano ulteriori strumenti di pressione politica ed economica. Nel caso ***SolarWinds*** **(2020)**, gruppi riconducibili a interessi statali hanno ottenuto accesso a reti governative e industriali, mostrando la vulnerabilità di catene di fornitura *software* ampiamente diffuse.

Nel **2024** sono stati gestiti **1.979 eventi** ***cyber*** e **573 incidenti (48 al mese)** con impatto confermato, con un incremento rispettivamente del **+40%** e del **+89%** rispetto al 2023. Le vittime complessive sono state **2.734**[9].

Nel primo semestre **2025** sono stati censiti **1.549 eventi cyber**, in **aumento** del **53%** rispetto allo stesso periodo dell'anno precedente (1° semestre 2024). Il numero di **incidenti con impatto confermato** è stato pari a **346**, in **aumento** del **98%**[10].

Numeri impressionanti, in forte e costante accelerazione.

Il **settore sanitario** si conferma tra i più colpiti da attacchi cibernetici, con impatti potenzialmente gravissimi su pronto soccorso, terapie intensive, sale operatorie e trattamenti salvavita. Anche il **comparto manifatturiero** risulta particolarmente bersagliato, in gran parte a causa della prevalenza di **piccole e medie imprese** prive di strutture di difesa adeguate, che lo rendono uno dei settori più colpiti dai *ransomware*. Le nostre piccole aziende sono bersagli facili. Tra i

[9] Agenzia per la Cybersicurezza Nazionale. ***Relazione annuale al Parlamento 2024. Roma: ACN, 2024.***

[10] Agenzia per la Cybersicurezza Nazionale. **OPERATIONAL SUMMARY 1° SEMESTRE 2025.**

principali vettori di compromissione si conferma la posta elettronica, utilizzata per carpire credenziali e informazioni sensibili.

Nel processo di continuo adattamento alle sfide che siamo chiamati ad affrontare è utile fornire un quadro sintetico di quali siano gli approcci adottati da altri Paesi (approfondimento in **APPENDICE I**).

Dall'analisi della postura assunta dalle organizzazioni internazionali di riferimento (NATO e UE) e da Nazioni *like-minded*, come ad esempio USA, UK, Francia e Germania, emerge, in estrema sintesi:

- il forte orientamento ad **integrare il dominio *cyber* e lo spettro elettromagnetico** in un'unica struttura di comando (c.d. *Cyber Electromagnetic Operations* HQ) con l'obiettivo di operare "*as a whole*";
- la necessità di sviluppare specifiche **capacità militari nel dominio *cyber* e negli ambienti informativo e cognitivo** per contribuire a contrastare la minaccia ibrida, incrementare la resilienza e la deterrenza del sistema Paese a tutela dei prioritari interessi strategici nazionali;
- l'esigenza di realizzare una ***Work-Force*** in grado di sviluppare **capacità operative "*full-spectrum*", "*ready to warfight*" e tecnologicamente avanzate**, idonee ad operare nell'ambito di una più ampia minaccia ibrida e "non convenzionale", tipica degli attuali scenari di confronto internazionale;
- l'opportunità di istituire, in analogia con gli altri domini, una **Riserva *Cyber* della Difesa** a supporto della *Cyber Work-Force*, articolata in due componenti: una riserva operativa, costituita da personale con pregressa esperienza tecnico-operativa in ambito difesa, e una riserva di volontari civili, in grado di offrire contributi aggiuntivi di natura tecnica, strategica o accademica;
- la creazione all'interno dei *Cyber Command* di **laboratori per la "ricerca e sviluppo"** nell'ambito dell'innovazione digitale e tecnologica (i.e. ***Emerging Disruptive Technologies***, quali

l'Intelligenza Artificiale e le Tecnologie Quantistiche) per ampliare, automatizzare ed ottimizzare le capacità esprimibili;

- il significativo **potenziamento** degli **organici** militari, anche dell'ordine di **10/15 mila unità**, dedicati ai settori ***cyber***, **spettro elettromagnetico** e **nuove tecnologie** con un **ramo operativo** molto **robusto**, idoneo ad integrarsi con continuità nelle operazioni multi-dominio, su suolo nazionale e nei teatri operativi, dove le esigenze sono preventive, difensive e, ove necessario, controffensive;
- i ***Cyber Command***, in seno agli **apparati militari stranieri**, rappresentano punti di riferimento nazionali per la **protezione delle infrastrutture critiche** e il contrasto delle attività di **manipolazione cognitiva**. Tali Comandi svolgono un ruolo di primaria responsabilità nella difesa nazionale, analogamente a quanto accade nei domini fisici: semplificando, con l'Esercito a protezione del suolo patrio, la Marina per le nostre acque, l'Aeronautica per i nostri cieli e, pertanto, i *Cyber Command* per lo spazio cibernetico di interesse dello Stato;
- nei Paesi analizzati poi, pur permanendo distinzione tra i precipui compiti e responsabilità, **Difesa** e **Comparto *Intelligence*** hanno sviluppato un legame ancor più forte ed imprescindibile nell'ambito cibernetico, funzionale allo sviluppo dei ***Cyber Command*** e allo svolgimento delle collegate operazioni *full spectrum* di contrasto attivo e continuativo alle minacce. Stessa distinzione di compiti permane in ambito Difesa, dove la funzione "*intelligence*" è a supporto delle operazioni.

Dal quadro emerso discendono quindi delle considerazioni sulla costituzione, l'organizzazione e i compiti di un **Comando congiunto** che sia responsabile del dominio ***Cyber***, dell'ambiente **elettromagnetico** e di quello **cognitivo**. Nello specifico, occorre:

- assegnare la **condotta** di tutte le "**operazioni militari cibernetiche**" **univocamente al nuovo Comando congiunto**, prevedendo una

funzione di supporto da parte dell'*Intelligence* militare per la valorizzazione e la condivisione dei dati;

- far operare tale Comando sulla base della ***policy*** emanata dallo Stato Maggiore della Difesa (in analogia a quanto avviene per gli altri domini) e in coerenza con gli indirizzi di livello politico;
- raggiungere la necessaria **"massa critica" di risorse**, accentrando il **personale militare** dotato di specifiche abilitazioni in ambito delle ICT[11] e delle EDT[12] (AI, *Quantum Technologies, High Performance Computing*), e avvalendosi di **personale specialistico civile** proveniente dagli istituti di formazione, dal settore industriale e dal mondo accademico e della ricerca;
- individuare strumenti e meccanismi per **acquisire/adeguare**, in maniera agile e tempestiva, **prodotti e servizi "allo stato dell'arte" nei settori ICT e *Cyber*;**
- **valorizzare il ruolo del nuovo Comando congiunto** come strumento di sicurezza del Paese per il contrasto, sin dal tempo di pace, delle **minacce cibernetiche e ibride**.

Occorre, pertanto, promuovere con urgenza[13] le iniziative che seguono:

1. **identificare lo Spazio *cyber* di interesse nazionale** per la difesa e la sicurezza dello Stato: un "campo di operazioni" all'interno del quale il Ministero della Difesa possa operare, senza soluzione di continuità, per adempiere ai propri compiti istituzionali;
2. **creare un'Arma *Cyber***:
   - **civile e militare;**
   - **numericamente adeguata** al livello di minaccia osservata;
   - che sia **operativa e continuamente capace di intervenire** su tutto lo spettro delle minacce.
   - che abbia **adeguate tutele funzionali** per il personale incaricato.

[11] *Information & Communication Technologies*
[12] *Emerging Disruptive Technologies*
[13] Audizione del Ministro della Difesa **Guido Crosetto** dinanzi alla **IV Commissione Difesa della Camera** sul tema della **sicurezza cibernetica**, 23 gennaio 2025

In tale prospettiva, mentre proseguono gli approfondimenti tecnici e il confronto con i Paesi amici e alleati, si può ritenere che una forza realmente congrua e rassicurante debba attestarsi su almeno **5.000 unità**, con una **prevalente componente operativa**.

In termini più realistici, tuttavia, un primo obiettivo può consistere nella creazione di una **capacità iniziale** di **1.200-1.500 unità**, di cui circa il **75% dedicato a compiti operativi**, così da garantire continuità d'azione **h24, 7 giorni su 7, 365 giorni l'anno** — secondo il modello già consolidato in altri settori della Difesa, come ad esempio quello aereo;

3. Istituire un **Centro per il Contrasto alla Guerra Ibrida**, che esprima le capacità di:
   - **Comando e Controllo**;
   - condivisione di ***best practice***, per lo scambio informativo e per il contrasto alla **propaganda disinformativa**;
   - sviluppare **sinergie** tra Istituzioni e mondo accademico per creare gli "**anticorpi di base**" contro i fenomeni di **disinformazione**.

5.2. LA DISINFORMAZIONE E L'INTERFERENZA NEI PROCESSI ELETTORALI. LA NORMATIVA EUROPEA

Le potenziali minacce nella sfera informativa europea derivanti da interferenze straniere nei processi elettorali sono da tempo al centro dell'attenzione dell'Unione Europea, attenzione rafforzata in occasione del **rinnovo del Parlamento Europeo del giugno 2024**.

A livello di *governance* UE, dopo che il **Consiglio Europeo** (17-18 aprile 2024) ha invitato le **istituzioni** dell'**UE** e le **autorità nazionali** a **cooperare** sui rischi di **disinformazione** e interferenze nei **processi elettorali**, la Presidenza belga *pro tempore* del Consiglio UE ha attivato il meccanismo ***Integrated Political Crisis Response*** (**IPCR**) dedicato alle "interferenze straniere in occasione delle elezioni europee di giugno

2024". Tale meccanismo ha facilitato lo scambio informativo per monitorare e contenere i rischi di ingerenza esterna nel processo elettorale e migliorare la preparazione a eventuali crisi.

Il **Consiglio UE** del 21 maggio 2024 ha adottato conclusioni sulla resilienza democratica e l'interferenza straniera nelle elezioni, enfatizzando le possibili interconnessioni tra campagne ***Foreign Information Manipulation and Interference*** (**FIMI**), attività **informatiche dolose** e l'uso di **intelligenza artificiale** e ***deepfake*** a fini manipolativi[14].

Il messaggio è chiaro: disinformazione, *cyber*-attacchi e *deepfake* vanno affrontati insieme.

Nel marzo 2024, la **Commissione Europea** ha adottato specifiche **linee guida (C/2024/3014)** per le **piattaforme** ***online*** e i **motori di ricerca** di dimensioni molto grandi che mirano a mitigare i rischi sistemici per i processi elettorali.

In particolare, queste linee guida invitano le piattaforme a:

- **agevolare l'accesso degli utenti** alle informazioni ufficiali sui **processi elettorali**;
- realizzare iniziative e **campagne di alfabetizzazione** mediatica incentrate sulle **elezioni**;
- adottare misure per fornire agli utenti **informazioni** sui contenuti e sugli ***account*** con cui interagiscono;
- aggiornare e **perfezionare** i sistemi di **raccomandazione** dei **contenuti** ***online***;
- **prevenire** l'ambiguità e l'uso improprio dei messaggi di **pubblicità politica**;
- **demonetizzare** i **contenuti disinformativi**, tramite misure mirate che evitino che la collocazione di pubblicità fornisca incentivi finanziari alla diffusione della disinformazione, nonché **contrastare** i contenuti

[14] Consiglio dell'UE, "***Resilienza democratica: il Consiglio approva conclusioni sulla salvaguardia dei processi elettorali dalle interferenze straniere***" *comunicato stampa, 21 maggio 2024,* https://www.consilium.europa.eu/it

di **incitamento all'odio**, di estremismo violento o radicalizzanti che possano influenzare le scelte elettorali degli utenti.

In pratica l'UE ha chiesto ai "giganti del *web*" di fare pulizia e garantire più trasparenza.

Per quanto riguarda il **Parlamento Europeo**, la **risoluzione 2024/2696** adottata il 25 aprile 2024 ha invitato la *leadership* politica dell'UE e degli Stati membri a **contrastare** i tentativi di **ingerenza russa**, anche in vista delle **elezioni europee** del giugno dello stesso anno.

Nel contesto della **Bussola Strategica**[15], è stato adottato il **FIMI *Toolbox***, un insieme di misure per rispondere a tali minacce, concentrato su quattro ambiti principali:

- **conoscenza situazionale;**
- **sviluppo della resilienza;**
- **azioni di perturbazione e regolamentazione;**
- **misure di politica estera UE** (incluse quelle diplomatiche).

La Bussola Strategica ha inoltre previsto l'istituzione di **squadre europee di risposta rapida** alle minacce ibride (***Hybrid Rapid Response Teams***, HRRT).

In poche parole, l'Europa si sta attrezzando con strumenti dedicati e squadre anti-minacce ibride.

In questo contesto emerge come la **sicurezza nazionale** – in particolare la **protezione** della **società civile** e la **salvaguardia dei valori democratici** – sia esposta a una crescente minaccia ibrida che si cela dietro strategie mediatiche ostili e manovre di influenza geopolitica e sociale. Ormai è chiaro che la nostra **sicurezza interna** dipende anche e soprattutto dalla difesa dello spazio informativo.

Le recenti campagne di **disinformazione** hanno evidenziato come gli attori ostili elaborino e diffondano contenuti in concomitanza di

[15] Documento adottato dall'UE nel 2022 che definisce la visione comune di sicurezza e difesa, fissando obiettivi concreti al 2030.

importanti appuntamenti elettorali (come le **elezioni del Parlamento UE** o le **Presidenziali USA**), interferendo con il loro normale svolgimento. In tali casi, le campagne FIMI mirano a:

- **influenzare** l'**opinione pubblica**;
- **screditare partiti politici** e candidati;
- **minare** la **fiducia** in **enti** e **istituzioni**;
- **accentuare** le **divergenze socio-politiche** preesistenti.

Lo schema è sempre lo stesso: influenzare, screditare, far perdere fiducia e creare divisioni.

La **diffusione di notizie false o manipolate** costituisce una minaccia rilevante per l'integrità dei processi elettorali. La manipolazione informativa può generare sfiducia nei *media* tradizionali, nelle istituzioni e nelle autorità, erodendo questi tre pilastri delle società democratiche e potenzialmente alimentando l'apatia dei cittadini verso i processi elettorali (fino a **scoraggiare l'affluenza alle urne**).

La formula è semplice: diffondere bugie per far perdere fiducia nella democrazia e scoraggiare il voto.

Inoltre, la **propagazione di narrazioni estreme** o **anti-sistema** può aumentare la visibilità di personaggi di nicchia le cui posizioni risultano in parte o del tutto allineate con quelle veicolate da attori ostili, fungendo da moltiplicatore di consenso per tali narrazioni. In pratica sembra che vogliano due cose: che la gente non voti e che emergano candidati estremisti utili ai loro interessi.

5.3. LA COERCIZIONE GEO-ECONOMICA

La **coercizione geo-economica** si manifesta attraverso l'uso di **strumenti economici** come **leve di pressione politica e strategica**:

- ***export controls***: le restrizioni sulle **terre rare** e sui **semiconduttori** sono diventate centrali nella competizione globale. Secondo numerosi analisti, nel 2023 la **Cina** avrebbe limitato l'*export* di **gallio e germanio**, fondamentali per l'industria elettronica europea;
- **acquisizioni mirate**: attori esterni hanno più volte tentato di acquisire imprese europee strategiche nei settori **energetico, tecnologico e delle infrastrutture critiche**;
- **uso del debito**: utilizzo di strumenti finanziari come leva geopolitica, imponendo condizioni vincolanti ai Paesi più vulnerabili. Tra i casi spesso citati in relazione alla ***Belt and Road Initiative*** (BRI) figura lo **Sri Lanka**, che ha affidato la gestione del porto di **Hambantota** a investitori cinesi a seguito di difficoltà nel ripagare i debiti contratti. Tale dinamica è talvolta descritta in ambito analitico con l'espressione *"**debt-trap diplomacy**"*.

  Secondo alcuni analisti, la Cina, infatti, tenderebbe a utilizzare leve economiche come strumento di pressione silenziosa: può limitare l'accesso a risorse critiche o vincolare altri Paesi attraverso il debito.

  Con la stessa logica, si starebbe sviluppando la penetrazione in **Africa**, dove Paesi come l'**Angola** sono fortemente esposti rispetto al debito contratto con società cinesi di fornitura di servizi.

5.4. I *CHOKE POINTS* LOGISTICI

Il controllo e la vulnerabilità dei ***choke points* logistici** – ovvero i passaggi obbligati delle reti marittime ed energetiche – rappresentano un ulteriore vettore della minaccia ibrida:

- **rotte marittime**: il **Mar Rosso** è divenuto un teatro centrale della guerra economica. Gli **attacchi degli Houthi** a navi mercantili internazionali nel 2023–2024 hanno costretto numerosi operatori, tra cui **Maersk** e **MSC**, a sospendere i transiti attraverso il Canale di Suez. Lo stretto di **Bab el-Mandeb**, che collega il Mar Rosso al Golfo di Aden, è diventato uno dei punti più vulnerabili, poiché da esso transita circa il **10% del commercio marittimo mondiale**, inclusi volumi significativi di petrolio e gas liquefatto diretti verso l'Europa;
- **infrastrutture energetiche**: il sabotaggio dei gasdotti "***Nord Stream* 1 e 2**" nel settembre 2022 ha mostrato la vulnerabilità delle infrastrutture sottomarine;
- ***supply chain* globali**: le strozzature logistiche causate da conflitti o incidenti – come il blocco del **Canale di Suez nel 2021** dovuto alla nave ***Ever Given*** – dimostrano come anche un singolo evento possa avere ripercussioni sistemiche sul commercio mondiale e sulla stabilità economica.

Abbiamo visto che basta una nave incagliata o un gasdotto sabotato per mettere in difficoltà interi continenti.

5.5. LA DIMENSIONE MILITARE "GRIGIA"

La cosiddetta **zona grigia** comprende attività che non raggiungono la soglia del conflitto armato aperto, ma che mirano a esercitare pressione strategica sugli avversari:

- **sconfinamenti** – si registrano con crescente frequenza **violazioni dello spazio aereo baltico** da parte di velivoli russi senza piano di volo, con conseguente decollo immediato di caccia NATO (*scramble*) per intercettarli. Episodi analoghi avvengono nel **Mar Cinese Orientale**, dove la Cina entra nelle zone aeree di identificazione giapponesi e taiwanesi. Ormai queste provocazioni sono all'ordine del giorno.
  Negli ultimi mesi si è inoltre registrato un aumento dei **sorvoli di droni** – spesso non identificabili – su infrastrutture civili e militari in numerosi Paesi europei;

- **mercenari e *contractors*** – la presenza di gruppi armati privati, come il ***Wagner Group***, ha inciso in diversi scenari africani (Mali, Repubblica Centrafricana, Sudan), dove operano a supporto di regimi locali, influenzando dinamiche di sicurezza. Di fatto, gruppi paramilitari come il ***Wagner Group*** risulterebbero operare a tutela degli interessi russi su vari scacchieri, svolgendo compiti che Mosca preferirebbe non attribuirsi direttamente;

- **esercitazioni provocatorie** – Mosca continuerebbe a condurre **manovre navali e aeree nel Mediterraneo e nel Mar Nero**, spesso in prossimità dei confini NATO. Parallelamente, Pechino starebbe intensificando le **esercitazioni militari intorno a Taiwan**, con simulazioni di blocco navale che mettono in evidenza la capacità di strangolare rotte commerciali vitali.

A titolo di esempio, come evidenziato da più fonti indipendenti anche a livello mediatico[16], il **1° settembre 2025** un presunto attacco di **interferenza russa** ha colpito i sistemi di navigazione GPS dell'aereo

[16] ANSA, "EU Chief's plane hit by suspected Russian GPS jamming," 1 settembre 2025, ANSA Europa-UE (testo che richiama il Financial Times)

della presidente della **Commissione europea Ursula von der Leyen**. L'incidente ha costretto l'equipaggio a ricorrere a **mappe cartacee** per completare l'atterraggio in sicurezza.

Queste attività, pur restando al di sotto della soglia di guerra dichiarata, generano **pressione costante** e hanno lo scopo di **logorare la resilienza politica, militare ed economica** degli avversari.

5.6. LE SFIDE PER LE FORZE ARMATE

La minaccia ibrida pone alle **Forze Armate (FF.AA.)** sfide molteplici e complesse nell'assolvimento delle missioni istituzionali. Le FF.AA. devono essere pronte ad affrontare uno **spettro molto ampio di operazioni**, che supera la difesa convenzionale e copre l'intero *continuum* **del conflitto.**

Una delle sfide principali è l'adattamento a nuove forme di confronto, che richiedono la capacità di operare senza soluzione di continuità nei **cinque domini operativi**: terrestre, marittimo, aereo, cibernetico e spaziale. Non basta più avere carri armati e caccia: ora bisogna saper combattere anche con i *byte* e nello spazio.

Tra le nuove sfide che la Difesa è chiamata ad affrontare è possibile annoverare:

- **integrazione delle capacità *cyber* nelle operazioni multi-dominio**;
- **sviluppo di sistemi di difesa automatizzati basati su IA**, per contrastare attacchi *cyber* in tempo reale;
- **rafforzamento cooperazione pubblico-privato**, così da proteggere le ***supply-chain* della Difesa** e ridurre i rischi di **spionaggio industriale** e **compromissione tecnologica**;
- **sviluppo di tecnologie *Cyber Electromagnetic Activities* (CEMA)** a supporto delle operazioni militari e, in ottica duale, dei servizi essenziali dello Stato;
- **potenziamento della formazione del personale** rispetto alle **minacce** ibride e **cognitive**, con addestramento all'impiego delle nuove tecnologie.

Passiamo ora a vedere "**come**" **rispondiamo**, insieme ai nostri Alleati, a questa minaccia.

6. RISPOSTE E COOPERAZIONE INTERNAZIONALE

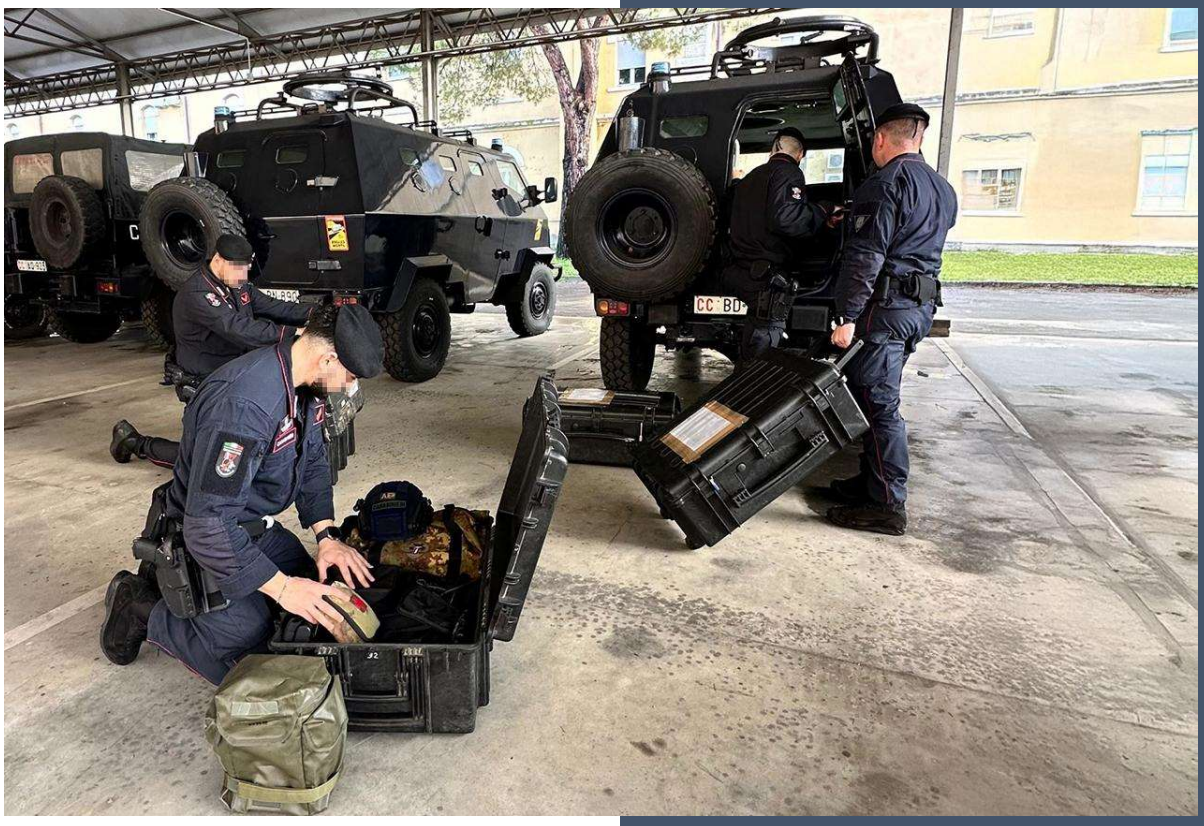


*Figura 12 – **Carabinieri del 7° Reggimento "Trentino-Alto Adige"** in partenza per il valico di Rafah (febbraio 2025), per operare con EUROGENDFOR a tutela del personale internazionale e dei controlli frontalieri, contribuendo alla stabilità in un'area segnata da minacce ibride e da tensioni sotto-soglia.*
Fonte Ministero della Difesa.

6.1. RUOLO DELLA NATO, DELL'UE E DEL G7

*Figura 13 – Foto di gruppo del **Vertice G7 dei Ministri della Difesa (Napoli, ottobre 2024)**, presieduto dall'Italia. All'evento hanno partecipato anche il Segretario Generale della NATO e l'Alto Rappresentante UE: segnale della **stretta cooperazione tra alleati e partner** per **contrastare** in modo coordinato le **minacce ibride** su scala globale.*
Fonte: Ministero della Difesa

La **minaccia ibrida sfuma il confine tra conflitto armato e competizione strategica**. Affrontarla richiede un'integrazione di strumenti di difesa civili e militari e un forte coordinamento tra gli Stati colpiti.

Per fronteggiare questa minaccia, la **NATO**, l'**Unione Europea** e il **G7** hanno sviluppato **approcci** e **strategie complementari** che vanno dalla cooperazione tra agenzie di *intelligence* e forze armate al rafforzamento della resilienza politico-economica. Sia la NATO che l'UE dispongono di alcuni **strumenti specifici** per contrastare le minacce ibride.

Da soli non si va da nessuna parte: dobbiamo muoverci compatti, civili e militari insieme, tra Paesi alleati.

NATO

In ambito **NATO**, la terminologia impiegata per descrivere queste minacce è evoluta significativamente nel corso degli anni, adattandosi alla natura mutevole del fenomeno. La NATO ha, infatti, aggiornato il vocabolario man mano che il nemico cambiava tattica. Inizialmente, **dopo** la **crisi ucraina** del 2014, si parlava di "***hybrid warfare***", riferito a uno scenario bellico in cui metodi di conflitto convenzionali e non convenzionali venivano combinati. Successivamente, è emerso il termine "***hybrid threats***" per indicare attività coordinate e sinergiche **al di sotto della soglia** di un conflitto armato aperto, perpetrate per danneggiare istituzioni, indebolire società e sistemi economici o minare processi democratici. Più di recente, sono state utilizzate – quasi come sinonimi di minaccia ibrida – espressioni quali ***"hybrid campaign***" e "***hybrid activities***" per evidenziare l'aumento quantitativo e qualitativo, e quindi la pervasività, degli attacchi. In sintesi, possiamo chiamarla come vogliamo (guerra ibrida, minacce ibride), il fatto è che gli attacchi sono aumentati e si fanno più insidiosi.

L'attenzione strategica più recente si è concretizzata nella nuova **strategia NATO per la minaccia ibrida**, adottata in occasione della riunione ministeriale della Difesa del **5 giugno 2025**.

Parallelamente, l'Alleanza ha **rafforzato** la propria **postura** di deterrenza e difesa sul **fianco orientale** – con un potenziamento delle forze in Polonia e nei Paesi Baltici – e ha accresciuto l'attenzione sul "**Fianco Sud**", riconoscendo la centralità del bacino **Mediterraneo** per la sicurezza energetica e logistica europea.

Tale strategia mira a rafforzare la capacità dell'Alleanza di prevenire, dissuadere e difendersi dalle campagne ibride ostili, con l'obiettivo ultimo di ridurne la portata e l'impatto sugli Alleati.

La NATO ha sviluppato un quadro per la condivisione informativa e la cooperazione tra i Paesi membri, anche grazie alla creazione di **centri di eccellenza dedicati**, come il **Centro di Eccellenza per**

l'analisi della minaccia ibrida di **Helsinki** e il **Centro di Eccellenza per la difesa cibernetica** di **Tallinn**.

Il ruolo che l'Alleanza può giocare sul fronte *cyber* è essenziale, in primo luogo in termini di *situational awareness* (consapevolezza della situazione), condivisione delle informazioni e capacità di deterrenza verso potenziali minacce. Rilevanti sono inoltre le attività di *capacity building*, la disponibilità di **capacità di supporto e di risposta** in caso di crisi, lo svolgimento di esercitazioni mirate e il rafforzamento della collaborazione con i Paesi *partner*. In quest'ottica rivestono importanza strumenti cooperativi come le squadre di intervento rapido (***Cyber Rapid Response Teams***) e i meccanismi **VCISC** (***Virtual Cyber Incident Support Capability***) e **SCEPVA** (***Sovereign Cyber Effects Provided Voluntarily by Allies***).

In pratica la NATO sta creando personale specializzato (Helsinki, Tallinn) e strumenti comuni (VCISC, SCEPVA) per rispondere meglio alla minaccia.

Le principali **sfide** operative permangono, tuttavia, nella necessità di assicurare un'effettiva e costante **condivisione di informazioni classificate in tempi rapidi**, nella **semplificazione dei processi decisionali** interni all'Alleanza e nel miglior **coordinamento** tra le componenti civili e militari. In altre parole, le idee ci sono, ma se le informazioni non circolano e la burocrazia frena, diventa tutto più difficile.

Per questo, in maniera coerente ed armonica al quadro strategico implementato, è stato istituito il **NATO *Integrated Cyber Center* (NICC)**, centro civile-militare per la gestione coordinata delle informazioni e delle capacità sopra esposte.

Da segnalare, inoltre, l'adozione da parte dei **Ministri della Difesa NATO**, il **18 ottobre 2024**, del nuovo "**Approccio NATO per contrastare le minacce informative**", finalizzato a potenziare la capacità dell'Alleanza su **quattro priorità strategiche**:

- **comprendere** l'**ambiente informativo**;
- **prevenire** l'**efficacia** delle minacce informative;
- contenere e **mitigare** specifici **incidenti** informativi (anche tramite comunicazione proattiva);
- trarre **insegnamento** dagli episodi passati di manipolazione.

In sostanza: la NATO sa che deve combattere anche sul fronte delle *fake news*, smascherandole e imparando dagli errori passati.

A dicembre 2024, infine, la **Divisione NATO di Diplomazia Pubblica** ha presentato la **Strategia di comunicazione dell'Alleanza per il 2025**, che dedica particolare attenzione all'azione di ***debunking***, evidenziando la necessità di **aumentare la consapevolezza** delle società alleate sulle false narrazioni riguardanti la NATO e di smascherarle.

Non basta la forza militare: bisogna vincere anche la battaglia delle idee, contrastando falsità e propaganda in tempo reale.

In sintesi:

Data / Periodo	Evento chiave	Sintesi
2014	Crisi ucraina – introduzione termine "*Hybrid Warfare*"	Conflitti che combinano metodi convenzionali e non convenzionali.
2015–2019	Diffusione termine "*Hybrid Threats*"	Attività coordinate sotto la soglia di conflitto armato per danneggiare istituzioni e processi democratici
2020–2023	"*Hybrid Campaign*" e "*Hybrid Activities*"	Aumento quantitativo e qualitativo attacchi ibridi
18 ottobre 2024	Adozione "*NATO Approach to Countering Information Threats*"	Priorità: 1. comprensione ambiente informativo; 2. prevenzione; 3. contenimento/mitigazione; 4. apprendimento da casi passati.
Dicembre 2024	Strategia di comunicazione NATO 2025	*Focus* su *debunking* e consapevolezza contro false narrazioni anti-NATO.
5 giugno 2025	Nuova strategia NATO per la minaccia ibrida	• Rafforzamento prevenzione, deterrenza e difesa contro campagne ibride ostili; • uso strumenti VCISC e SCEPVA; • centralità centri di eccellenza Helsinki e Tallinn; • rafforzamento postura su fianco est e Mediterraneo

Figura 14 – Riunione UE Difesa – Incontro informale dei Ministri della Difesa dell'Unione Europea (Bruxelles, 31 gennaio 2024). Fonte: Ministero della Difesa

L'**UE** ha messo a punto un articolato quadro normativo e di strumenti per fronteggiare le minacce ibride, che comprende – tra gli altri – la Direttiva **NIS** (aggiornata dalla **NIS2**), il ***Cybersecurity Act***, il ***Cyber Resilience Act***, il ***Cyber Solidarity Act***, il ***Digital Operational Resilience Act***, la **Direttiva sulle infrastrutture critiche** (**CER**), il ***Digital Services Act*** (DSA) e un **codice di buone pratiche per il contrasto alla disinformazione**.

Nel **2023**, inoltre, l'UE ha adottato il ***Critical Raw Materials Act*** (CRMA), volto a **ridurre** la **dipendenza** da forniture esterne di **materie prime critiche**, e l'***Anti-Coercion Instrument*** (ACI), che consente di rispondere in maniera coordinata a pratiche di coercizione economica da parte di Paesi terzi. Entrambi gli strumenti puntano a salvaguardare l'**autonomia strategica UE**.

L'Unione ha inoltre creato strutture apposite: il **Centro di coordinamento per la risposta alle crisi** (**ERCC**) e il **NIS** ***Cooperation Group*** per la sicurezza cibernetica, l'**Agenzia UE per**

la cybersicurezza (**ENISA**), il **Centro europeo di competenza per la cybersicurezza** (**ECCC**) e il **Centro di Coordinamento di *Cyber Defence***. Da segnalare altresì l'***European Cyber Crisis Liaison Organisation Network*** (**EU-CyCLONe**) e la ***Military Computer Emergency Response Team Operational Network*** (**MICNET**), quali reti di cooperazione con lo scopo di sviluppare e condividere tempestivamente consapevolezza situazionale a supporto delle Autorità nazionali degli Stati membri responsabili della gestione di incidenti, attacchi e crisi informatiche su larga scala e transfrontaliere.

Questi organismi operano in stretto **raccordo** con la **NATO** per migliorare la cooperazione e lo scambio di informazioni in ambito civile-militare al fine di ottenere un quadro unico e sempre aggiornato sulle minacce.

L'UE ha creato quindi agenzie e centri, ma il difficile è reagire uniti e in fretta quando scatta l'allarme.

Le principali sfide per l'UE riguardano la definizione di **strategie operative** di **lungo periodo** nei confronti degli Stati da cui originano le minacce cibernetiche all'Unione, nonché l'eventuale **armonizzazione delle procedure di attribuzione degli attacchi** (ovvero l'individuazione di criteri minimi comuni che possano facilitare l'adozione di prese di posizione pubbliche o **misure di contrasto condivise**).

Nell'incessante dibattito europeo sulle modalità di risposta alla minaccia ibrida, le conclusioni del **Consiglio UE del 27 giugno 2024** hanno sottolineato l'esigenza di una **reazione unitaria** e determinata di fronte alla **campagna ibrida russa**. A tale riguardo, va menzionato il "**nuovo quadro per misure restrittive in risposta alle azioni destabilizzanti della Russia all'estero***",* adottato dal Consiglio UE il **18 ottobre 2024**. Si comincia a passare dalle parole ai fatti, con sanzioni mirate contro le interferenze di potenziali attori ostili.

Inoltre, da un evento tematico tenutosi a margine del Consiglio Affari Esteri del 25 gennaio 2025 sono emerse indicazioni per il **SEAE** (**Servizio Europeo per l'Azione Esterna**) e la Commissione, volte all'**elaborazione di una strategia più ampia di contrasto alla minaccia ibrida russa.**

Per favorire una consapevolezza condivisa sulla natura della minaccia ibrida, l'UE si avvale del **centro di analisi di *intelligence*** del SEAE, l'**INTCEN** (inserito nel ***Single Intelligence Analysis Capacity*, SIAC**), che utilizza contributi informativi forniti dagli Stati membri. Le analisi prodotte – e che alimentano il dibattito nei competenti *fora* UE – risultano inevitabilmente influenzate dal punto di vista degli **Stati** che **forniscono** tali **contributi**, non necessariamente rappresentativi della piena pluralità di vedute e interessi esistente nell'Unione. La verità è che le analisi dipendono da ciò che i Paesi condividono: se mancano pezzi, la visione resta parziale.

A **livello operativo**, la questione della risposta alla minaccia ibrida è affidata in sede Consiglio UE a un apposito **gruppo di lavoro** nell'ambito del **Comitato Politico e di Sicurezza** (**COPS**): l'***Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats*** (**HWP ERCHT**). Questo gruppo elabora analisi orizzontali sulle problematiche connesse alle minacce ibride, esaminando le opzioni e individuando gli strumenti atti a rafforzare la preparazione e la resilienza dell'UE di fronte ad attività ibride ostili (incluso il cosiddetto "**EU *Hybrid Toolbox***").

Tra gli obiettivi dell'**HWP ERCHT** vi è anche quello di assicurare un **approccio coerente e coordinato** nella gestione delle minacce ibride, tramite un **insieme integrato di strumenti e azioni** (risposte diplomatiche, economiche, informatiche, legali e militari, a seconda degli aspetti della minaccia da affrontare). Si cerca di combinare diplomazia, economia, difesa e legge per rispondere a 360° a chi ci attacca.

La **cooperazione a livello UE** si è sviluppata anche attraverso il *Rapid Alert System* (RAS), una rete che riunisce **istituzioni UE e Stati membri** per facilitare la condivisione di informazioni sulle minacce **FIMI**.

Il **RAS facilita** lo **scambio di segnalazioni** relative a campagne di disinformazione e, all'occorrenza, il coordinamento delle risposte, avvalendosi di una **piattaforma *online* protetta** (limitata però a informazioni non classificate).

L'Unione ha inoltre istituito ***hub* dedicati al tracciamento e all'analisi** delle attività di **disinformazione *online***, come l'**Osservatorio Europeo dei *Media* Digitali** (**EDMO**), la rete europea delle entità di ***fact-checking*** (**EFCSN**) e il progetto ***EUvsDisinfo***, orientato prevalentemente al contrasto della disinformazione di matrice russa.

Sempre sul piano operativo, l'UE ha avviato nel **febbraio 2024** l'Operazione **EUNAVFOR ASPIDES**, missione navale volta a **garantire** la **libertà di navigazione** e la sicurezza dei traffici commerciali nel **Mar Rosso** e nello **Stretto di Bab el-Mandeb**, a fronte degli attacchi portati da gruppi armati non statali.

Finalmente, l'UE è passata all'azione inviando navi dove serviva, come nel Mar Rosso, per proteggere le rotte.

In sintesi:

Data / Periodo	Evento chiave	Sintesi
2016–2023	Adozione e aggiornamento quadro normativo UE contro minacce ibride	Introduzione strumenti legislativi: **Direttiva NIS → NIS2**, ***Cybersecurity Act, Cyber Resilience Act, Cyber Solidarity Act***, **DORA, Direttiva CER,** ***Digital Services Act***, **Codice di buone pratiche sulla disinformazione,** ***Critical Raw Materials Act*** **(CRMA) e l'***Anti-Coercion Instrument* **(ACI)**.
	Creazione strutture specializzate	Attivazione di **ERCC, NIS Cooperation Group, ENISA, ECCC**; rafforzata la **cooperazione NATO-UE** per lo **scambio informativo.**
27 giugno 2024	Conclusioni Consiglio UE su minaccia ibrida russa	Richiamo necessità risposta unitaria e determinata.
18 ottobre 2024	Quadro UE per misure restrittive contro la Russia	Adozione di nuove sanzioni mirate a contrastare azioni destabilizzanti attribuibili alla Russia all'estero.
dicembre 2024	Sviluppo capacità analisi e risposta	**SEAE-INTCEN** rafforza l'analisi delle minacce ibride tramite contributi informativi degli Stati membri.
25 gennaio 2025	Indicazioni strategiche al SEAE e alla Commissione	Proposte per strategia UE più ampia di contrasto alla minaccia ibrida russa.
2025	Ruolo operativo dell'**HWP ERCHT**	Gruppo di lavoro **COPS** elabora analisi e opzioni per rafforzare resilienza UE contro attività ibride ostili, attraverso l'"***EU Hybrid Toolbox***"
	Cooperazione e condivisione tramite **RAS** e ***hub*** dedicati	Potenziamento *Rapid Alert System* per minacce **FIMI**; operativi **EDMO**, **EFCSN** e progetto ***EUvsDisinfo*** per contrastare disinformazione russa.

Il **G7** ha inserito la **cybersicurezza** nella propria agenda a partire dal 2016, anche in seguito all'avvio dei lavori del **Gruppo di esperti governativi ONU** del 2015 in materia. Di particolare rilievo la **Dichiarazione dei Ministri degli Esteri di Lucca** (2017, Presidenza italiana), incentrata sul **comportamento responsabile** degli Stati nello spazio cibernetico.

La prevenzione e il contrasto delle minacce alla democrazia sono oggetto delle attività del ***Rapid Response Mechanism*** (RRM) del G7, istituito su iniziativa canadese in occasione del **Vertice di Charlevoix del 2018**, al quale partecipano anche alcuni Paesi osservatori. Tale meccanismo è stato creato per rafforzare il coordinamento nel monitoraggio e nella risposta alle minacce straniere verso la democrazia. Finora le attività dell'RRM si sono concentrate prevalentemente su:

- **condivisione di informazioni e valutazioni** sulle minacce in ambito **FIMI**;
- sulla **mappatura** delle **capacità nazionali** di **monitoraggio** della **disinformazione**;
- sulle iniziative di ***capacity building*** a favore di Paesi terzi.

Con la presidenza italiana (2024) il G7 ha alzato il tiro: tutti hanno riconosciuto che disinformazione e ingerenze sono minacce globali da affrontare insieme. Infatti, la **Dichiarazione Ministeriale di Capri dei Ministri degli Esteri** (17–19 aprile 2024) contiene un capitolo dedicato alle **minacce ibride e** alla **manipolazione informativa**, che definisce le FIMI "una sfida crescente per le società democratiche di tutto il mondo".

Nel **comunicato** finale del Vertice di **Borgo Egnazia** (14 giugno 2024), i *leader* del G7 si sono impegnati a rafforzare l'azione comune per rispondere alla manipolazione informativa, affidando al gruppo **RRM del G7** il compito di creare un **meccanismo di risposta collettiva**, ampliandone il mandato al contrasto alle forme

di coercizione economica, oltre alla disinformazione e alle interferenze straniere nei processi democratici.

La **Dichiarazione Ministeriale di Fiuggi** adottata dai Ministri degli Esteri G7 (26 novembre 2024) ha infine condannato il ricorso – da parte del governo russo e dei relativi intermediari – alla manipolazione e all'interferenza informativa per sostenere la guerra contro l'Ucraina e alimentare tensioni globali, evidenziando la necessità di fornire una risposta collettiva a tale fenomeno.

In questo quadro, l'**Italia** può svolgere un ruolo di rilievo quale **ponte mediterraneo** tra **Europa, Africa e Medio Oriente** e quale **potenza manifatturiera** al centro delle catene del valore europee.

Questi elementi costituiscono *asset* strategici da valorizzare in chiave europea per rafforzare la resilienza collettiva contro le minacce ibride.

In sintesi:

Data / Periodo	Evento chiave	Sintesi
2015	Avvio lavori **Gruppo esperti governativi ONU**	Avvio discussioni su comportamento responsabile Stati nello spazio cibernetico.
2016	Inclusione cybersicurezza nell'agenda G7	Sicurezza cibernetica diventa tema stabile dell'agenda.
2017	Dichiarazione di Lucca (Presidenza italiana)	*Focus* su comportamento responsabile Stati nello spazio cibernetico.
2018	Creazione *Rapid Response Mechanism (RRM)*	Istituito al Vertice di Charlevoix su iniziativa canadese; obiettivo: coordinamento monitoraggio e risposta minacce straniere alla democrazia.
2018–2023	Attività dell'RRM	• Condivisione informazioni su FIMI; • mappatura capacità nazionali anti-disinformazione; • *capacity building* per Paesi terzi.
17–19 aprile 2024	Dichiarazione **Ministeriale di Capri** (G7 Esteri)	Minacce ibride e manipolazione informativa definite "sfida crescente" per le democrazie; priorità durante Presidenza italiana.

Ma mentre rafforziamo le difese comuni, **la minaccia evolve**: "**in quali forme nuove si manifesta?**"

7. SCENARI DELL'EVOLUZIONE DELLA MINACCIA IBRIDA

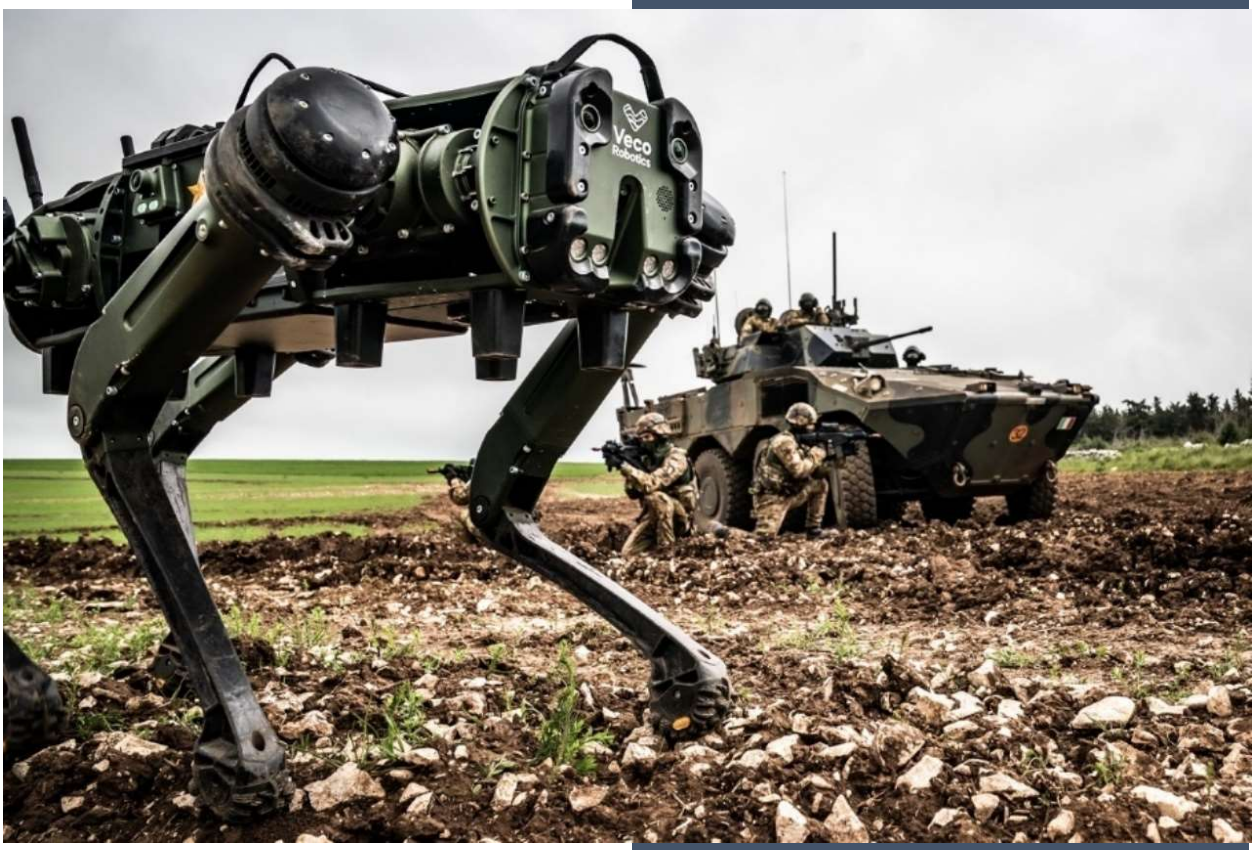


Figura 15 – Unità dell'Esercito testano l'impiego di **droni tattici ed equipaggiamenti CEMA** durante l'esercitazione tecnologica **"Scudo 25"**
Fonte: Ministero della Difesa

La pubblicazione, a novembre 2024, del **rapporto Niinistö** [17] sulla preparazione europea nella risposta civile e militare alle crisi ha segnato un salto di qualità nelle ambizioni dell'UE nel contrasto alla minaccia ibrida, richiamando la necessità che **l'Unione adotti un approccio più rapido e assertivo**. Tale rapporto riflette il diffuso senso di **vulnerabilità** presente soprattutto tra i Paesi dell'**Europa nord-orientale**, legato alla percezione di un'assenza di efficaci forme di deterrenza verso la minaccia ibrida.

Nel rapporto si richiama la necessità di:

- rafforzare la **resilienza** *("deterrence by denial")*;
- migliorare la ***situational awareness***, proponendo la creazione di un **servizio d'*intelligence* dell'UE** pienamente operativo, capace di favorire la cooperazione internazionale e integrare le capacità informative offerte dai servizi nazionali;
- sviluppare una capacità UE di risposta alla minaccia ibrida attraverso azioni che colpiscano gli attori malevoli *("deterrence by punishment")*.

In sostanza, Niinistö raccomanda di rafforzarci in casa e difenderci da chi ci attacca, non solo parare i colpi.

Ciò presuppone una piena comprensione delle vulnerabilità e delle dipendenze strategiche degli attori ostili, il rafforzamento dell'**ambiguità strategica** europea in funzione deterrente, un approccio più accorto nella valutazione degli attori della minaccia e delle loro possibili reazioni e l'adozione di **risposte anche asimmetriche**.

In definitiva, il rapporto Niinistö legittima la **minaccia ibrida come un nuovo ambito di confronto** di potenza per l'Unione e i suoi Stati membri.

[17] Sauli Niinistö, ***Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*** (Bruxelles: Commissione europea, 30 ottobre 2024).

7.1. L'EVOLUZIONE TECNOLOGICA E L'IMPIEGO DELL'IA

*Figura 16 – Unità dell'**Esercito** si addestrano all'impiego di **quadricotteri**.*
Fonte: Esercito Italiano.

L'**evoluzione** della **minaccia ibrida** è strettamente connessa al progresso tecnologico, che funge da acceleratore e moltiplicatore delle capacità offensive sia degli attori statuali sia di quelli non-statuali. La **tecnologia** ha **influito** profondamente sui processi di trasformazione e **potenziamento** sia degli **attacchi cibernetici** sia delle **campagne FIMI**, semplificandone la realizzazione e la diffusione.

Di seguito si evidenziano alcune tendenze tecnologiche rilevanti:

- **sabotaggi cinetici di infrastrutture critiche** – attacchi fisici deliberati contro infrastrutture vitali (ad esempio reti elettriche o di comunicazione) che un attore statuale sufficientemente sofisticato può condurre impiegando risorse e competenze tecniche avanzate;
- ***deepfake* ad altissimo realismo** – contenuti multimediali artefatti mediante IA che hanno raggiunto livelli di realismo tali da rendere

estremamente difficile distinguere il vero dal falso, minando la fiducia nelle fonti informative e polarizzando l'opinione pubblica;

- ***microtargeting* basato su *big data* e IA** – l'analisi di **grandi quantità di dati** combinata con algoritmi di IA consente di effettuare forme di persuasione mirata estremamente precise, con messaggi su misura che sfruttano le vulnerabilità psicologiche di specifici individui o gruppi;
- **automazione della propaganda sui *social media*** – l'impiego di *botnet* e *account* automatizzati amplifica la diffusione di messaggi manipolati *online*, creando una distorsione della realtà percepita e aumentando esponenzialmente la platea raggiunta dalla disinformazione;
- **sistemi di IA generativa per la creazione di contenuti multimediali altamente personalizzati e realistici** – se sfruttati da attori ostili questi sistemi possono essere impiegati in modo persistente, in particolare durante **campagne elettorali**, per influenzare la percezione pubblica;
- **possibile impiego ostile dell'IA** – l'utilizzo di sistemi di IA può essere indirizzato alla disinformazione e persino al "**terrorismo cibernetico**", oltre che a supportare attività di **spionaggio informatico**;
- **utilizzo di sistemi di IA generativa per facilitare e accelerare le fasi della *cyber kill chain*** – gli attori ostili potrebbero avvalersi di IA generativa per velocizzare le varie fasi di un **attacco informatico** (dalla ricognizione iniziale fino all'esecuzione vera e propria);
- **sviluppo di tecnologie come la robotica e i droni autonomi** – tali strumenti potrebbero far evolvere le azioni ibride in forme più "fisiche" e asimmetriche, riducendo ulteriormente i rischi per l'attaccante e aumentando la capacità di infliggere danni;
- **intensificazione** delle **campagne di disinformazione** e incremento dei **cyberattacchi**, in particolare in concomitanza con elezioni o crisi geopolitiche;

- **uso strumentale della pressione migratoria** – l'impiego dei **flussi migratori** come leva geopolitica da parte di attori statuali o non statuali per destabilizzare Paesi di frontiera dell'UE.

In breve, la tecnologia sta dando ai malintenzionati armi nuove e potenti, dai *deepfake* iper-realistici ai **droni autonomi.**

L'utilizzo delle nuove tecnologie, inclusa l'IA, sta cambiando radicalmente il panorama delle minacce ibride: con lo sviluppo – oltre a quanto sopra descritto – di strumenti come **robotica e droni autonomi**, le campagne ibride potrebbero assumere forme via via più "**fisiche**" e asimmetriche, **aumentando la portata dei danni** inflitti.

Un'ulteriore ipotesi particolarmente critica riguarda lo scenario della **"doppia leva"**, in cui un attore ostile **combina** la **dipendenza dell'UE da materie prime critiche** con l'**interruzione dei *choke points* marittimi**. Senza ricorrere a un conflitto aperto, questa strategia può logorare progressivamente l'Unione e l'Italia, mettendone a rischio la resilienza economica e la stabilità sociale. Basta immaginare: niente materie prime e rotte bloccate: uno scenario da incubo, ma possibile se restiamo con le mani in mano.

Per dare ancora più concretezza a quanto finora detto, volgiamo ora lo sguardo al conflitto russo-ucraino.

8. *CASE STUDY* - CONFLITTO RUSSO-UCRAINO

*Figura 17 – I Ministri della Difesa dei Paesi NATO e UE durante la **riunione di Bruxelles (31 gennaio 2024) dedicata alla crisi in Ucraina**.*
*L'aggressione russa ha messo in luce la **natura ibrida del conflitto russo-ucraino**, spingendo gli Alleati a rafforzare rapidamente cooperazione, strumenti militari e sostegno coordinato a favore dell'Ucraina.*
Fonte: Ministero della Difesa

8.1. LA RESISTENZA UCRAINA E I SUOI LIMITI

*Figura 18 – Joint Terminal Attack Controller (JTAC) del **Reggimento Ricognizione e Acquisizione Obiettivi (RRAO) dell'Esercito Italiano** insieme a forze statunitensi durante l'esercitazione congiunta "**Emerald Warrior 2025**" (febbraio 2025), impegnati nell'integrazione di capacità di ricognizione, targeting e supporto aereo in scenari multidominio tipici della guerra ibrida.*
Fonte: Ministero della Difesa,

La **situazione in Ucraina è ormai chiara e consolidata**: il sostegno internazionale, unito alla determinazione del popolo ucraino e alla resilienza delle sue Forze Armate, ha permesso finora di contenere l'aggressione russa.

Tale resistenza si traduce principalmente in una capacità di "**guadagnare tempo**", senza riuscire verosimilmente a generare le condizioni necessarie per riconquistare i territori occupati o invertire in modo significativo l'andamento del conflitto. Condizione ancor più esacerbata dall'**esaurimento del bacino di volontari ucraini, almeno fino alla fine del 2025** (come dichiarato dal *Commander of Ukrainian Unmanned Aerial Vehicle Forces* nel corso di un suo recente intervento).

L'Ucraina sta comunque fronteggiando con coraggio la minaccia russa, la stessa minaccia per la quale i Paesi europei stanno rafforzando le proprie **capacità di difesa e deterrenza.**

8.2. IL VANTAGGIO STRATEGICO RUSSO

La **Federazione Russa** dal canto suo dispone di **risorse superiori**, sia in termini di mezzi – con un'industria bellica più forte rispetto all'inizio del conflitto – sia sul piano umano, e non è vincolata da considerazioni morali riguardo al numero di perdite subite.

Inoltre, può contare sul supporto diretto o indiretto (palese o occulto) di **numerosi Paesi, che continuano a fornire equipaggiamenti, medici, genieri, manodopera specialistica e contingenti militari in quantità significative**. Mentre ogni ferita, caduto, giorno di combattimento conta e pesa tanto per l'Ucraina quanto per le opinioni pubbliche dei Paesi che la sostengono, la *leadership* russa sembra dare scarso peso al fattore tempo e al costo umano del conflitto.

Le perdite complessive russe sono stimate intorno al milione dall'inizio dell'invasione, senza che la popolazione russa ne sia consapevole; pochi in Russia sanno quante giovani vite sia già costata loro questa aggressione.

8.3. ECONOMIA DI GUERRA E CONDIZIONI NEGOZIALI

La *leadership* russa sfrutta questo vantaggio e prosegue la sua azione sulla base di una **economia interna oramai di guerra**, con costi di produzione degli armamenti che non seguono le regole del mercato – quindi molto più economici – e volumi e ritmi di produzione molto più alti di quelli occidentali.

Si tratta di un'economia che difficilmente potrebbe tornare sostenibile in assenza del conflitto, alimentata da reclutamenti che sfiorano le **30.000 unità al mese**, su un bacino di **5 milioni di riservisti**, e da piani che mirano a portare l'Esercito a **1,6 milioni di soldati**.

La Federazione Russa appare oggi configurata secondo una logica di guerra totale, caratterizzata da un'intensa produzione industriale e da arruolamenti di massa impensabili in tempo di pace.

8.4. IL RISCHIO PER L'EUROPA

In questo scenario, **l'Europa si trova coinvolta in un conflitto asimmetrico che mira a indebolire il fronte occidentale a supporto di Kiev**. Pur non essendo direttamente coinvolta nel conflitto in Ucraina, l'Europa rischia di **assistere passivamente a una vittoria russa** ottenuta per logoramento. Al contempo, l'Europa predispone strumenti e regole di risposta in costante ritardo rispetto alle azioni della controparte.

Mosca può quindi godere dell'**iniziativa operativa** (in quanto aggressore) e di quella strategica (puntando sul prolungamento del conflitto).

Questa situazione rafforza ulteriormente la posizione di Mosca, orientata a conseguire vantaggi politici sfruttando i tempi più lunghi richiesti per costruire consenso e prendere decisioni in ambito europeo e NATO. La lentezza decisionale europea è quindi il miglior alleato di potenziali attori ostili: loro agiscono subito, noi discutiamo a lungo e intanto perdiamo terreno.

8.5. IL RUOLO DELLA RUSSIA NEL CONTESTO DELL'*HYBRID WARFARE*: IL QUADRO STRATEGICO

Nel quadro di sicurezza attuale, in costante deterioramento, secondo numerosi analisti la Russia sembrerebbe aver intensificato, ormai da anni, la pressione sull'Occidente tramite un impiego sempre più sofisticato e aggressivo degli **strumenti della guerra ibrida**.

Il paradigma della sicurezza internazionale è entrato in una nuova fase, caratterizzata da una forma di conflitto che sfugge alle tradizionali categorie di guerra convenzionale.

La **Federazione Russa** avrebbe quindi adottato un approccio sistemico e spregiudicato, fondato sull'impiego integrato di **strumenti militari e non militari**, con l'obiettivo di destabilizzare i suoi *competitor*, eroderne la **coesione interna** e influenzarne la **volontà politica.** La *leadership* russa parrebbe disposta a impiegare ogni strumento – dalla propaganda disinformativa agli attacchi informatici fino alle pressioni economiche – pur di indebolire la resilienza dei Paesi occidentali.

8.6. GLI STRUMENTI DELLA GUERRA IBRIDA

In questo contesto, la **guerra ibrida** non è più una minaccia teorica, ma un *modus* operativo che si manifesta quotidianamente, anche in assenza di un conflitto dichiarato, e viene perpetrata non solo contro i Paesi europei ma anche nelle aree dove risiedono i **nostri interessi strategici.**

Gli strumenti impiegati non sono più limitati alle attività *cyber* dagli effetti non cinetici, ma comprendono **azioni quotidiane** – spesso minacciando infrastrutture critiche – che provocano **danni concreti e misurabili**, sempre più spesso al di sopra della **soglia di tollerabilità**.

È un **insieme coordinato di azioni** che si sviluppano in modo sinergico nell'ambito dello stesso **disegno offensivo,** in modo più o meno palese, sfruttando in maniera sempre più significativa le ***Emerging***

and Disruptive Technologies. Stanno colpendo le nostre opinioni, la nostra capacità di resistere e la stabilità politica, non solo le infrastrutture.

Ciò si realizza tramite **campagne** di manipolazione delle opinioni pubbliche, **disinformazione – oramai vera e propria guerra cognitiva** – pressione economica e **sabotaggi**, sfruttando le vulnerabilità normative e istituzionali degli Stati democratici.

Questi strumenti non mirano soltanto a produrre effetti diretti nei domini fisici tradizionali, ma agiscono indirettamente sulle convinzioni, sulla capacità di resistenza, sulla **sovranità decisionale** e sulla **stabilità politica** degli Stati.

In pratica, mirano alla testa e al cuore della società, non solo agli obiettivi militari.

8.7. I RECENTI SVILUPPI: EVOLUZIONE DEGLI OBIETTIVI E DELLE MODALITÀ

Nel **2024** si è registrato un rafforzamento delle attività ibride riconducibili alla **Federazione Russa**, attraverso l'impiego coordinato di strumenti informativi, economici, cibernetici, diplomatici e militari – regolari, privati e locali. Tali attività vengono segnalate con frequenza quotidiana e risultano particolarmente rivolte ai Paesi che sostengono l'Ucraina. Tra le manifestazioni più ricorrenti si registrano: **sabotaggi** a infrastrutture critiche, **roghi** dolosi in prossimità di siti strategici, **attacchi informatici** di matrice statale, campagne di **disinformazione** organizzate e la strumentalizzazione dei **flussi migratori** a fini destabilizzanti.

Tali azioni mirano a **influenzare il dibattito democratico**, a minare la coesione del fronte occidentale e a gestire **a proprio vantaggio** le forniture di beni di primaria importanza (soprattutto **energia** e **materie prime**). Questo aspetto risulta ancor più significativo se si considera che **nel 2024 oltre la metà della popolazione mondiale è**

stata chiamata alle urne[18]. Metà del mondo andava al voto e la **Federazione Russa** avrebbe colto l'occasione per intensificare campagne di disinformazione e azioni di sabotaggio a proprio vantaggio.

Rispetto agli anni precedenti, le sue attività ibride sembrano contraddistinte da una **crescente spregiudicatezza** e da una minore attenzione per le possibili ripercussioni.

8.8. ESEMPI CONCRETI DI OPERAZIONI IBRIDE

Si è registrato un **ampliamento della portata** e del **ritmo** delle **operazioni asimmetriche** contro gli Stati occidentali, con atti fisici di sabotaggio a siti militari o ad aziende coinvolte nel sostegno degli sforzi militari dell'Ucraina. Alcune di queste azioni sarebbero peraltro state condotte da individui privi di cittadinanza russa, in modo da poter meglio rivendicare la propria estraneità alle operazioni e rendere più complessa la fase dell'*attribution* tecnica, ancor prima di quella politica[19].

La volontà russa di compiere azioni violente in Europa occidentale è verosimilmente il segnale di una strategia finalizzata a **manipolare la percezione di sicurezza** delle opinioni pubbliche europee e a delegittimare i Governi schierati a fianco dell'Ucraina.

L'obiettivo è creare **crepe all'interno dei Paesi e tra di loro,** mettendo in discussione le politiche governative e sovranazionali.

In questo scenario, a oltre tre anni dall'inizio dell'offensiva, la questione del conflitto in Ucraina resta al centro della propaganda del Cremlino. Attività volte anzitutto a giustificare le ragioni di Mosca nei confronti del popolo russo e della comunità internazionale, nell'ottica

[18] Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, ***Relazione annuale sulla politica dell'informazione per la sicurezza - 2025*** (Roma, 2025), infografica "**La guerra ibrida nell'anno elettorale**"

[19] Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, *Relazione annuale sulla politica dell'informazione per la sicurezza - 2025* (Roma, 2025), sezione "**La minaccia ibrida alle democrazie liberali**"

di minare la solidità di alleanze sovranazionali, quali la **NATO** e l'**Unione Europea.**

Tra le numerose operazioni ibride attribuite alla Federazione Russa nel 2024, le azioni più palesi sono state[20]:

a. l'operazione **Doppelgänger** che ha simulato siti *web* di testate giornalistiche europee come *Le Monde, Der Spiegel* e La Repubblica, diffondendo notizie false e contenuti manipolati per minare la fiducia dell'opinione pubblica nelle istituzioni democratiche e nel sostegno all'Ucraina (in **APPENDICE II**[21] alcuni dettagli ulteriori relativi alle campagne di disinformazione operate dalla Federazione);

b. in **Germania**, un **attacco** coordinato alla **rete ferroviaria** che ha causato l'interruzione del traffico merci e passeggeri in diverse regioni. L'azione pare sia stata condotta da attori non statali con legami con i servizi russi, con l'obiettivo di colpire infrastrutture critiche (in **APPENDICE III**[22] alcuni dettagli ulteriori relativi agli atti di sabotaggio registrati);

c. in **Polonia**, un **incendio doloso** che ha distrutto un **deposito militare contenente equipaggiamenti destinati all'Ucraina**. Le indagini hanno rivelato la presenza di agenti infiltrati e l'utilizzo di tecniche di sabotaggio riconducibili a operazioni ibride (vds **APPENDICE III**);

d. il **danneggiamento di cavi sottomarini** per le telecomunicazioni tra Finlandia e Germania e tra Svezia e Lituania (vds **APPENDICE III**);

e. la **pressione migratoria dalla Bielorussia verso la Polonia**, che secondo alcuni analisti risulterebbe strumentalizzata a fini politici

[20] Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza, *Relazione annuale sulla politica dell'informazione per la sicurezza – 2025* (Roma, 2025), infografica "La minaccia ibrida," sezione "Disinformazione russa"

[21] Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza, *Relazione annuale sulla politica dell'informazione per la sicurezza – 2025* (Roma, 2025), infografica "La minaccia ibrida," sezione "Disinformazione russa"

[22] Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza, *Relazione annuale sulla politica dell'informazione per la sicurezza – 2025* (Roma, 2025), infografica "La minaccia ibrida," sezione "Disinformazione russa"

anche dalla Russia. Nel solo **2024** sono stati intercettati oltre **30.000 tentativi di attraversamento illegale della frontiera**, costringendo Varsavia ad istituire una "zona di esclusione lungo circa 60 chilometri del confine polacco-bielorusso;

f. **influenza** sui governi locali nel **Continente africano** (in particolare nel Sahel) attraverso campagne di disinformazione che fanno leva sui sentimenti anticoloniali e la fornitura di servizi securitari attraverso ***Private Military Companies*** **(PMC)** con l'obiettivo di rafforzare la propria posizione geopolitica, economica e di sicurezza energetica e, al contempo, delegittimare la presenza europea e, sempre secondo alcune analisi, incentivare indirettamente i flussi migratori illegali verso l'Europa – avvalendosi anche di reti criminali – utilizzandoli come potenziale **"fattore di pressione sociale"** nei confronti dell'UE (vds **APPENDICE IV**[23]);

g. le **elezioni presidenziali in Romania del 2024** avrebbero subito pesanti **interferenze ibride** (**attacchi informatici, disinformazione** e persino ***deepfake***) che ne avrebbero compromesso la regolarità, portando alla decisione di annullare il voto. L'episodio rappresenta un caso emblematico di come un processo democratico possa essere compromesso da attori esterni (vds **APPENDICE V**[24]).

La varietà di questi attacchi è impressionante: *fake news*, ferrovie sabotate, cavi tranciati, pressione migratoria, elezioni annullate…

Questi esempi – non esaustivi e che escludono gli attacchi quotidiani alle nostre infrastrutture critiche – dimostrano come la **guerra ibrida** si manifesti, senza soluzione di continuità, attraverso **azioni concrete e coordinate**, capaci di colpire simultaneamente le dimensioni fisica, informativa e cognitiva della sicurezza Nazionale ed europea.

[23] Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, *Relazione annuale sulla politica dell'informazione per la sicurezza - 2025* (Roma, 2025), infografica "**L'insicurezza in Africa," sezione "Presenza russa in Africa"**

[24] Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, Relazione annuale sulla politica dell'informazione per la sicurezza - 2025 (Roma, 2025), infografica "L'insicurezza in Africa," sezione "**Presenza russa in Africa**"

8.9. LA VULNERABILITÀ OCCIDENTALE NELLA "ZONA GRIGIA"

*Figura 19 – Cooperazione internazionale – **Gruppo di Contatto per la Difesa dell'Ucraina** riunito a **Ramstein (Germania, gennaio 2025)**.*
Fonte: Ministero della Difesa

Per la Russia, dunque, operare nella cosiddetta "**zona grigia**" sembrerebbe essere ormai una **prassi consolidata, continua e destinata ad espandersi**, che consente di **danneggiare** sempre più significativamente l'**Occidente**, anche in assenza di uno stato di guerra dichiarato.

Al contrario, molti Paesi occidentali faticano a gestire politicamente e operativamente tali situazioni, vincolati da una **visione binaria del conflitto che distingue rigidamente pace e guerra**, e da una cultura strategica che privilegia la reazione all'azione. In altre parole, rischiamo di restare imbrigliati nelle nostre regole.

Questo approccio rigido rappresenta una **vulnerabilità** nel confronto ibrido con qualunque attore che si sottragga alle norme del diritto internazionale per provocare danni e ottenere vantaggi ingiusti.

Questa vulnerabilità è aggravata dall'irrinunciabile necessità delle nostre democrazie di costruire e mantenere adeguato **consenso** – politico e pubblico – prima di poter attuare una **risposta proporzionata**.

In estrema sintesi, per motivi strutturali – alcuni dei quali nobili, come la difesa degli elementi fondanti della democrazia – altri culturali, che ci obbligano ad un confronto impari destinato, proprio per questo, a vederci soccombere, la postura occidentale si limita a reagire, cercando di limitare i danni e, nel migliore dei casi, a ristabilire lo *status quo* o a denunciare gli attacchi subiti.

A parere di numerosi analisti, nel frattempo numerosi attori continuano ad alzare progressivamente il livello delle aggressioni ibride. Dato l'atteggiamento occidentale attuale, il costo dell'aggressione, dell'offesa, è prossimo allo zero. Oggi l'aggressore non paga, e può sottrarsi alla responsabilità delle proprie azioni.

A valle dell'esempio del conflitto russo-ucraino, è chiaro che **contenere non basta**: servono passi concreti per prevenire e dissuadere queste minacce.

9. WAY-AHEAD

*Figura 20 - F-35A dell'Aeronautica Militare durante la **Ramstein Flag 2025** (aprile 2025), esercitazione in cui — insieme agli assetti E-550A Conformal Airborne Early Warning (CAEW) e KC-767A per il rifornimento in volo — vengono integrate capacità di 4ª e 5ª generazione, gestione avanzata del battle space e missioni Composite Air Operations (COMAO) in ambienti Integrated Air Defence System (IADS), rafforzando la preparazione nazionale a scenari ibridi e non-permissivi.*
Fonte: Aeronautica Militare.

9.1. PRINCIPALI SFIDE

La minaccia ibrida si configura come una **sfida complessa e multiforme** per la sicurezza nazionale e l'integrità dei processi democratici.

L'impiego di tattiche ibride da parte di attori statuali – e dei loro *proxy* – attraverso manipolazione informativa, attacchi informatici, sabotaggi e interferenze nei processi elettorali mina la fiducia nelle istituzioni democratiche e alimenta divisioni all'interno della società.

La **principale sfida prospettica** in questo ambito risiede nella capacità di sviluppare una **sintesi più costante e strutturata** tra tutte le visioni e le competenze degli attori istituzionali coinvolti, i quali – nel caso italiano – sono attualmente coordinati nel **gruppo di lavoro interministeriale sulla minaccia ibrida presieduto dal Dipartimento delle Informazioni per la Sicurezza (DIS)** inquadrato nella struttura della Presidenza del Consiglio dei Ministri.

Le **campagne di disinformazione** e le **operazioni di manipolazione** associate alla minaccia ibrida sfruttano vulnerabilità politiche, sociali ed economiche, avvalendosi di tecniche sofisticate come il controllo delle narrazioni, la disinformazione digitale e l'uso strategico dei *social media.*

Contrastare efficacemente queste forme di interferenza straniera presenta notevoli criticità, dovute alla **mancanza di piena collaborazione da parte delle piattaforme *social***, ai **limiti tecnologici** nell'**individuazione** tempestiva dei **contenuti manipolativi** e anche a divergenze o pregiudizi di natura politica.

Per far fronte a tali minacce è necessario un approccio coordinato tra tutti gli attori coinvolti, l'uso di strumenti avanzati di monitoraggio e la collaborazione con enti indipendenti di *fact-checking*, mantenendo al contempo un **equilibrio** tra le **esigenze di sicurezza** e la tutela della **libertà di espressione**.

Serve un gioco di squadra vero: *intelligence*, istituzioni, aziende *tech* e cittadini, tutti uniti contro queste interferenze.

L'adozione di **misure preventive**, azioni di **deterrenza** mirate e una maggiore **consapevolezza** delle tecniche impiegate dagli attori ostili sono passi fondamentali per difendere l'integrità delle istituzioni democratiche e garantire la coesione sociale. Non possiamo aspettare di subire un attacco per reagire: prevenire e dissuadere è l'unica strada.

La **minaccia ibrida** attribuita a **Russia** e **Cina** è divenuta un tema centrale anche per la sicurezza nazionale italiana. Secondo diverse analisi, tali Paesi farebbero ricorso a una combinazione di attacchi cibernetici, disinformazione e altre strategie non convenzionali per influenzare la politica e l'economia dell'Italia.

Minacce cibernetiche, **attività di spionaggio e campagne di disinformazione** sono tra le principali modalità con cui questi attori cercano di destabilizzare il nostro Paese.

Gli **strumenti utilizzati nelle campagne ibride** sono in continua evoluzione e vengono adattati al contesto specifico. Tra i più comuni, **in Italia** si possono individuare:

- **attacchi informatici** diretti contro istituzioni governative, aziende private e infrastrutture critiche, che possono compromettere dati sensibili, interrompere servizi essenziali e causare danni economici;
- campagne di **disinformazione** mediante la diffusione di notizie false e propaganda attraverso i *social media* o altri canali *online*, finalizzate a manipolare l'opinione pubblica, alimentare tensioni sociali e influenzare i processi elettorali;
- utilizzo di leve **economiche** – come sanzioni commerciali mirate o investimenti strategici – impiegate per esercitare pressione politica e influenzare le decisioni del governo italiano;
- **sabotaggi** contro infrastrutture critiche (reti elettriche, sistemi di comunicazione, trasporti), capaci di provocare disagi significativi e generare panico tra la popolazione.

La **minaccia ibrida** è in grado di **colpire trasversalmente infrastrutture**, **centri nevralgici**, istituzioni pubbliche e private, sfruttando – anche grazie alla rivoluzione tecnologica in atto – **nuovi ambiti di manifestazione, vettori e modalità operative** che consentono di perseguire gli obiettivi prefissati senza ricorrere a un conflitto armato convenzionale.

Queste minacce colpiscono tutto e tutti, sfruttando ogni spiraglio offerto dalla tecnologia.

Ogni ritardo nella piena comprensione del contesto e nell'adeguamento della *governance* e del quadro giuridico di riferimento **può comportare perdite di vantaggio** competitivo nei confronti degli avversari, perdite che rischiano di risultare difficilmente colmabili. Ogni minuto perso a capire il fenomeno è un vantaggio regalato a chi ci attacca.

La **guerra ibrida** è inoltre destinata a **evolvere ulteriormente**, sfruttando le **innovazioni tecnologiche** e le nuove vulnerabilità delle società moderne. L'**intelligenza artificiale**, la **realtà aumentata** e le **tecnologie quantistiche** vengono già impiegate per creare attacchi sempre più sofisticati, pericolosi e difficili da attribuire.

Alla luce di quanto esposto, se non si intende restare spettatori di un esito più che prevedibile e indesiderato, è necessario un **cambiamento radicale** nell'approccio occidentale alla guerra ibrida.

Occorrono **decisioni coraggiose** – in primo luogo **politiche**, poi **operative** – e riforme da attuare sfruttando l'unico aspetto non tragico che il conflitto in Ucraina ha portato con sé: la ritrovata percezione condivisa del pericolo e una maggiore coesione tra i Paesi europei.

9.2. RUOLO DELLE ISTITUZIONI E COOPERAZIONE

La **strategia** efficace di contrasto alla guerra ibrida dovrà rafforzare la **resilienza democratica**, **informativa e cognitiva dell'Europa**; promuovere una cultura della sicurezza e definire un quadro normativo che consenta di agire efficacemente sotto soglia, con **responsabilità chiare, regole d'ingaggio e soglie di attivazione definite**.

Diventa fondamentale **anticipare le minacce** attraverso ricerca e sviluppo, simulazioni strategiche e scenari previsionali.

Le **democrazie occidentali** devono dotarsi di una **cultura** della **sicurezza proattiva**, capace di adattarsi rapidamente ai cambiamenti e di rispondere con decisione alle aggressioni ibride. Solo attraverso una visione strategica condivisa e un impegno politico costante sarà possibile preservare la sovranità, la stabilità e i valori democratici dell'Europa e di ogni Nazione.

Le istituzioni europee devono assumere un ruolo guida nella definizione di una **strategia comune contro la guerra ibrida**. **Commissione, Consiglio e Parlamento UE** devono lavorare in sinergia per adottare normative che rafforzino la sicurezza informatica, contrastino proattivamente la disinformazione – ad esempio tramite strumenti comuni di certificazione delle notizie – e proteggano le infrastrutture critiche. Occorre istituire un meccanismo permanente di **monitoraggio delle minacce ibride**, con un **centro operativo europeo** dedicato che coordini le risposte e supporti gli Stati membri.

Inoltre, bisogna investire in **programmi di educazione civica** e **alfabetizzazione digitale** per aumentare la consapevolezza dei cittadini e ridurre la vulnerabilità alle campagne di manipolazione.

Cittadini consapevoli sono la nostra migliore difesa a lungo termine.

In tale ottica, l'istituzione del **Centro Europeo per il Contrasto alla Guerra Ibrida** può senza dubbio agevolare questo nuovo approccio, esercitando funzioni di coordinamento strategico, analisi, risposta e formazione. Esso dovrà operare in stretto raccordo con le strutture

esistenti; promuovere l'integrazione tra i diversi attori istituzionali e favorire la cooperazione internazionale.

Un Centro Europeo, quindi, agirebbe come cabina di regia, valorizzando ciò che esiste e orientandolo verso una direzione comune.

L'Unione Europea deve sviluppare una **politica estera e di sicurezza comune più incisiva**, capace di affrontare le sfide ibride con **strumenti concreti, efficaci, coordinati e tempestivi** (in **APPENDICE VI** alcuni degli interventi/obiettivi ritenuti prioritari).

Vanno ulteriormente promossi **partenariati strategici** tra Paesi europei e gli alleati transatlantici, **condividendo** ***intelligence***, tecnologie e buone pratiche.

La **cooperazione con i Paesi terzi**, in particolare quelli del vicinato orientale e meridionale, è essenziale per contenere l'influenza di attori ostili e promuovere la stabilità regionale.

9.3. SUPERARE L'INERZIA

Questo **processo di cambiamento** deve avvenire attraverso un'azione congiunta a livello **nazionale, intergovernativo, sovranazionale**.

Da un lato, il **sostegno dei Parlamenti e dell'opinione pubblica** è fondamentale, dall'altro, solo la forza degli organismi sovranazionali permette una risposta univoca, legittima, rapida e al contempo efficace, coordinata e al riparo da iniziative isolate.

Alcuni Paesi del **fianco est europeo** hanno già maturato una **consapevolezza avanzata** in tal senso.

Tuttavia, la **natura democratica e burocratica delle nostre istituzioni** comporta risposte che rischiano di essere asincrone rispetto alla minaccia, in virtù dei tempi dettati dai processi di approvazione. Questo approccio non è più al passo con i tempi. È ora di snellire i nostri meccanismi: il mondo corre e noi non possiamo restare indietro!

Serve una riflessione collettiva su questo come su altri temi analoghi.

Un altro aspetto riguarda gli **Stati non appartenenti a UE e NATO**, con approcci multi-vettoriali: questi Paesi rappresentano un **terreno di confronto** che, secondo numerosi analisti, è attualmente in mano alla **disinformazione russa e alla penetrazione culturale cinese**. Possono però ancora essere portati dalla nostra parte.

Non ci si riferisce solo agli **Stati africani ma anche ai Paesi balcanici**. Diventa dunque fondamentale promuovere **meccanismi graduali e inclusivi di integrazione**, capaci di attrarre quei Paesi che aspirano a entrare nella nostra sfera di influenza, mostrando così una maggiore efficacia nel contrastare le narrazioni di disinformazione basate sul nostro passato coloniale occidentale.

Il lento e macchinoso processo di allargamento dell'Unione Europea e della NATO proprio verso i Balcani sta, ad esempio, rappresentando un'opportunità per attori esterni – come la Russia – di sviluppare **processi di integrazione alternativi**, **sottraendo terreno d'influenza all'Europa**.

Per analogia è necessario **concentrare l'attenzione politica sul fronte sud** (come nel caso del **Sahel**) sempre più vulnerabile alle lusinghe "ibride" e dove l'Unione Europea deve recuperare lo spazio strategico che attori ostili stanno sfruttando a proprio vantaggio.

Infine, l'approccio occidentale del *"**comprehensive approach**"*, pur valido nei principi, deve essere affiancato da una **strategia più dinamica e coerente** con l'attuale compromesso contesto securitario. Occorre evitare che il sistema si abitui alla costante aggressione ibrida, normalizzandola come una *routine* **tollerabile**.

Basta abituarsi all'aggressione costante: non è la nuova normalità, è un'emergenza continua e va affrontata come tale!

Il contrasto alla guerra ibrida richiede – ora più che mai – un **approccio integrato, multilivello e multidimensionale,** avendo essa dimostrato di poter produrre effetti analoghi, se non superiori, alle minacce tradizionali, con un **potere destabilizzante** persino **maggiore**.

L'Unione Europea deve assumere un **ruolo proattivo nella definizione di una strategia comune**, investendo in capacità di difesa, resilienza e deterrenza.

È necessario superare le logiche frammentarie e adottare una **visione sistemica della sicurezza**, che consideri le interconnessioni tra i diversi domini – **fisico, digitale, cognitivo**.

L'istituzione di un **Centro operativo europeo per il contrasto alla guerra ibrida,** l'adozione di strumenti e criteri moderni per il contrasto alla disinformazione, il rafforzamento della cooperazione interistituzionale, l'adozione di un quadro normativo europeo per la sicurezza ibrida e l'incremento degli investimenti in educazione, ricerca e innovazione sono passaggi obbligati.

La **guerra ibrida** non mira a trionfo immediato, ma a **logoramento costante**. Solo un'**azione coordinata**, *whole-of-government* e integrata con NATO e UE potrà garantire stabilità, competitività e sicurezza alle nostre società democratiche.

In sintesi, è necessario passare da **approccio contenitivo a *difensivo* (che nell'*hybrid warfare* non può che essere *proattivo*)**: mantenersi attivi nel dominio, prevenendo azioni ostili e riducendo la libertà di manovra degli opponenti ibridi. Serve una strategia unitaria e continuativa, con **attenzione a teatri particolarmente a rischio** (e.g. **Balcani** e **Sahel**), per prevenire la normalizzazione della minaccia come nuovo stato di fatto.

Insomma, basta limitarci a contenere: dobbiamo prevenire questi attacchi sul nascere e togliere spazio di manovra agli avversari. E dobbiamo farlo ora.

Passiamo ora a tirare le somme e a ribadire i messaggi chiave.

10. CONCLUSIONI

Figura 21 - Satellite della Costellazione ***COSMO-SkyMed*** *(COnstellation of small Satellites for Mediterranean basin Observation), sistema satellitare italiano dual use che fornisce immagini radar ad alta risoluzione per sorveglianza, sicurezza e risposta a minacce ibride.*
Fonte: Ministero della Difesa.

È in atto una **guerra continua** che ci minaccia **senza sosta, giorno e notte**.

Gli obiettivi sono le nostre **infrastrutture critiche**, i **centri decisionali**, i **servizi essenziali**, le **strutture commerciali**, le nostre **industrie**, le **catene di approvvigionamento**, il **patrimonio cognitivo** delle nostre popolazioni, e, in ultima analisi, la **tenuta complessiva del Paese**.

Questa **offensiva**, in corso da **anni**, procede a un **ritmo sempre più incalzante**, con il rischio crescente che, prima o poi, le **difese** — mai del tutto sufficienti — **non riescano a prevenire** gli **effetti catastrofici** che gli attaccanti perseguono: **il blocco dei trasporti pubblici** (treni, aerei), gravi **incidenti**, il malfunzionamento delle **sale operatorie** e dei **reparti di rianimazione**, il collasso del **servizio sanitario**, la paralisi del **sistema bancario**, la **corruzione dei dati** su cui si basano **pensioni** e **stipendi**.

Si tratta di un **rischio quotidiano**, costruito per mano di **attori malevoli** e privi di scrupoli — ora anche legati a Governi — che hanno di fatto abbandonato ogni riferimento al **Diritto Internazionale**, alla **convivenza pacifica** e ai **valori** che invece noi continuiamo a condividere e difendere.

È una **guerra** combattuta con **"bombe" meno visibili** di quelle fisiche, ma che cadono **incessantemente**, producendo **danni** che, se guardiamo le tendenze e se non cambiamo l'approccio, potremmo non essere in grado di contenere. Ci sveglieremo, un giorno, di fronte a un **danno catastrofico** e ci chiederemo, "sorpresi", cosa sia avvenuto. La risposta sarà: "è avvenuto esattamente ciò che era più probabile — anzi, prevedibile — che accadesse", se non faremo nulla di ulteriormente concreto per evitarlo.

Chi ci muove **quotidianamente** attacchi ibridi, in particolare sul piano della **disinformazione**, della **guerra cognitiva** e nel **dominio *cyber***, oggi sa che l'occidente spesso sceglie **di non reagire**.

Tutto questo **è assurdo**. Questo atteggiamento è **insostenibile**.

Se volessimo fare un parallelo, se un velivolo violasse il nostro **spazio aereo**, non terremmo l'**Aeronautica, i nostri intercettori** fermi a terra negli aeroporti. Se navi nemiche o non autorizzate entrassero nei nostri **mari**, non lasceremmo la nostra **Marina all'ancora** nei porti. Se forze ostili varcassero i nostri **confini terrestri** per colpire infrastrutture critiche, centri

decisionali, servizi, o la nostra industria, non terremmo il nostro **Esercito** nelle caserme, né ci limiteremmo a barricarci in casa al meglio delle nostre possibilità, sperando che se ne vadano.

Per il **dominio *cyber***, per la **guerra cognitiva** e per la **guerra ibrida** nel suo complesso **deve valere esattamente lo stesso principio**: è necessario predisporsi per difendersi efficacemente, il che, per la natura del contesto, non può prescindere da posture proattive e **reazioni legittime e tempestive.**

È il compimento del ragionamento di questo *non-paper*, che apre la strada all'azione concreta: l'**aggiornamento urgente** del **quadro normativo**, allineandolo alle migliori prassi internazionali, con l'obiettivo di abilitare una Difesa pronta ed efficace, coerente con gli scenari presenti e futuri.

La riforma dovrà quindi tradursi nelle **quattro direttrici** già menzionate:

- definire lo **Spazio *cyber* di interesse nazionale** come vero e proprio "**campo di operazioni**" su cui il Ministero della Difesa possa agire senza soluzione di continuità;
- dotarsi di un'**Arma *Cyber***, civile e militare, adeguatamente dimensionata e capace di operare senza soluzione di continuità su tutto lo spettro delle operazioni necessarie. In tale prospettiva, mentre proseguono gli approfondimenti tecnici e il confronto con i Paesi amici e alleati, si può ritenere che una forza realmente congrua e rassicurante debba attestarsi su circa **5.000 unità**, a **prevalente componente operativa**.

  In termini più realistici, tuttavia, un primo obiettivo può consistere nella creazione di una **capacità iniziale** di **1.200-1.500 unità**, di cui circa il **75% dedicato a compiti operativi**, così da garantire continuità d'azione **h24, 7 giorni su 7, 365 giorni l'anno** — secondo il modello già consolidato in altri settori della Difesa, come ad esempio quello della Difesa Aerea;
- garantire a tale Arma adeguate **tutele funzionali** per gli specialisti civili e militari impiegati;
- istituire infine un **Centro per il Contrasto alla Guerra Ibrida** dotato di comando e controllo, meccanismi di condivisione rapida di *best practice* per contrastare la disinformazione e le azioni ostili nel campo della guerra cognitiva.

Tale impianto trova attuazione nei **disegni di legge** recentemente presentati dai membri della **IV Commissione Difesa, a valle della specifica Audizione** sul tema della **sicurezza cibernetica** di **gennaio 2025.**

Queste non sono opzioni: sono le **condizioni necessarie e improcrastinabili** per **proteggere** i **cittadini**, le nostre **case**, i nostri **territori, il nostro Paese, come già fanno altri**.

È infatti un percorso che bisogna fare **individualmente** e collettivamente nell'ambito delle **alleanze**.

Le **"bombe" ibride** continuano a cadere mentre scrivo.

Per questo la vera questione non è **"cosa dobbiamo fare"** — che appare quindi scontato — bensì **la velocità con cui dobbiamo passare dall'attuale postura "contenitiva" a una postura concretamente difensiva, che in ambito *hybrid* non può che essere proattiva, sia a livello nazionale sia in ambito alleanze.**

E il momento per farlo **è adesso**!

APPENDICE I

TAVOLE SINOTTICHE "PER CAPIRE MEGLIO": LA SITUAZIONE NEGLI ALTRI PAESI OCCIDENTALI

GERMANIA

La Germania, Paese all'avanguardia in ambito *Cyber* e *Digital Transformation*, presenta una architettura di sicurezza cibernetica gestita dall'**Ufficio federale per la sicurezza informatica** (***Bundesamt für Sicherheit in der Informationstechnik*** – **BSI**)[25], organo inter-istituzionale dipendente dal Ministero dell'Interno. Il BSI, con un organico di circa **1650 unità**, gestisce il rapporto con il comparto militare, data la notevole importanza di quest'ultimo nel settore *cyber*.

Inoltre, il **Centro Nazionale di Risposta informatica** (***Nationale Cyber-Abwehrzentrum*** – **Cyber-AZ**)[26], sotto l'egida del BSI, istituito nel 2011, riunisce tutti gli *stakeholders* nazionali per cooperare, condividere informazioni e rispondere in modo coordinato in caso di evento/crisi.

La **difesa informatica** è **costituzionalmente** demandata alle **Forze Armate** e, nello specifico, al ***Kommando Cyber und Informationsraum*** (**CIR**) istituito nel 2017, struttura dipendente dal ***Cyber and Information Domain Service*** (**CIDS**), servizio interforze con rango pari a Forza armata (**15500 militari**)[27]. Il citato CIR, con un organico di **1260 militari**[28], è responsabile della sicurezza delle infrastrutture informatiche e dei sistemi d'arma della difesa e, seguito preventiva autorizzazione parlamentare, è incaricato altresì ad intervenire in risposta a un attacco cibernetico di portata nazionale.

---

[25] https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/organisation-und-aufbau_node.html

[26] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum_node.html

[27] https://www.bundeswehr.de/de/organisation/zahlen-daten-fakten/personalzahlen-bundeswehr

[28] https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum

Nello specifico, l'organizzazione militare *cyber* si basa su:

- il **Direttorato Generale *Cyber*/IT**: gestione degli aspetti della digitalizzazione, Innovazione, Ricerca e Sviluppo, IT *Strategy*, IT *Security*, *Geospatial Information* e *Policy cyber*, cooperazione nazionale e internazionale[29];
- il **CIDS** ha alle dipendenze le unità IT, *cyber*, *Information Enviroment* ed *Electronic Warfare* e svolge compiti di prevenzione e sicurezza del "sistema informatico *Bundeswehr*"[30] (missione permanente), di *intelligence* militare (missione permanente), di *reconnaissance and Effects* (spettro elettromagnetico, cyberspazio, ambiente informativo), di *geo-Information support* e di *Cyber Security* (vedi sopra CIR);
- il ***Federal Office of Military Counterintelligence*** (***Militärische Abschirmdienst*** – **MAD**) [31] *:* servizio di controspionaggio militare (*intelligence* difensiva) con il compito di sostenere la missione delle Forze armate e, in particolare:
  - proteggere il *Bundeswehr* dallo spionaggio e dal sabotaggio nel cyberspazio;
  - raccogliere le informazioni necessarie anche nel dominio cibernetico;
  - supportare il ***Zentrum Cyber-Operationen*** (**ZCO**) del CIR, collaborando alla conduzione di operazioni offensive nell'ambito della sfera di competenza della Difesa/in risposta a un attacco [32];
  - cooperare con le altre agenzie di *intelligence* nazionali;
- il ***Cyber Innovation Hub*** *(*CIHBw*)*: organizzazione inserita nell'ambito del FMoD quale laboratorio di innovazione delle Forze Armate tedesche per supportarne, tra l'altro, la trasformazione digitale.

[29] https://www.bmvg.de/en/organisation/the-directorates-general

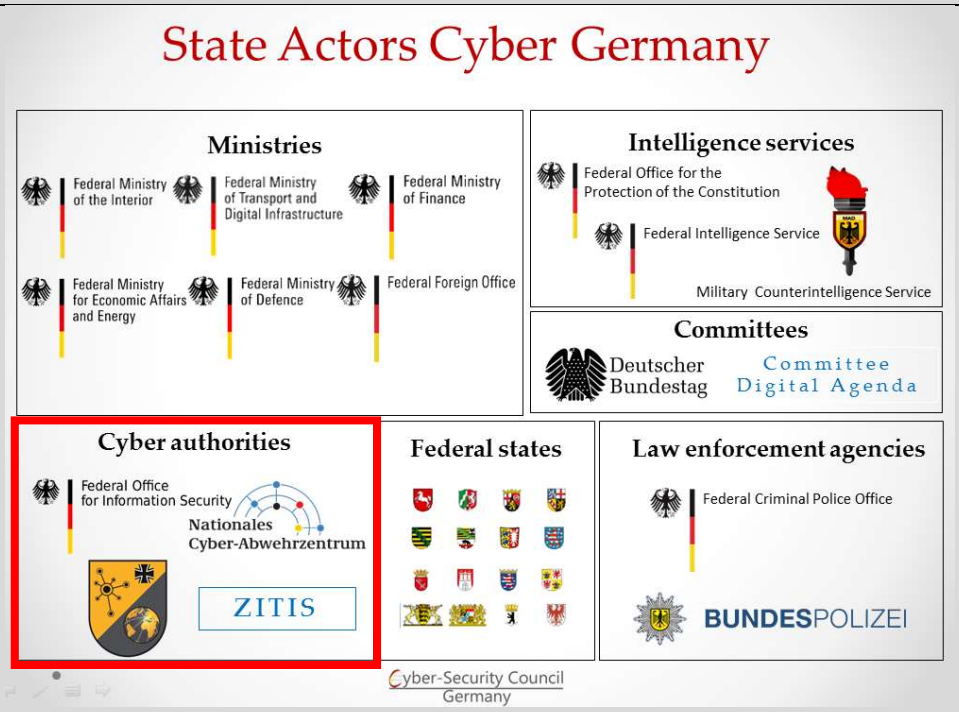
[30] https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service

[31] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=3. Cfr. pag. 20 per competenze generali MAD ambito "Strategia per la sicurezza cyber per la Germania" Ed. 2021

[32] https://www.bundeswehr.de/de/organisation/mad-bundesamt-fuer-den-militaerischen-abschirmdienst

DIREZIONE		ESECUZIONE			
	MoD Cyber/IT Directorate		*CIDS Cyber and Information Domain Service*		*Military Counter-Intelligence Service*
- **Consulenza alla** ***leadership*** MoD per aspetti Cyber/IT; - ***Policy*** in ambito cyber, trasformazione digitale, innovazione e IT *security*; - **Ricerca e sviluppo** per *cyber* e IT; - **Cooperazione** con gli altri attori nazionali; - Supervisione **architettura IT**; - **Strategia**, programmi IT.		- *Cyber Security* e ***Cyber Defence (Kommando Cyber – CIR con 1260 unità)***; - ***Intelligence*** militare; - **Gestione integrata ambiente informativo, spettro elettromagnetico** e cyberspazio; - ***Geo-Information*** *support*; - Supporto ***Whole-of-Government.***		• **Supporto al CIR operazioni *cyber* offensive**; • **Controspionaggio militare nel cyberspazio;** • Cooperazione con comparto ***intelligence*** nazionale.	
		15500 unità			

INTERAGENZIA



REGNO UNITO

Al centro dell'organizzazione *cyber* spicca la ***National Cyber Force*** (NCF) che, riunendo le capacità espresse dalla Difesa e dalla comunità *Intelligence*, conduce operazioni cibernetiche offensive per sostenere le priorità di sicurezza nazionale del Regno Unito.

La NCF si avvale del personale del ***Government Communications Headquarters*** (**GCHQ**) e del Ministero della Difesa, oltre che del ***Secret Intelligence Service*** (**SIS**) e del ***Defence Science and Technology Laboratory*** (**DSTL**).

Il **GCHQ** è l'agenzia governativa che si occupa di **sicurezza** ed ***intelligence***, anche in materia *cyber*, operando su 5 principali *Mission Areas*:

- *Counter Terrorism,*
- *Cyber Security,*
- *Strategic Advantage,*
- *Serious & Organised Crime,*
- *Support to Defence*.

La missione di ***Cyber Security*** del Regno Unito è guidata dal ***National Cyber Security Center*** (NCSC), che fa parte del GCHQ. L'**NCSC** aiuta a proteggere i **servizi critici nazionali** (settore pubblico e industria) dagli attacchi informatici, gestisce gli incidenti gravi e migliora la sicurezza di base di Internet attraverso miglioramenti tecnologici e consulenza a cittadini e organizzazioni. L'NCSC fornisce una risposta agli incidenti per ridurre al minimo i danni, aiuta nella ripresa e apprende lezioni per il futuro.

Il Ministero della Difesa è responsabile della sicurezza delle proprie reti e piattaforme digitali attraverso il "***Cyber & Specialist Operations Command***" (CSOC- 4*). Tale Comando, in collaborazione con il GCHQ, assicura la capacità cibernetica offensiva e il sostegno alle autorità civili in caso di un incidente cibernetico nazionale significativo.

Precedentemente chiamato *United Kingdom Strategic Command* (**UKSTRATCOM**), il Comando ha assunto l'attuale denominazione dal 1° settembre 2025 quale parte del processo nazionale di trasformazione strategica delineata da *Defense Reform* e dagli esiti delle ***Strategic Defence Review*** **2025**. Il CSOC quale ente esecutivo militare in materia *Cyber* è posto

sotto l'autorità del *Chief of Defence Staff,* attraverso il recentemente istituito *Military Strategic Headquarters* (MSHQ).

La riorganizzazione attuata risponde all'evoluzione della guerra moderna, segnata da tecnologie digitali, minacce ibride e dall'erosione dei confini tradizionali tra pace e conflitto. Il nuovo nome vuole enfatizzare da un lato il ruolo centrale del **dominio *Cyber* ed elettromagnetico**, oggi considerato al pari dei tradizionali domini terrestre, marittimo e aereo, dall'altro l'ampiezza delle operazioni specialistiche di cui si occupa il Comando. Volendo fare un parallelo con le forze armate, il CSOC rappresenterà la ***leadership* nel dominio cibernetico ed elettromagnetico**, con la responsabilità di:

- coordinare la difesa del Regno Unito nel cyberspazio;
- integrare gli effetti cibernetici nella pianificazione operativa;
- attraverso la partnership la NCF, e specialmente con il GCHQ, condurre operazioni offensive cibernetiche.

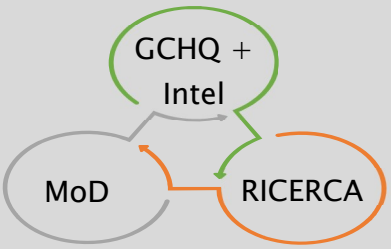
Inoltre, con *Specialist Operations*, si vuole sottolineare l'ampiezza del portafoglio di competenze professionali che, oltre al dominio *cyber* e elettromagnetico, includono:

- comando e controllo delle operazioni globali congiunte tramite (PJHQ);
- *Defence Intelligence*;
- Forze Speciali;
- *Info Ops*;
- *Integrated Global Defence Network* e basi d'oltremare;
- formazione della nuova generazione di *leader* presso la *Defence Academy;*
- sviluppo della guerra integrata,
- capacità C4ISR e *Defence Targeting Enterprise*.

Un comando, quindi, non definito da una singola funzione, ma dall'integrazione di competenze specialistiche diverse (oltre **26.000 specialisti** in **130 sedi globali**, unendo competenze in operazioni informatiche, supporto medico, *intelligence*, forze speciali, istruzione e i nostri addetti alla Difesa all'estero) che operano insieme per fornire effetti congiunti complessi a livello globale, offrendo vantaggi operativi e opzioni strategiche ai decisori politici.

Il Comando ha alle dipendenze:

- *Defense Digital Organization,* con a capo il *Chief Information Officer* (CIO), per la gestione di tutti i servizi digitali ed informatici nonché della sicurezza delle reti. Dispone di un *budget* annuale di oltre **2 miliardi di sterline** e di circa **2.400 dipendenti** tra cui militari, dipendenti pubblici e appaltatori;
- *Chief Defense Intelligence* (CDI) per il supporto alle operazioni cibernetiche offensive. Lavora in stretta cooperazione con la comunità *intelligence* britannica (GCHQ, MI5 e MI6) nell'ambito della NCF e per fornire prodotti di *intelligence* ai responsabili politici del Ministero della Difesa e del Governo. L'*intelligence* della Difesa conta circa **5.000 dipendenti**, di cui **due terzi** sono membri delle **forze armate** e **un terzo** sono **civili**;
- *Cyber & ElectroMagnetic Command* (CEMC), istituito in seguito a quanto previsto dalla *Strategic Defence Review* 2025, con *Initial Operating Capability* prevista entro la fine del 2025. Il CEMC è stato concepito per "coordinare le operazioni digitali e cibernetiche difensive e offensive", integrando le competenze nell'ambito del cyberspazio e dello spettro elettromagnetico, e agendo come un "*hub*" di coerenza strategica. Il compito di condurre le operazioni offensive rimane assegnato alla *National Cyber Force*. Questo nuovo Comando gioca quindi un **ruolo di integrazione, non di esecuzione diretta delle azioni militari**.

DIREZIONE		ESECUZIONE		INTERAGENZIA	
Ministry of Defence	*Ministry of Defence*	Strategic Command	*Cyber & Specialist Operations Command*	National Cyber Force A Defence and Intelligence Partnership	*National Cyber Force (NCF)*
- **sicurezza** delle reti proprie; - capacità **offensiva** (in collaborazione con il GCHQ); - supporto **autorità civili** in caso evento cibernetico significativo.		- **CIO**: gestione di tutti i **servizi digitali** e informatici della Difesa e la sicurezza delle reti; - **CDI**: supporto ad operazioni cyber **offensive** in cooperazione con la comunità *intelligence* britannica nell'ambito della NCF; - **CEMC**: coordinamento operazioni digitali e cibernetiche difensive e offensive		**MoD** e **GCHQ**, in collaborazione con il **DSTL** e il **SIS**, fornisce una capacità offensiva. 	

La riorganizzazione effettuata assume un valore politico e strategico, rafforzando il riconoscimento del ruolo centrale delle capacità cibernetiche ed elettromagnetiche per la difesa nazionale e, nel contempo, chiarire la missione del CSOC. Il nuovo Comando rappresenta un elemento centrale della trasformazione militare britannica, con una *leadership* dedicata, visibile e immediatamente riconoscibile anche agli alleati, confermando l'ambizione del Regno Unito di posizionarsi come attore *leader* nella difesa cibernetica e nelle operazioni multi-dominio.

FRANCIA

La Francia ha sviluppato un modello di difesa cibernetica **integrato e interministeriale**, concepito per proteggere lo Stato, i cittadini e le infrastrutture vitali dalle minacce digitali, garantendo al contempo la capacità di condurre operazioni nel cyberspazio. In questo quadro il pilastro fondamentale è rappresentato dall'***Agence nationale de la sécurité des systèmes d'information*** **(ANSSI)**.

L'**ANSSI**, creata nel 2009 e posta sotto l'autorità del **Primo ministro tramite il *Secrétariat général de la défense et de la sécurité nationale*** **(SGDSN)**, rappresenta l'autorità tecnica nazionale per la sicurezza dei sistemi d'informazione. L'Agenzia svolge un'ampia varietà di attività:

- definisce la **politica di cybersicurezza** dello Stato;
- emette norme vincolanti e regolamenti per amministrazioni, operatori di servizi essenziali **(OSE)** ed operatori d'importanza vitale **(OIV)**, e verifica la loro applicazione;
- gestisce, attraverso il **CERT-FR**[33], gli attacchi informatici e la protezione del sistema d'informazione dello Stato;
- monitora i meccanismi di allerta e risposta rapida, e coordina le crisi cibernetiche attraverso il ***Centre de coordination des crises cyber*** **(C4)**;
- inoltre, provvede al rilascio dei **certificati di sicurezza** per prodotti e fornitori di servizi **ICT**.

Il suo perimetro è civile e interministeriale, a tutela della continuità dello Stato e delle infrastrutture critiche.

Dal punto di vista organizzativo, quindi, la *Cyber Defense* dello Stato è di competenza dell'ANSSI ma in caso di evento cibernetico ostile di portata nazionale o diretto verso le Forze armate, il Ministero della Difesa interviene attraverso il ***Commandement de la cyberdéfense*** **(COMCYBER – ca. 4000 unità)**. Questo Comando, istituito nel 2017 e responsabile della sicurezza e difesa *cyber* di sistemi, infrastrutture e operazioni del Ministero della Difesa, coopera con l'ANSSI per acquisire un quadro completo della minaccia e i

[33] CSIRT nazionale, volto a monitorare e difendere i sistemi francesi da attacchi informatici, nonché a fornire contemporaneamente servizi di *training* e *awareness*.

rispettivi reparti operativi sono collocati presso lo stesso sito per assicurare il necessario coordinamento tecnico-operativo.

Il **COMCYBER**, subordinato al **Capo di Stato Maggiore della Difesa**, pianifica e conduce le operazioni cibernetiche coordinandosi strettamente con l'ANSSI e operando all'interno di una catena di comando unificata, centralizzata e composta da specialisti.

Il **COMCYBER** è articolato su:

- **État-Major de la cyberdéfense (EM-CYBER),** inserito nel polo operazioni dello Stato Maggiore della Difesa:
  - **pianificazione strategica** e la **condotta operativa** delle missioni di cyberdifesa;
  - protezione dei **sistemi d'informazione del Ministero**, fatta eccezione per quelli della DGSE e della DRSD;
  - comprende il ***Centre opérationnel cyber*** **(CO-CYBER)**, centro C2 delle operazioni cibernetiche;
- ***Groupement de la cyberdéfense des armées*** **(GCA)**, dislocato a Rennes e in Île-de-France:
  - riunisce e sviluppa le competenze specialistiche di cyberdifesa;
  - garantisce il supporto tecnico-operativo a favore delle forze schierate;
  - è il centro di gravità per la formazione, la certificazione e l'innovazione cibernetica;
- ***Communauté cyber des armées*** **(CCA)**, composta da circa venti unità operative delle diverse Forze Armate:
  - fornisce capacità specialistiche distribuite sul territorio nazionale;
  - rafforza la massa critica a disposizione del COMCYBER in caso di crisi;
- **Riserva di cyberdifesa:**
  - riserva **operativa (RCD)** di personale militare e civile in servizio o con esperienza pregressa, impiegabile in rinforzo alle unità operative;
  - riserva di volontari civili che apportano contributi di natura tecnica, strategica o accademica.

L'organizzazione francese in materia "*Cyber* militare" vede poi una separazione tra le capacità operative:

- **offensive** (raccolta delle informazioni e operazioni di attacco) – la nuova dottrina autorizza la Difesa a compiere attacchi come parte integrante o sostitutiva delle operazioni militari convenzionali*;*

- **difensive** – protezione e difesa degli assetti della Difesa;
- ***influence*** – a supporto delle operazioni militari.

Questa divisione permette una reazione agli attacchi cibernetici più veloce e un migliore coordinamento con la difesa cibernetica militare, assicurato dal C4.

L'integrazione tra ANSSI e Forze Armate, infatti, si concretizza principalmente nel **C4**, che riunisce attori civili e militari (ANSSI, COMCYBER, DGA, DGSE, DGSI)[34] per la gestione centralizzata delle crisi. La collaborazione si sviluppa inoltre attraverso la condivisione di *intelligence* tecnica, la complementarità delle funzioni (ANSSI per sistemi civili/statali, COMCYBER per quelli militari), nonché esercitazioni di ampia scala, che mettono in sinergia tutte le componenti. Questa architettura, basata sulla netta ripartizione dei compiti ma fondata su stretta cooperazione, consente alla Francia di garantire al tempo stesso la resilienza dello Stato e la capacità di condurre operazioni cibernetiche a difesa degli interessi nazionali.

Focus – **Attività *Cyber* Forze Armate francesi**

Per rispondere alla sfida dettata dalla trasformazione digitale dei sistemi e delle attività del *Ministère des Armées*, nel febbraio 2018 sono state definite:

- **Lotta Informatica Difensiva (LID)**,
- **Lotta Informatica Offensiva (LIO)**,
- **Lotta Informatica d'Influenza (L2I)**,

quali indirizzi strategici imprescindibili per garantire la continuità operativa, la libertà d'azione e la supremazia operativa in un conflitto, aperto o sotto soglia.

La **LID** si costituisce di **sei missioni** fondamentali per:

1. **prevenire**, sensibilizzando gli operatori sui rischi connessi alla digitalizzazione;
2. **anticipare**, valutando costantemente la probabilità di attacchi e predisponendo misure preventive in caso di minaccia elevata;
3. **proteggere**, riducendo le vulnerabilità e rendendo più difficile l'azione degli attaccanti, garantendo al contempo la capacità di individuare le intrusioni;

[34] *Direction Générale de l'Armement (DGA), Direction Générale de la Sécurité Extérieure (DGSE) e Direction Générale de la Sécurité Intérieure (DGSI).*

4. **rilevare**, individuando tempestivamente segni di attività ostili;
5. **attribuire**, identificando con prove o indizi l'autore dell'attacco, per consentire una decisione politica;
6. **reagire**, resistendo agli attacchi per mantenere la continuità delle operazioni e, se necessario, attivando strumenti di risposta anche extra-militari.

La **LID** concentra la sua azione principalmente nell'anticipare, rilevare e reagire, pur completando le altre funzioni. Essa contribuisce alla resilienza delle Forze Armate e si inserisce nella strategia di risposta del Ministero, sia a livello ministeriale che interministeriale.

Il principio di sussidiarietà prevede che ogni stato maggiore, direzione o servizio del Ministero adotti misure di LID sul proprio perimetro, attraverso **centri operativi di sicurezza** (**SOC**) incaricati della supervisione e della rilevazione primaria degli attacchi. A livello centrale, il **CALID** (**Centro di Analisi nella Lotta Informatica Difensiva**) assicura una supervisione tecnica dell'insieme della rete di SOC, mentre il **CO-Cyber** (**Centro Operazioni Cyber**) coordina, orienta e supporta la gestione degli incidenti più rilevanti.

La rapida trasformazione digitale e la crescente interconnessione dei sistemi, non solo all'interno del Ministero ma anche con *partner* esterni, inclusi gli industriali della difesa, impongono una LID condivisa e coordinata. Per questo, la **Direzione Generale degli Armamenti (DGA)** e il **COMCYBER**, in collaborazione con l'ANSSI, propongono accordi specifici con l'industria, definendo ruoli e responsabilità nella prevenzione e nella gestione degli attacchi. La LID opera in maniera permanente, anche in tempo di pace, attraverso la **Postura Permanente di Cyberdifesa (PPC)**, sotto la guida del COMCYBER. Tale postura assicura la **difesa continua (24 ore su 24, 7 giorni su 7)** dei sistemi informatici nel continuum pace-crisi-guerra.

Gli **attacchi *cyber*** vengono classificati in base al loro impatto e alla possibilità di considerarli un'aggressione armata, individuando diversi livelli di minaccia:

- **Giallo e Arancione**: rischi potenziali di entità variabile.
- **Rosso**: rischi ostili plausibili.
- **Scarlatto**: rischi maggiori e simultanei.

Questi livelli si associano a stati di allerta – vigilanza, vigilanza rinforzata, crisi – che indicano se l'attacco è imminente o in corso, consentendo di modulare le misure di risposta e di adattarle a zone o domini specifici.

La dottrina in materia di **LIO** a finalità militare delinea una capacità strategica di primaria importanza, concepita per garantire la **sovranità nazionale** e consolidare la **superiorità operativa** della Francia nel dominio del cyberspazio. Il testo si colloca in un contesto strategico caratterizzato da un'intensificazione delle minacce ibride e da attacchi informatici di vasta portata che hanno dimostrato come lo spazio digitale sia ormai un vero e proprio teatro di confronto. La LIO viene definita come l'insieme delle operazioni condotte nel cyberspazio, sia autonomamente sia in combinazione con mezzi militari convenzionali, volte a compromettere la disponibilità, l'integrità o la riservatezza dei sistemi informatici avversari, nel pieno rispetto del diritto internazionale. Essa si fonda sulla capacità di operare sulle **tre componenti strutturali** del cyberspazio:

- la **dimensione fisica** (infrastrutture e apparati),
- quella **logica** (dati, processi, protocolli e applicazioni) e
- quella **semantico-sociale** (informazioni e identità digitali).

Gli effetti prodotti possono essere materiali o immateriali, temporanei o permanenti, con potenziale impatto determinante sulla condotta delle operazioni.

Gli **obiettivi operativi** della LIO si articolano su **tre direttrici principali**:

1. **raccolta** di **informazioni**,
2. **valutazione** delle **capacità avversarie**, neutralizzazione o degradazione delle capacità operative nemiche,
3. **alterazione** delle percezioni o delle **capacità di analisi** dell'avversario.

L'impiego può avvenire a **livello tattico**, ad esempio con la neutralizzazione di un sistema d'arma o di un posto di comando, o a livello **strategico**, come nel caso della disorganizzazione di strutture di propaganda o dell'interdizione di capacità critiche.

La condotta di tali operazioni è posta **sotto l'autorità** del **Presidente della Repubblica** e del **Capo di Stato Maggiore delle Forze Armate**, con il **COMCYBER** quale autorità operativa responsabile della pianificazione e coordinamento, in stretta sinergia con stati maggiori operativi e servizi di

intelligence, e con l'impiego di unità specializzate integrate nella manovra interforze. Particolare rilievo è attribuito alla gestione dei rischi — politici, giuridici e militari — intrinseci alle caratteristiche del cyberspazio, quali l'immediatezza dell'azione, l'elevata interconnessione dei sistemi e la natura duale delle infrastrutture bersaglio. L'azione offensiva deve conformarsi ai principi del ***jus in bello***, alle regole d'ingaggio e a un rigoroso controllo strategico, per evitare effetti collaterali, propagazioni non previste o l'eventuale riutilizzo degli strumenti offensivi da parte dell'avversario. Sul piano internazionale, la Francia ribadisce il proprio impegno nello sviluppo di una cultura *cyber* condivisa in ambito NATO, in attuazione del *Cyber Defense Pledge*, e nel contesto dell'Unione Europea, promuovendo l'interoperabilità con i principali partner pur mantenendo il pieno controllo nazionale delle capacità LIO, considerate parte integrante della sovranità dello Stato.

Per il futuro, la dottrina individua **cinque priorità di sviluppo**:

1. accelerare la **produzione** di **capacità LIO** a favore delle Forze Armate;
2. definire una **politica delle risorse umane** in grado di sostenere l'elevata specializzazione richiesta;
3. sviluppare **attività formative** dedicate presso gli stati maggiori di pianificazione e condotta delle operazioni;
4. **adattare** i **processi di acquisizione e sviluppo** capacitivo alla rapidità dell'innovazione tecnologica nel settore cyber;
5. e, infine, **rafforzare** la **convergenza operativa con i *partner*** per garantire la possibilità di impiego in coalizione anche in contesti di crisi.

Per affrontare il contesto strategico attuale, dove la natura della **conflittualità** è profondamente **mutata** dallo **schema tradizionale "pace – crisi – guerra"**, occorre considerare un ***continuum*** segnato da "**competizione, contestazione e confronto**". In questo nuovo quadro, la guerra dell'informazione è diventata una componente imprescindibile di ogni strategia militare.

L'evoluzione dei mezzi di comunicazione e, in particolare, l'avvento dei ***social network*** ha radicalmente trasformato l'ambiente operativo, accelerando la diffusione di informazioni – vere o false – e ampliandone la portata. Questa dinamica offre ad attori statali e non statuali la possibilità di influenzare rapidamente le percezioni, mobilitare l'opinione pubblica e minare la legittimità delle Forze Armate.

Per fronteggiare questa minaccia crescente, la Francia ha definito la dottrina specifica **L2I**. Essa si sviluppa nello strato informativo del cyberspazio e ha come finalità la **rilevazione, caratterizzazione e neutralizzazione degli attacchi informativi avversari**, il **sostegno alla comunicazione strategica** del *Ministère des Armées*, la **raccolta di informazioni** di interesse operativo e la **conduzione di operazioni di inganno**.

Tali attività si svolgono nel pieno rispetto del diritto nazionale e internazionale e sono circoscritte alle operazioni militari al di fuori del territorio nazionale. Il comando e il **coordinamento** delle operazioni di L2I sono affidati al **Capo di Stato Maggiore delle Forze Armate e al Comandante del COMCYBER** che opera in stretta integrazione con le altre componenti della *Cyber Defense* – difensiva e offensiva – e possono cooperare con altri ministeri, con le strutture NATO, nonché con *partner* privati del settore digitale.

La dottrina definisce **tre assi d'azione principali**:

1. **informare**, comprendendo l'ambiente informativo, identificando ed analizzando le minacce, conoscendo le intenzioni e le capacità dell'avversario;
2. **difendere**, neutralizzando/attenuando gli effetti delle campagne di disinformazione e salvaguardando la credibilità e la legittimità delle Forze Armate;
3. **agire**, influenzando il comportamento dell'avversario, valorizzando l'operato delle proprie Forze Armate, conducendo manovre di inganno a supporto delle operazioni fisiche.

La padronanza del dominio informativo richiede sia risorse umane altamente qualificate – come linguisti, specialisti dell'influenza, esperti in comunicazione, psicologi e tecnici informatici – sia strumenti tecnologici avanzati, basati su big data e intelligenza artificiale, in grado di monitorare le reti e analizzare i contenuti in tempo reale.

Infine, la dottrina riconosce che la L2I si inserisce in una strategia più ampia di cooperazione per contrastare la manipolazione dell'informazione e la propaganda, soprattutto di matrice terroristica, impone di lavorare in sinergia con attori istituzionali, partner internazionali e aziende del settore digitale.

Aspetti finanziari

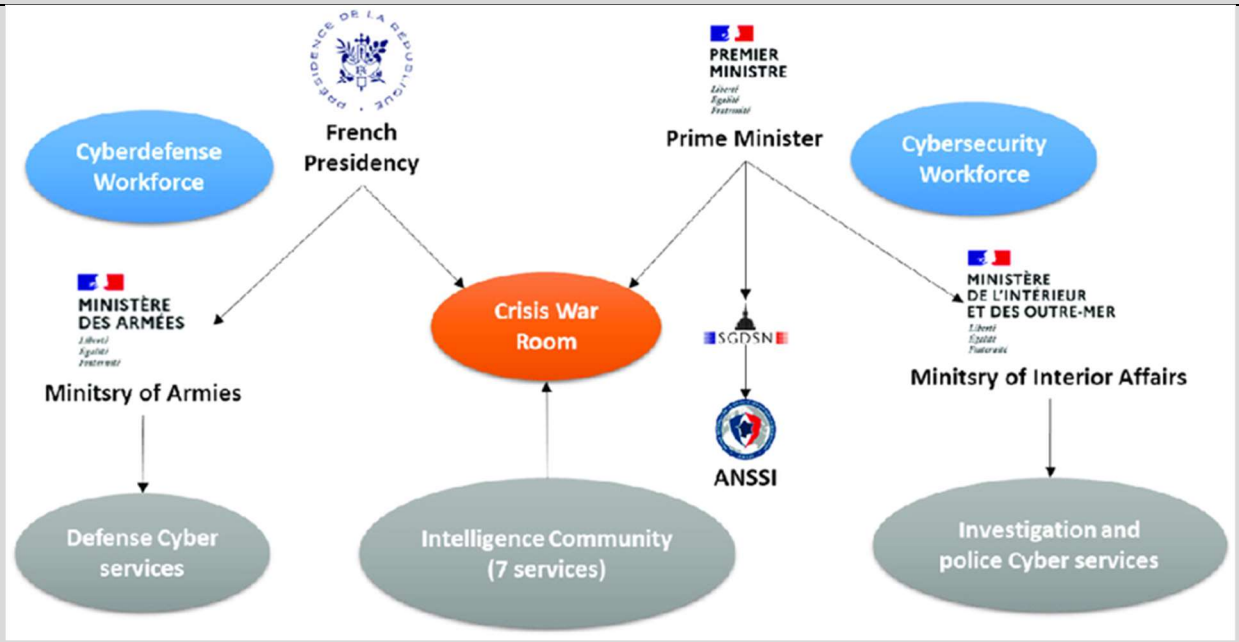
Con la *Loi de Programmation Militaire* (LPM) 2019-2025 è stato previsto un investimento di 1,6 miliardi di Euro per la lotta nel dominio cibernetico, l'evoluzione tecnologica in ambito cyber. L'organico previsto entro il 2025 è di 4.500 unità, da distribuire tra il COMCYBER, la DGSE e la DGA.

Di questi, la metà (ca. 2250) verrà dedicata alla protezione dei sistemi d'informazione, un quarto (ca. 1100) alla difesa *cyber* e la restante parte (ca. 1100) alle operazioni cibernetiche offensive.

DIREZIONE ED ESECUZIONE	
	COMCYBER **(dipendente dal ChoD e si coordina con il *Chief Joint Ops*)**

- ***Cyber security, Defence*** (reti e sistemi Difesa e coordinamento con ANSSI)
- ***Cyber offensive***
- ***Cyber influence***
- CERT della Difesa (collocato insieme al CERT nazionale);
- Certificazioni sistemi IT
- Centro studi per aspetti di sicurezza dei nuovi sistemi
- Reclutamento e formazione (incluso riservisti c*yber)*

INTERAGENZIA



SPAGNA

La Spagna ha adottato un approccio interministeriale e multilivello alla sicurezza cibernetica, con il coinvolgimento di enti civili, militari e di *intelligence*, per rispondere alle nuove minacce digitali e armonizzarsi con le normative europee.

Il **Sistema di Sicurezza Nazionale in materia di cybersicurezza**, posto sotto la guida del Presidente del Governo, è composta da **tre organi**:

- il **Consiglio di Sicurezza Nazionale** (*Consejo de Seguridad Nacional* – **CSN**), in qualità di Commissione Delegata del Governo per la Sicurezza Nazionale;
- il **Consiglio Nazionale per la Cybersicurezza** (*Consejo Nacional de Ciberseguridad* – **CNC**), che coadiuva il CSN e assiste il Presidente del Governo nell'indirizzo e nel coordinamento della politica in materia di cybersicurezza e promuove il coordinamento, la collaborazione e i rapporti di cooperazione tra le Pubbliche Amministrazioni e tra queste e il settore privato;
- il **Comitato di Situazione** (*Comité de Situación* – **CdS**) che, con il supporto del Dipartimento per la Sicurezza Interna, supporterà la gestione di situazioni di crisi in qualsiasi ambito, che, per la loro trasversalità o dimensione, superano le capacità di risposta dei consueti meccanismi.

Il Sistema nazionale di cybersicurezza della Spagna è fondato principalmente sull'apporto di **4 Amministrazioni pubbliche**:

- Ministero della Trasformazione Digitale e della Funzione Pubblica,
- Dipartimento per la Sicurezza Nazionale (DSN),
- Ministero dell'Interno
- Ministero della Difesa.

La risposta nazionale agli attacchi *cyber*, a seconda delle situazioni, è assicurata dalle rispettive articolazioni tecniche attraverso una stretta collaborazione.

Nello specifico, le entità civili coinvolte sono:

- l'*Istituto Nacional de Ciber seguridad* (**INCIBE**)[35]: dipendente dal Ministero della Trasformazione Digitale e della Funzione Pubblica attraverso la Segreteria di Stato delle telecomunicazioni e infrastrutture digitali, è l'ente di riferimento per lo sviluppo della sicurezza informatica e della fiducia digitale di cittadini, *network* accademici e di ricerca, professionisti, aziende e soprattutto per settori strategici. Dispone di un *Computer Emergency Response Team* (**INCIBE-CERT**) quale centro di riferimento per la risposta agli incidenti di sicurezza per cittadini, imprese ed enti privati. Nel caso della gestione degli incidenti che interessano operatori critici del settore privato, INCIBE-CERT è gestito congiuntamente da INCIBE e dal Ministero dell'Interno (Ufficio di coordinamento della sicurezza informatica).
- la *Oficina de Coordinación de Ciberseguridad* (**OCC**)[36]: è l'agenzia della Direzione Generale del Coordinamento e degli Studi della Segreteria di Stato per la Sicurezza, attraverso la quale vengono attuate le politiche di sicurezza informatica del Ministero dell'Interno.
  È il punto di contatto nazionale per il coordinamento operativo dello scambio di informazioni sugli attacchi contro i sistemi informativi e costituisce il Centro di Risposta agli Incidenti Cibernetici del Ministero dell'Interno per il supporto e il coordinamento con la Polizia Giudiziaria (CSIRT-MIR-PJ). Funge da Osservatorio sulla Criminalità Informatica del Ministero dell'Interno.
  Svolge le funzioni assegnate alla Segreteria di Stato per la Sicurezza sulla sicurezza delle reti e dei sistemi informativi, in qualità di autorità competente per gli operatori di servizi essenziali designati come operatori critici. Insieme a INCIBE, gestisce INCIBE-CERT in tutte le questioni relative alla gestione degli incidenti che interessano gli operatori critici.
  Coordina le operazioni di sicurezza informatica in occasione di eventi su scala nazionale e processi elettorali e risponde alle minacce alla sicurezza informatica, alla criminalità informatica e alle campagne di disinformazione;
- il *Computer Emergency Response Team* del *Centro Criptológico Nacional* (**CCN-CERT**): creata nel 2006 come CERT del Governo Nazionale spagnolo per la risposta agli incidenti di sicurezza informatica ad attacchi diretti

[35] Decreto Reale n° 1185/2024 – www.incibe.es.
[36] La OCC – Oficina de Coordinación de Ciberseguridad.

contro istituzioni governative, la struttura dipendente dal ***Centro Nacional de Inteligencia*** **(CNI)**, organismo dipendente dal Ministero della Difesa e responsabile di fornire al Presidente del Governo e al Governo Nazionale informazioni, analisi, studi e proposte che consentano loro di prevenire ed evitare qualsiasi pericolo, minaccia o aggressione contro l'indipendenza o l'integrità territoriale della Spagna, gli interessi nazionali e la stabilità dello Stato di diritto e delle sue istituzioni.

Dal 2020, è stato adottato un approccio che prevede la stretta collaborazione delle Forze Armate per l'integrazione delle attività di difesa cibernetica con il Sistema di Sicurezza Nazionale per assicurare la piena e pronta protezione dello Stato e dei cittadini.

Con riferimento all'organizzazione *cyber* in ambito militare, nel 2013 è stato costituito il *Mando Conjunto de Ciberdefensa de las Fuerzas Armadas* (MCCD), divenuto ***Mando Conjunto del Ciberespacio*** (**MCCE**) dal 2020 (ca. **450 unità**). Il MCCE è l'organismo responsabile della pianificazione, direzione, coordinamento, controllo ed esecuzione delle azioni volte a garantire la libertà d'azione del FFAA spagnole nel campo del cyberspazio ed inoltre contribuisce allo sviluppo e potenziamento della *cyber* sicurezza.

Il **Comandante del MCCE**:

- fornisce consulenza al Capo di Stato Maggiore della Difesa (*Jefe del Estado Mayor de la Defensa* – JEMAD) su argomenti di cybersicurezza;
- è il rappresentante del Ministero della Difesa nel Consiglio Nazionale per la Cybersicurezza;
- mantiene e promuove la cooperazione con il Dipartimento per la Sicurezza Nazionale, con gli altri *CERT* nazionali di riferimento (INCIBE e CCN) e con le organizzazioni responsabili della *Cybersecurity* e della *Cyber-Intelligence*, a livello nazionale e internazionale, quest'ultima in coordinamento con ***Estado Major Conjunto de la Defensa*** (**EMACON**).

Il MCCE svolge le seguenti **funzioni**:

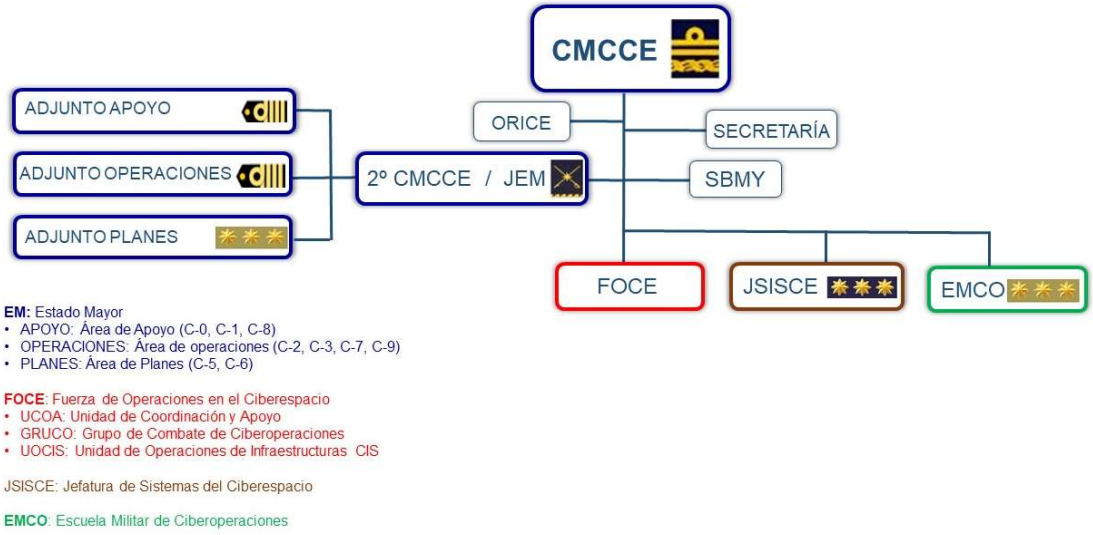
- fornisce **supporto CIS** alla struttura dello Stato Maggiore della Difesa (*Estado Mayor de la Defensa* – EMAD) ed è responsabile delle apparecchiature di crittografia e delle chiavi crittografiche assegnate;
- contribuisce al processo **JISR** (*Joint, Intelligence, Surveillance and Reconnaisance*) nel quadro del Sistema di ***intelligence*** delle FFAA e delle operazioni militari;

- **gestisce** e coordina lo **spettro elettromagnetico** assegnato alle FFAA, comprensivo quello dei satelliti militari;
- effettua **controlli di sicurezza** sulle reti e sui sistemi comuni di informazione e telecomunicazione delle Forze armate;
- attraverso il **CERT militare** (**ESP-DEF-CERT**), assicura il monitoraggio e la sicurezza delle reti e dei sistemi di informazione e telecomunicazione delle Forze Armate, nonché delle altre reti e sistemi che le sono specificatamente affidati e che interessano la Difesa Nazionale;
- responsabile per contribuire alla **risposta in caso di attacco cibernetico ai danni della Nazione**. In situazioni di impiego multinazionale delle Forze armate, le operazioni cyber del MCCE sono integrate nella catena di comando. **In assenza di uno scontro armato dichiarato, non è al momento prevista la possibilità di condurre operazioni offensive**.

Nel 2025, la Spagna ha lanciato un **Piano di Sicurezza e Difesa da 10,47 miliardi di Euro** basato su tre linee principali:

- potenziamento delle **Forze Armate;**
- ammodernamento delle **infrastrutture militari e degli armamenti,** inclusa una **reindustrializzazione del settore difesa;**
- costruzione di uno **Scudo Digitale Nazionale** (31% del *budget*).

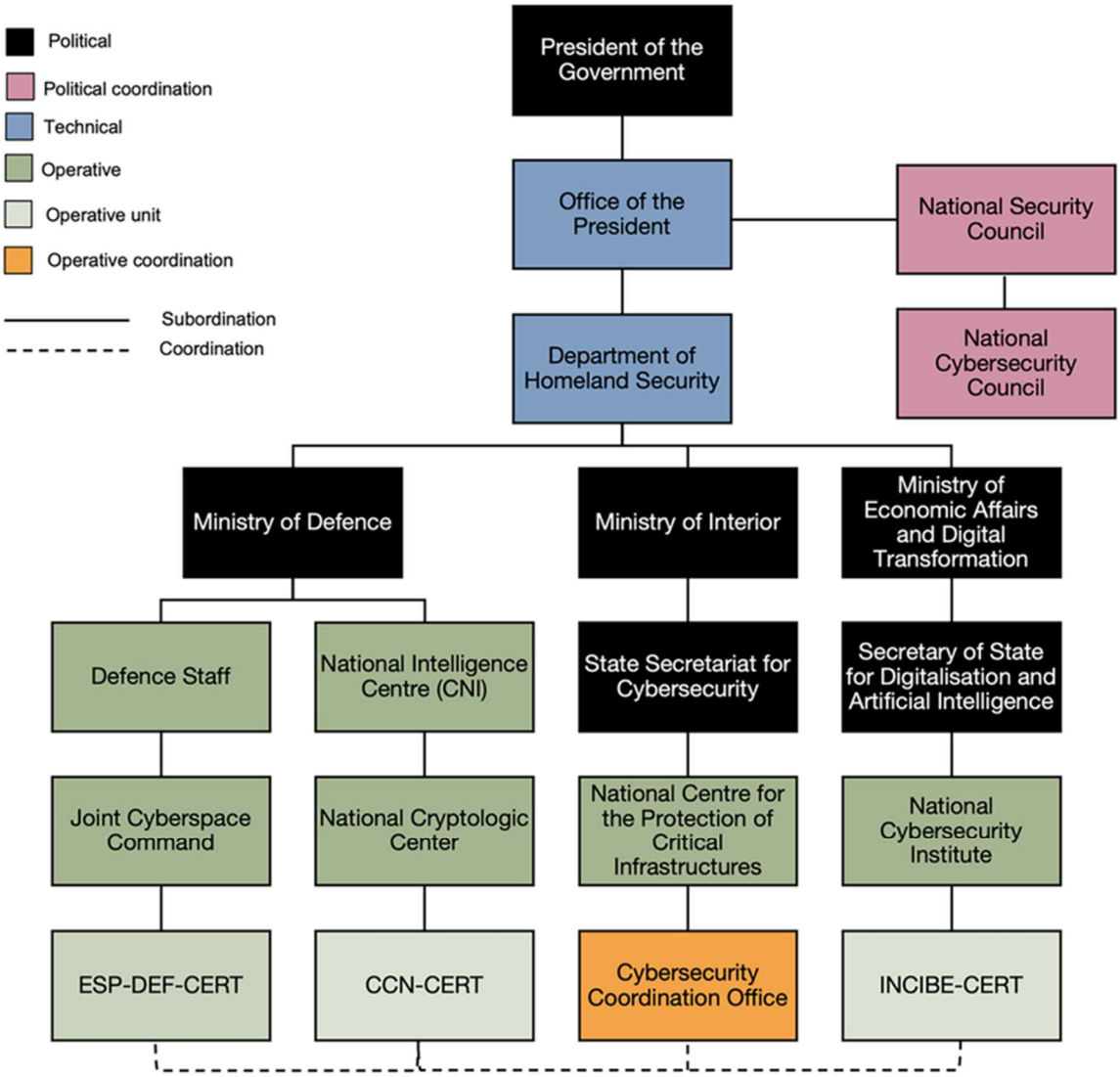
Organigramma del MCCE:



Lo *staff* di comando è così strutturato:

- *Jefe del Estado Mayor y Segundo Comandante*;
- Servizio di Appoggio (*Adjunto Apoyo*):
  - Coordinamento (C-0),
  - Personale (C-1),
  - Logistica (C-4),
  - Risorse e Finanze (C-8);
- Servizio Operazioni (*Adjunto Operaciones*):
  - *Intelligence* (C-2),
  - Operazioni (C-3),
  - Preparazione (C-7),
  - Comunicazione strategica (C-9);
- Servizio Piani (*Adjunto Planes*):
  - Piani (C-5),
  - *Command and Control, Communications, Cyberdefense & Digital*, C4D (C-6).

Sistema nazionale di Cybersicurezza della Spagna (Decreto Reale n°311 del 3 Maggio 2022):



USA

Le capacità cibernetiche degli Stati Uniti sono tra le più avanzate al mondo e si basano su una combinazione di *intelligence*, difesa e attacchi proattivi per proteggere gli interessi nazionali e contrastare le minacce esterne.

Le operazioni cibernetiche statunitensi sono guidate da diverse agenzie interconnesse:

- *U.S. Cyber Command* (USCYBERCOM): è il principale comando militare responsabile sia delle operazioni offensive che difensive nel cyberspazio. La sua missione è quella di condurre operazioni per difendere le reti del Dipartimento della Difesa e per contrastare gli avversari;
- *National Security Agency* (NSA): l'NSA è l'agenzia di *intelligence* che si occupa della crittografia e dello spionaggio dei segnali. Collabora strettamente con USCYBERCOM e fornisce il supporto tecnologico e l'*intelligence* necessari per le operazioni cibernetiche;
- *Cybersecurity and Infrastructure Security Agency* (CISA): questa agenzia si concentra sulla difesa delle infrastrutture civili critiche degli Stati Uniti, come reti elettriche, sistemi finanziari e ospedali, e collabora con il settore privato per prevenire attacchi.

Le **capacità informatiche** statunitensi si dividono in **due ambiti principali**:

- **Capacità offensive**: gli Stati Uniti sono in grado di condurre **attacchi informatici** per interrompere, degradare o distruggere le reti di avversari, rubare informazioni sensibili e condurre operazioni di guerra psicologica. Un esempio noto è l'operazione "*Olympic Games*", che ha utilizzato il malware *Stuxnet* per sabotare il programma nucleare iraniano;
- **Capacità difensive**: oltre a proteggere le proprie reti, le agenzie statunitensi si occupano attivamente di "caccia alle minacce" (*Threat Hunting*) per individuare e neutralizzare le minacce prima che possano causare danni. Questo include la sorveglianza delle reti avversarie per intercettare e bloccare gli attacchi. L'obiettivo è prevenire gli attacchi futuri attraverso una politica di "difesa in avanti".

L'arsenale informatico statunitense è considerato uno strumento cruciale di sicurezza nazionale, utilizzato per deterrenza, spionaggio e, se necessario, per azioni di forza.

USCYBERCOM

Con sede presso la *National Security Agency* a Fort George G. Meade, nel Maryland, lo *United States Cyber Command* è un comando militare che opera a livello globale, in tempo reale. È **uno degli undici Comandi di combattimento unificati**[37] del *Department of Defense* degli Stati Uniti (DoD).

Missione

- direzione, coordinamento, sincronizzazione e pianificazione delle operazioni di **contrasto alla minaccia** nel dominio cibernetico;
- gestione e **difesa dei sistemi di informazione** e comunicazione, sia militari che dell'intero Paese, da attacchi informatici per assicurare resilienza e affidabilità;
- **supporta gli altri Comandi operativi e i Comandanti delle Forze Armate** per l'esecuzione delle loro missioni nel dominio cibernetico in tutto il mondo e garantisce l'accesso sicuro al cyberspazio.

Il Comando, in particolare, lavora a stretto contatto con *partner* inter-agenzia e internazionali per l'esecuzione di tutte le proprie attività, in particolare per abilitare la *Department of Defense Information Network*[38] (DoDIN), rafforzare le capacità e le competenze informatiche del DoD nel cyberspazio.

[37] Un comando combattente (CCMD), o comando combattente unificato (COCOM), è un comando militare congiunto di alto livello all'interno del Dipartimento della Difesa degli Stati Uniti, responsabile di missioni ampie e continuative in una specifica regione geografica o area funzionale, come la sicurezza informatica. Composto da forze provenienti da diverse forze armate e guidato da un ufficiale a quattro stelle, ogni Comando fornisce il "comando e controllo" per tutte le forze militari statunitensi nell'ambito del Piano di Comando Unificato (UCP) per eseguire operazioni in pace, guerra o crisi.

[38] Insieme di capacità informative *end-to-end* interconnesse a livello globale e processi associati (inclusi sistemi e servizi di comunicazione e di elaborazione dati di proprietà e in *leasing*, *software*, dati, servizi di sicurezza, altri servizi e sistemi di sicurezza nazionale) per: raccolta, elaborazione, archiviazione, diffusione e gestione delle informazioni ad uso di operazioni militari, decisori politici e personale di supporto.

Focus – Capacità Operativa

La capacità operativa nella condotta delle operazioni cibernetiche del USCYBERCOM è assicurata dalla *Cyber National Mission Force* e dalle Componenti operative direttamente dipendenti sulla base dell'orientamento di impiego e responsabilità (*Head Quarter* diversi).

Nello specifico:

- *Army Cyber Command*

  Il *Cyber Command* dell'Esercito degli Stati Uniti dirige e conduce operazioni integrate di guerra elettronica, informazione e cyberspazio, come autorizzato o diretto, per garantire la libertà di azione nel cyberspazio e l'ambiente informativo e per negarla agli avversari;

- *Fleet Cyber Command/Tenth Fleet*

  La missione del *Fleet Cyber Command* è quella di agire da autorità operativa centrale per le reti, l'*intelligence* crittografica e dei segnali, le operazioni di informazione, la guerra informatica, elettronica e le capacità spaziali a supporto delle forze navali; di dirigere le operazioni nel cyberspazio della *US Navy* a livello globale per scoraggiare e sconfiggere le aggressioni e garantire la libertà di azione per raggiungere obiettivi militari nel cyberspazio;

- *Sixteenth Air Force (Air Forces Cyber Command)*

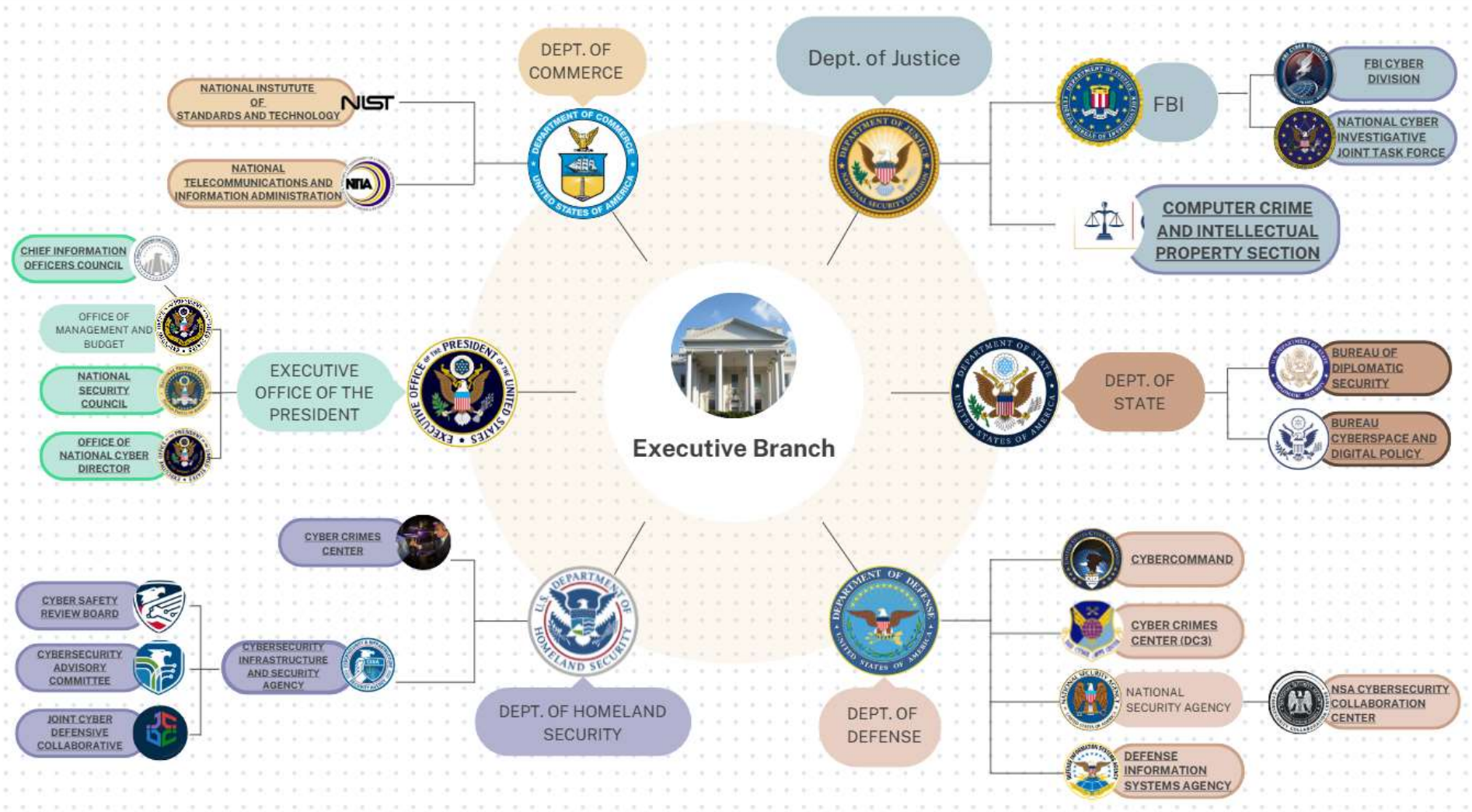
  La *AFCYBERCOM*, con sede presso la *Joint Base San Antonio-Lackland-Texas*, integra capacità di *intelligence*, sorveglianza e ricognizione, guerra informatica, guerra elettronica e operazioni di informazione lungo tutto il continuum del conflitto per garantire che la *US Air Force* sia veloce, letale e pienamente integrata;

- *Marine Corps Forces Cyberspace Command*

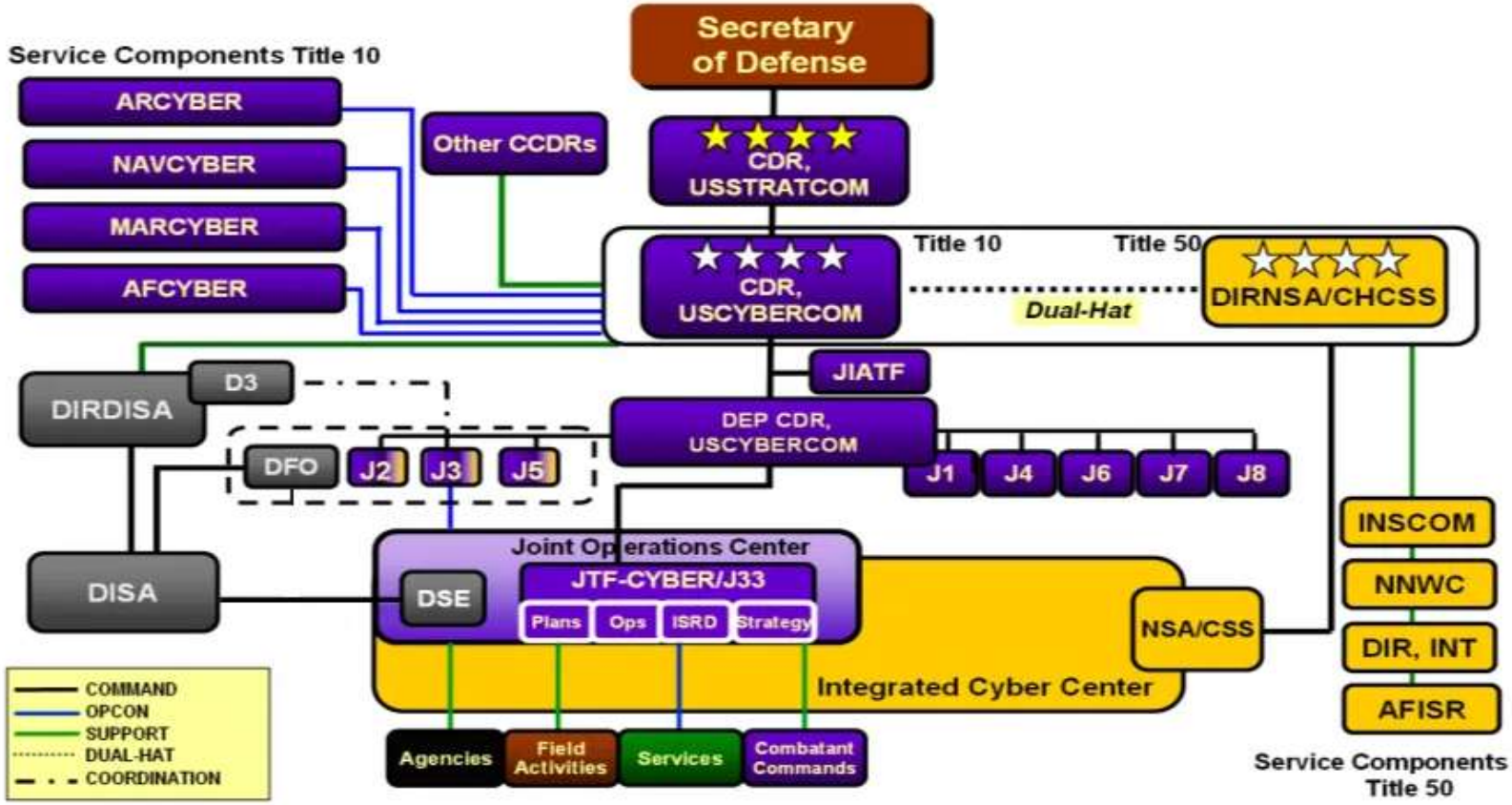
  Il *Marine Corps Forces Cyberspace Command* ha lo scopo di condurre lo spettro completo delle attività nel cyberspazio, inclusa la gestione e la difesa della *Marine Corps Enterprise Network* (MCEN), condurre operazioni difensive nel cyberspazio all'interno delle MCEN e *Joint Force Network* e, quando indicato, condurre operazioni offensive nel cyberspazio a supporto delle *Joint & Coalition Forces* al fine di consentire la libertà di azione in tutti i domini e negarla agli avversari;

- *Cyber National Mission Force (CNMF)*
  La CNMF dell'USCYBERCOM pianifica, dirige e sincronizza lo spettro completo delle operazioni nel cyberspazio per scoraggiare, interrompere e, se necessario, sconfiggere gli attori informatici avversari per difendere gli Stati Uniti;
- *Joint Force Headquarters – DoD Information Network*
  La missione del JFHQ-DoDIN è supervisionare il funzionamento quotidiano delle reti del Dipartimento della Difesa e organizzarne una difesa attiva, essendo pronti a neutralizzare qualsiasi avversario che riesca a aggirare le difese perimetrali.

Organizzazione di Cybersicurezza degli USA:



USCYBERCOM Organization



CANADA

Il Canada ha recentemente intrapreso passi significativi per rafforzare la sua architettura nazionale di sicurezza cibernetica, con un *focus* sul consolidamento delle capacità, la collaborazione internazionale e la protezione delle infrastrutture critiche. Questo impegno si manifesta attraverso l'istituzione di nuovi comandi e il rafforzamento delle agenzie esistenti.

L'organizzazione militare per le operazioni cibernetiche in Canada è il ***Canadian Forces Cyber Command*** (**CAF-CYBERCOM**), una nuova autorità centrale all'interno del Dipartimento della Difesa Nazionale (DND), responsabile della gestione e dello sviluppo della forza cibernetica e delle operazioni difensive e offensive per proteggere gli interessi del Canada e supportare le Forze Armate. Questo comando è supportato e coordinato dal ***Communications Security Establishment*** (CSE – una delle tre agenzie del DND), che è l'autorità nazionale per l'*intelligence* delle comunicazioni e le operazioni cibernetiche, mentre il ***Canadian Centre for Cyber Security***, parte del CSE, fornisce consulenza e servizi per tutta la nazione.

1. ***CANADIAN ARMED FORCES CYBER COMMAND*** **(CAF-CYBERCOM)**
   - **Istituzione e Scopo**: annunciato ufficialmente il 26 settembre 2024, il CAF CYBERCOM è un nuovo comando dedicato che consolida le capacità cibernetiche delle Forze Armate Canadesi (CAF) in un'unica entità unificata. Il suo obiettivo primario è migliorare la prontezza militare per affrontare le minacce nel dominio cibernetico;
   - ***Leadership***: il comandante è responsabile delle operazioni cibernetiche, del mantenimento della forza cibernetica, della gestione e dello sviluppo;
   - **Capacità e Cooperazione**: Attraverso il CAF CYBERCOM, le CAF continueranno a sviluppare e scalare le loro capacità di **operazioni cibernetiche offensive e difensive** in stretta collaborazione con il *Communications Security Establishment* (CSE). Il Comando includerà l'*intelligence* dei Segnali (***Signals Intelligence***) e la Guerra Elettronica Congiunta (***Joint Electronic Warfare***) ed è in grado di condurre e supportare **operazioni cibernetiche "*full spectrum*"**;

- **Allineamento Internazionale**: l'istituzione del CAF CYBERCOM rappresenta un passo importante per il Dipartimento della Difesa Nazionale (DND) e le CAF, dimostrando l'impegno del Canada a operare nel dominio cibernetico. Contribuisce a soddisfare gli **impegni NATO** e si allinea con investimenti simili da parte di *partner* e alleati in NORAD, l'alleanza "*Five Eyes*" (con Australia, Nuova Zelanda, Regno Unito e Stati Uniti) e la NATO, promuovendo una maggiore interoperabilità e capacità di contrastare le minacce cibernetiche.

2. ***COMMUNICATIONS SECURITY ESTABLISHMENT*** **(CSE)**
   - **Mandato Multiplo**: il CSE è l'agenzia canadese per l'***intelligence*** **dei segnali esteri** e l'**autorità tecnica per la sicurezza cibernetica e l'assicurazione dell'informazione**. Il suo mandato comprende cinque aspetti fondamentali:
     1. *intelligence* dei segnali esteri;
     2. sicurezza cibernetica;
     3. operazioni cibernetiche attive;
     4. operazioni cibernetiche difensive;
     5. assistenza tecnica e operativa ai *partner* federali.
   - **Ruolo *Leader* nella Cibersicurezza**: il CSE è il **responsabile operativo del governo federale per la sicurezza cibernetica** e al suo interno opera il *Canadian Centre for Cyber Security*;
   - ***Partnership*** **e Collaborazione**: collabora anche strettamente con il DND/CAF, sviluppando capacità tecniche e specializzate per supportare le operazioni militari, compresa la cibersicurezza e le operazioni cibernetiche difensive. Il CSE è un **membro dell'alleanza di *intelligence Five Eyes***. Oltre al DND/CAF, il CSE collabora con la *Canadian Security Intelligence Service* (CSIS), la *Royal Canadian Mounted Police* (RCMP) e *Global Affairs Canada* (GAC) in vari aspetti della sicurezza nazionale, inclusa la sicurezza elettorale;
   - ***Oversight*** **e Trasparenza**: le sue attività sono soggette a rigorosa revisione esterna da parte di organismi come la *National Security and Intelligence Review Agency* (NSIRA) e il *National Security and Intelligence Committee of Parliamentarians* (NSICOP), garantendo che siano legali e necessarie.

3. *CANADIAN CENTRE FOR CYBER SECURITY*

- **Funzione Centrale**: gestito dal CSE, il *Cyber Centre* è la **fonte unica e unificata di consulenza esperta, guida, servizi e supporto per la sicurezza cibernetica** per il governo, gli operatori di infrastrutture critiche, il settore privato e il pubblico canadese;
- **Capacità Difensive**: unisce l'esperienza operativa di sicurezza cibernetica di *Public Safety Canada, Shared Services Canada* e CSE per formare un'organizzazione altamente funzionale e reattiva. Le sue difese automatizzate proteggono il governo del Canada da una media di **6,6 miliardi di azioni dannose al giorno**;
- **Aree d'Intervento**: le sue attività principali includono informare i canadesi sulla sicurezza cibernetica, proteggere gli interessi di sicurezza cibernetica dei canadesi, sviluppare e condividere tecnologie di difesa cibernetica specializzate, difendere i sistemi cibernetici, e agire come leader operativo e portavoce durante gli eventi di sicurezza cibernetica.

4. SUPERVISIONE E REVISIONE ESTERNA

Nella piramide di responsabilità che vede al vertice il Parlamento e il Gabinetto, con il Ministro della Difesa Nazionale a capo delle principali agenzie operative (CSE, focalizzato sull'*intelligence* e la protezione tecnica, e CAF-CYBERCOM, operazioni militari *cyber* e supporto a CSE), si collocano anche gli "organismi di supervisione esterna" per garantire trasparenza e legalità, e collaborano orizzontalmente con altre agenzie e partner internazionali per una difesa *cyber* completa.

Tali organismi sono:

- ***Intelligence Commissioner*** **(IC): s**upervisione esterna indipendente delle Autorizzazioni Ministeriali (MA) del CSE, le rivede e le approva prima dell'esecuzione delle attività;
- ***National Security and Intelligence Review Agency*** **(NSIRA): r**evisione esterna delle attività del governo del Canada in materia di sicurezza nazionale e *intelligence* per garantirne legalità, ragionevolezza e necessità;
- ***National Security and Intelligence Committee of Parliamentarians*** **(NSICOP):** composto da membri di entrambe le Camere del Parlamento,

esamina le organizzazioni di sicurezza nazionale e intelligence del Canada.

Focus sulla Sicurezza Elettorale

La protezione dei processi democratici canadesi dalle interferenze straniere è una priorità che si è tradotta nella costituzione della ***Security and Intelligence Threats to Elections (SITE) Task Force***, costituita dal CSE insieme al Public Safety Department, attraverso il *Canadian Security Intelligence Service* e la *Royal Canadian Mounted Police*, oltre che dal *Global Affair* Canada. Questo gruppo monitora *l'intelligence* dei segnali stranieri e l'attività cibernetica per rilevare segni di interferenza straniera nei processi elettorali.

Di seguito gli specifici ruoli delle entità nazionali:

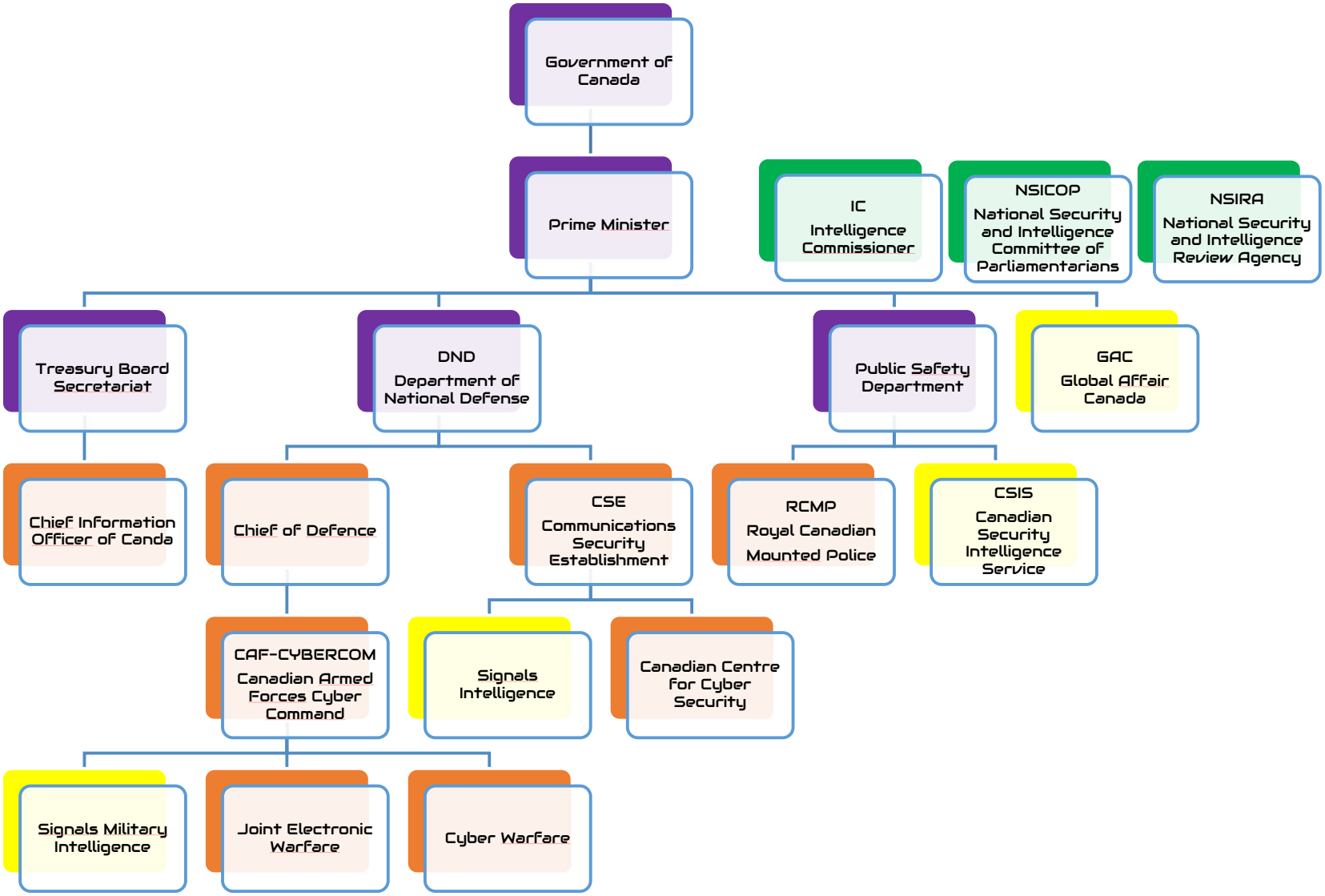
- **CSE**: fornisce *intelligence* e valutazioni cibernetiche sulle intenzioni e capacità degli attori di minaccia stranieri. Protegge i sistemi e le reti del governo legati alle elezioni tramite misure di difesa cibernetica e offre consulenza e guida sulla sicurezza cibernetica a partiti politici, province e altre istituzioni coinvolte nei processi democratici;
- ***Canadian Security Intelligence Service*** **(CSIS)**: raccoglie informazioni su attività influenzate da attori stranieri che sono dannose per gli interessi del Canada e fornisce valutazioni di *intelligence*;
- ***Royal Canadian Mounted Police*** **(RCMP)**: ha la responsabilità primaria per la prevenzione, il rilevamento e la risposta alle minacce criminali legate alla sicurezza nazionale e indaga sui reati criminali legati a terrorismo, spionaggio, attacchi cibernetici e attività di influenza straniera nelle elezioni;
- ***Global Affair Canada*** **(GAC)**: conduce ricerche sulle tendenze globali e i dati sulle minacce alla democrazia e coordina le risposte con i Paesi del G7.

Sfide e Investimenti

Nonostante i progressi, le CAF devono affrontare sfide come carenze di personale specialista cibernetico e processi di autorizzazione di sicurezza lenti. Per far fronte a ciò, le CAF stanno cercando di reclutare talenti

collaborando con istituzioni educative private e attraverso programmi di istruzione continua.

Il ***Budget* 2024** prevede investimenti significativi per il DND, il CSE e il GAC finalizzati a migliorare i programmi di *intelligence* e operazioni cibernetiche. Si parla di **8,1 miliardi di dollari in cinque anni** (a partire dal 2024-25), con 73,0 miliardi di dollari in 20 anni per DND, CSE e GAC, di cui 917,4 milioni di dollari in cinque anni, con 10,9 miliardi di dollari negli anni futuri e 145,8 milioni di dollari all'anno per CSE e GAC specificamente destinati a migliorare l'*intelligence* e le operazioni cibernetiche.



	Direzione Politica		Autorità per la Sicurezza Cibernetica		Entità di *Intelligence*		Organismi di Supervisione Esterna

La disinformazione russa

Fonte: Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, Relazione annuale sulla politica dell'informazione per la sicurezza - 2025 (Roma, 2025), infografica "La minaccia ibrida," sezione "Disinformazione russa"

Contenuti disinformativi pubblicati da outlet pro-Cremlino rilevati da EUvsDisinfo nelle principali lingue di produzione, escluso il russo (2024)

Le maggiori operazioni attribuite al Cremlino

NOME OPERAZIONE	QUANTO	COSA	QUANDO	COME
operazione **UNDERCUT**	oltre **500**	account social inautentici coinvolti nell'operazione	almeno da dicembre 2023	1. diffusione di contenuti audio-visivi generati dall'intelligenza artificiale; 2. promozione di contenuti che simulano note testate giornalistiche
operazione **OVERLOAD**	circa **800**	organizzazioni raggiunte dalla rete di account X (già Twitter) inautentici	almeno da agosto 2023	1. campagna coordinata di messaggi mail diretti a fact-checker e media; 2. ecosistema di siti per la produzione di contenuti manipolati; 3. reti di canali Telegram per diffondere contenuti falsi; 4. campagna di amplificazione su X tramite comportamenti inautentici coordinati
	circa **200**	fact-checker, giornalisti e media raggiunti da messaggi mail	da gennaio a settembre 2024	
	71.000	la stima di email inviate da Overload	da gennaio a settembre 2024	
operazione **DOPPELGÄNGER**	oltre **6.000**	domini web attribuiti da Meta a Doppelgänger	dal 2022	1. ecosistema di siti web per la produzione di contenuti disinformativi; 2. realizzazione di siti-clone di media occidentali e di enti governativi; 3. reti di account inautentici su social media per la promozione dei contenuti
	242	domini che imitano o simulano siti di informazione o governativi attribuiti da Meta a Doppelgänger	dal 2022	
	32	i domini legati a Doppelgänger sequestrati dal Dipartimento di Giustizia USA	4 settembre 2024	
	oltre **5.000**	account e pagine legate a Doppelgänger rimosse da Meta	da maggio ad agosto 2024	

PER

- **Promuovere narrazioni favorevoli alla Russia in Occidente**
- **Minare il supporto occidentale all'Ucraina**
- **Demonizzare la leadership ucraina accusandola di nazismo e corruzione**
- **Alimentare divisioni e polarizzare il dibattito pubblico nei Paesi occidentali**
- **Saturare l'attività di media, fact-checker e giornalisti, in particolare in Francia e Germania**

*Le tre principali operazioni/campagne di disinformazione attribuite alla Federazione russa e rilevate nel **2024** sono state:*

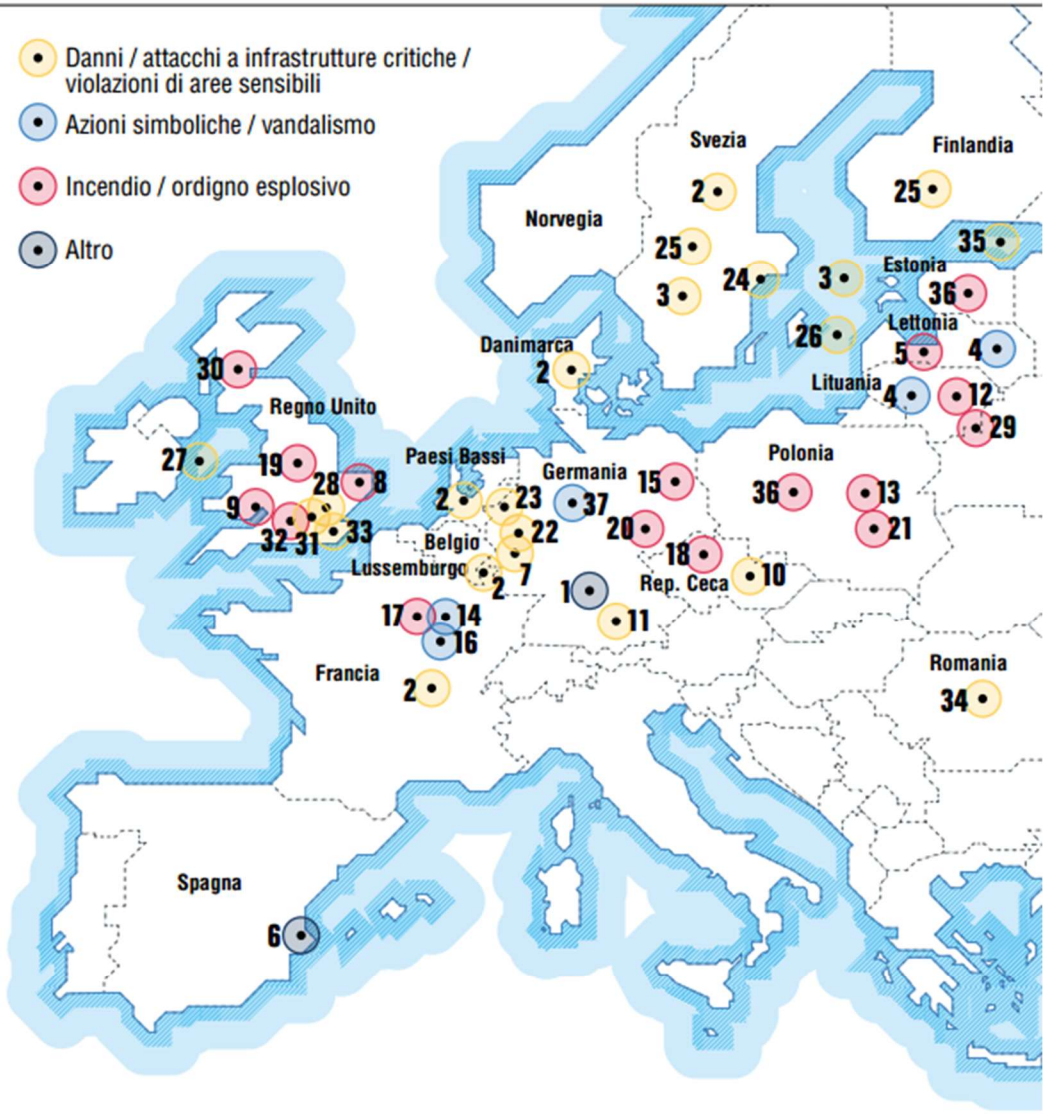
- ***operazione UNDERCUT;***
- ***operazione OVERLOAD;***
- ***operazione DOPPELGÄNGER.***

Le attività, condotte in molteplici lingue e attraverso molteplici strumenti, hanno avuto i seguenti obiettivi strategici:

- *promuovere narrazioni favorevoli alla Russia in Occidente;*
- *minare il supporto occidentale all'Ucraina;*
- *demonizzare la leadership ucraina accusandola di nazismo e corruzione;*
- *alimentare divisioni e polarizzare il dibattito pubblico nei Paesi occidentali;*
- *saturare l'attività dei media, fact-checker e giornalisti, in particolare in Francia e Germania.*

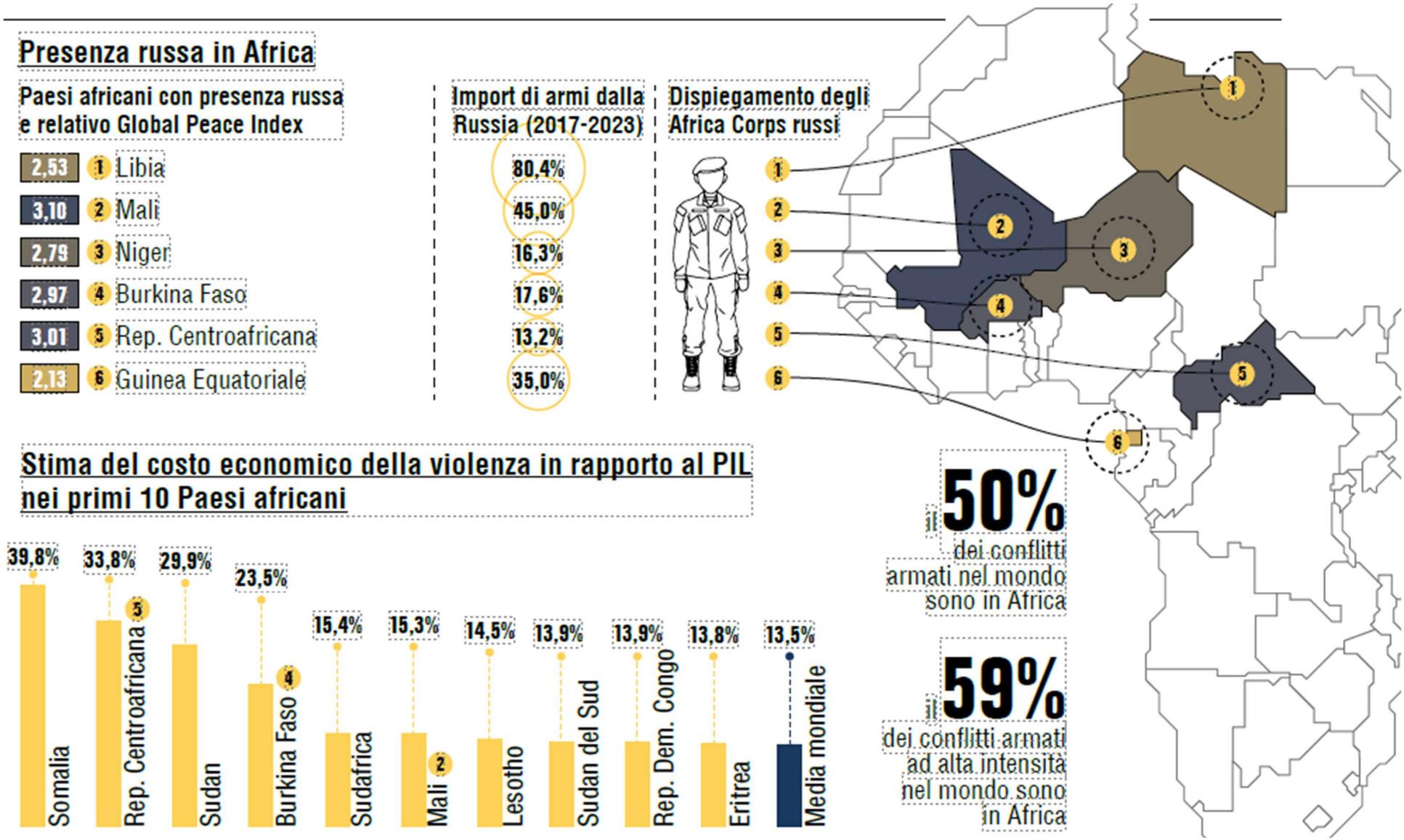
I sabotaggi in Europa | Incidenti sospetti, atti di sabotaggio e operazioni ibride denunciate in Europa nel corso del 2024

1 - Sventato piano russo per uccidere Armin Papperger, CEO di Rheinmetall
2 - Ripetute interferenze contro le reti satellitari di diversi Paesi europei nel corso dell'anno
3 - Ripetute azioni di disturbo su sistemi GPS in danno di diversi Paesi europei nel corso dell'anno
4 - Atti di vandalismo contro siti commemorativi della guerra contro l'Armata Rossa
5 - Incendio doloso al Museo dell'Occupazione di Riga
6 - Assassinio di Maxim Kuzminov, pilota russo che aveva disertato in favore di Kiev
7 - Furti di metallo e atti di vandalismo a linee dell'alta velocità ferroviaria
8 - Incendio doloso presso un magazzino industriale di proprietà ucraina a Londra
9 - Esplosione presso un sito di BAE Systems in Galles
10 - Denunciati tentativi di hackeraggio sul sistema ferroviario
11 - Due arresti per la pianificazione di atti di sabotaggio ai danni di una base militare
12 - Incendio doloso presso un centro IKEA a Vilnius
13 - Incendio distrugge il principale centro commerciale cittadino di Varsavia
14 - Imbrattamento del Muro dei Giusti al Memoriale dell'Olocausto di Parigi
15 - Incendio doloso in una fabbrica legata all'azienda della difesa Diehl
16 - Cinque bare con la scritta "soldati francesi in Ucraina" rinvenute sotto la Torre Eiffel
17 - Un arresto in seguito a un'esplosione accidentale durante la fabbricazione di un ordigno
18 - Fallito attentato incendiario a un deposito di autobus di Praga
19 - Incendio presso un magazzino in uso a DHL a Minworth
20 - Prende fuoco a Lipsia un pacco destinato a un volo cargo DHL
21 - Incendio presso un'azienda di trasporti a Varsavia
22 - Effrazione in un'area di sicurezza contenente un bacino idrico
23 - Allerta nella base di Geilenkirchen per un sospetto piano russo di sabotaggio con droni
24 - Sospensione del traffico aereo sull'aeroporto di Arlanda per l'avvistamento di quattro droni
25 - Effrazioni in alcuni impianti di trattamento delle acque
26 - Danneggiamento di due cavi sottomarini per TLC tra Finlandia-Germania e Svezia-Lituania
27 - Operazioni della nave spia russa Yantar in un'area con infrastrutture critiche
28 - Evacuazione dell'aeroporto di Gatwick a seguito del ritrovamento di un oggetto sospetto
29 - Aereo cargo della DHL partito dalla Germania precipita in un'area periferica di Vilnius
30 - Esplosione controllata di un pacco sospetto presso una stazione di bus di Glasgow
31 - Esplosione controllata di un pacco sospetto nelle vicinanze dell'Ambasciata USA a Londra
32 - Evacuata la stazione metropolitana di Euston per il ritrovamento di un pacco sospetto
33 - Droni di piccole dimensioni avvistati su tre basi militari in uso alle forze USA
34 - Attacchi ibridi aggressivi sul processo elettorale
35 - Danneggiamento cavo elettrico sottomarino tra Finlandia ed Estonia
36 - Molteplici arresti in Polonia ed Estonia per sabotaggi, incendi e pianificazioni degli stessi
37 - Sabotate con schiuma centinaia di auto in alcune città tedesche per attribuirne la responsabilità all'attivismo green



*Nel **2024** sono stati registrati **37 eventi maggiori di sabotaggio** in territorio europeo (con una media di **uno ogni 10 giorni**)*

Fonte: Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, Relazione annuale sulla politica dell'informazione per la sicurezza - 2025 (Roma, 2025), infografica "La minaccia ibrida," sezione "Disinformazione russa"



Fonte: Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, Relazione annuale sulla politica dell'informazione per la sicurezza - 2025 (Roma, 2025), infografica "L'insicurezza in Africa," sezione "Presenza russa in Africa"

Attacchi ibridi contro le elezioni in Romania

22 novembre → Gli ultimi sondaggi prima del voto danno per favorito per accedere al secondo turno, tra i 13 candidati, il Primo Ministro Marcel Ciolacu

24 novembre → L'ultranazionalista e filorusso Călin Georgescu vince a sorpresa il primo turno, ottenendo il 22,59% dei voti, accedendo al ballottaggio con la liberale Elena Lasconi (19,18%)

28 novembre → Il Consiglio Supremo di Difesa Nazionale evidenzia attacchi cyber contro infrastrutture IT&C relative al processo elettorale e il trattamento preferenziale di TikTok nei confronti di Georgescu

4 dicembre → Vengono declassificati e resi pubblici documenti di istituzioni e agenzie di sicurezza che confermano "attacchi ibridi aggressivi" condotti dall'estero sul processo elettorale

6 dicembre La Corte Costituzionale annulla il processo elettorale, compreso il ballottaggio previsto per l'8 dicembre

La rete su TikTok denunciata dalle autorità rumene nell'ambito delle ingerenze sul processo elettorale

QUANTO	COSA	QUANDO	COME	PER
25.000	account TikTok molto attivi nel sostenere Călin Georgescu	a partire da due settimane prima del voto	creando, diffondendo e promuovendo contenuti di propaganda politica, anche attraverso influencer e reti di account inautentici	sostenere il candidato alle presidenziali Călin Georgescu
797	account della rete creati nel 2016 con attività molto ridotta fino all'11 novembre 2024	almeno da agosto 2023		
5.005	iscritti al canale Telegram "Propagator", ritenuto responsabile di coordinare la rete	il primo dicembre, circa quattromila iscritti in più rispetto a sei gioni prima		
381.000	i dollari spesi per sponsorizzare i contenuti della rete	a partire dal 24 ottobre		

Gli attacchi cyber sul voto denunciati dalla Romania

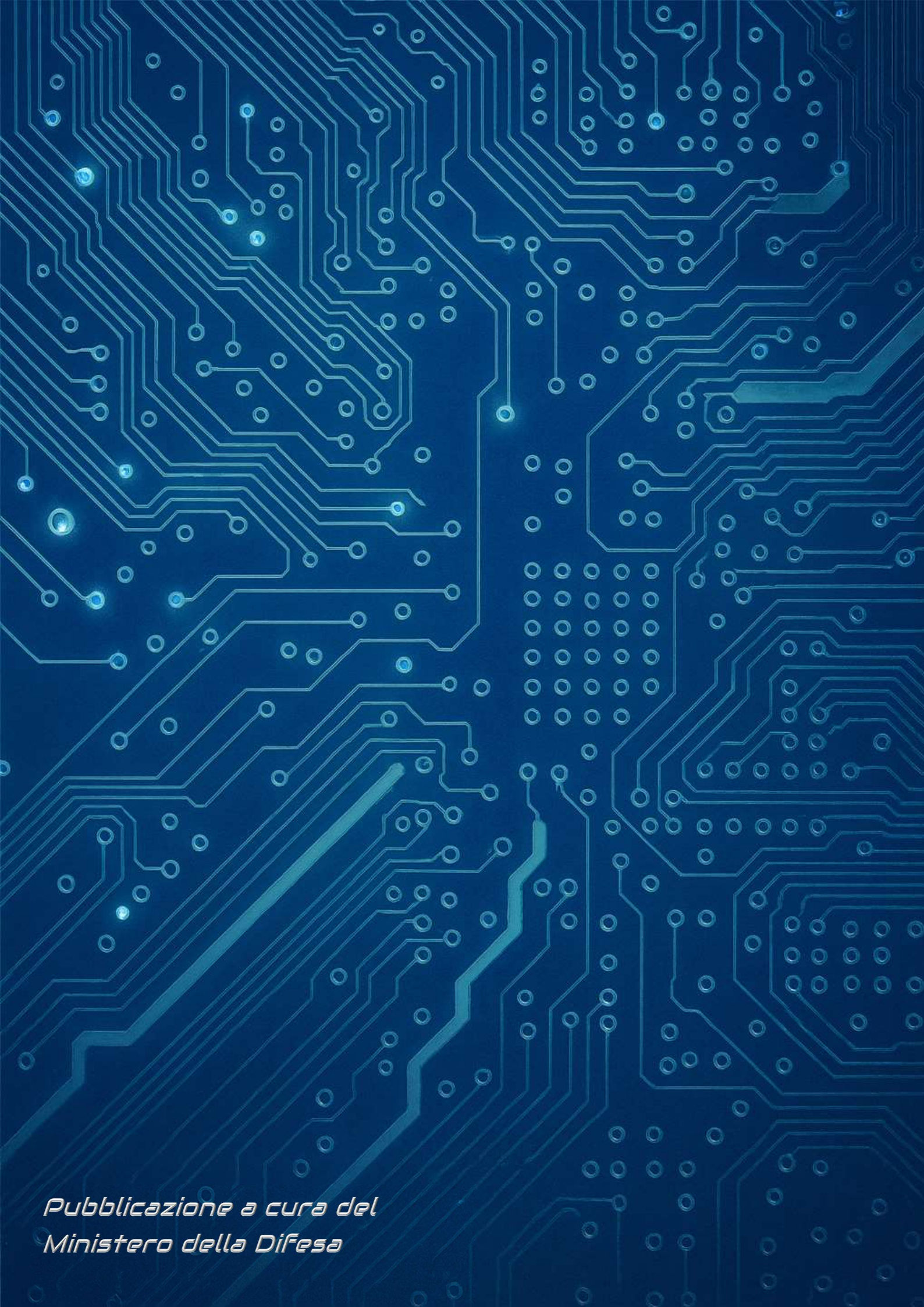
85.000	attacchi cyber contro l'infrastruttura IT&C elettorale del Paese	fino al 25 novembre	sfruttando le vulnerabilità dei sistemi informatici a supporto del processo elettorale	accedere ai dati presenti, alterarne l'integrità, modificare il contenuto presentato al pubblico, rendere l'infrastruttura non disponibile
33	i Paesi entro cui erano localizzati i sistemi informatici usati per gli attacchi	fino al 25 novembre	utilizzando metodi avanzati di anonimizzazione	rendere difficile il proccesso di attribuzione

Fonte: Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza, Relazione annuale sulla politica dell'informazione per la sicurezza - 2025 (Roma, 2025), infografica "L'insicurezza in Africa," sezione "Presenza russa in Africa"

APPENDICE VI

Area di intervento – Guerra Ibrida, Informazione e Resilienza

Obiettivo	Ruolo	Unità/Direzione	Istituzione
Istituire un Centro Europeo per il contrasto alla guerra ibrida	*Threat Analyst*	*SECDEFPOL.2 – Hybrid & Cyber Division*	EEAS
Costruire un Centro UE per la fusione delle informazioni classificate	*Info Security Expert*	*INTCEN – Technical Coordination Cell*	EEAS
Definire una strategia UE multi-dominio	*Strategic Planner*	*ISP.1 – Planning & Programming*	EEAS



Pubblicazione a cura del
Ministero della Difesa