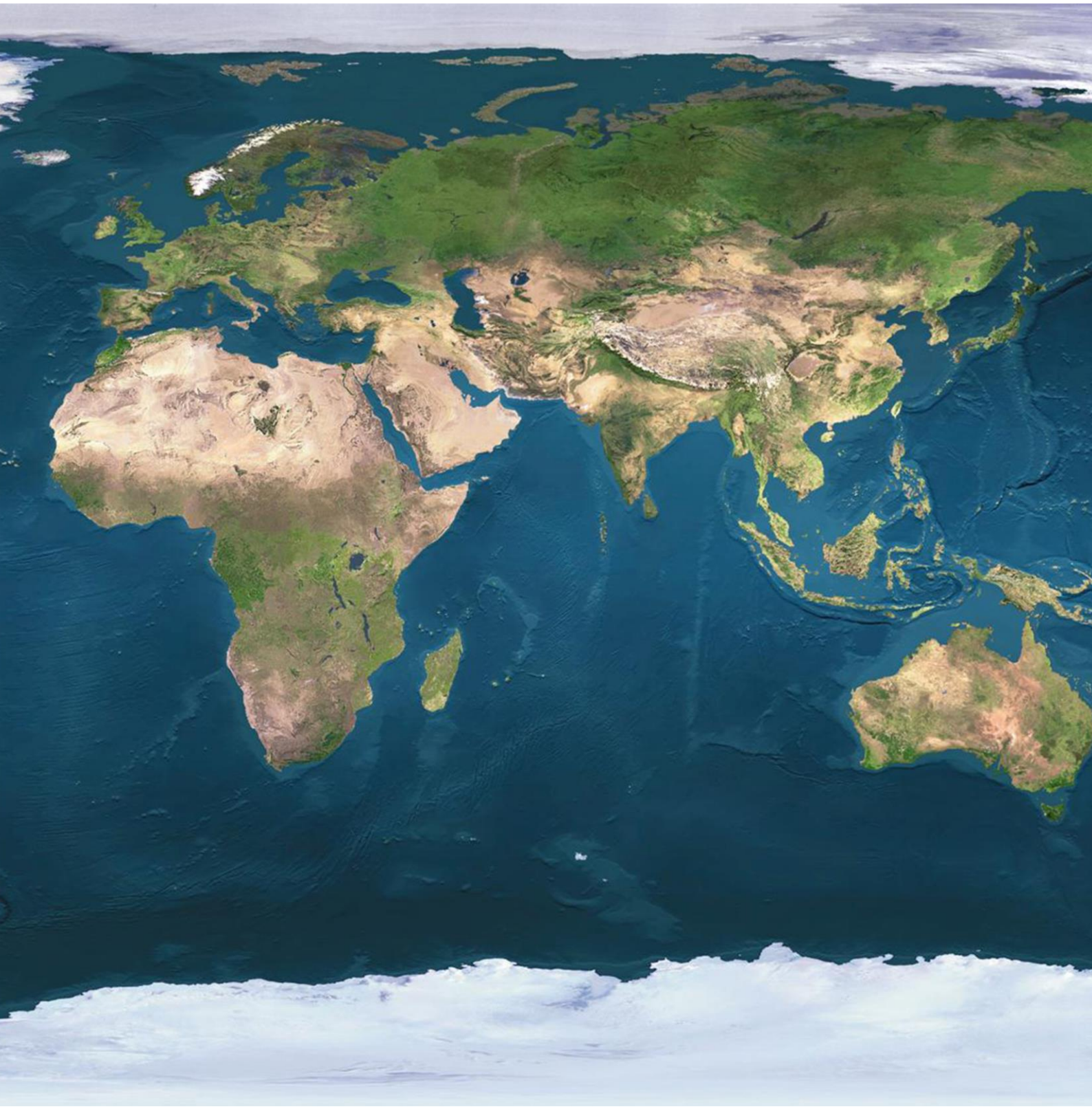
# Osservatorio Strategico

## Speciale Ucraina


Anno XXV – numero 1

https://casd-irad.it



CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

# Osservatorio Strategico

## Speciale Ucraina

## 2023
## N.- 1

# Osservatorio Strategico

Anno XXV numero I - 2023

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dei singoli autori, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali gli autori stessi appartengono.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

L'Osservatorio Strategico è disponibile anche in formato elettronico (file .pdf) al seguente link:
http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OsservatorioStrategico/Pagine/default.aspx

**Osservatorio Strategico 2023**

Questo volume è stato curato
**dall'Istituto di Ricerca e Analisi della Difesa**

Direttore
**Col. c. (li) s. SM Gualtiero Iacono**

Vice Direttore
Capo Ufficio Studi, Analisi e Innovazioni
**Col. A.A.r.n.n. Pil. (AM) Loris Tabacchi**

Redazione

Addetti
**1º Mar. Massimo Lanfranco – Cº 2ª cl. Gianluca Bisanti – 1° Aviere Capo Alessandro Del Pinto**

Progetto grafico
**1º Mar. Massimo Lanfranco – Cº 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello – Assistente Amm. Massimo Bilotta**

Revisione e coordinamento
**G.M. Riccardo Pareggiani – S.Ten. Elena Picchi – Funz. Amm. Aurora Buttinelli – Ass. Amm. Anna Rita Marra**

Autori
**Antonino Cambria, Anna Clara Cantelli, Alessia Melcangi, Valentina Alessandra Mele, Luigi Olita, Gabriele Olivieri, Matteo Pignatti, Valentina Riggio.**

Stampato dalla tipografia del **Centro Alti Studi per la Difesa**

**Istituto di Ricerca e Analisi della Difesa**
Ufficio Studi, Analisi e Innovazioni
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3208
e-mail irad.usai@casd.difesa.it

Chiuso a **aprile 2023**

**ISBN 979-12-5515-043-5**

# Osservatorio Strategico
# Speciale Ucraina

## Indice



## Sotto la lente

# Pagina bianca

# Osservatorio Strategico
# Speciale Ucraina

Pagina bianca

## Applicazioni militari dell'Intelligenza Artificiale

A partire dallo scoppio della guerra in Ucraina, il 24 Febbraio del 2022, si è assistito ad un sempre più frequente dispiegamento dei droni Bayraktar TB2, un sistema d'arma UAV tattico, sviluppato e prodotto dalla Baykar Technologies (Turchia). I Bayraktar TB2 sono droni della categoria MALE (*Medium Altitude Long Endurance*: noti anche come MALE RPAS (*Remotely Piloted Aircraft System*), sono UAV telecomandati che volano a media altitudine (in modo da essere invisibili a occhio nudo) e hanno una lunga autonomia di volo. Sono comandati da remoto da un operatore e sono utilizzati per missioni di intelligence o missioni di attacco in un raggio molto più ampio rispetto ai droni tattici (Ioualalen e Limousin 2021), capaci di controllare mansioni di IRS (*Intelligence, Surveillance and Reconnaissance*) e anche missioni armate. Una suite avionica a bordo, con un sistema avionico triplo ridondante, comprende unità che consentono rullaggio, decollo, atterraggio e crociera completamente autonomi. TB2 ha dimostrato la sua efficacia con oltre 500.000 ore di volo operative. Dal 2014, svolge con successo missioni all'interno delle Forze Armate turche, della gendarmeria e della polizia nazionale turca. Attualmente, 257 piattaforme Bayraktar sono al servizio di Turchia, Qatar, Ucraina e Azerbaijan. Bayraktar TB2 detiene il record nella storia dell'aviazione turca per la resistenza in volo (con 27 ore 3 minuti) e per l'altitudine raggiunta (con 25.030 piedi). Bayraktar TB2 è anche il primo aereo della sua categoria ad essere esportato all'estero (https://baykartech.com/en/uav/bayraktar-tb2/). Stando a quanto dichiarato dall'azienda in merito alle prospettive produttive future, i prossimi progetti di UAV prodotti dalla Baykar Technologies saranno integrati di diverse *features* a Intelligenza Artificiale. Le tecnologie AI (Intelligenza Artificiale) sono già entrate ampiamente a fare parte di numerose attività civili e gli intenti progettuali dichiarati dalla società turca si inseriscono in una tendenza di graduale trasformazione della concezione contemporanea dell'arte della guerra, entro un panorama in cui le AI assumono un ruolo sempre più rilevante. Sin dagli albori della storia umana, la forza dell'Esercito è stata lo specchio della potenza dello Stato. Con ciò si intende che, nei corsi e ricorsi storici, gli Stati hanno sempre fatto in modo di assicurare considerevoli investimenti al settore militare. Più nello specifico, va sottolineato come una parte rilevante di tali investimenti sia sempre stata dedicata alla ricerca e allo sviluppo delle più avanzate tecnologie, come le AI. Per l'appunto, sistemi militari equipaggiati con tecnologie AI sono noti per essere in grado di gestire grandi quantità di informazioni, oltre alle loro già note capacità di autocontrollo e autoregolazione, dovute soprattutto alle loro avanzate capacità di calcolo e *decision-making* (Goled 2020).

Più precisamente, i progetti della Baykar Technologies (https://baykartech.com/en/artificial-intelligence/) riguardano:

- *Visual Posture Detection*: il progetto, basato su sistemi di AI hi-tech, è stato sviluppato per rilevare l'inclinazione dell'aeromobile, verso l'alto e verso il basso, e gli angoli di orientamento senza la necessità di sensori esterni o Global Positioning System (GPS). Le caratteristiche più rilevanti sono:
  - controllo automatico dell'aeromobile mediante intelligenza artificiale in caso di perdita del segnale GPS o guasto del sensore;
  - sistema di allarme quando il veicolo aereo supera determinati limiti dell'angolo di orientamento e, se necessario, consente al pilota di assumere il controllo dell'UAV;
  - modello di apprendimento continuo e progressivo del sistema AI;
  - miglioramento del modello con i dati raccolti dai sensori durante il volo.

- *Basic Object Detection*: questo progetto mira a identificare gli oggetti identificati dai dati di immagine ottenuti dalla telecamera posteriore dell'UAV. Sono stati applicati i più recenti modelli di tecnologia di *deep learning*;
- *Gimbal Object Detection*: l'obiettivo è quello di rilevare e tracciare gli oggetti e i dati identificati con l'aiuto dei dati di immagine ad alta risoluzione ricevuti dal giunto cardanico (gimbal);
- *Operation Beyond the Line of View*: è inteso ad assistere all'atterraggio dello UAV mediante l'uso delle immagini ottenute con il *Visual Landing System*;
- *Landmark Recognition*: gli UAV utilizzano sistemi di posizionamento convenzionali per rilevare la loro posizione del mondo. Grazie al progetto Landmark Recognition, gli UAV acquisiranno la capacità di calcolare la loro posizione in base alle posizioni contrassegnate note, per navigare senza il supporto GPS e altri sistemi simili.
  (Ulteriori informazioni reperibili a: https://baykartech.com/en/).

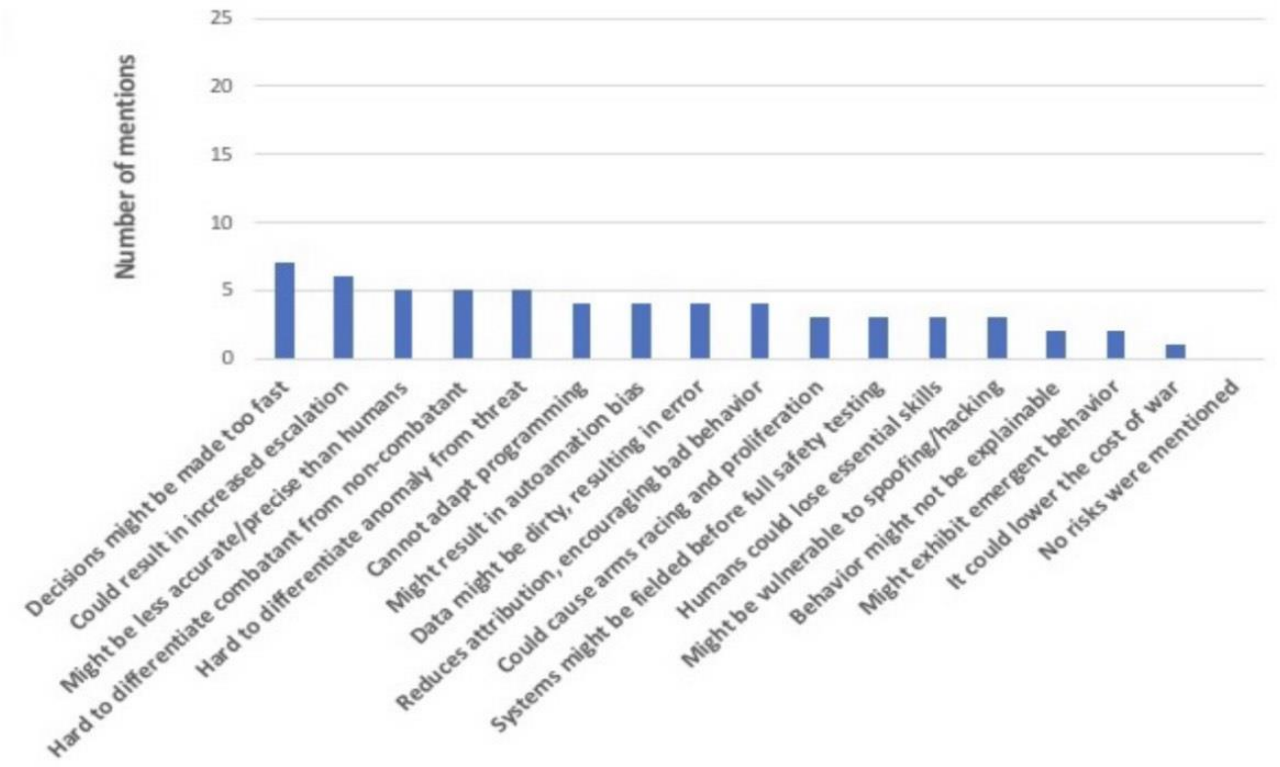
Al fine di procedere a un'analisi comprensiva di tali tecnologie, è importante tenere a mente che le AI, sin dalla loro primordiale concettualizzazione, circa settant'anni fa, hanno attraversato tre fondamentali stadi di sviluppo. La prima fase si identifica nell'attività di codificazione delle conoscenze di esperti, criteri legislativi o altre fonti rilevanti entro un programma informatico che prende il nome di *expert system*. Durante la seconda fase, l'attenzione è stata maggiormente diretta allo sviluppo e applicazione di metodi statistici utili alla formulazione degli attuali concetti e metodologia del *machine learning* (o *statistical learning*). Idee e metodi che includono, tra le altre cose, il riconoscimento vocale, l'elaborazione informatica del linguaggio naturale e lo sviluppo delle tecnologie di visione computerizzata. Infine, nella terza fase, tutt'ora in corso, vengono combinati i risultati positivi raggiunti nelle due fasi precedenti, rendendo così possibile anche lo svolgimento di operazioni di sofisticazione contestuale, astrazione ed elaborazione. In questa fase è stata introdotta la novità di impiego di metodi di apprendimento per i sistemi informatici simili a quelli utilizzabili per i sistemi cognitivi umani (RAND 2020). Ad esempio, è il caso dei *neural networks* che definiscono i principi e la tecnologia fondamentale del *deep learning*. Proprio in questo ambito, il *deep learning*, si osservano sviluppi interessanti, parallelamente ad altre aree di studio proprie della famiglia delle tecnologie AI. Ad esempio, è il caso del *neuromorphic computing* (ingegneria neuromorfica), una tecnologia che descrive l'uso di sistemi VLSI (*very large scale integration)* contenenti circuiti elettronici analogici per imitare le architetture biologico-neurali del sistema nervoso umano. Occorre inoltre sottolineare che vengono costantemente sviluppate tecniche "antagoniste" di ML (*machine learning*) al fine di perfezionarne le capacità di deviazione di sistemi AI nemici. Oggigiorno, la difesa dell'integrità, anche etica, dei sistemi AI rappresenta una sfida a tutti gli effetti, considerandone anche l'applicazione proattiva (Szabadföldi 2021).

Volendo fare un esercizio di previsione, prendendo in considerazione i prossimi dieci anni, ci si può sicuramente attendere che alcune delle tecniche possibili, grazie all'applicazione delle AI, ridefiniranno importanti tecnologie militari. Si consideri, ad esempio, il vantaggio comportato da una integrazione intelligente, nell'industria tecnologica militare, di capacità analitiche focalizzate alla conoscenza e all'apprendimento, basate su *network* di domini fisici e virtuali che operano per tramite di tecnologie *blockchain* garanti dell'integrità dei dati trattati. Ancor più rilevante per l'industria militare è l'aspetto che riguarda le modalità quasi immediate in cui le AI agevolano la collaborazione del dominio umano, fisico e dell'informazione, al fine di sviluppare sempre nuovi effetti "di disturbo". I sistemi AI hanno già influenzato profondamente le idee generalmente condivise riguardo gli arsenali nucleari, la guerra cibernetica e dell'informazione, la scienza dei materiali, le biotecnologie e l'aerospazio. Non è sbagliato, quindi, aspettarsi che gli stessi effetti possano essere avvertiti anche sulla concezione generale dell'ordine internazionale, allo stesso modo in cui le medesime idee vennero sostanzialmente influenzate nel 1945, a seguito degli effetti disastrosi dello scoppio delle bombe nucleari su Hiroshima e Nagasaki. Allo stesso modo, non è sbagliato attendersi che un

utilizzo estensivo dei sistemi AI incoraggi anche un certo grado di antagonismo entro una dinamica di corsa alle armi ad intelligenza artificiale; ciò è evidente, ad esempio, nei processi di sviluppo di tecnologie ML, basate prevalentemente su algoritmi e formule matematiche, utilizzate principalmente per estrarre dei modelli a partire da masse di dati. Tenere a mente considerazioni di questo tipo serve, dal punto di vista di un esercito, a calibrare i propri piani di azione valutando anche la possibilità che l'avversario sia in grado di decifrare gli input e gli output del sistema AI. Laddove gli operatori siano in grado di dedurre gli algoritmi che operano nel sistema, ottenuti con operazioni di ingegneria inversa, allora la guerra non è più totalmente tra schieramenti avversari sul campo, ma tra matematici.

A questo punto sembra opportuno descrivere alcune specifiche applicazioni militari delle AI, in dipartimenti in cui effettivamente ci si attende che questo tipo di tecnologia abbia effetti significativi. Un primo esempio è quello della struttura operativa C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*), in base alla quale è previsto che le unità operative sul campo siano equipaggiate con sistemi autonomi in grado di eseguire mansioni generalmente considerate pericolose, e utilizzando le capacità delle AI per fornire supporto decisionale sui possibili scenari di combattimento e su raccomandate linee d'azione (RCOA, *recommended course of action*). Gli equipaggiamenti tecnologici forniti agli analisti d'intelligence sono dotati di migliorate capacità TCPED (*Tasking, Collecting, Processing, Exploiting, Disseminating*), che consentono anche una più affidabile raccolta di informazioni utili, basata principalmente su sistemi di fusione, categorizzazione e selezione dei dati operati proprio dalle AI. A ragion veduta, integrando la tecnologia AI nei processi C4ISR è possibile ottenere sia migliori indicazioni e avvertimenti più accurati, ma è anche possibile sviluppare migliori mezzi di gestione delle conoscenze, giungendo quindi alla produzione di analisi di intelligence più chiare e precise. La maggiore efficienza e sicurezza offerta dal supporto delle AI è evidente anche in riferimento alle potenziali capacità operative dei sistemi autonomi UxVs (veicoli senza equipaggio, come gli UAV, UGV, AUV, etc…). Infatti, implementando sistemi di *deep learning* su queste piattaforme sarebbe anche possibile estendere in modo sostanziale le funzionalità robotiche per la navigazione satellitare. L'integrazione delle AI nei processi analitici risulta, inoltre, vantaggiosa soprattutto in situazioni di pianificazione e *decision making*, in virtù della rapidità di analisi anche di fattori molto complessi. Infine, l'analisi e previsione di pericoli CBRN (*Chemical, Biological, Radioactive, Nuclear*) ottenute secondo i parametri DIM (*Detection, Identification and Monitoring*) trae giovamento dall'autonomia decisionale propria dei sistemi AI, operanti in questo caso tramite integrazione di sensori e fusione di dati.

Sembra appropriato concludere questa analisi descrivendo brevemente i maggiori rischi associati all'integrazione delle AI nelle tecnologie militari. Una valutazione preliminare imprescindibile riguarda, infatti, la valutazione degli effettivi vantaggi offerti dalle capacità delle AI in confronto ai rischi che presentano. Il grafico sottostante illustra i principali rischi che un gruppo di esperti e studiosi intervistati, nel 2020, dalla RAND Corporation ha individuato in relazione alle applicazioni belliche delle AI, categorizzati in base alla frequenza con cui sono stati menzionati:




(In figura: Rischi di Applicazione Militare delle Intelligenze Artificiali Individuati in Interviste Strutturate; *Military Applications of Artificial Intelligence – Ethical Concerns in an Uncertain World*, RAND Corporation 2020, pagina 21)

Come deducibile dal grafico, gli intervistati hanno sollevato serie preoccupazioni riguardo le applicazioni militari delle AI, in generale. È comunque possibile suddividere tali preoccupazioni in tre macro-gruppi, precisamente: rischio di errore, maggiore rischio di scontro e rischio che i soldati e i leader possano porre troppa fiducia nelle capacità delle AI.

In primo luogo, per quanto concerne il rischio di errore dei sistemi AI, gli studiosi hanno menzionato che questi sistemi tendono a prendere decisioni troppo velocemente o addirittura non sono pienamente in grado di adattarsi alle complessità di uno scenario di guerra. Ciò significa che i sistemi AI potrebbero, ad esempio, non essere in grado di distinguere accuratamente tra i combattenti e i non combattenti/civili o, addirittura, tra effettive minacce o semplici anomalie di sistema, risultando quindi meno accurati e precisi anche di operatori umani. Problemi di questo genere potrebbero diventare ancora più rilevanti se questi sistemi venissero messi in campo prima ancora di essere stati adeguatamente testati o, ancora peggio, se gli avversari fossero riusciti ad hackerarli. Segue, poi, la preoccupazione in merito a un incrementato rischio di conflitto, basata sulla possibilità effettiva che ogni nazione possa perseguire l'integrazione di sistemi AI nei propri arsenali, nella speranza di guadagnare un vantaggio in una plausibile guerra contro ipotetici nemici, e questo comporterebbe una potenziale proliferazione di armi AI e una vera e propria corsa agli armamenti. Le armi autonome in guerra potrebbero, infatti, non essere sufficientemente sensibili a considerazioni politiche o a non sorpassare eventuali soglie di *escalation*. In effetti, questi sistemi sono in grado di promuovere attacchi con livelli tali da incrementare il conflitto. In aggiunta a ciò, la questione diventerebbe ancor più difficoltosa nell'eventualità in cui si scelga di attribuire la responsabilità degli eventi ad operatori umani. A questo proposito è opportuno aggiungere, però, che all'integrazione dei sistemi AI negli arsenali conseguirebbe una effettiva possibilità di diminuzione del costo totale delle guerre, soprattutto in termini di perdite umane, e ciò potrebbe incoraggiare i comandanti ad assumersi maggiori rischi e ad agire in maniera più aggressiva,

incentivando ulteriori dinamiche di *escalation*. Infine, per quanto riguarda il troppo alto grado di fiducia riposto nelle AI da parte degli operatori militari, questo si traduce nella possibilità per gli operatori di mostrare degli *automation bias*, affidandosi agli output del sistema anche nel caso in cui questi non siano pienamente comprensibili. Ciò si rende ancor più evidente in riferimento a sistemi in cui il processo algoritmico è estremamente complesso e, dunque, gli output risultano praticamente impossibili da decifrare. Di conseguenza, ciò comporta che gli operatori sono impossibilitati a determinare in modo rapido il motivo per cui i loro sistemi si comportano in un modo piuttosto che in un altro (RAND 2020). Un altro problema degno di considerazione è il *Black Box Problem*, ovvero un *device* o un sistema che permette il controllo degli input e degli output, senza però consentire l'analisi dei processi intermedi. Più precisamente, riguardo alla AI *Black Box*, si intende che in diversi strumenti basati su AI, l'algoritmo che processa le sezioni connesse in sequenza per il perfezionamento dei dati, non sono esplicative in termini di input e output. Una possibile soluzione al problema è rappresentata dal c.d. *Explainable AI*, che è uno strumento basato su AI che processa i dati oggetto di interesse, fornendo poi risultati comprensibili circa i processi interni al sistema. Considerando, però, che soluzioni di questo tipo non sono ancora disponibili per ogni tipo di malfunzionamento, il *Black Box Problem* rimane un rischio indicativo sul quale ha posto l'attenzione anche il Programma Europeo di Sviluppo del Settore Industriale della Difesa (EU EDIDP) (RAND 2020).

Ciononostante, è necessario che vengano svolte ricerche più approfondite soprattutto nell'ambito dello *Human-Machine Teaming*, tenuto presente che il coinvolgimento dell'uomo in guerra è destinato a rimanere invariato, a prescindere dal livello di avanguardia dei sistemi AI di oggi e di domani (Szabadföldi 2021). L'intelligenza artificiale è una tecnologia capace di migliorare in maniera importante le capacità di analisi dei dati predittivi e cognitivi, in modo tale per cui diventa cruciale per la sostenibilità del sistema comprendere la necessità di mantenere attivi tutti i processi già in funzionamento per la trasformazione dei dati strutturati e non in informazioni concrete da fornire ai *decision-makers* (Goled 2020). I dati strutturati possono essere processati tramite tecnologie ML basate su *neural networks*, mentre invece i dati non strutturati vengono processati da sistemi DL (*Deep Learning*) e tecnologie basate sulle strutture del linguaggio naturale. Tutti questi strumenti possono essere applicati al fine di produrre analisi molto più realistiche per le simulazioni e la costruzione di modelli, che si traducono poi nella messa a punto di tecniche adattive per la guerra elettronica e lo sviluppo di agenti AI pensati appositamente per operazioni cyber offensive e difensive da svolgere per intero nel solo *Infospace* (RAND 2020).

**Bibliografia**


- *Artificial Intelligence in Military Applications – Opportunities and Challenges*, I. Szabadföldi, National University of Public Service, Budapest (Hungary), disponibile a: https://sciendo.com/pdf/10.2478/raft-2021-0022
- *Autonomous Military Drones Soon Equipped with AI, Reality or Fiction*? A. Ioualalen, L. Limousin, disponibile a: https://numalis.com/publications-37-autonomous_military_drones_soon_equipped_with_ai_reality_or_fiction.php
- *Military Applications of Artificial Intelligence – Ethical Concerns in an Uncertain World*, F.E. Morgan, B. Bordeaux, A.J. Lohn, M. Ashby, C. Curriden, K. Klima, D. Grossman; RAND Corporation, disponibile a: https://www.rand.org/pubs/research_reports/RR3139-1.html
- *What are the Scope and Challenges of Using Artificial Intelligence in Military Operations*, S. Goled, disponibile a: https://analyticsindiamag.com/what-are-the-scope-and-challenges-of-using-ai-in-military-operations/


**Sitografia**


- https://baykartech.com/en
- https://baykartech.com/en/uav/bayraktar-tb2/
- https://baykartech.com/en/artificial-intelligence/

# Bayraktar: il ruolo della Turchia nel conflitto russo-ucraino

**Abstract**

L'invasione dell'Ucraina da parte della Federazione Russa, il 24 febbraio 2022, ha segnato uno spartiacque e un nuovo cambio di paradigma all'interno del sistema internazionale. Un evento che, secondo le logiche del Cremlino, avrebbe come obiettivo quello di cambiare il sistema globale trainato dagli Stati Uniti d'America avviando, quindi, il passaggio dall'eccezionalismo americano al mondo multipolare. La divisione che ha segnato, dal punto di vista delle alleanze, è fondamentale per capire il ruolo della NATO negli anni a venire e soprattutto in che modo alcuni suoi membri si muoveranno nei confronti di Washington. Ungheria e Turchia sono i due membri della NATO che hanno fatto sentire di più la loro vicinanza a Mosca, seppur con sfumature diverse. Ankara, infatti, diversamente da Budapest, rifornisce di droni Bayraktar TB-2 l'esercito ucraino contro la Russia, ma allo stesso tempo non si è unita alla campagna sanzionatoria messa in piedi dalla NATO. Ciò è dettato dal fatto che l'obiettivo di Ankara sarebbe proprio quello di sfruttare la sua posizione di membro dell'Alleanza Atlantica e partner commerciale di Mosca per guadagnare peso a livello internazionale, cosa che sta avvenendo sia a livello energetico che commerciale. Anche dal punto di vista delle mire geostrategiche, Ankara sta guadagnando terreno poiché l'ultima operazione militare lanciata nel nord ovest della Siria ha visto una Russia accondiscendente e gli USA silenziosi.

## 1. 2015-2016, il risveglio della Turchia

Il ruolo di Ankara all'interno del sistema internazionale è fondamentale per capire sia il futuro del Medio Oriente, sia quello di un ipotetico futuro mondo multipolare teorizzato da Vladimir Putin. Di rilevante caratura all'interno della politica turca, Recep Tayyip Erdogan ha scalato le gerarchie per diventare Presidente della Repubblica di Turchia ed imprimere, a piccoli passi, dei grandi cambiamenti al suo Paese. Sin dal novembre del 2015, la Turchia era balzata agli onori delle cronache nel panorama siriano per l'abbattimento dell'aereo da guerra russo Sukhoi-24 dopo lo sconfinamento in territorio turco.

Dopo una prima indignazione da parte del Presidente russo Putin ed un raffreddamento dei rapporti tra i due Paesi, la situazione sembrò ricomporsi nei mesi successivi con un nuovo riavvicinamento che culminò con l'acquisto da parte di Ankara del sistema antimissile russo S-400.

A ciò si aggiunge anche la campagna militare lanciata da Erdogan nel Kurdistan siriano, durante l'estate del 2016, soprannominata operazione "Scudo dell'Eufrate", che diede una forte scossa alla presenza sia americana che russa in territorio siriano.

Il 2016, quindi, si può considerare come l'anno di espansione geopolitica della Turchia che ha consentito al Presidente Erdogan di sfruttare anche il colpo di Stato del 15 luglio del medesimo anno per attuare un *repulisti* interno in svariati settori della società. Giornalisti, accademici, Ufficiali militari e personaggi della politica, ritenuti di essere golpisti ed oppositori politici, sono stati vittime delle purghe "erdoganiane". Il colpo di Stato dell'estate del 2016 può essere considerato anche il catalizzatore per la trasformazione dello Stato turco in una Repubblica Presidenziale e fu il primo avvenimento che sancì, ancor prima dell'acquisto degli S 400 russi, una battuta d'arresto da parte di Ankara verso l'alleato americano poiché, in quel caso, fu proprio Erdogan a chiedere all'ex Presidente Barack Obama di estradare in Turchia il predicatore turco Fetullah Gulen. Quest'ultimo, vecchio amico di Erdogan e cittadino americano risiedente nello Stato della Pennsylvania, era stato accusato dal Presidente turco di essere la mente dietro il *golpe* di luglio, e quindi nemico della nazione. Il rifiuto di Washington nel soddisfare la richiesta di Erdogan fu un crescendo di sospetti e

tensioni che portano fino alla situazione attuale dei rapporti che si proiettano soprattutto nel conflitto militare tra Russia e Ucraina.

La crescita del potere interno e soprattutto del partito al governo del Presidente, cioè il Partito di Giustizia e Sviluppo, hanno permesso ad Erdogan di intraprendere una politica estera sia regionale, sia più allargata, concedendogli di arrivare a rappresentare, al momento, l'ago della bilancia nell'attuale conflitto in Ucraina. In questo contesto, la Turchia di Erdogan, intraprendendo una politica estera realista e machiavellica, ha contribuito ad infastidire gli USA, essendo appunto Ankara membro della Nato e secondo esercito più potente all'interno dell'Alleanza Atlantica dopo quello statunitense. La posizione geostrategica della Repubblica di Turchia è infatti fondamentale per gli USA, sia per l'accesso al Medioriente sia per la presenza sul territorio nazionale turco della Incirlik Air Base. Costruita nel 1951, quindi nel pieno della Guerra Fredda, e gestita sia dalla Turk Hava Kuvvetleri che dalla US Air Force, la base aerea è fondamentale e strategica per quanto riguarda le operazioni aeree soprattutto degli USA in Medioriente. I rapporti tra Washington ed Ankara dall'acquisto da parte di quest'ultima dei primi sistemi S 400 dalla Russia si sono a mano a mano raffreddati, con l'aumentato sospetto da parte degli USA verso Erdogan per la sua politica del doppio forno con Mosca.

## 2. Strette di mano tra Kiev ed Ankara

Tra la fine del 2013 e l'inizio del 2014, con lo scoppio delle proteste a Piazza Maidan in Ucraina contro il governo Janukovič, Erdogan era fortemente ancorato all'interno della NATO ed a sostegno dell'Ucraina. Dall'elezione del Presidente Volodymir Zelensky, nel maggio 2019, fino all'aumento delle tensioni tra Mosca e Kiev - nel 2021 - che hanno portato una completa rottura il 24 febbraio 2022 con l'invasione russa dell'ucraina, il ruolo di Erdogan è stato sicuramente molto vicino a Kiev, sancendo un avvicinamento ed inaugurando accordi di cooperazione in ambito commerciale, sanitario e militare ma, allo stesso tempo, continuando a mantenere uno stretto dialogo con Mosca.

Lo stesso Erdogan ha visitato Kiev nell'aprile del 2021 mostrandosi molto vicino al governo ed al popolo ucraino nella loro opposizione a Mosca ed ai filo russi delle due Repubbliche separatiste del Luhansk e Donetsk. Una questione fondamentale affrontata da Erdogan durante la sua visita al suo omologo ucraino, è stata proprio la Crimea, che non viene riconosciuta da Ankara come territorio russo dopo l'annessione fatta da Mosca nel 2014, giocando soprattutto sul ruolo dei tatari di Crimea e sulla violenza subita da questi ultimi proprio dall'Esercito russo.

La diplomazia attuata da Erdogan quindi non è soltanto incentrata su accordi appena citati, ma ha come fulcro proprio il fattore religioso. La componente musulmana in Ucraina ed i tatari di Crimea, citati poc'anzi, sono uno dei *trait d'union* che unisce Kiev ed Ankara, consentendo quindi alla diplomazia religiosa di Erdogan di puntare proprio alla costruzione di infrastrutture religiose in territorio straniero. Uno degli obiettivi di Ankara sarebbe stato, infatti, quello di costruire una grande moschea a Kiev con il beneplacito del governo Zelensky.

La strategia messa in atto da Erdogan pone la Turchia come uno dei perni della NATO per godere di una polizza assicurativa sulla vita in un ipotetico scontro con Mosca e quindi sfidarla non solo sostenendo l'Ucraina, ma anche l'Esercito azero contro gli armeni nel Nagorno Karabakh e nella sua guerra contro i curdi in Siria. Allo stesso tempo, il rapporto di Ankara con Mosca è più vivo che mai, sia nel campo degli affari commerciali che energetici, dimostrando una politica estremamente cinica dotata di grande visione strategica.

Da non dimenticare che proprio gli ultimi avvenimenti in Ucraina hanno incoronato Erdogan non solo come grande mediatore per quanto riguarda lo sblocco delle navi cariche di grano dai porti ucraini, ma anche ago della bilancia nell'approvazione dell'entrata di Finlandia e Svezia all'interno dell'Alleanza Atlantica. Nella polveriera ucraina, Erdogan non si è unito alla campagna sanzionatoria contro la Russia ed allo stesso tempo, pur condannando l'invasione, non si è mai espresso in modo negativo nei confronti del Presidente Putin. Due sono state le occasioni che hanno consentito ad

Erdogan di dettare legge in questo contesto, e che stanno avendo ripercussioni anche nei suoi rapporti con lo storico alleato americano; la mediazione tra Russia e Ucraina, con il coinvolgimento delle Nazioni Unite, sullo sblocco delle navi cariche di grano ancorate nei porti dell'Ucraina, ma bloccate da Mosca poiché situate nella zona sud del Paese controllata in parte dalle autorità militari russe, ed il veto posto sull'entrata di Svezia e Finlandia all'interno della NATO.

Proprio su questo ultimo punto, prettamente collegato al contesto ucraino, si sta giocando una delle partite più difficili tra Washington ed Ankara, ponendo quest'ultima in rotta di collisione con i suoi alleati. La posizione della Turchia continua a rimanere la stessa dal novembre 2022, poiché le accuse della Turchia verso la Svezia vertono sul fatto che quest'ultima offra rifugio a militanti kurdi del PKK, cioè il Partito dei lavoratori del Kurdistan, ritenuti terroristi da Ankara in quanto il PKK è nella *black list* del terrorismo dell'intelligence turca. Questa opposizione sta dando una forte mano alla Russia, poiché ritarderebbe sempre di più l'iter per l'ingresso di Stoccolma ed Helsinki nell'Alleanza Atlantica, garantendo in questo caso anche ad Erdogan di aumentare la posta in gioco per quanto riguarda le sue richieste negli scacchieri geopolitici di sua influenza.

La questione del veto turco all'ingresso di Svezia e Finlandia è strettamente correlata alla politica estera della Turchia in Siria, poiché proprio negli ultimi mesi l'esercito turco ha messo in atto un'operazione militare nel Nord ovest della Siria contro i miliziani kurdi, riuscendo ad ottenere il consenso da parte di Mosca e mettendo in difficoltà gli USA, i quali da alleati hanno lasciato mano libera all'Esercito turco. Nel contesto siriano, Mosca concedendo l'avanzata delle truppe turche in territorio siriano, del quale proprio Mosca è protettrice, si ascrive proprio nel ruolo ambiguo svolto da Ankara fino ad adesso, non presentandosi quindi come un vero e proprio ostacolo nei confronti del Cremlino, ma in un certo senso, agevolando la sua politica. Ovviamente, non mancano le prese di posizioni turche che nel contesto della guerra in Ucraina stanno danneggiando proprio la Russia, infatti sia la chiusura del passaggio alle navi da guerra russe attraverso lo stretto dei Dardanelli, azione spesso vietata anche alle navi statunitensi e britanniche e la vendita di droni Bayraktar TB-2 all'Ucraina, sono due dei punti che hanno messo in seria difficoltà Mosca sin dall'inizio dell'invasione. La chiusura dello Stretto del Mar Nero, secondo la Convenzione di Montreaux del 1936, alle navi russe che non appartengono alla flotta del Mar Nero, ha sicuramente avuto un impatto meno significativo rispetto ai droni Bayraktar utilizzati dall'Esercito ucraino poiché il passaggio delle navi da guerra russe, seppur rallentato, non si è protratto nel tempo.

## 3. Tra "Baykar Diplomacy" e Realpolitik

Come accennato precedentemente, uno dei migliori *business* di Ankara con l'Ucraina, ma in generale con numerosi Paesi che sono stati stregati dalle capacità della creazione turca in ambito militare, riguarda proprio il drone Bayraktar TB-2. Terrore nei cieli dell'Ucraina, il Bayraktar è un sistema tattico armato in grado di compiere attività di intelligence, ricognizione, sorveglianza ed attacco armato. Il sistema è costituito da una piattaforma armata ed una struttura avionica con un triplo sistema avionico comprendente unità che consentono rullaggio, decollo, atterraggio e crociera in modo totalmente autonomo. Il Bayraktar TB2 ha un'apertura alare di 12 metri, un'altezza di 2,2 metri ed una lunghezza di 6,5 metri. Il peso massimo al decollo è di 700 kg con una capacità di resistenza di 27 ore e 3 minuti e di 25.030 piedi di altitudine. È dotato di quattro munizioni intelligenti a guida laser ed una velocità in volo che va dai 70 ai 120 nodi. Essendo armato di quattro munizioni intelligenti, l'UAV è in grado di individuare il bersaglio utilizzando un dispositivo laser a bordo. Proprio queste capacità e la sua manovrabilità e versatilità in volo ne fanno una vera e propria macchina da guerra e "terrore dei cieli", richiesto fortemente da numerosi eserciti come appunto quello ucraino

Prodotto dalla Baykar, azienda attiva dal 1994, di cui Selcuk Bayraktar è *Chief Technology Officer*. Selcuk Bayraktar, genero del Presidente turco Erdogan avendo sposato la figlia nel 2016, ha rivoluzionato il piano di sviluppo dell'industria della difesa turca secondo gli obiettivi del capo di stato di rendere la Turchia una delle prime nazioni della regione nella produzione di armi.

La vendita di Bayraktar TB-2 all'Ucraina viene sancita con gli accordi di cooperazione economica e militare tra Kiev ed Ankara del 2021, inaugurando quindi anche la fornitura militare che sarà decisiva contro l'Esercito russo a partire dall'invasione del febbraio 2022. L'utilizzo dei droni turchi sta creando, infatti, non pochi problemi all'Esercito russo in Ucraina e ciò ha trasformato la guerra tra i due Paesi in un vero e proprio conflitto aereo condotto con gli UAV. Ciò detto, il Bayraktar TB-2 si sta dimostrando il drone più letale in combattimento rispetto ai suoi omologhi britannici e statunitensi, tanto da essere richiesto non solo dall'Esercito ucraino, ma da altri Paesi impegnati in conflitti e non. Rilevante l'esempio dell'Albania, la quale ha richiesto droni Bayraktar così come l'Azerbaijan, stretto alleato di Ankara dal punto di vista storico ed etnico, soprattutto nel conflitto contro l'Armenia nella guerra del Nagorno Karabakh. Proprio in questa contesa l'utilizzo di droni turchi è stato, ed è, fondamentale, consentendo all'Esercito azero di avanzare oltre le linee del Karabakh, infliggendo numerosi danni agli armeni. Fondamentali sono anche gli interventi in ambito siriano da parte dei medesimi droni, contro lo Stato Islamico ed i miliziani kurdi del PKK, i quali si stanno dimostrando delle efficaci macchine da guerra. In questo contesto dominato da conflitti nascenti, il ruolo della diplomazia dei droni, che si potrebbe definire come una vera e propria "Baykar diplomacy", consente alla Turchia di implementare le vendite di UAV all'estero ed allo stesso tempo incrementare la produzione industriale militare degli stessi. La "Baykar diplomacy" di Ankara si sta dimostrando estremamente vincente all'interno della crisi ucraina, poiché gli UAV turchi sono lo strumento indispensabile dei militari ucraini per danneggiare il più possibile il nemico russo, il quale non poche volte ha fatto emergere la propria indignazione a riguardo, ma che non può permettersi di perdere un partner-alleato come la Turchia per rallentare sempre di più le decisioni dell'Alleanza Atlantica nel contesto ucraino.

## 4. Conclusioni

Il ruolo della Turchia, appena analizzato si inserisce in una cornice di otto anni in cui dalle prime azioni in Siria contro la Russia, è andato crescendo sempre di più, fino ad arrivare ad essere ambiguo, ma determinante, all'interno della guerra in Ucraina. Il rapporto tra Ankara e Mosca è stata la vera miccia che ha permesso alla Turchia di inserirsi in modo così cinico e machiavellico all'interno dell'arena internazionale, giocando su più fronti e determinando l'inasprimento dei rapporti con la NATO, ad iniziare dagli Stati Uniti d'America. Non è un caso se, secondo numerosi sondaggi, il popolo turco ritiene gli USA come una minaccia per la nazione, considerando a pari grado l'Alleanza Atlantica. Determinanti anche le parole del Ministro dell'Interno turco, il quale ha affermato che gli USA non dovranno intromettersi negli affari interni del Paese utilizzando una frase molto forte ed emblematica: "*tenere giù le mani dalla Turchia*". Da tenere presente, comunque, che nonostante la politica estera vincente nello scacchiere ucraino ed il controllo dell'arma migratoria, vero terrore per tutta l'Europa come fenomeno estremamente difficile da gestire, in patria il recente terremoto, l'inflazione e le imminenti elezioni di maggio 2023 sono i tre problemi principali sulla scrivania del Presidente Erdogan. Tre eventi legati inevitabilmente, poiché proprio a maggio si deciderà se il "Sultano" continuerà a guidare il Paese oppure sarà a prevalere Kemal Kilicdaroglu, a capo della più estesa coalizione della storia repubblicana.

**Sitografia**


- https://www.agi.it/estero/news/2022-05-30/storia-inventore-turco-drone-bayraktar-chi-e-16914552/
- https://www.baykartech.com/en/uav/bayraktar-tb2/
- https://it.insideover.com/politica/il-piano-dell-opposizione-turca-per-sconfiggere-erdogan.html
- https://www.osw.waw.pl/en/publikacje/analyses/2023-03-07/anti-western-sentiments-turkeys-politics
- https://it.insideover.com/religioni/la-turchia-costruira-la-piu-grande-moschea-dellucraina.html
- https://formiche.net/2021/04/il-patto-del-mar-nero-se-lasse-turchia-e-ucraina-irrita-putin/
- https://it.insideover.com/politica/turchia-ed-ucraina-fanno-fronte-comune-e-minacciano-la-russia.html
- https://it.insideover.com/difesa/lasse-tra-turchia-e-ucraina-si-fa-sempre-piu-solido.html
- https://it.insideover.com/politica/turchia-e-ucraina-sempre-piu-vicine-obiettivo-russia.html
- https://www.osw.waw.pl/en/publikacje/analyses/2022-05-18/turkeys-veto-towards-finlands-and-swedens-nato-membership-bid
- https://www.osw.waw.pl/en/publikacje/osw-commentary/2022-07-01/turkish-dilemmas-shadow-war-ukraine
- https://rusi.org/explore-our-research/publications/commentary/turkey-forges-new-geo-strategic-axis-azerbaijan-ukraine
- https://www.startmag.it/innovazione/la-turca-baykar-costruira-fabbrica-di-droni-in-ucraina/

Pagina bianca

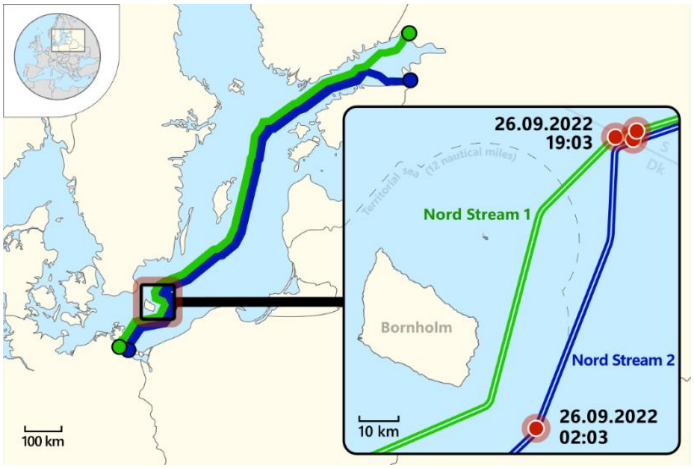
## NORD STREAM *o dell'ultima connessione euroasiatica*

Ultima connessione è da intendere sia in termini prettamente temporali, considerando come i due gasdotti Nord Stream siano le più recenti opere infrastrutturali a collegare le riserve naturali di risorse gasiere russe con l'Europa Occidentale, potenzialmente in grado di ricalibrare gli equilibri energetici del continente; sia interpretando "ultima" connessione in termini assoluti, considerando come il perdurare della guerra in terra ucraina non lasci presagire il volere di ripristinare lo stesso volume di fornitura.

### 1) Attacco ai Nord Stream, il caso mediatico

Il 26 Settembre 2022 si sono registrate quattro ingenti fuoriuscite di gas metano provenienti dai due gasdotti sottomarini Nord Stream, imponenti infrastrutture "gemelle" che espandendosi per 1224 km attraverso il Mar Baltico collegano le coste occidentali della Federazione Russa, partendo dai porti di Vyborg e Ust-Luga, alle città tedesche di Lubmin e Greifswald, e che vantano un potenziale volume di rifornimento gasiero annuo di 110 miliardi di metri cubi. Il primo episodio di dispersione di gas metano si è verificato alle ore 2:00 nell'area situata a sud est rispetto all'isola danese di Bornholm, i successivi tre alle ore 19:00 a nord est rispetto alla suddetta isola, nello spazio marittimo che valica all'interno della zona economica esclusiva svedese.

Fin dalle prime ore dall'accaduto si è palesato come fossero esigue le possibilità che il guasto fosse riconducibile a cause naturali, considerando come l'episodio si sia ripetuto a distanza di 17 ore e siano state registrate diverse scosse sismiche nelle medesime aree e orari attribuibili all'utilizzo di esplosivi, come da dichiarazione del sismologo e direttore della rete sismica nazionale svedese Bjorn Lund: "*Si può vedere chiaramente come le onde rimbalzano dal fondo alla superficie. Non c'è dubbio che è stata un'esplosione*".

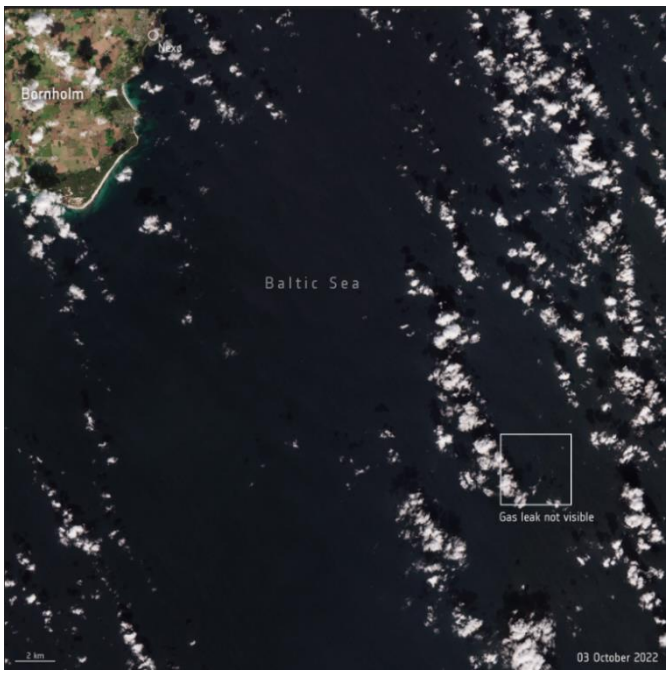



(SVG, Karte der Explosionen, die an den Nord-Stream-Pipelines am 26, 2022)

Al momento del danneggiamento nessuno dei due condotti era in funzione, il Nord Stream ufficialmente per dei lavori di manutenzione dichiarati da Gazprom mentre il Nord Stream 2 non ha mai iniziato a essere operativo, ma nonostante le forniture di gas fossero di fatto bloccate, ingenti quantità risiedono all'interno delle due infrastrutture. L'entità dei danni riportati sembra tale da poter compromettere definitivamente il funzionamento dell'opera, visto il rischio di corrosione dovuto alle infiltrazioni di acqua marina all'interno del sistema di condotti.

Dal punto di vista dei danni ambientali si sta registrando, inoltre, uno dei maggiori impatti climalteranti di gas metano dovuto alla perdita riconducibile a un singolo sito da quando se ne ha contezza: le stime più recenti pubblicate dall'International Methane Emissions Observatory (IMEO) dell'United Nations Environment Programme (Unep) attestano l'emissione in atmosfera di una quantità che varia da un minimo di 75.000 tonnellate di gas metano a un massimo di 230.000 (IMEO, 2023).

Risulta centrale focalizzare come il metano "vanti" un potenziale climalterante fino a 30 volte superiore rispetto a quello della CO2.




(Gas leak detected by Copernicus Sentinel-2, European Space Agency, 2022)

Nei giorni immediatamente successivi diversi rappresentanti di autorità governative hanno perentoriamente ricondotto la causa dell'incidente a un'azione di sabotaggio, l'allora Prima Ministra Danese Mette Frederiksen ha dichiarato: "*It is now the clear assessment by authorities that these are deliberate actions. It was not an accident*", e il 18 Novembre un comunicato del Säkerhetspolisen, ramo dei servizi segreti di sicurezza svedesi, ha confermato ufficialmente l'ipotesi del sabotaggio (SP,2022).

Il 28 Settembre The Daily Telegraph, quotidiano britannico di stampo conservatore, e The New York Times, faro mediatico dei "liberals" americani e non solo, hanno pubblicato due articoli, rispettivamente intitolati "Nord Stream sabotage mapped: How Putin could have carried out the attack" e "Sabotaged Pipelines and a Mystery: Who Did It? (Was It Russia?)" nei quali si ipotizzavano modalità e ragioni di un coinvolgimento diretto del Cremlino nell'azione di sabotaggio, citando l'ormai noto alla cronaca paradigma della "guerra ibrida", in particolare assumendo come sia nella tradizione recente russa colpire infrastrutture civili per porre pressione sui decisori politici, citando le dichiarazioni della Presidentessa della commissione difesa tedesca Marie-Agnes Strack-Zimmermann: "*Putin is going to use every hybrid measure at his disposal to fluster Europeans, from food to refugees to energy*". È emblematico come testate anglo-americane abbiano posto l'accento proprio sulle dichiarazioni di un membro del Bundestag, rimarcando, peraltro, come nonostante si chiarisca che non vi sia alcuna prova incriminante, Zimmerman ritenga che la Russia possa essere "*the most "plausible" culprit*" (NYT, 2022).

Il portavoce del Presidente Putin Dmitry Peskov non ha tardato a rilasciare dichiarazioni nelle quali ha definito "prevedibili, stupide e assurde" le accuse di un coinvolgimento diretto del Cremlino

nell'azione di sabotaggio, aggiungendo come a beneficiare economicamente dell'interruzione di flussi di rifornimento di gas russo verso la Germania e gli altri Paese europei siano *in primis* le compagnie energetiche americane, riportando, peraltro, le celebri dichiarazioni rilasciate dal POTUS a febbraio 2022 in una conferenza stampa congiunta con il Cancelliere tedesco Scholtz, nelle quali assicurava che dal momento in cui la Russia avesse invaso nuovamente i confini ucraini non ci sarebbe più stato nessun Nord Stream 2, nonostante una giornalista tedesca gli abbia fatto notare come anche la Germania fosse parte integrante del progetto.

La Casa Bianca aveva poi rilasciato una dichiarazione ufficiale nella quale specificava che il Presidente Joe Biden alludesse a un'azione di pressione diplomatica nei confronti della Germania per impedire l'avvio del funzionamento dell'opera e in nessun caso a un azione di intervento militare, come di fatto avvenne appena due giorni prima dell'invasione russa in terra ucraina: il 22 Febbraio 2022 il Primo Cancelliere Scholtz annunciò l'interruzione del processo di revisione dell'opera da parte dell'autorità tedesca di regolamentazione. Va, inoltre, segnalato come il Cremlino, mediante una conferenza stampa sempre indetta il primo Novembre dal portavoce del Presidente Putin, Peskov, abbia rincarato pesantemente la dose dichiarando che fonti di intelligence russe sarebbero in possesso di evidenze che testimonierebbero il coinvolgimento diretto nel sabotaggio dei gasdotti di forze speciali inglesi che avrebbero coordinato l'azione.

Nonostante le affermazioni lasciassero intendere come la Federazione Russa non possa ignorare o lasciar impunito un simile attacco, fino ad oggi non è stata registrata alcuna condivisione pubblica delle suddette prove.

Le caratteristiche peculiari proprie dello spazio subacqueo condizionano direttamente le possibilità di risalire a concrete evidenze che provino la responsabilità dell'atto di sabotaggio, essendo uno spazio privo di controllo satellitare. Le specifiche caratteristiche geo morfologiche dello spazio subacqueo baltico, la cui profondità non va oltre i 460 metri (dato che acquisisce di rilevanza relativa se paragonato ad esempio ai 5.267 metri di profondità massima che contraddistingue le acque del Mar Mediterraneo) dovrebbero, inoltre, facilitare il monitoraggio dell'area da parte delle forze di difesa degli attori statali prossimi, ma allo stesso tempo ciò implica che la totalità di essi dispone delle capacità necessarie per compiere tale azione. Ciò considerato le prevedibili e sterili accuse mediatiche mosse dai vari rappresentanti delle autorità governative non ci restituiscono altro che un giallo destinato a rimanere irrisolto.

In ultimo, è interessante riportare una dichiarazione condivisa online sulla piattaforma Twitter da parte di un ex Ministro della Difesa polacco, Radoslaw Sikorski, oggi membro del Parlamento Europeo, che recitava "Thank you, USA" riportando in allegato l'immagine delle perdite di gas proveniente dai Nord Stream.

Il *tweet* è stato velocemente eliminato e l'autore ha poi "corretto" il tiro definendo l'accaduto "un'operazione di manutenzione speciale russa".

Lo spiccato entusiasmo manifestato da Sikorski verso il plausibile danneggiamento irreversibile dell'opera di rifornimento gasiero è lo specchio del sentimento avverso che sempre più esplicitamente i decisori politici polacchi stanno esprimendo nei confronti della Germania, ben riassunto in una nota diplomatica recapitata dal Ministero degli Esteri di Varsavia a Berlino il 3 Ottobre 2022 nella quale si richiede il risarcimento di 1300 miliardi di euro per i danni di guerra risalenti all'occupazione tedesca della Polonia dal 1939 al 1945. Le cause dell'astio verso la Russia sono più note, comprensibili e "strutturali", dal momento che la recente nascita dell'ultimo soggetto statuale polacco, dotato di effettiva sovranità, sia intrinsecamente consequenziale al crollo del modello comunista sovietico, e considerando come nell'interpretazione di Varsavia la guerra d'invasione ucraina sia la manifestazione plastica di come le mire espansionistiche verso occidente, mosse dallo spirito imperiale russo, fossero sopite ma mai rimosse dagli obiettivi strategici di Mosca.

**2) Valore strategico e geo economico dei gasdotti Nord Stream**

La reazione, forse esplicita e "scomposta", da parte dell'ex Ministro della Difesa polacco va inquadrata analizzando quali fossero le caratteristiche peculiari dell'opera e le implicazioni strategiche ed economiche sottese a un suo funzionamento.

La struttura che compone il primo Nord Stream è caratterizzata da una coppia di condotti, dei quali il primo fu inaugurato nel 2011, e garantiva un flusso gasiero di 27,5 miliardi di metri cubi, mentre l'anno successivo iniziò a essere operativo il secondo, con le medesime capacità di rifornimento. Si stimava che l'infrastruttura energetica fosse in grado di garantire approvvigionamento gasiero per almeno mezzo secolo. Il costo totale delle spese per la costruzione dell'opera ammonta a 7,4 miliardi di euro, sostenute da Nord Stream AG, società costituita dal colosso energetico russo Gazprom che ne detiene il 51% delle quote, da Ruhrgas e Wintershall, aziende energetiche tedesche che ne detengono il 15,5 % cadauna, da Gasunie, società olandese attiva nel settore delle infrastrutture che ne detiene il 9%, e da Engie, multinazionale francese che opera nel mercato energetico, detentrice anch'essa del 9% delle quote.

I progetti relativi alla costruzione dell'infrastruttura "gemella", il Nord Stream 2, ebbero inizio nel 2018 e terminarono nel 2021, realizzando un'opera caratterizzata dalla medesima struttura e capacità di rifornimento rispetto alla prima: una coppia di condotti, ognuno dei quali con una capacità di rifornimento annuo di 27,5 miliardi di metri cubi, che si espande analogamente al primo Nord Stream nello spazio subacqueo del Mar Baltico, seguendone parallelamente la quasi totalità del perimetro. In linea del tutto teorica, poiché come sopracitato il Nord Stream 2 non è mai entrato in funzione, la quota totale del gas veicolato dai entrambi i sistemi di conduttura Nord Stream si sarebbe attestata a 110 miliardi di metri cubi annuali.

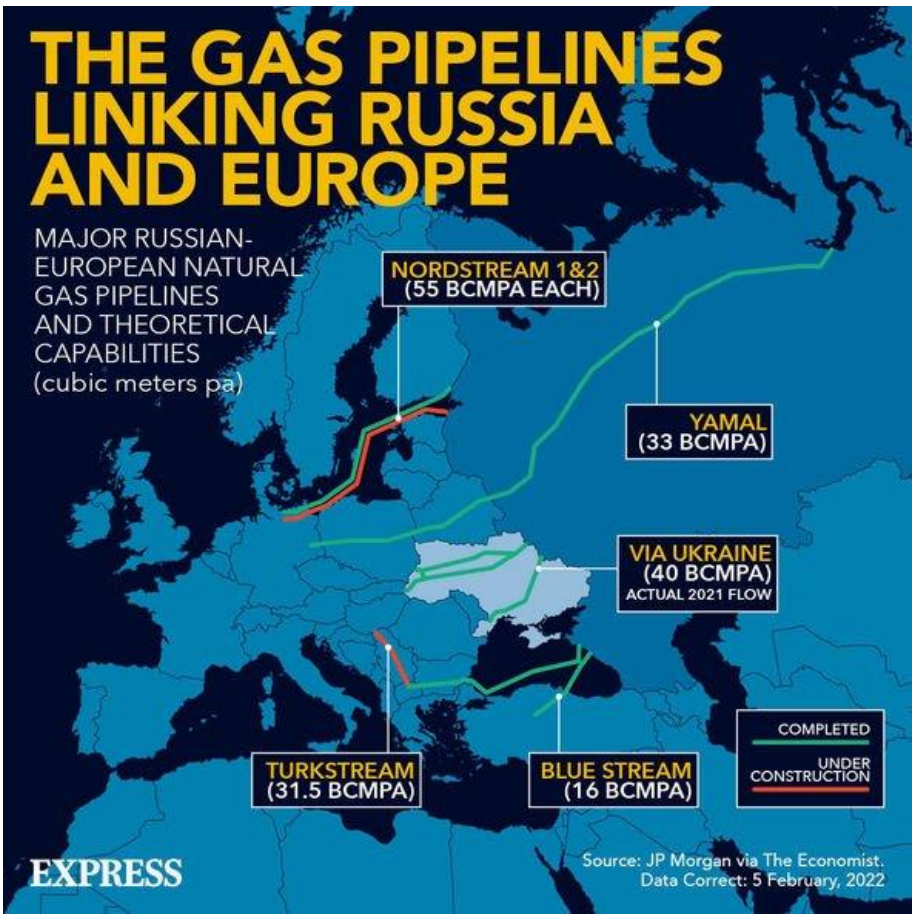
I vantaggi relativi al transito di un volume di gas così ingente sono molteplici, per la Germania ciò significherebbe assicurarsi un ulteriore e significativo approvvigionamento a costo contenuto di una materia prima essenziale per la proliferazione del proprio comparto industriale e benessere sociale, rinforzando così il paradigma economico di crescita progressiva e costante che ha trainato il processo di riunificazione interno, permesso di attuare politiche di immigrazione proficue, e "cementato" lo *status* di potenza economica leader dell'Unione Europea. Avrebbe determinato, inoltre, la possibilità di ultimare il processo verso un mix energetico nazionale che non facesse più affidamento sull'energia nucleare. Non ultimo, per lo Stato tedesco ciò significherebbe ottenere il ruolo di principale polo di ricezione, raccordo e smistamento di gas in Europa.

Dal punto di vista russo tale opera di collegamento mediante lo spazio subacqueo, che attraversa le acque territoriali di Svezia, Finlandia e Germania, permetterebbe di ridimensionare l'importanza strategica degli altri sistemi di conduttura terrestri, che prima di ricongiungersi con la Germania e connettersi agli altri maggiori importatori europei di gas russo, passano attraverso territori di Stati progressivamente sempre più ostili al Cremlino, Ucraina e Polonia *in primis*.

L'interpretazione per cui la messa in funzione di tale gasdotto avrebbe aumentato enormemente l'interdipendenza fra Germania e Russia, con la possibilità per il Cremlino di utilizzare quest'importante leva negoziale in fasi di attrito o di vero e proprio scontro con gli Stati europei limitrofi fu propria della quasi moltitudine degli Stati ex-sovietici, che manifestarono pubblicamente il proprio dissenso fin dal concepimento del primo progetto Nord Stream. La possibilità di mantenere nel proprio territorio sovrano parte delle uniche "direttrici" del gas russo che rifornivano il centro economico del continente, rappresentando esse base strutturale del sostentamento interno per l'economia russa, era considerata come una sorta di "assicurazione" strategica della quale Mosca avrebbe dovuto tener conto nel soppesare eventuali politiche di ingerenza o di aggressione multilivello. Ciò considerato i Paesi europei dell'ex blocco sovietico mal digerirono la costruzione del primo gasdotto Nord Stream, che con i suoi 55 milioni di metri cubi annui si attestava come l'opera infrastrutturale che esportava maggior volume di gas dalla Russia, e la prospettiva concreta di un raddoppio dei volumi di esportazione attraverso un'infrastruttura che collegasse (quasi) direttamente

Russia e Germania era considerata un vero e proprio fattore destabilizzante per la propria sicurezza nazionale.

La messa in funzione di Nord Stream 2 avrebbe determinato, inoltre, significative conseguenze anche sul piano economico: ogni Paese nel quale transiti parte delle infrastrutture di rifornimento percepisce *royalties* percentuali rispetto al volume di gas, l'Ucraina ad esempio, riferendosi ovviamente allo *status quo ante bellum*, rappresentava il principale polo di smistamento del gas russo, e avrebbe visto diminuire di circa il 40% il valore delle *royalties* percepite (Politi, 2021).




(JP Morgan via The Economist, 2022)

Gli Stati Uniti caldeggiarono l'interpretazione strategica promossa dai Paesi dell'Europa Orientale circa le conseguenze negative implicite alla realizzazione del Nord Stream 2, mettendo in atto tentativi concreti di osteggiamento alla costruzione dell'opera, mossi da diversi interessi eterogenei, ma interconnessi fra loro, fra i quali spicca quello di creare un approdo europeo per l'esportazione del proprio gas liquefatto.

Tuttavia, gli interessi prettamente economici sono orientati dalla bussola strategica che guida le scelte politiche americane nel continente europeo fin dall'intervento nella Prima Guerra Mondiale. Non permettere, cioè, che si presenti il rischio concreto di un allineamento "strutturale" fra due potenze interne al macro-continente euro asiatico la quale convergenza di capacità e interessi possa consentire loro di ambire legittimamente al controllo su tutto lo spazio continentale.

Risulta lapalissiano (ma doveroso) constatare come una solida *partnership* energetica russo tedesca da sola non potesse bastare a rappresentare un rischio concreto per l'egemonia americana sul continente, nonostante diverse fonti mediatiche polacche avessero ribattezzato il gasdotto Nord Stream 2 "Molotov-Ribbentrop bis".

Da tale presupposto ne conseguì la concreta "minaccia" di applicazione di sanzioni economiche inserita nel "Protecting Europe's Energy Security Act of 2019" firmato dal Presidente Donald Trump il 20 Dicembre 2019, mediante il quale tali sanzioni si sarebbero applicate alle navi che si stavano occupando della posa dei tubi e che convinse la società "Allseas", con sede in Svizzera, ad abbandonare il progetto.

Per quanto politiche estere di pieno contrasto agli interessi nazionali russi siano storicamente un collante fondamentale per il partito democratico e quello repubblicano negli Stati Uniti, e nonostante una distensione di facciata, più mediatica che concreta, verso il Cremlino dell'ala repubblicana che appoggiava fedelmente il Presidente Trump, furono gli stessi rappresentanti del partito repubblicano i responsabili dell'adozione di politiche sempre più restrittive mirate a impedire la concreta realizzazione e l'avvio del funzionamento del progetto Nord Stream 2.

Il 15 Luglio 2020, il dipartimento di Stato americano inserì nella sezione 232 del "Countering America's Adversaries Through Sanctions Act" del 2017 una clausola di validità retroattiva delle sanzioni per le compagnie che avessero collaborato o investito su "condotti russi per l'esportazione di energia". L'Alto Rappresentante per la Politica Estera dell'Unione Europea, Josep Borrell, bollò senza mezzi termini tale misura come una "violazione del diritto internazionale". Poco più di un mese dopo fu noto alla cronaca il tentato avvelenamento del dissidente politico russo Aleksej Naval'nyj, che contribuì a complicare un quadro politico internazionale già di per sé intricatissimo.

Negli ultimi giorni della presidenza Trump tali sanzioni furono adottate nei confronti della società russa KVT-RUS, mentre successivamente all'insediamento del nuovo Presidente degli USA Joe Biden, furono estese a nove navi della flotta Nord Stream 2 del Servizio Marittimo Russo, ma non si procedette all'applicazione di sanzioni verso la società Nord Stream AG. Ciononostante i lavori di realizzazione del progetto proseguirono fino a realizzare il 98% dell'opera, alla quale mancava di fatto solamente pochi km finali di tubature da apporre nei fondali delle acque territoriali tedesche.

Di fronte al fatto compiuto del sostanziale completamento dell'opera, considerando peraltro come Nord Stream AG avesse sostenuto una spesa di circa 9 miliardi per il progetto, sotto la guida del Presidente Biden, politico quantomeno più esperto del predecessore, gli Stati Uniti si mostrarono "pacatamente" aperti ad un dialogo costruttivo con gli alleati tedeschi finalizzato a superare l'*impasse*.

Questo fu quindi il dossier principale dell'ultimo incontro ufficiale a Washington di Angela Merkel nelle vesti di Cancelliera Federale della Germania con il Presidente degli Stati Uniti, e nel comunicato congiunto pubblicato la sera del 21 Luglio 2021 emersero i termini e le condizioni pattuite per permettere di ritirare le sanzioni americane e di deliberare le ultime operazioni per il completamento finale e la messa in funzione del Nord Stream 2. L'incontro sancì la nascita del "U.S. - Germany climate and energy partnership", formalizzato poi a Maggio 2022 in seno al G7, e prevedeva come entrambe le Nazioni sostenessero la transizione energetica eco-sostenibile dei Paese dell'Europa Orientale. Esso conteneva una particolare menzione per l'Ucraina, specificando come la Germania si impegnasse diplomaticamente a garantire il transito e la fornitura di gas russo in territorio ucraino almeno per i dieci anni successivi. In ultimo, ma assolutamente non per importanza storica, l'accordo prevedeva come in caso la Federazione Russa "utilizzi l'energia come un'arma o compia ulteriori atti aggressivi verso l'Ucraina" la Germania risponderebbe con contromisure adeguate, sanzioni economiche incluse, sia a livello nazionale sia premendo perché vengano adottate dal consesso dell'Unione Europea "per limitare le capacità di esportazione russe verso l'Europa in campo energetico" (U.S. Department of State, 2021).

Come ogni compromesso "che si rispetti", atto a regolare interessi internazionali di tale portata, l'accordo suscitò un manifesto malcontento sia sul versante russo che su quello ucraino-polacco, avanzando essi posizioni antitetiche e inconciliabili.

Diversi analisti interpretarono il nulla osta americano alla realizzazione del Nord Stream 2 come una mossa indiretta per compattare la Germania in chiave anti-cinese, considerando i crescenti flussi commerciali di *import-export* sull'asse Berlino-Pechino e il ruolo centrale che la Cina sta assumendo nell'industria digitale e dell'energia elettrica e rinnovabile. Ad oggi, possiamo riscontrare come, nello scetticismo generale che imperava fra i media e gli analisti nell'Europa occidentale, gli organi di intelligence americani furono i primi ad esternare pubblicamente informazioni circa un'invasione su larga scala del territorio ucraino pianificata dal Cremlino che aveva iniziato ad inviare un numero significativo e crescente di truppe al confine con l'Ucraina fin da Novembre 2021. La progressiva tensione sul fronte ucraino decretò l'impossibilità della messa in funzione del Nord Stream 2, dapprima temporanea, ad oggi sempre più tendente a risultare definitiva.

### 3) Yamal: il primo gasdotto sovietico a rifornire l'Europa Occidentale

La storia delle esportazioni di gas dalla Russia verso i Paesi occidentali del continente europeo affonda le radici "nel l'inizio della fine" del modello ordinatore politico del continente dalla fine della Seconda Guerra Mondiale: il primo gasdotto che interconnetteva i Paesi europei che aderirono al Patto Atlantico a quelli compresi nel Patto di Varsavia, denominato Yamal, entrò in funzione nel 1984.

Analogamente al dossier Nord Stream, anche questo destabilizzò l'equilibrio internazionale, ma a differenza di quest'ultimo la comunità di Stati europei occidentali si dimostrò ben più coesa nell'intenzione di finanziare e portare a termine un accordo che senz'altro giovava ad entrambe le parti contraenti. Da un lato la crescita esponenziale dei sistemi economici industriali europei, che ebbe luogo dagli anni '60, stava subendo un brusco arresto con ricadute avverse per le industrie manifatturiere e per la disoccupazione giovanile, riconducibile in una rilevante parte alle frequenti crisi internazionali che condizionavano il prezzo e l'offerta di idrocarburi; da parte sovietica, invece, il bisogno di immettere in un sistema sull'orlo del fallimento strutturale valuta economicamente salda, come quella occidentale, era più che mai imminente. A questo proposito enti bancari, *in primis* tedeschi, ma anche francesi, olandesi, belgi, inglesi e italiani stanziarono i fondi necessari alla realizzazione dell'opera, a fronte di un rifornimento annuo di dieci miliardi di gas alla Germania dell'Ovest, otto a Francia e Italia, cinque al Belgio, quattro ai Paesi Bassi e Austria.

La reazione statunitense al progetto fu caratterizzata da un approccio teso ad osteggiarne la realizzazione, ma analogamente al caso Nord Stream se ne registrarono due velatamente dissimili fra la presidenza democratica a guida Carter e quella successiva guidata dal repubblicano Reagan. Se il primo, alla prova dei fatti, non mise in atto tentativi concreti di pressione diplomatica, comprendendo forse come in termini di interdipendenza fosse l'Unione Sovietica l'anello debole vincolato per ragioni esistenziali ad assecondare gli interessi europei, la presidenza Reagan al contrario, tre anni prima dell'effettiva messa in funzione del gasdotto, mosse diverse azioni sottese al boicottaggio del completamento dell'opera, comprese sanzioni economiche unilaterali, tentativi di sabotaggio materiale dell'infrastruttura e pressioni diplomatiche verso l'Arabia Saudita, finalizzate a un abbassamento del prezzo degli idrocarburi.

La risposta europea, al tempo, fu netta e coesa verso quella che venne percepita come un'ingerenza non tollerabile persino se mossa dagli Stati Uniti d'America, rimarcando come il completamento dei lavori e la messa in funzione del gasdotto non fosse negoziabile, e di fatto portò alla cancellazione delle sanzioni da parte americana.

Risultano particolarmente emblematiche le dichiarazioni che furono rilasciate dal Presidente francese Mitterand, ancor più se messe in relazione alla situazione di crisi odierna, riguardo le sanzioni implementate dal governo americano: "*Non siamo in guerra; il blocco economico è un atto di guerra, che d'altronde non riesce mai, tranne che non sia la prima fase di una guerra vinta*" (Politi, 2021).

A questo proposito è bene precisare alcune caratteristiche intrinseche delle risorse gasiere: esse sono caratterizzate da costi di produzione nettamente inferiori rispetto a quelli di trasporto, che prevede un *iter* particolarmente complesso e dispendioso se lo si vuole attuare mediante interconnessioni marittime, ovvero attraverso un processo di liquefazione a una temperatura di almeno 160 gradi sottozero, per poi essere trasportato su navi appositamente progettate e predisposte, dette metaniere. Il costo del trasporto si abbassa notevolmente se viene attuato per mezzo di gasdotti, a patto che le spese stanziate per la costruzione di tali infrastrutture vengano ammortizzate nel tempo da quantità di rifornimenti ingenti e prolungate tali da giustificarne l'investimento iniziale.

Uno dei celebri parallelismi che descrive a pieno quale sia il peso strategico e geo-economico della costruzione di un gasdotto transfrontaliero è quello che lo definisce al pari di un matrimonio fra i due o più Stati interconnessi.

La costruzione di tali infrastrutture lega, infatti, i destini degli attori statali coinvolti che di fatto accettano come le scelte politiche e le eventuali destabilizzazioni interne di una delle due parti contraenti dell'accordo possano condizionare direttamente le variabili economiche e strategiche della propria traiettoria geopolitica, ovviamente essendo ciò direttamente proporzionale alla quantità di gas importata o esportata.

Risulta quindi centrale constare come una delle conseguenze dirette maggiormente significative dell'invasione russa di larga scala sul territorio ucraino sia il cambio radicale di un paradigma considerato di mutuo beneficio da Federazione Russa e Germania, con evidenti ricadute a pioggia sui comparti industriali di tutti i Paesi europei che usufruivano, direttamente o indirettamente, di rifornimento di gas a prezzo contenuto, essendo l'offerta sul mercato congrua rispetto alla domanda.

Ciò che quindi è rappresentato plasticamente dal sabotaggio delle condutture dei gasdotti Nord Stream è la frattura scomposta fra Germania e Russia, "matrimonio" combinato da interessi di natura strategica, economica e di prossimità territoriale, che sembrava essere destinato a raddoppiare la propria dote in termini di volume di gas, mentre oggi si trova ridotta ben al di sotto del minimo sindacale, ciò a prescindere se la fine di questo matrimonio sia frutto di separazione consensuale, riconducibile al volere di un Don Rodrigo determinato ad ostacolarlo, o al condizionamento di entrambi i fattori.

## 4) Conclusioni

Per comprendere a pieno la moltitudine di effetti diretti e indiretti che la scelta russa di compiere un'invasione su larga scala in terra ucraina, la notte del 24 Febbraio 2022, comporterà (e sta già comportando) sul piano internazionale, occorrerebbe adottare un approccio storiografico che soltanto il tempo potrà restituirci, tuttavia è già possibile focalizzare come per la Germania, la Federazione Russa e la moltitudine di Paesi che componevano il Patto di Varsavia essa rappresenti un vero e proprio crocevia della propria storia moderna. Il progetto tedesco, volto a perseguire un'interdipendenza con un sistema economico, politico e valoriale progressivamente sempre più dissimile dal proprio come quello russo, ne esce fortemente ridimensionato, a prescindere se intrapreso non soppesando sapientemente gli interessi economici rispetto a quelli strategici o coscienti e sicuri di come favorire tale interdipendenza potesse essere un'arma per placare i piani revisionisti del Cremlino. Le ferite riportate dalla coppia di gasdotti Nord Stream evidenziano come l'ultimo progetto infrastrutturale, che potesse giustificare un appiglio concreto per le possibilità che tale visione si realizzi, sia morente.

Oltre a Russia ed Ucraina, che per ovvie ragioni usciranno profondamente colpite sul piano economico, sociale e demografico, il perdurare di questa guerra ci restituirà una Germania radicalmente destabilizzata nelle proprie certezze strutturali e solo la capacità di formularne di nuove

potrà assicurarle lo status di potenza leader in Europa sul piano politico e non più esclusivamente economico.

Rispetto allo *status quo ante bellum* i tedeschi dovranno rimodellare profondamente e repentinamente il proprio assetto energetico, economico e industriale interno, considerando come dalla prospettiva di divenire il maggior polo di ricezione e smistamento di gas in Europa, conseguentemente alla mai avvenuta messa in funzione del Nord Stream 2, si è passati ad una realtà nella quale la Germania risulta uno degli Stati europei maggiormente colpiti dalla crisi energetica in atto.

L'annunciato riarmo nazionale volto a rendere nelle disponibilità di Berlino il maggior esercito dell'Unione Europea, per il quale verrà stanziata la roboante cifra di 100 miliardi di euro, e le ripetute dichiarazioni riguardo al bisogno di un'Europa "geopolitica", seppur intrisi di vacuo stile propagandistico, sembrano quantomeno riflettere la volontà tedesca di ridiscutere i modelli politici imperanti dalla fine della Guerra Fredda.

Il Cancelliere Scholz, in un discorso tenuto il 29 Agosto presso l'Università Carolina di Praga nella capitale ceca, ha voluto enunciare al mondo quali, nella sua visione, debbano essere i valori trainanti di questa nuova fase. In un eloquio volto a nobilitare le comuni radici europee di integrazione multiculturale e di difesa del valore della libertà dall'ingerenza delle autarchie, il Cancelliere tedesco ha rimarcato come un momento di profonda crisi come quello attuale debba essere interpretato dai Paesi dell'Unione come la possibilità per l'Europa di abbracciare una sovranità inedita, così definendola: "*European sovereignty means in essence is that we grow more autonomous in all fields; that we assume greater responsibility for our own security; that we work more closely together and stand yet more united in defence of our values and interests around the world*". Ha inoltre aggiunto una particolare interpretazione di realismo politico: "*Realpolitik must mean involving friends and partners with shared values and supporting them in order to be strong in global competition through cooperation*" (Scholtz, 2022).

La scelta della città di Praga, per enunciare il proprio panegirico sui nuovi valori che dovranno guidare le azioni politiche dei governi europei, è intrisa di valore storico: il fondatore dell'Università Carolina, Carlo IV, che rappresentava un europeo *ante litteram* secondo Scholtz, il legame della città con lo sviluppo dell'Umanesimo europeo, la defenestrazione che fu la scintilla per il principio della Guerra dei Trent'anni dalla quale originò un nuovo modello ordinatore del continente, la Pace di Vestfalia, ma anche l'eterna onta dell'occupazione nazista e "La tragedia dell'Europa Centrale" che all'indomani del secondo conflitto mondiale si trovò divisa dall'occidente, sono riferimenti che emergono direttamente delle parole del cancelliere.

Di fronte a una crisi che pone ai decisori politici europei domande alle quali da troppo tempo sono stati chiamati a dare risposta, la prospettiva di una cooperazione rafforzata fra popoli europei e, in particolare, fra popolazioni germaniche e slave, sembra essere la proposta caldeggiata, o quantomeno mediaticamente esposta da Berlino per affrontare le dure implicazioni sottese al ritorno di un conflitto interno ai confini europei.

Ciò assume particolare rilevanza considerando come alcuni Stati dell'Europa Orientale sono chiamati a interpretare il delicato ruolo di Paesi contigui ad una frontiera mediante la quale l'import – export di materie prime e gli scambi commerciali non saranno verosimilmente ripristinati quantomeno nel breve-medio periodo, inficiando sulle condizioni economiche e sociali, mentre gli investimenti per sostenere l'apparato militare e securitario dovranno essere gioco forza aumentati rispetto allo *status quo ante bellum*.

**Bibliografia e Sitografia**


- "Goodbye, Merkel", Alessandro Politi e Letizia Tortello, 2021
- "Gas e potere - Geopolitica dell'energia dalla guerra fredda a oggi", Leonardo Bellodi, 2022
- "Ernesto Massi e Karl Haushofer: la scienza alla conquista della politica", Matteo Marconi, Rivista dell'istituto di alti studi in geopolitica e scienze ausiliarie, 2016
- "Multi-Modal Transportation and Commodity Flow Modeling in N-ABLE" Mark A. Ehlen, National Infrastructure Simulation & Analysis Center, 2006
- "Noi tedeschi vogliamo la pace ma otterremo solo più guerra", Andreas Heinemann-Grüder, "Tutto un altro mondo", Limes, 2022.
- "Seismologists suspect explosions damaged undersea pipelines that carry Russian gas", George Brumfiel, Rob Schmitz, Public Broadcasting Service, 2022 https://www.gpb.org/news/2022/09/27/seismologists-suspect-explosions-damaged-undersea-pipelines-carry-russian-gas.
- "L'attacco ai gasdotti Nord Stream: il bersaglio è l'Europa", Gianandrea Gaiani, Analisi Difesa, 1 ottobre 2022. https://www.analisidifesa.it/2022/10/lattacco-ai-gasdotti-nord-stream-lobiettivo-e-leuropa/
- "Nord Stream leaks caused by deliberate actions, Denmark's prime minister says", Jacob Gronholt-Pedersen, Stine Jacobsen, Nikolaj Skydsgaard, Reuters, September 27, 2022. https://www.reuters.com/business/energy/nord-stream-leaks-caused-by-deliberate-actions-denmarks-prime-minister-says-2022-09-27/
- "Nord Stream sabotage mapped: How Putin could have carried out the attack", Dominic Nicholls, The Telegraph, September 28, 2022. https://www.telegraph.co.uk/world-news/2022/09/27/how-putin-could-have-carried-nord-stream-attack-may-have-set/
- "Sabotaged Pipelines and a Mystery: Who Did It? (Was It Russia?)", Katrin Bennhold, David E.Sanger, The New York Times, Sept. 28, 2022. https://www.nytimes.com/2022/09/28/world/europe/pipeline-sabotage-mystery-russia.html
- "Estimate of Total Methane Emissions from the Nord Stream Gas Leak Incident - Draft Working Paper" International Methane Emissions Observatory (IMEO), United Nations Environment Programme (UNEP), 20 Feb. 2023. https://wedocs.unep.org/handle/20.500.11822/41838
- "Confirmed sabotage of the Nord Stream gas pipelines", Säkerhetspolisen -Swedish Security Service, 18 November 2022 https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/news/news/2022-11-18-confirmed-sabotage-of-the-nord-stream-gas-pipelines.html
- "Protecting EuropÈs Energy Security Act of 2019", USA 116th Congress (2019-2020). https://www.congress.gov/bill/116th-congress/senate bill/1441?q=%7B%22search%22%3A%5B%22nord+stream+2%22%5D%7D&r=1&s=4
- -"Joint Statement of the United States and Germany on Support for Ukraine, European Energy Security, and our Climate Goals", U.S Department of State, July 21, 2021. https://www.state.gov/joint-statement-of-the-united-states-and-germany-on-support-for-ukraine-european-energy-security-and-our-climate-goals/
- "German go-ahead for China's Cosco stake in Hamburg port unleashes protest", Andreas Rinke, Jan Schwartz, Reuters, October 26, 2022. https://www.reuters.com/markets/deals/german-cabinet-approves-investment-by-chinas-cosco-hamburg-port-terminal-sources-2022-10-26/

- "We don't want to decouple from China, but can't be overreliant" Federal Chancellor Olaf Scholtz, Politico, 2022
  https://www.bundesregierung.de/breg-en/search/chancellor-guest-article-politico-china-2139576
- "Speech by Federal Chancellor Olaf Scholz at the Charles University in Prague on Monday, 29 August 2022", The German Federal Government, 2022
  https://www.bundesregierung.de/breg-en/news/scholz-speech-prague-charles-university-2080752

Pagina bianca

# La Cina nella guerra russo-ucraina

## Introduzione

Negli ultimi anni, la Repubblica Popolare Cinese (RPC) ha dimostrato grande abilità e determinazione nel creare nuovi legami diplomatici e nell'esercitare le sue capacità di *soft* e *hard power* per trasformare situazioni svantaggiose in guadagni. Un esempio importante di questa tattica è rappresentato dalle numerose interazioni con i Paesi dell'Europa orientale. Pur essendo storicamente avversi a qualsiasi forma di comunismo, questi Paesi sono stati attratti dai vantaggi economici offerti da Pechino e si sono impegnati in intensi rapporti con la RPC, che in quest'area è riuscita a svolgere il ruolo di controparte delle potenze occidentali (Brattberg, 2021). Questo atteggiamento della RPC, di posizionarsi in opposizione, ma non in confronto diretto con gli Stati Uniti e l'Unione Europea, è stato chiaramente visibile fin dall'inizio del conflitto russo-ucraino. Pur sostenendo l'integrità territoriale dell'Ucraina e non avendo mai riconosciuto l'annessione di Donetsk e Luhansk, la RPC non ha in alcun modo condannato l'invasione russa, né ha mai sostenuto o partecipato alle sanzioni internazionali contro la Russia. In questo modo, ha mantenuto la sua posizione filo-russa "neutrale", che ha fornito alla RPC un notevole potere diplomatico e crescita economica.

## Relazioni sino-russe pre e post scoppio del conflitto

Per comprendere al meglio la posizione della Cina durante il conflitto, è indispensabile avere una solida conoscenza delle relazioni economiche e diplomatiche che condivide con la Russia. Inizialmente i due Paesi comunisti non avevano rapporti stabili. Questi erano anzi caratterizzati da atteggiamenti irrispettosi e negato sostengo in situazioni di bisogno. Sostegno che si presumeva naturale dati i valori politici comuni. Questa situazione ha raggiunto il suo apice con la scissione sino-russa della fine degli anni Cinquanta, che ha reso impossibile qualsiasi tipo di ipotetica relazione amichevole tra i due Paesi, portandoli fino a uno stato di aperta ostilità. Tuttavia, con la dissoluzione dell'Unione Sovietica nel 1992, i due Paesi ripresero la loro lunga collaborazione. Gli anni successivi alla dissoluzione dello Stato sovietico videro un graduale miglioramento delle loro relazioni, con una marcata accelerazione della cooperazione negli ultimi vent'anni. Ciò è testimoniato dalla firma del "Trattato di buon vicinato e di cooperazione amichevole" nel 2001, con il quale intesero rafforzare ulteriormente la loro *partnership*, e nello stesso anno dall'adesione della Russia all'Organizzazione di cooperazione di Shanghai (SCO), un'organizzazione eurasiatica incentrata sulla cooperazione politica, economica, di sicurezza e di difesa. Nel 2004, i due Paesi risolsero, inoltre, le loro dispute territoriali: una delle controversie più intense durante gli anni della separazione. Sebbene la Russia abbia sempre cercato di mantenere la sua "natura europea", evitando relazioni forti con i suoi vicini orientali, ha scartato questa nozione e ha abbracciato la sua posizione mediana tra est e ovest nel 2013-2014, quando, dopo la presa della penisola di Crimea, ha subito sanzioni americane e ha costruito un legame più stretto con la RPC. Ad oggi, la qualità dei rapporti fra i due Paesi ha raggiunto il miglior livello mai stabilito, in parte grazie alle simili posizioni critiche che entrambi nutrono nei confronti degli Stati Uniti in merito alle dispute territoriali (il controllo del Mar Cinese Orientale per la RPC e la penisola di Crimea per la Russia).

Questa relazione ha avuto un effetto profondo sulle economie e sulla cooperazione militare dei due Paesi. Come si può vedere nella Figura 1, dal 2000 al 2021 il commercio annuale della RPC con la Russia (solo le esportazioni) è cresciuto di otto volte, passando da meno di 10 miliardi di dollari a più di 65 miliardi di dollari, soprattutto per quanto riguarda i prodotti e le attrezzature meccaniche ed elettriche e, in particolare, i prodotti ad alta e nuova tecnologia.

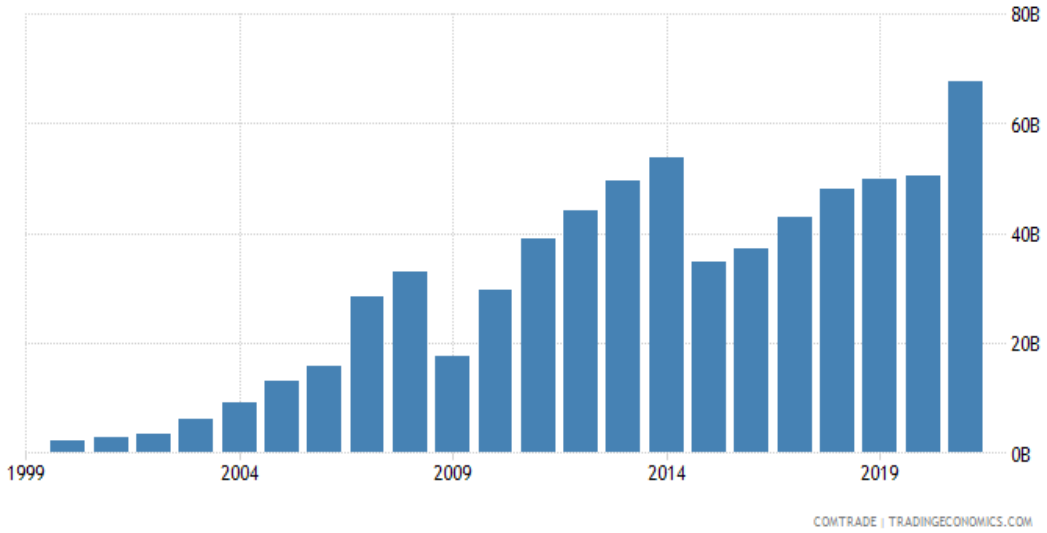



*Figure 1 China Exports to Russia 2000-2021*

Sul fronte militare si è registrata la stessa tendenza, con un numero crescente di esercitazioni congiunte, la prima delle quali si è svolta nel 2005 e l'ultima alla fine del 2022, e un costante scambio di armamenti e prodotti *high-tech*. Solo nel primo decennio del XXI secolo, la RPC ha aumentato l'acquisto di armi dalla Russia del 258% rispetto al decennio precedente; attualmente ha acquistato l'81% delle sue importazioni di armi dalla Russia (SIPRI, 2022). Un esempio di rilievo di acquisizione militare da parte della RPC è stato l'acquisto dell'incrociatore pesante porta-aerei Varyag nel 1998; il naviglio ha subito un'ampia modernizzazione dello scafo, del radar e dei sistemi elettronici divenendo nel 2012 la Liaoning, prima portaerei cinese. Inizialmente usata come nave scuola, nel 2016 diviene pienamente operativo (China Power Team, 2015).

Dall'inizio della guerra russo-ucraina le relazioni economiche e diplomatiche tra la Russia e la RPC sono cambiate in modo significativo, soprattutto riguardo l'importazione cinese di petrolio grezzo. Inizialmente le aziende e le banche cinesi hanno evitato di rinnovare o stringere nuovi accordi con le aziende russe, anche se a prezzi più bassi, per mantenere una posizione neutrale e non essere viste come filo-russe dalla comunità internazionale (Tan & Aizhu, 2022). Dalla tarda primavera del 2022, però, con il perdurare della guerra e delle sanzioni dell'UE, il petrolio russo è stato dirottato dall'Europa verso Cina, India e Turchia (Cinda Securities, 2022). In estate, la RPC è diventata il più grande importatore di petrolio russo, acquistandolo in *renminbi*. Se, inoltre, si prende in considerazione il gas naturale, ad oggi la Russia è il secondo esportatore verso la Cina, secondo solo al Turkmenistan, e con gli accordi firmati all'inizio del 2022 per la costruzione di un secondo gasdotto "Power of Siberia 2" ha la possibilità di diventare il suo principale fornitore (Jian, 2022). La costruzione e l'ampliamento di gasdotti e oleodotti è vista con favore dalla RPC, soprattutto se paragonata alle spedizioni di gas naturale liquefatto e petrolio che presentano un rischio strategico più elevato per il fatto che dovendo passare attraverso lo stretto di Malacca sarebbero un facile bersaglio per gli embarghi e le sanzioni energetiche di Stati Uniti e Unione Europea. Alla luce di ciò, secondo il Professor Zhao Huasheng, esperto cinese della Russia, diventa imperativo per la RPC mantenere un rapporto amichevole con la Russia e conservare gli attuali livelli di fiducia e di *partnership*. Qualsiasi azione di condanna o sanzione da parte di Pechino verrebbe vista come una pugnalata alle spalle e distruggerebbe tutta la fiducia fino ad ora costruita. È da considerare, inoltre, che la RPC è circondata dalla strategia americana sull'indo pacifico ed ha bisogno di un *partner* nell'area euroasiatica. Nell'ipotesi di un'eventuale *escalation* nello stretto di Taiwan, sarebbe imperativo per la RPC avere la Russia come retrovia strategica stabile.

**Vuoto di potere diplomatico**

Dal febbraio 2022, l'attenzione dei Paesi occidentali si è concentrata sulla guerra in Ucraina, lasciando ad altre Nazioni lo spazio per riempire questo vuoto di potere diplomatico. Mentre l'Unione Europea e gli Stati Uniti si sono schierati contro la Russia, trasformando quello che era un conflitto regionale in un crisi molto più ampia, altri Paesi come la Cina e l'India non hanno sentito alcuna necessità di partecipare attivamente al conflitto e si sono limitati a pronunciarsi sulla situazione. Emblema di questo sentimento comune sono state le parole del Ministro degli Affari Esteri indiano, S. Jaishankar, pronunciate durante la 17ª edizione del GLOBSEC Bratislava Forum in Slovacchia: "*Da qualche parte l'Europa deve uscire dalla mentalità secondo cui i problemi dell'Europa sono i problemi del mondo, ma i problemi del mondo non sono i problemi dell'Europa. Che se si tratta di te, è tuo, se si tratta di me è nostro"*.

Molti Stati condividono questo pensiero e, a loro volta, hanno iniziato a modificare la propria posizione, allontanandosi dagli Stati Uniti e avvicinandosi a concorrenti analoghi, soprattutto la RPC. La guerra ha costretto Stati Uniti e EU a concentrare la propria attenzione sulla Russia e sulla situazione in Ucraina, nel mentre, siccome già da tempo si percepiva il fatto che gli Usa si trovano in uno stato di *overstretching* diplomatico, hanno dato spazio ad altri Stati di interagire con nuovi attori. Prima fra questi è stata la RPC che, utilizzando la sua posizione mediana, ha saputo sfruttare i vuoti lasciati da gli USA. Alcuni chiari esempi di questa tendenza sono il nuovo accordo mediato dalla Cina tra l'Arabia Saudita e l'Iran (Baker, 2023), l'apertura ufficiale delle relazioni diplomatiche tra l'Honduras e la RPC che comporterebbe il disconoscimento da parte dell'Honduras di Taiwan come Stato (Reuters, 2023) e, infine, la sua posizione come unico mediatore in queste ultime fasi della guerra.

**Un anno dallo scoppio della guerra**

Ad un anno dello scoppio della guerra in Ucraina i rapporti tra Russia e Cina mantengono la loro traiettoria positiva. Come viene evidenziato nella conferenza della Carnegie Endowment for International Peace (2023), il conflitto non ha intaccato in alcun modo la stabile collaborazione tra i due Paesi. Al contrario, la loro *partnership* e la sua linea di tendenza sono rimasti inalterati. Sta diventando sempre più fitta, grande ed asimmetrica, con una Cina che ha sempre più influenza, più anzianità ed opzioni in questo partenariato.

Alla luce di questo rafforzamento delle relazioni asimmetriche, la domanda che molti osservatori si sono posti è se la Cina medierà la fine della guerra, a suo favore, o se continuerà a lasciare che si svolga. Ci sono molti fattori divergenti che rendono possibili entrambi i risultati: i benefici economici e l'approvvigionamento energetico riscontrati dalla Cina, il completamento della "Belt and Road Initiative" (BRI) e la questione dell'area dell'indo-pacifico.

Per quanto riguarda i benefici economici che la RPC è riuscita a trarre dal conflitto ucraino, si tratta di un fattore che può entrare in gioco in entrambi gli scenari. Se da un lato la RPC è riuscita a mantenere la propria crescita economica dopo la devastante politica dello "zero-covid" grazie al petrolio a basso prezzo proveniente dalla Russia e all'espansione nel mercato russo delle imprese cinesi. Dall'altro l'India, uno dei sui principali concorrenti, è riuscita a sfruttare questi stessi vantaggi a proprio favore (Hale, 2023). Ciò costituisce un grave rischio per l'economia cinese, la quale sta avendo difficoltà a stare al passo con la crescita economica indiana.

Per quanto riguarda la relazione tra la guerra e la BRI, il fattore principale in gioco è la perdita di fiducia nella Cina da parte dei Paesi dell'Europa orientale. Come si può vedere nella Figura 2, un elemento chiave per la rotta terrestre sono le infrastrutture nell'Europa orientale. Nell'ultimo decennio Pechino e i suoi partner hanno annunciato, infatti, centinaia di investimenti per decine di miliardi di euro in quest'area (Matura, 2021). Con l'inizio della guerra in Ucraina, molti dei partner cinesi nell'area si sono ritirati e sono reticenti ad accettare nuovi investimenti dalla RPC, data la sua posizione nel conflitto. Questo potrebbe considerarsi uno dei fattori chiave per cui la

RPC potrebbe volere una conclusione celere al conflitto, in modo da recuperare la fiducia persa nell'area e continuare con uno dei progetti fondamentali portati avanti dal Presidente Xi.


Figura 2

Un elemento chiave per questa discussione è, infine, la situazione nell'area indo-pacifica. Fin dall'inizio della sua amministrazione, il Presidente Biden ha chiarito che la regione indo-pacifica sarebbe stata al centro della nuova strategia estera americana. L'inizio della guerra ha fatto sì che molti si domandassero se gli Stati Uniti sarebbero stati in grado di seguire questa linea (Baronio, 2022). Si percepisce, difatti, un certo livello di timore da parte di Taiwan, Giappone e Corea del Sud che prevedono in caso di una *escalation* della situazione nel Mar Cinese, gli USA troppo impegnati nel conflitto ucraino per fornire un adeguato sostegno.

Come evidenziato, la RPC si potrebbe muovere in entrambe le direzioni a seconda di come evolverà la situazione nei prossimi mesi. Bisognerà prestare particolare attenzione ai recenti incontri tra il Presidente Xi Jinping e il Presidente Putin a Mosca, e al recentissimo incontro tra il Presidente Zelensky e il Primo Ministro giapponese Kishida, visita inaspettata avvenuta subito dopo il vertice tra Corea del Sud e Giappone (Kim et al., 2023).

**Bibliografia**


- Appel, H., & Liu, B. (2022, October 17). *The limits of the Russia-China Partnership after the Ukraine invasion*. PONARS Eurasia. Retrieved March 21, 2023, from https://www.ponarseurasia.org/the-limits-of-the-russia-china-partnership-after-the-ukraine-invasion/
- Baker, P. (2023, March 13). *Chinese-brokered deal upends Middle East Diplomacy and challenges U.S.* The Japan Times. Retrieved March 23, 2023, from https://www.japantimes.co.jp/news/2023/03/13/asia-pacific/china-middle-east-diplomacy-challenges-us/
- Baronio, F. (2022, March 22). *The consequences of the war in Ukraine for the Indo-Pacific*. ISPI Italian Institute for International Political Studies. Retrieved March 22, 2023, from https://www.ispionline.it/en/publication/consequences-war-ukraine-indo-pacific-34377
- Brattberg, E., Le Corre, P., Stronski, P., & De Waal, T. (2021, October 13). *China's influence in southeastern, Central, and Eastern Europe: Vulnerabilities and Resilience in Four Countries*. Carnegie Endowment for International Peace. Retrieved March 15, 2023, from https://carnegieendowment.org/2021/10/13/china-s-influence-in-southeastern-central-and-eastern-europe-vulnerabilities-and-resilience-in-four-countries-pub-85415
- China Power Team. (2020, August 26). *How does China's first aircraft carrier stack up?: China Power Project*. ChinaPower Project. Retrieved March 21, 2023, from https://chinapower.csis.org/aircraft-carrier/
- China Power Team. (2022, May 12). *How has the China-Russia relationship evolved?* ChinaPower Project. Retrieved March 21, 2023, from https://chinapower.csis.org/history-china-russia-relations/
- Haenle, P., Gabuev, A., Li, M., & Hoang, T. H. (2023). In *China-Russia Relations One Year into the Ukraine War*. Retrieved March 21, 2023, from https://carnegieendowment.org/2023/02/15/china-russia-relations-one-year-into-ukraine-war-event-8029.
- Hale, E. (2023, February 24). *How China and India's appetite for oil and gas kept Russia afloat*. Energy | Al Jazeera. Retrieved March 22, 2023, from https://www.aljazeera.com/economy/2023/2/24/how-china-and-indias-appetite-for-oil-and-gas-kept-russia-afloat
- Jian, Y. (2022, December 14). *The economic meaning of the Russia-Ukraine War for China*. DIIS. Retrieved March 21, 2023, from https://www.diis.dk/en/research/the-economic-meaning-of-the-russia-ukraine-war-china
- Kashin, V. (2022, June 15). *Ukraine's losses are China's gains*. East Asia Forum. Retrieved March 21, 2023, from https://www.eastasiaforum.org/2022/06/16/ukraines-losses-are-chinas-gains/
- Kim, E., Szechenyi, N., Cha, V., & Johnstone, C. B. (2023, March 15). *The kishida-yoon summit meeting: A new start for Japan-Korea relations*. CSIS. Retrieved March 23, 2023, from https://www.csis.org/analysis/kishida-yoon-summit-meeting-new-start-japan-korea-relations
- Matura, T. (2021, April). *Chinese Investment in Central and Eastern Europe. A reality check.* Central and Eastern European Center for Asian Studies. Retrieved March 22, 2023, from https://www.china-cee-investment.org/_files/ugd/72d38a_373928ea28c44c7f9c875ead7fc49c44.pdf

- Olson, S. (2022, March 22). *China will gain economically from the Ukraine War. What might it lose?* Hinrich Foundation. Retrieved March 21, 2023, from https://www.hinrichfoundation.com/research/article/us-china/china-gain-economically-ukraine-war/
- Reuters. (2023, March 15). Honduras president says government to seek official relations with China. *The Japan Times*. Retrieved March 20, 2023, from https://www.japantimes.co.jp/news/2023/03/15/world/honduras-china-diplomatic-ties/.
- SIPRI. (2022). *SIPRI Arms Tranfers Database, Chinese Imports.* Stockholm International Peace Research Institute. Retrieved March 21, 2023, from https://www.sipri.org/databases/armstransfers
- Tan, F., & Aizhu, C. (2022, April 7). *Exclusive: China state refiners shun new Russian oil trades, teapots fly under radar*. Reuters. Retrieved March 21, 2023, from https://www.reuters.com/business/energy/exclusive-china-state-refiners-shun-new-russian-oil-trades-teapots-fly-under-2022-04-06/
- Webster, J. (2023, January 9). *China-russia relations: 4 takeaways from 2022*. – The Diplomat. Retrieved March 21, 2023, from https://thediplomat.com/2023/01/china-russia-relations-4-takeaways-from-2022/
- Zhao, H. (2022, August 21). 赵华胜：*中俄关系：走出俄乌冲突的迷雾 (pinyin: Zhàohuáshèng: Zhōng é guānxì: Zǒuchū é wū chōngtú de míwù).* Aisixiang. Retrieved March22, 2023, from Zhao Huasheng: China-Russia relations: out of the fog of the Russian-Ukrainian conflict_Love thought (aisixiang.com)

# The geo-strategic impact of the Russia-Ukraine war on the international system and in the Mediterranean Basin: security threats and lessons learnt

## The wider frame of a changing international system

Russia's invasion of Ukraine has produced multiple effects at international but also regional levels: in addition to the rising death toll due to the escalation of the conflict and the increasing involvement of global powers in various capacities, the global economy and energy supply chains have been adversely affected with disastrous impacts on energy and food security. The world has yet to recover from the effects of the Covid-19 pandemic, and the hostilities between Russia and Ukraine have exacerbated the rise in energy prices, food shortages, inflation and receding markets.

Furthermore, there are different security threats that arise from the conflict which affected and, probably, will continue to affect the global geopolitical architecture for a long time.

Does the war just amplify preexisting trends? Is it a result or a cause of current ongoing transformations? Are its implications systemic and far-reaching both geographically and temporally, or are they overhyped and will soon be treated as a regional issue of European security? What concrete effects does the war have on the various domains of international peace and security?

## A) Starting from a geostrategic and systemic approach:

### 1. The war as a game-changer for the West

Russia's full-scale invasion of Ukraine brought open conventional war onto European soil for the first time since the end of the Second World War. We have perceived the conflict as a world and disruptive game-changer, because we were not used anymore to a real conventional conflict. On the eve of the first year of the war, it is possible to state that this conflict could have systemic consequences, above all, for the European political order.

### 2. A multipolar system

Since the world is not Eurocentric anymore, we should inscribe the Ukrainian war within the current geopolitical shift of the international system. The increasing multipolarity of the world and the geopolitical and military rise of China beyond the Pacific region (i.e. the growing Chinese engagement towards the Middle East, Africa, and the Mediterranean Basin with the Belt and Road Initiative) have already affected the former international balance of power, in a more structural way than Russian assertivity of these recent years. It provoked a sort of "repolarization" and growing tensions between the two super-power peer-competitors, that is the US and China with their system of alliances and relations.

### 3. US, China and Russia: a new "strategic triangle"?

The US, Russia and China represent the three main geopolitical actors at a global level; to the point that their initiatives and interactions have induced many political analysts to wonder if we are assisting to a new version of the famous "strategic triangle" of the Seventies. There is no doubt that any change in the interaction among the three elements of this triangle provokes a deep alteration in the balance of power within the international system. It is still difficult to assess how the current conflict is affecting the strategic triangle, but there is a wide consensus among analysts that it may

increase the convergence between Russia and China as strategic antagonists of the US. It is even more complex to make an assessment on the effect of these changes for the MENA region.

Here some hints:

- the Russian difficulties in the war might force Moscow to reduce and rebalance its activities in the wider Mediterranean;
- at the same time, China's presence is always growing in Africa and in the MENA countries, despite being more focused on commercial and economic ties rather than at a strategic-military level.

It is still unclear if Russia will try to use China as a sort of equalizer against the US and the West, or if the Russian and Chinese thrusts of geoeconomic and geostrategic penetration in the region are too different in kind and follow two different goals to be in some way strategically interconnected.

**B) Which are the effects of Ukraine war at a security level?**

1. **Repolarization, hard security approach and a new European order**

The repolarization and growing tensions between the US, China and Russia, the bolding activity of single regional powers and the war in Europe triggered a general return of the hard security approach, with the remilitarization of Germany, Poland and a marked increasing of European defense budgets. According to some analysts, it also represents the end of the European security system as set out in the final declaration of the Conference on Security and Co-operation in Europe signed in Helsinki in 1973.

Even more, this war is provoking a shift in the political and military pivot of Europe eastward. EU has supported Ukraine by sending military equipment and training to the Ukrainian Armed Forces (i.e., the EUMAM – European Union Military Assistance Measures Ukraine). However, this repolarization has also paved the way for the formalization of a new Strategic Compass for Security and Defence. This shift – which might become structural and with long-term effects well beyond the reasonable end of the Ukrainian war – will probably reduce the importance of the Euro-Mediterranean member states in favor of the central Eastern ones, especially Germany, Poland and the Baltic states. It has also reduced Western attention to other long-lasting crises such as the ones in Libya, Syria and Afghanistan. Among all the consequences of the Russian invasion of Ukraine, it is important to emphasize the effects of the already mentioned remilitarization of the West and the predominance of the central Eastern region within the European Union.

2. **The threat to the Cold War concept of deterrence**

An extremely worrying effect of the war and the NATO indirect involvement in the war is the hypothesis of a possible use of tactical short/medium range (counter-force) atomic weapon against Ukrainian troops, explicitly evoked by Russia.

Despite being considered unlikely, the risk of a nuclear escalation cannot be ruled out. Nuclear crises in the Cold War, such as the Berlin Blockade in 1948, the Korean War in 1950-53, the Cuba crisis in 1962 and the Yom Kippur War in 1973, pointed out that ground counter-offensives increase the possibility of a nuclear escalation between countries at war that share common borders. In the Ukrainian case, a possible reconquest of Donbass and/or Crimea or the use of Western weapons to attack strategic targets in Russia, might pave the way for Moscow to dramatically escalate.

This potential threat has re-launched the debate on the risk of the use of nuclear weapon and nuclear proliferation. Here few brief bullet points:

- A hypothetical use of a tactical counter-force weapon by Russia will be extremely dangerous since, in some way, it might legitimize the use of a tactical nuclear weapon during a

conventional conflict. A perception which represents a direct blow to the deterrence architecture, elaborated during the Cold War, which was based on the "impossibility" of the use of nuclear weapons. It might also have a triggering effect on other conflicts and countries;

- The current repolarization, intertwined with the technological development, might have a proliferation effect at a global level and specifically in sensitive areas, i.e., the Asia Pacific region (China military aggressivity, technological capability by Japan and South Korea, perception of a US decline and so on).

The increasing unstable multipolarity of the international system does not allow an inclusive and shared definition of a global order. In this scenario, the world nuclear balance might lose its strategic stability with an increased number of states being formal or informal members of the nuclear club (official nuclear powers or with latent nuclear capability).

- Focusing on our region, the collapse of Treaty on the Non-Proliferation of Nuclear Weapons (NPT), might also have consequences for the MENA region:
  - this area has a peculiarity: it is one of the few large regions without a formal nuclear state; however, there is a regional power, that is Israel, which maintains its nuclear opacity policy with a still unclear nuclear strategic doctrine. And there are states, such as the Islamic Republic of Iran, that are pursuing a latent nuclear capability which represents a new kind of informal proliferation;
  - in the past, there were several attempts to create a nuclear weapons-free zone (NWFZ) for the Middle East since geographical proximity and extreme polarization represents both an effective danger and a trigger for proliferation.

In the current situation, when the international architecture of nuclear safety is under stress, we should wonder if that debate is only an outdated vision of the past or the threat of a new global proliferation might relaunch it, giving it a new vitality.

## C) Which are the effects of Ukraine war at a regional level?

### 1. The Mediterranean: a region under stress

As already underlined, the shift of the center of gravity towards East, both of the NATO and the EU, reduces the importance of the Mediterranean Basin; it would likely be a systemic shift with long-term effects. This new European order impacts on a Mediterranean already under stress for a plurality of well-known causes:

- the real or perceived American disengagement in the region, which began under the Obama presidency, seems evident from the uncertain strategy carried out by Washington in Syria and in Libya;
- in recent years EU has been an ineffective actor in the Mediterranean. Any attempt to articulate a European regional security project has been weakened by the EU's internal divergence in political priorities and in the perception of risks and challenges within the enlarged borders of the Union. This condition is giving space to purely national logics that have exposed the Union to diverging policies, unilateral initiatives, or open intra-European rivalries;
- the US' apathy and the EU's strategic impasse have led to a rebalancing at a regional level that opened new opportunities for the ambitious agendas of regional and international actors, which have taken bold steps, either directly or through proxies, to advance their interests;
- the growing presence of China in the Mediterranean, as already underlined;

- the rise of sectarian and geopolitical rivalries among competing regional powers, evident in the Eastern Mediterranean geo-energetic dispute, in Syria and especially in Libya, which represent the main current drivers of conflict;
- despite this, last few years the MENA region entered in a new political phase, driven by some regional actors, characterized by the attempt to reduce the hotspots of crisis and internal tensions and to expand cooperation across the enlarged Mediterranean.

These "normalization process", that is underway, is not simply a reaction to common security threats and uncertainties provoked by the changing global and regional geopolitical dynamics, but it is part of an innovative proactive way to rethink and to re-imagine patterns of inter-state relations based on a new regional security architecture and on new alliances with international partners such as China and Russia.

**2. …and geopolitically contestable**

As a result of those dynamics and changes, the Mediterranean basin became geopolitically contestable with different international and regional actors competing for enhancing their influence in some sectors of the Basin, but without the capacity to propose an inclusive or coherent security arrangement.

In such scenario, which are the effects on those states that are not members of a stable defense alliance? The fact that there is more room for maneuvering for single local actors represents a source of opportunity to enhance their interest; but at the same times, it also means that the Mediterranean becomes an area with more challenges and potential threats.

**3. The increased importance of the Mediterranean as energy provider but its vulnerabilities in terms of food security**

The weaponization of energy, caused by the war, has significantly changed the architecture of the international energy market. In this framework, the issues of energy security and competitiveness of supplies are even more on the top of energy agenda of the EU's Member States. This context increased the importance of the Mediterranean, especially of the Eastern Mediterranean, as energy provider for Europe's energy security. Under this light, energy cooperation in the Basin is regaining priority starting from the ever-increasing development of the interconnections of electricity and gas networks between the European and North African shores, as well as in cooperation among many exporters of oil and gas such as the Gulf countries, Algeria, Egypt and Israel. On the contrary, a negative effect is an escalation of regional-level tensions among local actors.

At the same time, the war has underlined the vulnerability of MENA states in the disruption of the supply chains of agricultural products caused by the heavy dependence of these countries on grain imports from Ukraine and Russia. The consequent risk of food shortages and skyrocketing prices in several MENA countries could have serious repercussions for stability and security in an already fragile region.

Focusing specifically on Tunisia, this country is going through a hard economic crisis aggravated by the war's effects. In fact, it is one of the MENA countries more affected by the Ukraine's war consequences in term of food and energy security. The Russian-Ukrainian conflict drastically interrupts trans-Mediterranean supply chains and exacerbates inflationary pressures on fuel, wheat and fertilizers, causing shortages of commodities and shaping a double energy and food crisis. Tunisia is heavily reliant on foreign imports and vulnerable to market fluctuations. It generates 97% of its electricity through gas imports, mostly from neighboring Algeria, and imports about 60% of wheat from Ukraine and Russia. The Ukraine war has disrupted regular imports and accelerated hunger within the country.

The issue of food security is closely linked to the deterioration of the Tunisian agricultural sector. A trend accelerated in recent years by increased population growth and by the visible effects of climate change which make the high-water consumption required by Tunisian agriculture difficult to sustain. Rising temperatures have triggered wildfires in the hinterland, causing the destruction of part of the summer harvest and contributing to soaring food prices.

Regarding energy security, in December 2022, the European Union offered a loan of 307 million euro for the construction of the "El Med" electricity interconnection project between the Tunisian coasts and Sicily. Fundamental project also for Italy, which through the connection to Tunisia aims to assume the role of energy hub between the two sides of the Mediterranean basin.

**4. Weapons trade and terroristic insurgency**

From a security perspective, the war could indirectly contribute to further destabilizing the Mediterranean region through a backflow of weapons from the Ukraine war theater to those countries already plagued by military crises, insurgencies, civil wars, criminal and terrorist organizations. A clear example is represented by the assaults on weapons depots, utilized then in other conflict-torn countries, which happened during the collapse of al-Qadhafi regime in 2011.

At the same time, if the attention of the West continues to be focused only on the Eastern front, there could be a resurgence of jihadist terrorism characterized by its hybridization with criminal groups. Without an active containment of these terrorist groups scattered across Africa and parts of the Middle East, their strength could grow again quite rapidly.

**5. West/Middle East: different perception of the war**

Although this war represents a relevant game-changer for the West, for other powers this is just another regional conflict. In fact, MENA countries look at this war with much less involvement than the West. Some of these countries are drawing different conclusions from those of the Europeans and the Americans: first of all, the world order is going to be increasingly multipolar and the US and its allies much less capable of managing it; secondly, the economic future of the world belongs to the Global South countries and not to the old Western powers which appears less competitive and under pressure also at a demographic and natural resources level. This also means that alliances can constantly be reshuffled according to national interests.

**Final considerations. Combining hard security and human security**

In conclusion, it clearly emerges that in such difficult situation it is important to refocus on a hard security perspective; at the same time, it is vital to promote multilateral initiatives to reduce the number of regional conflicts and tensions. In particular, in our Basin, where we have a complex matrix of competing national interests, the most evident lesson learnt is that a state should try to build up a network of formal and informal alliances in order to increase protection and security cooperation.

However, it should be emphasized as hard security is not a goal but a tool to reach the more comprehensive concept of human security. This is very true when you have periods of instability and tensions, especially in countries with deep social unbalancing. The role of the armed forces cannot be perceived only in a straight security defense term, but according to the concept of human security, in supporting civilian population in time of crisis. As, for instance, to what the armed forces did in most of the countries, during the pandemic, in different fields (supplies of food, medicines, vaccination).

Therefore, it is important that armed forces should enhance their capacities as pivot actor of crisis management. That means also to be able to interact with civilian expertise (in Italy, for example, with the management of earthquakes and disasters).

This is an ongoing process of increasing skills for building up capacities and lessons learnt, extremely useful in order to organize crisis management, protocols and best practices. I do believe that a more robust cooperation with EU in this respect might foster closer ties between the two shores of the Mediterranean. Something that is in our interests as Mediterranean countries, also taking into consideration what was already stressed, that is the strategic European pivot is deeply rooted along its Eastern borders, with the risk of marginalize furthermore the Euro-Mediterranean partnership and connections.

# L'impact géostratégique de la guerre Russie-Ukraine sur le système international et dans le bassin méditerranéen: menaces sécuritaires et leçons apprises

## Le cadre plus large d'un système international en mutation

L'invasion de l'Ukraine par la Russie a produit de multiples effets au niveau international mais aussi régional: comme nous pouvons bien le constater, outre le nombre croissant de morts dû à l'escalade conflictuelle et l'implication croissante des puissances mondiales à divers titres, l'économie mondiale et les chaînes d'approvisionnement en énergie ont été mises à mal, avec des répercussions désastreuses sur la sécurité énergétique et alimentaire.

Tandis que le monde n'a pas encore résorbé les effets de la pandémie de Covid-19, les hostilités entre la Russie et l'Ukraine ont exacerbé la hausse des prix de l'énergie, les pénuries alimentaires, l'inflation et le recul des marchés.

En outre, de différentes menaces pour la sécurité ont découlé du conflit qui a affecté et continuera probablement d'affecter l'architecture géopolitique mondiale pendant longtemps.

Afin de mieux comprendre ces défis sécuritaires et réfléchir sur une solution viable, certaines questions devraient être analysées:

La guerre a-t-elle juste amplifié tendances qui existaient déjà avant son déclenchement? Ou bien est-elle un simple résultat, et non une cause, des transformations actuelles en cours? Ses implications sont-elles systémiques et d'une grande portée, sur le plan géographique et temporel, ou sont-elles exagérées et devraient plutôt être traitées comme une question régionale de sécurité européenne? Quels sont les effets concrets de la guerre sur les différents domaines de la paix et de la sécurité internationales?

## A) Partant d'une approche géostratégique et systémique:

### 1. La guerre, un changement de donne pour l'Occident

L'invasion à grande échelle de l'Ukraine par la Russie a amené une guerre conventionnelle ouverte sur le sol européen pour la première fois depuis la fin de la Seconde Guerre mondiale.

Le conflit pouvait être perçu comme un changement de donne mondial et un élément perturbateur, car nous n'étions plus habitués à de véritables conflits conventionnels.

A l'aube de la première année de la guerre, je crois qu'il était possible de présumer qu'un conflit pareil aura des conséquences systémiques sur l'ordre politique européen.

### 2. Un système multipolaire

Dans un monde de moins en moins euro-centrique, il convient d'inscrire la guerre ukrainienne dans la mutation géopolitique actuelle du système international. La multipolarité croissante du monde et la montée en puissance géopolitique et militaire de la Chine au-delà de la région du Pacifique (je ferai ici référence à l'engagement croissant de la Chine envers le Moyen-Orient, l'Afrique et le bassin méditerranéen avec l'initiative "Belt and Road", pour ne donner qu'un exemple) ont déjà affecté l'ancien équilibre des forces à l'échelle internationale, d'une manière plus structurelle que l'affirmation russe de ces dernières années.

Elle a provoqué une sorte de "repolarisation" et des tensions croissantes entre les deux superpuissances concurrentes, à savoir les États-Unis et la Chine, avec leurs systèmes d'alliances et de relations.

### 3. Etats-Unis, Chine et Russie: un nouveau triangle stratégique ?

Les États-Unis, la Russie et la Chine représentent les trois principaux acteurs géopolitiques au niveau mondial, à tel point que leurs initiatives et leurs interactions ont amené de nombreux analystes politiques à se demander si nous assistons à l'émergence d'une nouvelle version du fameux "triangle stratégique" des années 70.

Cela ne fait aucun doute que tout changement au niveau de l'interaction des trois côtés de ce triangle provoque une profonde modification de l'équilibre des pouvoirs au sein du système international. Il est encore difficile d'évaluer la manière dont le conflit actuel affecte le triangle stratégique, mais les analystes s'accordent largement à affirmer que cela accroit la convergence entre la Russie et la Chine en tant qu'antagonistes stratégiques des États-Unis.

Il est encore plus complexe de faire une évaluation de l'effet de ces changements sur la région MENA. Néanmoins, voici quelques pistes qui peuvent y ramener:

- Les charges de la guerre sur la Russie pourraient obliger Moscou à réduire et à rééquilibrer ses activités dans la grande Méditerranée;
- Au même temps, la présence de la Chine ne cesse de croître en Afrique et dans les pays de la région MENA, bien qu'elle soit davantage axée sur les relations commerciales et économiques que sur la coopération stratégico-militaire.

On ne sait toujours pas si la Russie tentera de recourir à la Chine comme force de régulation contre les États-Unis et l'Occident, ou si les poussées géoéconomiques et géostratégiques de la Russie et de la Chine dans la région sont de nature différente si les objectifs qu'ils poursuivent sont assez divergents pour être stratégiquement interconnectés.

## B) Quels sont les effets de la guerre en Ukraine au niveau de la sécurité?

### 1. Repolarisation, approche de sécurité dure et nouvel ordre européen

La repolarisation et les tensions croissantes entre les États-Unis, la Chine et la Russie, les actions audacieuses de certaines puissances régionales et le déclenchement de la guerre en Europe ont provoqué un retour général de l'approche de sécurité dure (hard security), associé à la remilitarisation de l'Allemagne et de la Pologne et une augmentation notoire des budgets européens relatifs à la défense.

Pour certains analystes, cela représente également la fin du système de sécurité européen tel que défini dans la déclaration finale de la Conférence sur la sécurité et la coopération en Europe signée à Helsinki en 1973.

Plus encore, cette guerre provoque un déplacement du centre de gravité politique et militaire de l'Europe vers l'Est. Ce changement – potentiellement structurel et qui pourrait générer des effets à long terme qui aillent au-delà de la fin raisonnable de la guerre ukrainienne – réduira probablement l'importance des États membres euro-méditerranéens en faveur des États du centre-est, notamment l'Allemagne, la Pologne et les pays baltes.

Elle a également réduit l'attention de l'Occident vis-à-vis d'autres crises de longue durée, comme celles de la Libye, de la Syrie et de l'Afghanistan.

Parmi toutes les conséquences de l'invasion russe de l'Ukraine, je voudrais souligner les effets de la remilitarisation de l'Occident, déjà mentionnée, et la prédominance accrue de la région centre-est au sein de l'Union européenne.

### 2. La menace de la dissuasion, concept de la guerre froide

Un effet extrêmement inquiétant de la guerre et de l'implication indirecte de l'OTAN dans la guerre reste lié à l'hypothèse, explicitement évoquée par la Russie, de recourir à une arme atomique tactique à courte/moyenne portée (contre-force) contre les troupes ukrainiennes.

Bien qu'il soit estimé peu probable, le risque d'escalade nucléaire ne peut être écarté. Les crises nucléaires de la guerre froide, comme le blocus de Berlin en 1948, la guerre de Corée en 1950-1953, la crise de Cuba en 1962 et la guerre du Yom Kippour en 1973, ont montré que les contre-attaques terrestres augmentent la possibilité d'une escalade nucléaire entre des pays en conflit qui partagent des frontières communes.

Dans le cas de l'Ukraine, une éventuelle reconquête du Donbass et/ou de la Crimée ainsi que l'utilisation d'armes occidentales pour attaquer des cibles stratégiques en Russie, pourrait ouvrir la voie à une escalade spectaculaire de la part de Moscou.

Cette menace potentielle a relancé le débat sur le risque d'utilisation et de prolifération d'armes nucléaires. Il s'agit d'une question très complexe, dont je me limiterai ici à quelques points très brefs:

- L'éventuel recours à une arme tactique de contre-force par la Russie sera extrêmement dangereux car, d'une certaine manière, elle pourrait légitimer l'utilisation d'une arme nucléaire tactique lors d'un conflit conventionnel. Cette perception représente un coup direct au concept de dissuasion, élaboré pendant la guerre froide, lequel était basée sur l'"impossibilité" de l'utilisation d'armes nucléaires. Cela pourrait également avoir un effet déclencheur d'autres conflits dans d'autres pays;
- La repolarisation actuelle, associée au développement technologique, pourrait avoir un effet de prolifération au niveau mondial et plus particulièrement dans les zones sensibles, à savoir la région Asie-Pacifique (agressivité militaire de la Chine, capacité technologique du Japon et de la Corée du Sud, perception d'un déclin des États-Unis, etc.).

La multipolarité croissante et instable du système international ne permet plus une définition inclusive et partagée de l'ordre mondial. Dans un scénario pareil, l'équilibre nucléaire mondial pourrait perdre sa stabilité stratégique avec un nombre accru d'États membres formels ou informels du club nucléaire (puissances nucléaires officielles ou ayant une capacité nucléaire latente).

- Si l'on se concentre sur notre région, l'effondrement du TNP pourrait également avoir des conséquences pour la région MENA:
  - Cette région présente la particularité d'être l'une des rares grandes régions sans État nucléaire officiel ; cependant, il existe une puissance régionale, à savoir l'Israël, qui maintient sa politique d'opacité nucléaire avec une doctrine stratégique nucléaire encore peu claire. Il existe également des États, comme la République islamique d'Iran, qui poursuivent une capacité nucléaire latente qui reflète un nouveau type de prolifération informelle;
  - Dans le passé, plusieurs tentatives ont été amorcées en vue de créer une zone exempte d'armes nucléaires (NWFZ/ZEAN) au Moyen-Orient, car la proximité géographique et l'extrême polarisation représentent à la fois un danger réel et un facteur de prolifération d'armes.

Dans la situation actuelle, alors que l'architecture internationale de la sécurité nucléaire est sous tension, nous devrions nous demander si ce débat n'est qu'une vision dépassée du passé ou si la menace d'une nouvelle prolifération mondiale pourrait le relancer, en lui donnant une nouvelle vitalité.

### C) Quels sont les effets de la guerre en Ukraine au niveau régional?

#### 1. La Méditerranée: une région sous tension et...

Comme je l'ai déjà souligné, le déplacement du centre de gravité, tant de l'OTAN que de l'UE, vers l'Est, réduit l'importance du bassin méditerranéen; un déplacement probablement systémique avec des effets à long terme.

Ce nouvel ordre européen produit un impact sur une Méditerranée déjà sous tension pour une pluralité de causes bien connues:

- Le désengagement américain réel ou perçu dans la région, qui a commencé sous la pulsion du Président *Barack Obama*, semble évident au regard de la stratégie incertaine menée par Washington en Syrie et en Libye;
- L'UE a été, durant ces dernières années, un acteur inefficace en Méditerranée. Toute tentative de conduire un projet européen de sécurité régionale a été affaiblie par la divergence interne de l'UE en matière d'identification de priorités politiques et de perception des risques et des défis à l'intérieur des frontières élargies de l'Union.
- Cette situation laisse la place à des logiques purement nationales qui ont exposé l'Union à des politiques divergentes, à des initiatives unilatérales ainsi qu'à des rivalités intra-européennes ouvertes;
- L'apathie des États-Unis et l'impasse stratégique de l'UE ont amené à un rééquilibrage de forces au niveau régional: cette situation a généré de nouvelles opportunités en faveur des agendas ambitieux des acteurs régionaux et internationaux, qui ont pris des mesures audacieuses, directement ou par le biais de mandataires, pour promouvoir leurs intérêts ;
- La présence croissante de la Chine en Méditerranée, comme déjà énoncé;
- La montée des rivalités sectaires et géopolitiques entre puissances régionales concurrentes, évidentes dans le conflit géo-énergétique de la Méditerranée orientale, en Syrie et surtout en Libye, qui représentent les principaux moteurs actuels du conflit;
- Cependant, la région MENA est entrée, durant ces dernières années, dans une nouvelle phase politique, sous l'impulsion de certains acteurs arabes, caractérisée par une tentative d'atténuer la crise et les tensions internes et d'étendre la coopération à travers la Méditerranée élargie.

Ce processus de normalisation en marche ne représente pas simplement une réaction aux menaces sécuritaires et aux incertitudes communes provoquées par la dynamique géopolitique mondiale et régionale, mais il reflète une démarche proactive innovante qui vise à repenser les modèles de relations interétatiques fondés sur une nouvelle architecture de sécurité régionale et sur de nouvelles alliances avec les partenaires internationaux puissants à l'instar de la Chine et la Russie.

**2. géopolitiquement contestable**

En raison de ces dynamiques et ces changements, le bassin méditerranéen est devenu géopolitiquement contestable, compte tenu des différents acteurs internationaux et régionaux qui disputent le renforcement de leur influence dans certains secteurs du bassin, sans toutefois avoir la capacité de proposer un arrangement inclusif ou cohérent de sécurité.

Dans un scénario pareil, l'on peut se demander sur les effets sur les États qui ne sont pas membres d'une alliance de défense stable? Le fait qu'il existe une plus grande marge de manœuvre pour les acteurs locaux individuels représente une source d'opportunités pour renforcer leurs intérêts; mais en même temps, cela signifie également que la Méditerranée devient une zone qui recèle plus de défis et de menaces potentielles.

**3. L'importance accrue de la Méditerranée comme fournisseur d'énergie mais ses vulnérabilités en termes de sécurité alimentaire**

La militarisation de l'énergie, provoquée par la guerre, a considérablement modifié l'architecture du marché international de l'énergie.

Dans ce cadre, les questions de sécurité énergétique et de compétitivité des approvisionnements figurent encore plus en tête de l'agenda énergétique des États membres de

l'UE. Ce contexte a accru l'importance de la Méditerranée, en particulier de la Méditerranée orientale, en tant que fournisseur d'énergie pour la sécurité énergétique de l'Europe.

Sous cet angle, la coopération énergétique dans le Bassin regagne de la priorité à partir du développement sans cesse croissant des interconnexions des réseaux d'électricité et de gaz entre les côtes européennes et nord-africaines, ainsi que de la coopération entre de nombreux exportateurs de pétrole et de gaz tels que les pays du Golfe, l'Algérie, l'Égypte et Israël. Mais, à côté de cela, il s'en suit une escalade de tensions au niveau régional entre les acteurs régionaux.

Au même temps, la guerre a mis en relief la vulnérabilité des États de la région MENA dans la perturbation des chaînes d'approvisionnement des produits agricoles causée par la forte dépendance de ces pays aux importations de céréales en provenance d'Ukraine et de Russie. Le risque de pénuries alimentaires et de flambée des prix dans plusieurs pays de la région MENA pourrait avoir de graves répercussions sur la stabilité et la sécurité dans une région qui est déjà assez fragile.

La Tunisie traverse une crise économique difficile, aggravée par les effets de la guerre. En effet, c'est l'un des pays de la région MENA les plus affectés par l'impact de la guerre en Ukraine en matière de sécurité alimentaire et énergétique.

Le conflit russo-ukrainien interrompt drastiquement les chaînes d'approvisionnement transméditerranéennes et exacerbe les pressions inflationnistes sur les carburants, le blé et les engrais, provoquant des pénuries de produits et suscitant une double crise énergétique et alimentaire.

La Tunisie dépend fortement des importations étrangères et elle est vulnérable aux fluctuations du marché. Elle produit 97% de son électricité grâce à des importations de gaz, provenant principalement de l'Algérie voisine, et importe environ 60 % du blé d'Ukraine et de Russie. La guerre en Ukraine a perturbé les importations régulières et accéléré la pénurie dans le pays.

La question de la sécurité alimentaire est étroitement liée à la détérioration du secteur agricole tunisien. Cette tendance a été accélérée ces dernières années par la croissance démographique accrue et les effets visibles du changement climatique qui a altéré les besoins de l'agriculture en matière d'eau. La hausse des températures a déclenché des incendies dans les forêts en Tunisie et au Maroc, provoquant la destruction d'une partie de la récolte d'été et contribuant à la flambée des prix alimentaires.

Concernant la sécurité énergétique, en décembre 2022, l'Union européenne a proposé un prêt de 307 millions d'euros pour la construction du projet d'interconnexion électrique "El Med" entre les côtes tunisiennes et la Sicile. Ce Projet est également fondamental pour l'Italie, qui à travers la connexion à la Tunisie vise à assumer le rôle de concentrateur énergétique entre les deux côtés du bassin méditerranéen.

### 4. Trafic d'armes et insurrection terroriste

D'un point de vue sécuritaire, la guerre pourrait indirectement contribuer à déstabiliser davantage la région méditerranéenne par un reflux d'armes du théâtre de la guerre en Ukraine vers les pays déjà victimes de crises militaires, des insurrections, des guerres civiles et des organisations criminelles et terroristes. Un exemple clair est représenté par les assauts sur les dépôts d'armes, suite à l'effondrement du régime d'Al-Qadhafi en 2011, et qui ont été utilisés ensuite dans d'autres pays déchirés par des conflits.

En même temps, si l'attention de l'Occident continue à se concentrer uniquement sur le front oriental, il pourrait y avoir une résurgence du terrorisme djihadiste accouplé à des groupes criminels. Si l'on ne parvient pas à contenir activement ces groupes terroristes disséminés en Afrique et dans certaines parties du Moyen-Orient, leur force pourrait croître à nouveau assez rapidement.

**5. Occident/Moyen-Orient : Une perception différente de la guerre**

Bien que cette guerre représente un changement de donne important pour l'Occident, il s'agit simplement pour d'autres puissances, d'un autre conflit régional. En effet, les pays de la région MENA sont moins impliqués dans cette guerre que l'Occident. Certains de ces pays tirent des conclusions différentes de celles des Européens et des Américains: tout d'abord, l'ordre mondial sera de plus en plus multipolaire et les États-Unis et leurs alliés seront beaucoup moins capables de le gérer ; ensuite, l'avenir économique du monde appartient aux pays du Sud et non aux anciennes puissances occidentales qui semblent moins compétitives et sous pression également au niveau démographique et des ressources naturelles. Cela signifie également que les alliances peuvent être constamment remaniées en fonction des intérêts nationaux.

**Considérations finales: Combiner sécurité dure et sécurité humaine**

Il ressort clairement de ce qui précède que dans une situation aussi difficile, il est important de se recentrer sur une perspective de sécurité dure; en même temps, il est vital de promouvoir des initiatives multilatérales pour réduire le nombre de conflits et de tensions régionaux.

Particulièrement dans notre bassin, où nous disposons d'une matrice complexe d'intérêts nationaux concurrents, la leçon la plus évidente à apprendre serait qu'un État devrait essayer de construire un réseau d'alliances formelles et informelles afin d'augmenter la protection et la coopération en matière de sécurité.

Toutefois, il convient de souligner que la sécurité dure n'est pas un objectif en soi mais un outil pour atteindre le concept plus global de sécurité humaine. Cela est d'autant plus vrai que lorsqu'on connaît des périodes d'instabilité et de tensions, notamment dans les pays où le déséquilibre social est profond, le rôle des forces armées ne peut être perçu uniquement sous l'angle de la sécurité et de la défense, mais selon le concept de sécurité humaine, à travers le soutien de la population civile en temps de crise. Il suffit de penser au rôle assumé par les forces armées dans la plupart des pays, pendant la pandémie, dans différents domaines (approvisionnement en nourriture, médicaments, vaccination).

Par conséquent, il est important que les forces armées renforcent leurs capacités en tant qu'acteur-clé de la gestion des crises. Cela signifie également être capable d'interagir avec l'expertise civile (en Italie, par exemple, avec la gestion des tremblements de terre et des catastrophes).

Il s'agit d'un processus continu de renforcement des capacités et les leçons apprises, extrêmement utiles pour la gestion de crise, et de promouvoir les protocoles et les meilleures pratiques.

Je suis convaincue qu'une coopération plus solide avec l'UE à cet égard pourrait favoriser des liens plus étroits entre les deux rives de la Méditerranée. Une chose qui est dans notre intérêt en tant que pays méditerranéens, compte tenu également de ce que j'ai déjà souligné, du fait que le pivot stratégique européen vire vers les frontières de l'Europe de l'est, au risque de marginaliser davantage le partenariat et les coopérations euro-méditerranéennes.

# Osservatorio Strategico
# Sotto la lente

Pagina bianca

# L'Intelligence: dai conflitti interstatali alla lotta alle minacce contemporanee

## Introduzione

Questo testo ha l'intenzione di mostrare in maniera sintetica, concisa e accurata il ruolo della funzione informativa dell'Intelligence, ovvero quello di ancella della forza bruta, di bussola che guida la condotta strategica dell'immensa macchina bellica verso la vittoria, facendo del supporto informativo uno strumento vitale del decisore politico/militare/civile per il suo processo di comando e controllo. Le informazioni, quali elementi essenziali, vengono elaborate e processate al fine di ottenere un vantaggio di superiorità conoscitiva.

"L'intelligence non è un elemento sufficiente alla vittoria della Guerra, perché questa si basa sul sangue dei contendenti e sullo scontro di volontà nel dominio fisico" (Clausewitz, 1832). Tuttavia è un cardine necessario ed imprescindibile nel perseguimento dei propri obiettivi.

L'elaborato si articola su quattro capitoli accompagnati da un'introduzione e una conclusione per definire concetti chiari che mostrino l'evoluzione del servizio di intelligence, il quale ha assistito con sorpresa e incredulità all'entrata in gioco di nuove minacce comportando un incremento di caos e entropia nel sistema statale precedente.

Il ruolo del Servizio di Informazione nella difesa del cittadino e della sicurezza dalle minacce esterne ed interne è sempre più vitale. Nelle conclusioni sono esposti i concetti da tenere a mente per soffermarci su alcune domande proponibili oggigiorno per comprendere l'operato dell'Intelligence. In che modo l'intelligence ha cambiato le sue sembianze? È riuscito in tale impresa? Quali sono i possibili mutamenti dell'intelligence per poter fronteggiare i nuovi nemici apparsi sulla scena delle Relazioni Internazionali? Ma soprattutto, che ruolo svolge l'intelligence in queste circostanze?

## L'Intelligence

L'intelligence è un ciclo di raccolta organizzata di notizie, elaborazione dati e di diffusione di informazioni, la quale va consegnata al decisore, sia esso politico, militare, civile, al fine di formulare ed eseguire le più efficaci politiche interne, militari, estere e finanziarie, nonché di provvedere alla difesa dello Stato dai pericoli esterni.

Il processo informativo è un ciclo ricorsivo, il cui risultato sarà il punto di partenza per l'inizio di un nuovo ciclo; l'informazione grezza arrivata alle "orecchie" dell'operatore viene elaborata per essere trasferita al "cervello" del decisore politico che la utilizzerà nel momento del bisogno. Lo scopo dell'acquisizione di informazioni è possedere una chiave di lettura delle situazioni costantemente in evoluzione al fine di essere pronti ad agire.

È un processo complesso nella pratica che tiene conto di tanti elementi per raggiungere un risultato finale che permetta la lettura tra le righe del fenomeno.

Il processo informativo si articola in due macro processi: uno di gestione della raccolta di informazioni e uno di analisi delle informazioni. L'informazione deve essere accurata, attendibile e affidabile e l'appropriatezza e la veridicità della fonte da cui si ricava devono essere verificate. In base poi alla tipologia di fonte che si cerca di utilizzare si distinguono varie tipologie di processi informativi:

- OSINT (Open-Source Intelligence);
- IMINT (Imagery Intelligence);
- HUMINT (Human Intelligence);
- SIGINT (Signal Intelligence);

- MASINT (Measurement and Signature Intelligence);
- TECHNICALINT (Technical Intelligence);
- UGS (Unattended Ground/Sea Sensors).

Tali processi ritrovano le loro origini nell'antichità; ad esempio i Sumeri o il giovane Alessandro il macedone raccoglievano le informazioni di porto in porto o di regno in regno, con differenti caratteri di natura religiosa, economica, culturale e strategica, permettendogli di arrivare sino all'Estremo Oriente. In Grecia ricordiamo l'esperienza degli *skopoi*, che erano delle truppe di ricognizione leggere. L'obiettivo della raccolta di informazioni consisteva nella semplice esplorazione e nella sorveglianza per la protezione di confini e di conoscenza del territorio.

Quindi l'intelligence è il frutto dell'analisi di tutti gli elementi essenziali informativi acquisiti in considerazione di determinati eventi che fungono da ambiente e da supporto informativo per la presa di decisione da parte del detentore del potere.

**I conflitti interstatali**

Nasce spontaneo chiedersi quanto sia utile l'apporto dell'intelligence in guerra? Come concepirlo oggigiorno e come viene visto l'intelligence che fronteggia qualcosa di astratto come il terrore? Come invece veniva visto durante scenari di lotta simmetrici e dottrinali?

Sun Tzu riporta alcuni concetti che descrivono l'arte informativa come "essenziale":

*"Ciò che permette ad un principe illuminato e ad un abile generale di sottomettere il nemico e conseguire risultati straordinari, è la capacità di previsione".*

*"Soltanto un sovrano illuminato e un abile generale, capaci di utilizzare per le operazioni segrete gli uomini più intelligenti, possono essere certi del successo. In guerra le operazioni segrete sono essenziali: prima di fare qualsiasi mossa ci si deve basare su di esse"* (Sun Tzu, 2013, cap13.).

Queste frasi a distanza di anni e con equilibri egemonici stravolti hanno ancora significato e sono attuali. Percorrendo la Storia ci sono esempi di battaglie in cui il possesso delle informazioni ha portato ad una vittoria e altre in cui l'informazione da sola non è bastata per vincere. Le informazioni sono elementi essenziali per la conduzione di un conflitto e per mantenere la sicurezza del proprio Stato. A volte, purtroppo, non è sufficiente. Infatti, un'informazione non interpretata o la mancanza di mezzi e uomini può comportare la perdita sul terreno più crudo della guerra, ovvero quello della forza fisica. Il valore dell'informazione dipende anche dall'uso che se ne fa.

Si può affermare che l'Intelligence sia una componente necessaria e obbligatoria per la conduzione di qualsiasi battaglia, ma purtroppo, a volte, non sufficiente per la vittoria.

Tra alcuni esempi di vittoria potremmo annoverare il caso dello scontro della brigata "Stonewall", la vittoria americana nella Guerra delle Midway, la missione Magic e Primerose, le operazioni di disinformazione delle armi segrete tedesche V-1 e V-2.

Un fattore comune, facilmente riscontrabile in queste battaglie, è la presenza di un risultato informativo che permette una superiorità strategica che, vincolata con le capacità del decisore politico o militare del momento, riescono a concretizzare il vantaggio portando ad un vero e proprio successo informativo e operativo.

Per esempio, il condottiero autoctono Jebediah Hotchkiss fu uno dei personaggi più importanti dell'episodio della brigata Stonewall. Jebediah fornì al suo Generale la mappa con le informazioni specifiche richieste, portandolo in una posizione di vantaggio (J. Keegan 2006). Gli alleati nella guerra contro i giapponesi e contro i tedeschi, con le interpretazioni delle comunicazioni cifrate e la rottura delle rispettive logiche crittografiche, riuscirono a risparmiare lacrime a tante famiglie.

Un episodio che fu una sconfitta da entrambe le parti fu il caso della Battaglia di Creta e dell'Operazione Merkur. Il 24 aprile del 1941 Hitler scrisse la direttiva n° 28 che illustrava gli scopi

e gli obiettivi di tale operazione. Nonostante le risorse informative, non si riuscì ad ottenere il vantaggio sperato.

L'apparato di Intelligence si è evoluto dai conflitti interstatali alla lotta al terrorismo attraverso successi ma anche grandi insuccessi. Questi si sono susseguiti nella stessa direzione dell'evoluzione dell'organizzazione e della società.

**La lotta al terrorismo**

Con il cambio dell'ordine egemonico e delle relazioni internazionali alla fine del XX secolo e inizio XXI secolo un vortice di 'nuove minacce' sono state liberate dal vaso di Pandora, scatenando delle forze di disordine e di anarchia che hanno destabilizzato, ancora maggiormente, il sistema di relazioni internazionali.

Giorno dopo giorno il bene comune hobbesiano, ovvero la sicurezza di ogni cittadino, diventa gravoso e difficile da assicurare e mantenere. I dilemmi della sicurezza, dell'abbandono, dell'inganno sono ormai intrecciati tra di loro e rischiano di intrappolare gli Stati nella cosiddetta trappola di Tucidide. Se un tempo l'aria della città e le sue mura rendevano sicuri gli abitanti, oggi, tra questi vaga sciolto il caos. Molteplici minacce asimmetriche e rischi vorticano in una danza irruenta e incontrollabile (Ansalone, G. et Zappalà, A., 2012, 100).

Tra le nuove minacce e tipologie di guerre, il nemico che prende maggior luce sul palcoscenico delle problematiche delle agende degli Stati è il Terrorismo.

Proprio sul terreno del riconoscimento e della neutralizzazione della minaccia si misurerà la capacità di sopravvivenza degli stessi sistemi socio-politici e culturali occidentali. Il lavoro dell'Intelligence non consta di una mera descrizione dei nuovi nemici, ma li deve capire, riconoscere ed eliminare. Il terrorismo non è qualcosa che nasce con Osama Bin Laden e Al-Qaeda. Si tratta di un fenomeno che affonda le sue radici nelle guerre passate. Tuttavia la guerra è rimasta intimamente sempre la stessa: la distruzione di un nemico e risoluzione di uno scontro di volontà con altri mezzi.

Si possono ricordare gli attentati a Napoleone Bonaparte III nel 1856, al principe Alessandro II in Russia nel 1882, al Re Umberto I con Gaetano Bianchi nel 1900, al regicidio che scatenò la Prima Guerra Mondiale nel giugno del 1914 per mano di Gavrilo Princip, presumibilmente sotto le fila della Crna Ruka, attentati irlandesi, israeliani, di metà secolo, fino ad arrivare ai dirottamenti aerei.

Molte rappresentazioni di terrorismo sono state date: stato di terrore, mezzo di politica per ottenere i propri obiettivi, per creare uno stato di inibizione nel nemico, arma brutale ed efficace, ma sicuramente quello più rappresentativo potrebbe essere arma di coloro che guerra non fanno.

Il terrorismo è lo strumento utilizzato da coloro che non si possono permettere di fare la guerra contro uno Stato e quindi, consapevoli di questa debolezza, utilizzano mezzi efficaci (le macchine esplodono, le persone muoiono, i grattacieli cadono) ed economici (comprare del C4 e dei detonatori). La logica del terrorismo si basa sulla paura di attacchi imprevedibili che si possono verificare in qualsiasi momento, colpendo obiettivi sensibili o chiunque senza discriminazioni. Questo provoca uno stato d'ansia nelle persone, facendole sentire impotenti. L'obiettivo di chi utilizza tale mezzo è che l'individuo comune inizi a mettere in discussione i fondamenti della sua società e la capacità dello Stato di garantire la sicurezza dei suoi cittadini.

Al-Qaeda ha una matrice ideologica, Osama Bin Laden parla di Islam e di Umma uniti contro l'Occidente, non utilizza il termine "arabi" durante un'intervista fatta da Abdel Bari Atwan. Lo sceicco saudita, aveva capito che per mettere in ginocchio gli americani, avrebbe dovuto utilizzare metodi non convenzionali di guerra su un terreno dove questi non fossero pronti a combattere. Il Terrorismo può essere jihadista o politico, religioso, ecoterrorismo, narcoterrorismo, terrorismo NBC e informatico. Si tenta in ogni modo di distruggere la società che viene vista come un male per il semplice fatto che esista. La motivazione religiosa è motore dei gruppi che da

fondamentalismi si trasformano in radicalismi, dove l'infedele è il male e deve essere annientato o, quanto meno, come riportato dai versetti del corano seconda *sura* n°190 et ss. (approssimativamente), combattuto.

Al-Qaeda nasce dalla decisione dell'Unione Sovietica di invadere militarmente l'Afghanistan. Alla resistenza antisovietica partecipò anche lo sceicco saudita Osama Bin Laden il quale, entrato in Afghanistan divenne il braccio destro di Abdullah Azzam. Insieme formarono il *Maktab al-khidmat* (ufficio servizi) e, successivamente, l'ufficio informazioni per i Musulmani a Peshwar in Pakistan. Entrambi, Osama e Azzam, si erano recati a Jedda per frequentare l'università ed erano stati influenzati dal professore Muhammed Qutb. Nel 1986 Bin Laden si trasferì a Peshawar e da lì fondò il suo primo campo di addestramento al-Ansar nella provincia di Paktia vicino al villaggio Jaji (M. A. Fabiano, S. Fonso, E. Greco, 2010, 87-100).

Osama, Azzam e Qutub fecero di Al-Qaeda una vera e propria multinazionale terroristica internazionale: potenze senza uno Stato, dislocate a livello globale, con un esercito, una finanza ed una politica. Una volta riscontrati problemi anche in Sudan, Osama tornò in Pakistan avvicinandosi a Khandar e da lì, una volta entrato nelle grazie del Mullah Omar, iniziò il suo operato da Kabul con l'aiuto dei Talebani.

La sua struttura è una massa informe composta di legami, tentacoli che si avvinghiano su determinati individui creando un'influenza, un sentimento di cooperazione, lasciando questi agenti dormienti dislocati per il globo, che non obbediscono ad un qualche vincolo di gerarchia, ma ad utilità e credenze. Viene lanciato un messaggio e si lascia agire il motore di influenza di questa cellula attraverso iniziativa e sorpresa, che sono gli elementi fondamentali. Il compito dell'intelligence è di operare in modo chirurgico, andando ad eliminare tutte queste cellule maligne (M. A. Fabiano, S. Fonso, E. Greco, 2010, 87-100).

**Il RIA, Revolution of Intelligence Affairs, Virtual Intelligence 3.0**

La Rivoluzione degli Affari Militari (RMA) è stata una dottrina persistente nella definizione della nuova era dell'Informazione. L'era della computerizzazione e della teoria net-centrica ha stravolto il mondo cambiando comportamenti, contraendo spazi e tempi, e non è ancora terminata, ma alla luce degli anni che passano l'incremento esponenziale è sempre più evidente. Alcuni studiosi parlano di evoluzione, altri di rivoluzione; tutti, però, sono d'accordo sull'idea che "*an accurate and useable intelligence will be critical to the succeful conduct of war*" (Alan Dupont, 2003, 1).

Premesso questo, bisogna domandarsi se l'evoluzione dell'Intelligence permetta ai Servizi di sicurezza di confermare la loro necessaria esistenza nella società, acquisendo in alcuni casi maggiore importanza per risolvere e fronteggiare le nuove minacce contemporanee.

La risposta è Sì, perché si prova a guardare l'Intelligence come un'arma vitale e precisa per la difesa e la sicurezza dei cittadini. La democratizzazione della tecnologia, fruibile da parte di tutti, ha portato grandissimi vantaggi, ma anche uno dei grandi mali dell'era dell'Informazione: "*the information overload*".

I *database* raccolgono miliardi di informazioni che in tempi millesimali viaggiano ad una velocità inimmaginabile e questo rende complicato applicare le capacità umane di elaborazione. L'evoluzione 4.0 è uno *step* possibile solo con l'utilizzo di Intelligenza Artificiale.

Una frase che riassume il concetto è quella espressa dall'imprenditore Mitchell Kapor: *"Getting information off the internet is like taking a drink from a fire hydrant"*. Con la scintilla della RMA, la Rivoluzione degli Affari di Intelligence (RIA) si innesca e mette in moto il processo di miglioramento.

I mezzi tradizionali di Intelligence non hanno avuto più lo stesso effetto contro le organizzazioni o gruppi terroristici e criminali, i quali non hanno un territorio o una base operativa o

dei confini lineati da attaccare o sorvegliare, come anche l'entrata nel mondo in evoluzione del digitale.

Sono cinque le importanti problematiche/sfide nella pratica di Intelligence che sono avvenute nel primo quindicennio degli anni 2000:

- Oltre al *focus* su obiettivi di carattere strategici, è importante una micro intelligence;
- Un'intelligence dove gli agenti operanti si trovano a dover rispettare le regole di ambienti difficili dove le loro garanzie funzionali o le capacità tecnologiche non risultano efficienti;
- Tecnologia in piena rivoluzione, ma con limitazioni, una corsa alla tecnologia senza precedenti a cui l'uomo si deve adattare rapidamente;
- Le collaborazioni con altre agenzie governative da adattare anche all'occhio critico dell'opinione pubblica;
- Rivalità e amicizia tra Stati in situazioni differenti.

Il supporto dell'Intelligence sia in ambito militare che civile deve essere ridisegnato in maniera tale da soddisfare le esigenze delle guerre moderne, ma anche di svilupparsi all'interno di un terreno economico e sociopolitico come quello della Democrazia. Diventa opportuno provvedere ad un *comprehensive approach*, ovvero un approccio completo e dominante sul campo di battaglia, che si estende su differenti dimensioni fino ad arrivare ad una quinta dimensione. Si allude anche alla creazione di una meta-dimensione come campo di battaglia. (Castagna 1997, 189-195). Oggigiorno i *bytes* sono diventati importanti quanto i proiettili. Si potrebbe parlare di *BitsKrieg* invece che di *BlitzKrieg* (Arquilla, 2011).

Il lavoro intellettivo, unito alla forza bruta e alla capacità delle Forze Armate permette di avere un vantaggio competitivo oltre ogni limite. Riformulando il concetto di Max Weber per cui la guerra nei tempi è una guerra di macchina, quella nell'era dell'Informazione è una guerra di informazioni.

La Guerra è diventata una professione che non viene combattuta solamente con semplici bombe di ferro, ma anche con proiettili elettronici composti da *bits*, i cosiddetti *binary bullets* (Allhoff, Henshcke, Strawser, 2016). L'evoluzione dell'Intelligence porta con sé una distinzione tra gli apparati che nel XXI secolo e in quello futuro dovranno fondersi, integrando tutti gli elementi che fino ad ora erano in parte divisi o frazionati, per avere una visione completa della situazione che si affronta a tutti i livelli, partendo dal tattico, quindi militare, a quello strategico, puramente politico.

In questa evoluzione informatica, l'investimento nella tecnologia e la formazione continua del personale sono strumenti strategici che devono essere perseguiti per ottenere risultati nel breve, medio e lungo termine. I risultati saranno differenti, ma riprendendo le parole dell'8° Segretario della Difesa, R. McNamara, con tale cambiamento, forse, sarà possibile diradare la nebbia che avvolge questa signora conosciuta come "Guerra".

**Conclusioni**

L'evoluzione della funzione informativa dell'Intelligence risulta essere un processo vitale nella realtà che viviamo oggigiorno, permettendo al servizio informativo di sopravvivere e di provvedere al bene più grande dello Stato, ovvero la difesa e sicurezza dei cittadini. I Servizi di Informazione si adattano e provano a raffigurare le possibili soluzioni, mitigazioni e difese alle minacce costantemente presenti al fine di tutelare gli interessi strategici, economici delle Istituzioni e della Democrazia.

Un fattore comune che sarà sempre riscontrabile ed identificabile è la fonte di questa evoluzione e cambiamento: il fattore umano. La presenza dell'uomo che svolge operazioni di attacco o difesa, le sensazioni, le emozioni impiegano millenni prima di cambiare, dando così la possibilità di poter delineare sempre la componente umana che si cela dietro le macchine o le azioni.

L'attuale scenario della realtà, sia nazionale che internazionale, è permeato da minacce e, come l'intelligence, è in continua evoluzione. Si sente sempre più necessario l'intervento di più assetti e di un *comprehensive approach* nella risoluzione di un problema e si ha bisogno di una competenza e di utilizzo delle varie attività di Intelligence a 360°. Queste azioni sono perseguibili se alla base sussiste una formazione continua del personale e un investimento nelle tecnologie in evoluzione.

Il risultato che verrà prodotto da tutte queste tecniche sarà un mosaico che sarà interpretato dal decisore politico per poter guidare lo Stato e raggiungere la sicurezza a livello internazionale ed interno.

Per conseguire questo obiettivo, coloro che svolgono il processo di raccolta, elaborazione e diffusione di informazioni devono essere sempre pronti ad operare, unici nel loro genere che sapranno mescolare una cultura umanistica con quella scientifica per poter rispondere alle domande e ai problemi che si troveranno di fronte. L'intelligence è un'arte che guarda oltre l'orizzonte per prevedere e risolvere le sfide con mente aperta e un pizzico di coraggio (M. Masci e L. Piacentini, 2014, 209).

**Bibliografia**


- Dupont, A. (2003) Intelligence for the Twenty-First Century, Intelligence and National Security, 18:4, 15- 39, DOI: 10.1080/02684520310001688862.
- Denécé, E. (2014) The Revolution in Intelligence Affairs: 1989–2003, International Journal of Intelligence and CounterIntelligence, 27:1, 27-41, DOI: 10.1080/08850607.2014.842796.
- Arquilla, J. (2011) From Blitzkrieg to Bitskrieg: The Military Encoutern with computers, in "Communication of the ACM", ottobre.
- Allhoff, F., Henschke, A., and Strawser, B., (2016) Binary Bullets: The Ethics of Cyberwarfare, Published to Oxford Scholarship Online: December, DOI: 10.1093/acprof:oso/9780190221072.001.0001.
- Ansalone, G. et Zappalà, A., (2012) 11 settembre 2021, le minacce del prossimo decennio, Milano, Franco Angeli s.r.l..
- Keegan J., (2006) Intelligence. Storia dello spionaggio militare da Napoleone a AlQaeda, Milano, Bruno Mondadori.
- Lauquer W., (1986) Un Mondo di Segreti, Rizzoli, traduzione stampata a Milano.
- Pasqualini M.G., (2014) Carte Segrete dell'Intelligence Italiana, il S.I.M in archivi stranieri, Ministero della Difesa, Ufficio Storico del V Reparto dello Stato Maggiore della Difesa.
- Rapetto U., Di Nunzio R., (2002) L'atlante delle spie: dall'antichità al Grande Gioco ad oggi, Rizzoli.
- Cappè F. et al, (2006) La minaccia del Terrorismo e le risposte dell'antiterrorismo, Franco Angeli s.r.l., Milano.

Pagina bianca

## Il mondo Cyber 4.0. Interconnessioni tra la vita reale e la minaccia cyber

Lo scoppio del conflitto in Ucraina ha amplificato l'uso delle tecnologie e dei sistemi di comunicazione. Il mondo cyber si è sempre prestato a mille diverse interpretazioni. Il cyberspazio, o *cyberspace* nella sua eccezione anglofona più utilizzata, è così ampio da essere definito *continente invisibile*, e consiste in "un dominio caratterizzato dall'uso dell'elettronica e dello spettro elettromagnetico per conservare, modificare e scambiare dati attraverso sistemi di rete ed infrastrutture fisiche associate". Secondo un'interpretazione più recente e complessa il *cyberspace* è "l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware e software, dati e utenti nonché delle relazioni logiche, comunque stabilite, tra di essi"[1].

Esso infatti convoglia, attraverso le reti di comunicazione dei dispositivi fissi e mobili connessi a Internet, la massa di informazioni e i dati più sensibili della vita dei singoli individui, così come quelli relativi alle attività politiche, economiche e sociali di un Paese. Da esso, però, dipende anche il funzionamento di settori nevralgici per la produzione economica, industriale e finanziaria nazionale: da qui l'emergenza per la sicurezza e l'incolumità dei cittadini, per via delle intrusioni esterne nella rete internet da parte di innumerevoli soggetti[2].

A queste definizioni tradizionali più generiche ne sono state aggiunte altre che rendono certamente unico lo spazio cibernetico. Si parla, infatti, di cyberspazio come luogo VUCA, ossia permeato da *volatility*, *uncertainty*, *complexity and ambiguity.* È, infatti, un ambiente in continua evoluzione tanto da renderlo volatile (*volatility*), che porta con sé un alto grado di incertezza (*uncertainty*), da cui la difficoltà a sondarlo; da ciò deriva una sua intrinseca complessità (*complexity*) perché formato da molteplici sistemi, impossibile infatti conoscere tutte le interazioni fra le sue parti, da cui la sua ambiguità (*ambiguity*). In questo contesto VUCA[3] deve essere collocata la minaccia cibernetica che assume sempre i caratteri di un attacco dalle diverse caratteristiche tecniche e con gli stessi obiettivi (individui, aziende, istituzioni, infrastrutture), sino a mettere a rischio la sicurezza anche di realtà complesse come le infrastrutture nazionali.

Si tratta, tuttavia, di un "non-spazio geografico" in quanto quello cibernetico non possiede limiti territoriali come la terra, il mare e addirittura il cielo: da qui la sua natura transnazionale che lo accomuna ad un *global common*, come le rotte marittime, i fondali marini e il cosmo, ossia quelle aree operative che non sono sotto la sovranità di precisi soggetti statuali, ma la cui disponibilità e sicurezza devono essere salvaguardate, questo stato di cose finisce per avere un ruolo fondamentale nella comprensione di fenomeni come i crimini informatici o la conflittualità fra i soggetti che vi operano e che determinano la c.d. crisi cibernetica nazionale. Si tratta di una "situazione in cui un incidente cyber assume dimensioni, intensità o natura tale da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole Amministrazioni competenti per via ordinaria, ma attraverso l'assunzione di decisioni coordinate in sede interministeriale".

Al momento, questa conflittualità o *cyber warfare* – preferibile alla più nota *cyberwar* diffusa dai mass media – è da intendersi come l'insieme di tutte quelle azioni riconducibili a crimini, minacce, sabotaggi e spionaggio attraverso le reti informatiche e computer. Minaccia che ha trovato terreno fertile con lo scoppio della guerra in Ucraina. Da tale minaccia deriva la necessità di una

---

1 Il glossario di sicurezza cibernetica, in Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, Glossario Intelligence, Appendice, Roma, maggio 2019.
2 G. Gori, Germani, La sfida della cyber intelligence al sistema italiano, Ed. Angeli, 2013:" di fronte alla manipolazione delle informazioni, le informazioni si equivalgono, determinando la scomparsa della verità", pagg. 183-185.
3 T. Shaman, Cyber risk leaders, Ed. My Security media, 2019, pag. 37.

*cyberdefence*, intesa come "l'insieme della dottrina, dell'organizzazione e delle attività volte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti nel e tramite il cyberspace, ovvero in danno di uno o più dei suoi elementi costitutivi".

Tuttavia, come per il terrorismo non esiste una definizione univoca, globale e condivisa, così per ciò che accade come *warfare* nell'ambiente cibernetico, vi sono differenti termini che, negli anni, sono andati accavallandosi per significato ed importanza. "*Cyber warfare"* in origine era da intendersi esclusivamente come l'uso militare di computer e reti telematiche e tutto ciò che ruotava attorno all'ambiente informatico per la difesa di una nazione oppure su un campo di battaglia, e tale rimane nelle definizioni ufficiali. Con il tempo, tuttavia, tale termine ha finito per definire comunemente quell'insieme di azioni condotte da una nazione, anche in tempo di pace, contro reti telematiche e computer di un'altra nazione al fine di causare danno o sabotaggio, per poi diventare un dominio in cui agiscono offensivamente anche attori non-statali, dalle organizzazioni criminali ai terroristi, o singoli individui e attivisti politici di frange estreme. Ciò è dovuto, come si vedrà in seguito, alla natura mutata della guerra moderna, ossia quella ibrida, dove molteplici attori intervengono a fianco degli strumenti tradizionali, convenzionali.

Per alcuni anni, tuttavia, la *cyber warfare* è stata prettamente di natura economica e ad essere colpiti sono stati, e continuano ad essere, quegli obiettivi propri della competizione economica fra soggetti, dai singoli individui a realtà più complesse come grandi aziende multinazionali o, appunto, Stati sovrani. Ora, tuttavia, la *cyber warfare* si sta profilando anche nei rapporti fra Stati o fra attori non-statuali e Stati, come si vedrà in seguito, e non su aspetti solo ed esclusivamente economici, ma addirittura militari.

Al momento, tuttavia, la competizione fra soggetti differenti è prevalentemente di carattere economico, laddove il cyber spazio rappresenta un ambito ricco di opportunità di facile guadagno. Non è un caso, infatti, che per primo sia stato configurato il *cybercrime,* o crimine nel cyber spazio, inteso come quell'insieme di "azioni illecite condotte in danno di sistemi informatici o attraverso l'utilizzo abusivo degli stessi, le cui condotte sono punite dal codice penale", il cui scopo immediato è il vantaggio economico, dal furto d'identità a dati bancari, transazioni finanziarie illecite e così via. Negli anni è sconfinato addirittura nello spionaggio industriale, con l'obiettivo di sottrarre informazioni e scatenare una competizione economica e finanziaria fra nazioni nello spazio cibernetico. Da queste azioni si è concretizzata la *cyber warfare*. Con essa, quindi, si è giunti ad intendere tutto l'insieme delle attività di preparazione e conduzione di operazioni attraverso l'uso di intercettazioni, alterazione e distruzione delle informazioni e dei sistemi di comunicazione degli avversari: inizialmente circoscritta all'ambiente militare, ora si è ampliata anche agli ambienti civili, sia politici, economici, finanziari ed industriali.

La *cyber warfare,* in quest'ultima evenienza, minaccia di colpire in particolare le infrastrutture critiche pubbliche e private, ossia il complesso di impianti e delle installazioni occorrenti all'espletamento di servizi in una nazione (le acque, le telecomunicazioni, le centrali elettriche, la raccolta e la distribuzione di idrocarburi etc.), e nello specifico i loro sistemi Supervisory Control and Data Acquisition (SCADA[4]), le cui vulnerabilità sono aumentate del 200% nel 2018, generalmente riferito all'insieme di Ics (i sistemi di controllo industriale che sorvegliano e gestiscono, a livello nazionale, le infrastrutture), i processi industriali (ideazione, produzione e assemblaggio) e le istituzioni economiche e finanziarie. Colpendo le infrastrutture critiche si mira alla paralisi di settori nevralgici di una nazione, danneggiandola economicamente ma soprattutto rendendo estremamente vulnerabile lo svolgimento della sua vita civile. È stato il caso del *malware* o virus Industroyer o Crashoverride legato, secondo gli esperti, all'attacco che provocò un *blackout* elettrico in Ucraina nel dicembre del 2016: questo virus, progettato sulla base di una profonda conoscenza dei sistemi di controllo industriali usati come bersaglio e, sfruttando, quindi, funzionalità legittime e protocolli di

[4] AA.VV., *Rapporto CLUSIT 2019 sulla sicurezza ICT in Italia*, Milano, 2019, p. 265.

sistemi di gestione della rete elettrica, ne bloccò il funzionamento. Sebbene con caratteristiche avanzate, Crashoverride non possedeva e non possiede (in quanto non si esclude che possa agire ancora in futuro) capacità altamente distruttive ma solo di blocco di servizi: secondo alcuni esperti, infatti, Crashoverride potrebbe essere stato paragonabile ad un attacco *cyber warfare*. Con essa, quindi, si è giunti ad intendere tutto l'insieme delle attività di preparazione e conduzione di operazioni attraverso l'uso di intercettazioni, alterazione e distruzione delle informazioni e dei sistemi di comunicazione degli avversari: inizialmente circoscritta all'ambiente militare, ora si è ampliata anche agli ambienti civili, siano essi politici, economici, finanziari ed industriali.

Ciò avviene perché le infrastrutture[5] di cui sono dotati gli Stati sono ormai talmente interconnesse e mutualmente dipendenti, sia fisicamente che attraverso sistemi *cyber-based* – ossia tecnologie di informazione e comunicazione su rete – per cui un attacco ad una infrastruttura può creare un effetto a cascata su altre, e non solo, ma anche su parte o l'intera popolazione della nazione colpita.

L'elemento che fa la differenza fra un crimine informatico e una guerra cibernetica entrambi propri della *cyber warfare* sta, quindi, nei soggetti che operano queste azioni e negli obiettivi colpiti: comuni ad entrambi, invece, sono le due categorie di attacco, ossia quelli "randomici" e quelli mirati. I primi richiedono uno sforzo minimo e hanno limitate capacità di danneggiare una rete se possiede un alto livello di resilienza, ossia capacità di adattarsi alla minaccia e all'attacco. Il secondo tipo di attacchi, invece, ossia quelli mirati, richiedono un impegno maggiore, sia nella scelta degli obiettivi da colpire che nel creare il tipo di danno.

Dalle analisi dei più recenti attacchi in rete e dalla tipologia degli obiettivi colpiti sino all'impatto che ne è derivato, è tuttavia emersa una più elevata sofisticazione delle capacità degli attaccanti. In particolare, per la sicurezza delle aziende e degli istituti finanziari è stata notata una progressiva saldatura fra le finalità economiche dei cyber criminali con quelle di comuni soggetti, come competitor interessati a compromettere la competitività e la reputazione dei loro concorrenti. Ciò è stato favorito anche dallo scarso livello di consapevolezza delle aziende in merito ai rischi provenienti dal cyberspazio. La complessità della rete e delle interrelazioni sia fra individui che fra Stati ha visto ampliare, negli anni, la gamma di operatori del crimine informatico, con strumenti innovativi e decisamente perniciosi per la sicurezza dei singoli come di intere comunità o di Stati. L'individuazione dei responsabili degli attacchi in rete o *attribution* (attraverso il c.d. "backtracking") risulta essere da sempre estremamente complessa, sebbene ogni attacco lasci tracce (tracciabilità di un attacco) che è possibile ripercorrere a ritroso per individuarne l'origine. Tuttavia, l'aggressore, chiunque esso sia, individuo o insieme di persone, proviene da un dominio de-territorializzato tanto che, raramente e a volte anche in maniera fortuita, si riesce ad individuare la fonte dell'attacco per via delle caratteristiche tecniche adottate o delle tracce linguistiche. Tutto ciò fa sì che i soggetti che operano illegalmente in rete siano ancora più occulti dei terroristi nella loro sfera di attività tradizionale in quanto costoro, di norma, hanno tutto l'interesse per propaganda a rivendicare un attentato.

Non è un caso, infatti, che il problema dell'attribuzione delle responsabilità di un attacco cyber sia oggetto di ricerca degli esperti del settore, al fine di sviluppare tecniche per il rilevamento geografico degli *hacker*. Lo stesso avviene per l'elaborazione di meccanismi di autenticazione al fine di ridurre l'anonimato in rete e risolvere questo problema in grado di compromettere qualsiasi forma di risposta, sia essa sanzionatoria o di rappresaglia vera e propria. Ciò è diventato oltremodo urgente dal momento che sono apparsi in rete i c.d. "virus asintomatici", ossia in grado di cancellare le proprie tracce e creare, con estrema rapidità, reti infettate di pc, c.d. "botnet". Ecco perché l'unica certezza che si ha in caso di attacchi informatici è l'identità della vittima, ossia l'obiettivo finale.

---

[5] Gori U, Bonfanti M.E., *L'attribuzione di operazioni cibernetiche quale requisito e strumento di risposta*, *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Cyber Warfare Conference, 2019, F. Angeli, Milano, 2019.

Vi è poi un'ulteriore complicazione data dal c.d. "deep web" ossia tutta la rete che non è indicizzata dai tradizionali motori di ricerca. Questo tipo di web non deve però essere confuso con il "dark web", un suo sottoinsieme, irraggiungibile attraverso la normale rete internet e solo con *software* particolari – il più noto è la rete TOR, The Onion Router – in cui si trovano tutti coloro (che così compongono il *darknet*, o reti oscure) che necessitano di utilizzare queste particolari funzionalità tecniche per *privacy* ed anonimato, come dissidenti politici che vogliono accedere a siti vietati nei loro Paesi.

La *cyber warfare* può essere condotta, inoltre, da singoli individui, comunità di soggetti statali o non-statali il cui scopo è raggiungere obiettivi economici oppure prettamente di tipo politico. Ad eccezione dei crimini per ottenere vantaggi economici immediati – come si vedrà meglio in seguito – gli attacchi propri della *cyber warfare* possono avere anche solo una funzione dimostrativa (per propaganda, ad esempio, ed è il caso del sedicente Stato Islamico, IS), oppure spionaggio militare circa la sicurezza e la difesa di una nazione (raccolta di dati), od anche la compromissione di strumenti militari o delle infrastrutture critiche (sabotaggio per vandalismo, o vero e proprio attacco), oppure possono contemplare in parte o tutte queste componenti messe insieme.

Se una nazione è esposta, invece, su scenari bellici, l'obiettivo di un'intrusione può essere il sistema di comando, controllo e comunicazioni delle operazioni militari che da tempo ha incorporato, oltre alla tradizionale *intelligence*, anche l'informatica. La violazione dello spazio cibernetico diventa, quindi, in questo caso un atto militare e la sua gravità dipende solo dall'obiettivo colpito e dal vantaggio che ne è derivato: un semplice pc portatile infettato, anche se di un alto Ufficiale delle Forze Armate avversarie, non crea un *casus belli*. Tuttavia, se questo virus si diffonde, copia dati, apre *backdoors* e attraverso queste invia informazioni a server remoti al punto da compromettere piani operativi e imporre una riorganizzazione della difesa e del sistema d'informazione di una nazione impegnata su un fronte militare, non vi è dubbio che rappresenti un'azione ostile, a cui opporre contromisure su piano operativo oltre che politico e diplomatico.

Possiamo aggiungere un ulteriore elemento: se ad essere colpito o infettato da un virus, quindi un'azione di sabotaggio, è una centrale nucleare, oppure un sistema di distribuzione delle acque o di controllo della rete ferroviaria od aeroportuale di una nazione, tali da compromettere l'incolumità dei civili, possiamo azzardare a definire un attacco cibernetico come uno strumento dal potenziale di "arma di distruzione di massa". Da tutto ciò si può dedurre la difficoltà nel distinguere fra semplice crimine informatico, *cybercrime,* e vera e propria conflittualità nello spazio cibernetico, in generale *cyber warfare*. Se si esclude il guadagno, infatti, le motivazioni dietro queste azioni possono essere molteplici, soprattutto nell'odierno contesto di relazioni internazionali, caratterizzato da numerosi conflitti non sempre armati, per cui arrecare danni ai sistemi informativi avversari o carpire informazioni strategiche può avere un significato elevato. Inoltre, secondo alcuni osservatori, l'aumento di attacchi informatici è da intendersi anche come un tentativo di destabilizzazione di una nazione, in quanto ne mostra l'inadeguatezza nella difesa o *cyber security*, imponendole quindi investimenti importanti in quella direzione.

Il soggetto che opera in maniera illecita sulla rete informatica genericamente, erroneamente e limitatamente, viene definito *hacker*. Tuttavia, nell'eccezione esatta del termine, l'*hacker* viola un sistema o una rete solo per modificare il codice sorgente di programmi per migliorarne le prestazioni, inducendo i gestori del sistema violato a prendere coscienza di un problema di sicurezza. L'*hacker* non agisce, infatti, per interesse economico e spartisce con la comunità cibernetica il principio per cui la condivisione della conoscenza è un punto di forza. Non a caso movimenti come l'*open source* e il *copyleft* sono nati e si sono sviluppati attraverso comunità di *hacker*. Sarebbe, quindi, più appropriato parlare di "crackers", ossia abili programmatori impegnati ad eludere o ad eliminare blocchi imposti a *software* e il cui fine è riuscire a trarre profitto dalle loro azioni. Tuttavia, per comodità e prassi nel linguaggio comune - come nel prosieguo di questo lavoro - si parla di *hacker* e di hackeraggio*.* Proprio perché non tutti gli *hacker* operano per fini illeciti, esiste in gergo una

distinzione che li connota in base al colore del cappello ("hat"). Vi sono così i *white hat* o *ethical hackers* appunto coloro che si limitano alla ricerca e alla violazione di sistemi – anche perché sovente ingaggiati dagli stessi proprietari dei servizi – condividendone le vulnerabilità scoperte con l'intera comunità informatica. Vi sono poi i *black hat* che operano spinti da motivi personali e per guadagno. Vi sono poi i *grey hat*, ossia coloro che una volta individuata una vulnerabilità, avanzano richieste finanziarie al produttore di quella tecnologia violata, ma escludono azioni malevoli nel caso di un diniego.

Gli *hacker* sono, quindi, i soggetti attivi di penetrazione e di violazione di un sistema e dagli obiettivi dei loro attacchi derivano le seguenti categorie.

Criminali/ladri informatici ("cyberthieves"), sono coloro che agiscono per mero interesse di lucro personale o per conto di una organizzazione criminale, e che accedono illegalmente per rubare, usare per sé stessi o vendere informazioni relative a nominativi e numeri di carte di credito e/o dati bancari. Il giro di affari illegali dei criminali/ladri informatici ha ormai raggiunto cifre inimmaginabili - e, sebbene non quantificabili con certezza, si ipotizza ormai un secondo posto dopo i guadagni legati al traffico di droghe - quando il costo annuale per il contrasto a quest'azione in 24 Paesi è di oltre 380 miliardi di dollari (dati Interpol). Tuttavia, ed è bene sottolinearlo, data la complessità e la natura ambigua dei costi associati al crimine informatico, così come la ricorrente riluttanza delle vittime a denunciare il furto o la frode online, non vi sono dati chiari, definitivi e disponibili pubblicamente circa questo tipo di attacchi. Le cosiddette "Spie informatiche" (*cyberspies*), ossia soggetti che rubano informazioni da siti o reti Intranet di enti governativi, istituzioni pubbliche o private, per ottenere un vantaggio strategico competitivo in politica, economia, finanza o nella sicurezza. Solitamente questi individui operano alle dipendenze di entità statali straniere e gli obiettivi includono, preferibilmente, reti informatiche governative o di aziende pubbliche o private che operano per conto della Difesa.

*Cyberwarriors*, sono agenti o presunti tali appartenenti a Stati che sviluppano capacità di intrusione malevola e intraprendono attacchi informatici in supporto ai propri obiettivi strategici nazionali. Sono i più difficili da individuare per le caratteristiche proprie degli attacchi e solitamente costoro sono alle dipendenze di governi stranieri. Quando una nazione viene attaccata, tuttavia, può solo presumere la provenienza dell'attacco e imputare ipoteticamente le responsabilità a nemici che, puntualmente, smentiscono o la addebitano ad azioni di singoli individui.

I Cyberterroristi, sono soggetti non statali, appartenenti ad organizzazioni terroristiche e forze eversive che utilizzano per lo più la rete come veicolo di comunicazione e di trasmissione di dati per l'indottrinamento ed il reclutamento attraverso la propaganda. Per quanto riguarda la minaccia terroristica ora prevalente, ossia quella jihadista, presentano delle capacità tecniche in grado di sferrare attacchi in rete con finalità e risultati in grado di creare vero e proprio terrore.

I Cyberattivisti o hacktivisti, in un termine già coniato negli anni '90, sono coloro che utilizzano le reti informatiche al fine di promuovere un'agenda politica o principi di connotazione sociale, ma mai a scopo di lucro. Vengono anche definiti attivisti digitali. Il gruppo Anonymous è sicuramente fra i più conosciuti. Le loro azioni si inquadrano per lo più come "azioni di disturbo", attraverso soprattutto attacchi DoS, come si vedrà in seguito, sia di siti istituzionali governativi che di aziende private.

È un fenomeno che si sta ampliando e, grazie ai *social network*, ottiene una rilevante eco sul web, definito, non a caso, anche "camera dell'eco" di fenomeni sociali. Sebbene non abbia conseguenze nefaste dal punto di vista tecnico, trattandosi per lo più di hackeraggio lieve con moderati danni operativi, di certo rappresenta una forma d'azione e di protesta politica che ha, però, un impatto forte sulle nuove generazioni più avvezze all'uso di strumenti informatici. L'*hacktivism* è, infatti, il principale responsabile di intrusioni malevoli contro aziende non per sottrarre informazioni o per interesse economico, ma per quel che esse rappresentano nello specifico. Si tratta per lo più di attacchi semplici, anche goffi tecnicamente ma efficaci perché, comunque, l'obiettivo dei cyberattivisti viene sempre raggiunto, ossia mandare un messaggio specifico di protesta contro

elementi considerati, a loro parere, come i principali responsabili di tutti i mali di cui soffre l'umanità: ecco che vengono colpite industrie legate alla difesa, alle comunicazioni ma anche quelle farmaceutiche e chimiche.

È necessario sottolineare che a nessuna di queste categorie di *hacker* appartiene un tipo esclusivo di attacco, così come possono convergere su un aggressore una o più caratteristiche sopraelencate. Ad esempio, un *hacker* che, violando un sistema informatico di un'azienda, si appropria dei documenti relativi a un brevetto (proprietà intellettuale) può essere al contempo un "ladro" e una "spia", ossia trarre un vantaggio economico vendendo le informazioni così trafugate a un competitor straniero, sia esso azienda o ente governativo. Lo stesso accade per il crimine informatico in generale che, secondo alcuni rapporti, ha superato il traffico di stupefacenti come fonte di guadagno per i gruppi terroristici. Non è facile, quindi, stabilire gli ambiti, le capacità e le intenzioni di un aggressore.

Ciò che sicuramente fa la differenza è la scelta degli obiettivi, da cui dipendono gli strumenti. Il più delle volte le azioni di hackeraggio operano attraverso le e-mail, considerate non a caso i principali vettori di attacchi informatici. I sistemi più utilizzati fanno parte della categoria c.d. "phishing", ossia tentativi di carpire informazioni sensibili con l'invio di email generiche, il cui scopo è convincere il destinatario ad aprire l'email. I dati ottenuti vengono utilizzabili per fini di lucro, oppure per trasferire somme di denaro o come ponte per altri attacchi, tra i quali troviamo *spam*[6], *spearphishing*[7] (nel solo 2018, è stato il preferito per il 65% degli attacchi criminosi e presente nel 78% dei casi di cyber spionaggio)[8], *malware* e così via.

Costoro concretizzano quella molteplicità di illeciti tipici del crimine informatico così come viene inteso dalla giurisprudenza nazionale e internazionale, dai più comuni furti d'identità alle truffe tramite *internet banking*, alle operazioni di frodo *ransom*, e così via. Si tratta, comunque, di azioni di intromissione a relativamente basso profilo tecnico, sebbene con rilevantissimi vantaggi economici, da distinguere da quelle a maggior impatto operativo come le DDoS, o quelle il cui obiettivo è la violazione dei diritti di proprietà intellettuale (IP), con più ragguardevoli propositi illeciti che si configurano, però, come spionaggio industriale vero e proprio.

Per il primo caso, infatti, ossia illeciti on-line per un guadagno immediato, si tratta perlopiù di *mass attacks*, ossia di azioni indiscriminate ad ampio spettro e con una pluralità di bersagli indistinti ma con un'unica caratteristica, ossia l'individuazione delle vittime di possibili obiettivi di furti e di truffe attraverso la raccolta di informazioni personali e l'aggancio alle loro email. In questo caso, un ruolo dominante è svolto dai *social network*, in particolare da *Facebook, Twitter* e *LinkedIn*, considerando che la logica che muove il criminale informatico è quella di colpire ciò che è popolare e utilizzato più diffusamente, a seconda dell'area geografica e delle abitudini, quindi, degli utenti della rete.

Quando invece l'irruzione criminale sulla rete giunge a violare l'IP di un'azienda e tenta, quindi, di impossessarsi di informazioni personali ma soprattutto di brevetti o di studi di ricerche scientifiche, oppure viola piani di gestione aziendali, l'azione assume il carattere di spionaggio industriale vero e proprio. In questo caso si utilizzano gli *spyware*, ossia *software* malevoli in grado di spiare la vittima scelta, raccoglierne i dati, e trasmetterli a terzi per il loro sfruttamento: la rilevazione di questi *spyware* è sovente difficoltosa a causa della natura delle tecniche di occultamento impiegate.

A tal proposito e con un linguaggio militare si parla di "targeted attacks", ossia di attacchi mirati, come in un conflitto. In definitiva, si tratta di una guerra economica che può provenire da entità statuali straniere e il cui obiettivo finale è l'indebolimento del potenziale strategico avversario.

---

6 Da cui "spamming", ossia l'invio indiscriminato e ripetuto di messaggi e-mail verso indirizzi generici e non verificati, soprattutto per fini commerciali.

7 Si tratta di una categoria di *phishing*. È però un attacco mirato.

8 Europol, IOCTA, Internet Organized Crime Threat Assessment, 2019, pag. 52.

Ecco perché diventa imperativo salvaguardare le aziende non solo dallo spionaggio industriale ma anche dal rischio di sabotaggio. Infatti, non sempre è chiaro il pretesto che sottostà a questi attacchi: il confine fra spionaggio e sabotaggio è tanto sottile quanto è grande la strategicità dei settori colpiti, come quella delle industrie per la difesa o quelle chimiche. Gli attacchi di questo tipo, con difficile individuazione del pretesto iniziale, sono cresciuti in maniera vertiginosa negli ultimi dieci anni anche per via dell'aumentata instabilità politica ed economica mondiale e l'emergere di una maggiore competizione fra potenze.

Genericamente sia per il crimine informatico che per la *cyber warfare* si parla di virus, anche se si sta tentando di dare definizioni formali e/o legali a questi strumenti di intrusione o "cyber tools" che, per via della conflittualità nel cyberspazio, alcuni ormai preferiscono definire *digital* o *cyber weapons*, le c.d. armi cibernetiche. Al momento, tuttavia, non vi sono né manuali militari né giurisprudenza internazionale che definiscano in modo condiviso ed esaustivo il termine di "cyber weapon". È fondamentale, però, sottolineare un aspetto, ossia che nel campo della battaglia digitale è proprio la qualità di questi strumenti e non semplicemente il numero di addetti alla *cyber warfare* a fare la grande differenza fra potenze.

Un aspetto terribilmente moderno, amplificato soprattutto dalle nuove e costanti esigenze geopolitiche, storiche e sociali è il fenomeno del terrorismo cibernetico. Il dibattito sull'esistenza e natura del cyber terrorismo risale già agli anni '90, periodo in cui vennero inventate dai media innumerevoli metafore, che ne definivano il carattere catastrofico, ma senza individuare chiaramente i soggetti responsabili di tale minaccia: si parlava così di Phantom Menace, Cyber-Scare, Cyber Doom, Cyber Katrinas, Digital Pearl Harbour etc. Se ne percepiva, quindi, la minaccia, ma – com'è d'altronde logico in un ordine internazionale ancora in divenire, come quello proprio all'indomani della fine della Guerra Fredda – non si percepiva la vera natura dell'identità dei responsabili.

Inevitabile che, con una più chiara identificazione di soggetti intesi come terroristi, come dopo l'11 settembre e la dichiarazione di "guerra al terrore" lanciata dall'amministrazione G.W. Bush, anche i contorni del cyber terrorismo sono andati via via definendosi. Fu infatti da allora che si prese in considerazione l'eventualità che gli "Stati canaglia" avessero anche capacità di lanciare attacchi cibernetici contro infrastrutture, interessi pubblici e privati, commercio internazionale, sia statunitensi che degli alleati. Ecco che, da quel momento in poi, le amministrazioni statunitensi iniziarono ad usare le espressioni *cyber terrorism* e *cyber warfare* senza alcuna distinzione, se non in base alla gravità e percezione di rischio in ogni specifica situazione. Un comportamento che ancora oggi persiste e che alimenta confusione circa la definizione esatta della natura della minaccia cyber da parte di entità-soggetti non statuali. È comunque anche un effetto derivante dalla difficoltà che ancora persiste nel definire ciò che si debba intendere per terrorismo: un dibattito sempre attuale, mai risolto, la cui complessità rispecchia quanto avviene a livello di disordine e caos internazionale.

Tentiamo, comunque, di darne una definizione.

Il cyber terrorismo, inteso come un ampliamento del concetto di *cyber warfare*, può essere quell'azione premeditata di disturbo o di minaccia attraverso internet al fine di recare danno o incoraggiare attività illecite, oppure per intimidire una o più persone, a fini ideologici, religiosi o politici. Tuttavia, secondo alcuni autori: "*il cyber terrorismo non esiste, perché in sé un cyber attack non può causare terrore*". Come si evince da questa dichiarazione, peraltro datata, si è nel campo dell'opinabilità, anche se al momento sono pochi gli elementi che dimostrino il contrario.

Per dare, tuttavia, un più chiaro riferimento a ciò che si intende per *cyber terrorism* è utile una griglia interpretativa che raccolga 4 approcci:

- Oggettivo, ossia basato sull'azione concreta, a cui concorrono 3 fattori:
  a. la presenza di strumenti elettronici, tecnologia informatica e internet (quest'ultimo strumento e obiettivo di attacchi);
  b. una motivazione terroristica, sia essa ideologica, etnica o religiosa;

c. l'autore dell'atto non deve essere vincolato ad uno Stato o agenzia governativa. Se viene a mancare questa caratteristica, l'atto rientra in un più ampio concetto di cyber guerra o di *information warfare*.

- Soggettivo, che si concentra sull'artefice dell'azione. Si sta rivelando come l'approccio preferito dagli enti preposti all'investigazione, sia per prevenire attacchi che smantellare reti di propaganda, indottrinamento, progettazione di attacchi e reclutamento, in particolare per il terrorismo di matrice jihadista. Rispecchia, altresì, l'evoluzione dell'approccio di contrasto al terrorismo, non più incentrato esclusivamente sul fatto/incidente terroristico in sé, quanto su informazioni, valutazioni e deduzioni che provengano dall'analisi del comportamento ante il fatto eversivo del singolo soggetto, sia costui un lupo solitario, un auto-radicalizzato, o un *would-be fighter*, ossia di un soggetto che, impossibilitato a raggiungere scenari di conflitto jihadista ma desiderando partecipare al jihad, operi attraverso il web, attuando quella che è stata definita "cyber jihad". Fra questi soggetti ritroviamo ora la figura del *cybercoaching* o *virtual entrepreneur*, imprenditore virtuale che sta sostituendo, in particolare nel mondo occidentale, sia le cellule che i lupi solitari. Si tratta di un ibrido fra queste due figure: esso opera sul web e attraverso piattaforme criptate per il reclutamento e la logistica per gli spostamenti di terzi che segue, sempre virtualmente, sino alla destinazione geografica, ossia le aree di conflitto jihadista.
- Approccio incentrato sull'Obiettivo, o "target approach", che considera come *cyber terrorism* "l'utilizzo di strumenti di reti di computer per il danneggiamento o messa fuori uso di infrastrutture critiche". Esso completa i due approcci precedenti, mettendo altresì in evidenza la criticità degli obiettivi e permettendo quindi di focalizzare la prevenzione e la sicurezza su *target* specifici, individuandone la loro vulnerabilità e, di conseguenza, permettendo la progettazione di piani di protezione, gestione del rischio e, se possibile, anche misure di deterrenza.
- Vi è poi l'ultimo approccio quello c.d. "Matrix approach", o a forma di griglia, che considera una moltitudine di elementi, come persone, gruppi, vittime, posti, metodologie, affiliazioni, motivazioni, etc. Più generico, questo approccio offre tuttavia maggior flessibilità, per cui più adattabile alle differenti definizioni ancora vigenti da parte dei diversi governi.

Rifacendosi a quanto scritto sopra, relativamente al limitato costo di programmi malevoli da lanciare in rete e infettare obiettivi sensibili, si potrebbe facilmente dedurre che il cyberspazio possa essere, quindi, un terreno d'azione per attacchi terroristici, capaci di colpire le infrastrutture critiche di una nazione. Al momento tutto ciò fa però parte di una narrazione che non ha trovato riscontri e conferme. Infatti, per il terrorismo di matrice jihadista - ossia la minaccia eversiva attualmente più potente, diffusa ed attiva - è più facile e meno costoso spargere terrore attraverso azioni fisiche vere e proprie che agire in rete. Si è quindi più propensi ora a considerare gli atti effettuati in rete da appartenenti al mondo jihadista più come azioni criminali per lucro o di incitamento all'odio, per proselitismo, reclutamento, etc. Tuttavia, il dibattito è molto ampio e presenta numerose sfaccettature che variano per via di impostazioni culturali differenti (il riconoscimento o meno di gruppi come eversivi) e soprattutto sul mancato accordo della comunità internazionale su un significato condiviso di "terrorismo". Al momento, e nell'evenienza, la distinzione fra un atto criminale e quello terroristico dipende, quindi, soprattutto dagli obiettivi colpiti e dagli scopi che si vogliono raggiungere.

Tuttavia, l'azione di contrasto alle forme eversive, di qualsiasi natura e sigla, agenti sul web a livello nazionale vede operare in attività preventiva ed informativa la Polizia Postale in collaborazione con la Direzione Centrale della Polizia di Prevenzione e le unità locali della Digos. Costoro concorrono con altri organismi e all'*intelligence* nazionale anche alla *prevenzione*, l'aspetto più difficile, allo stato attuale dell'attività di contro terrorismo, data la natura della moderna eversione, ossia giovane (e quindi, nel caso di terrorismo di matrice jihadista, facilmente vittima di auto-

radicalizzazione) ma soprattutto nativa digitale, per cui maggiormente avvezza all'uso di strumenti informatici. Competenze a volte anche di elevata qualità, a cui si aggiunge conoscenza linguistica (essendo sovente figli di immigrati) e, nel caso, religiosa o ideologica (se eversione legata a movimenti di estrema destra).

Ne è nata, quindi, una sinergia fra i differenti comparti nazionali di contrasto al terrorismo, che ha visto nel tempo la collaborazione sia in ambito di raccordo info-investigativo che di quello tecnico-operativo.

Fra le misure utilizzate dalla Polizia Postale, in particolar modo, la creazione *ad hoc* di profili fittizi per infiltrarsi, grazie anche all'aiuto di mediatori linguistici e culturali, in ambiente cyber in special modo dei *social media* e delle *app* di messaggistica. Dall'azione, per così dire, di controllo e monitoraggio "locale", la creazione di *account* fittizi è stata altresì utilizzata per l'accreditamento in gruppi sostenitori dell'IS, tanto da portare ad operazioni con arresti di cellule attive nella propaganda jihadista e nel reclutamento (*cybercoachings* visti in precedenza) su piattaforme *social*.

Non si tratta sempre di operazioni semplici, data la capacità dimostrata di alcuni soggetti finiti sotto controllo, di utilizzare differenti profili simultaneamente, collegandosi tra l'altro a rete *wireless* aperte che garantiscono l'anonimato.

Ulteriori risultati si sono avuti anche nel contrastare azioni di incitamento ad azioni terroristiche attraverso l'uso di Telegram: indagini molto complesse per identificare il/i responsabile/i vista l'impossibilità di collaborazione da parte dei gestori della piattaforma.

Trattandosi comunque di un fenomeno internazionale e addirittura transnazionale per via della sua presenza, appunto, in rete, risulta imprescindibile la cooperazione sovranazionale, con gli strumenti tradizionali ma in particolare con *l'information sharing* fra organismi preposti all'investigazione e al contrasto. Proprio il Servizio di Polizia Postale e delle Comunicazioni, al riguardo, è il punto di contatto nazionale dell'Internet Referral Unit (IRU) dell'Europol, ossia l'unità preposta a ricevere da tutti i Paesi membri dell'UE le segnalazioni relative a propaganda jihadista. In ambito IRU, infatti, vengono utilizzate piattaforme tecnologiche specifiche per lo scambio di informazioni, tra cui Check-the-Web (CTW) e Sirius, a supporto del monitoraggio e delle indagini sulla rete in ambito terroristico. Ancora una volta, la capacità di acquisire informazioni e soprattutto la loro condivisione fanno la differenza nel contrastare l'azione eversiva, anche in rete e salvaguardare l'integrità dello Stato.

**Bibliografia**


- AA.VV., 2016 Italian Cybersecurity Report. Controlli Essenziali di Cybersecurity, CINI, Roma, 2017.
- AA.VV., Rapporto CLUSIT 2019 sulla sicurezza ICT in Italia, Milano, 2019.
- EUROPOL, IOCTA, Internet Organised Crime Threat Assessment, 2019.
- Frediani C., Guerre di Rete, Bari-Roma, 2017.
- Gori U., Germani S.L. (a cura di), La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale, Milano, 2013.
- Gori U., Lisi S. (a cura di), La protezione cibernetica delle infrastrutture, Milano, 2014.
- Gori U., Martino L. (a cura di), Intelligence e interesse nazionale, Roma, 2015.
- Gori U. (a cura di), Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche, F. Angeli, Milano, 2019.
- Il glossario di sicurezza cibernetica, in Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, *Glossario Intelligence*, *Appendice,* Roma, maggio 2019.
- Presidenza del Consiglio dei Ministri, Piano nazionale per la Protezione Cibernetica e la Sicurezza Informatica, Roma, 2017.
- Presidenza del Consiglio dei Ministri, Quadro strategico nazionale per la sicurezza dello spazio cibernetico, Roma, 2013.
- T. Shamane, Cyber Risk Leaders, Ed. My Security Media, 2019.

# Il *Green Deal Industrial Plan*. La tutela del Mercato Unico e degli interessi economici nazionali

## 1. Il *Green Deal Industrial Plan*: le politiche europee per la tutela del Mercato Unico

La crisi economica, l'emergenza sanitaria (COVID-19) ed il conflitto in Ucraina del 2022 sono fattori che hanno contribuito a mutare le prospettive economiche e sociali nel contesto europeo e internazionale[1].

Lo sviluppo di economie solide, sostenibili e resilienti basate sull'innovazione (declinata nelle sue più ampie accezioni) sono i fattori individuati a livello europeo per evitare effetti asimmetrici per gli Stati membri[2] e favorire la ripresa economica in modo efficace, equo e inclusivo[3].

Parallelamente, il *Green Deal*[4] ha definito il percorso europeo verso la transizione ecologica, che prevede obiettivi climatici di "emissioni nette-zero" entro il 2050. Le misure "*Fit for* 55"[5] e il piano *REPowerEU*[6] intendono orientare l'economia europea in questa direzione.

Per favorire lo sviluppo economico, l'Unione Europea ha definito ulteriori sostegni finanziari per gli Stati membri attraverso il ricorso al debito per accelerare l'attuazione di riforme nazionali[7] volte ad una crescita economica degli Stati membri capace di superare le carenze strutturali delle economie nazionali, e garantire una maggiore competitività anche nel contesto internazionale, in linea con il processo di transizione verso i c.d. "sei pilastri" del dispositivo europeo per la ripresa e la resilienza. La transizione verde, la trasformazione digitale, la crescita intelligente, sostenibile e inclusiva (che comprenda coesione economica, occupazione, produttività, competitività, ricerca, sviluppo e innovazione, e un mercato interno ben funzionante con piccole e medie imprese forti), la coesione sociale e territoriale, la salute e resilienza economica, sociale e istituzionale e le politiche

---

1 *Ex multis*, cfr. in relazione alla cd. "crisi energetica": A. VITA, *Climate change e crisi energetica, quali prospettive*, in *Riv. trim. dir. econ*., 2021, 568 e s.

2 Commissione UE, *Relazione 2020 in materia di previsione. Previsione strategica: tracciare la rotta verso un'Europa più resiliente*, 9 settembre 2020; G. LUCHENA, *Crisi energetica e aiuti di stato*, in *Riv. trim. dir. eco*., 2022, suppl. 1, 129 e s.

3 Commissione UE, *New European Bauhaus. Beautiful, Sustainable, Together*, 15 settembre 2021; L. AMMANNATI, *Transizione energetica, "just transition" e finanza*, in *Riv. trim. dir. eco.*, 2022, supl. 1, 289 e s.

4 Commissione UE, *Il Green Deal europeo*, 11 dicembre 2019; Commissione UE, *European Green Deal: Commission proposes transformation of EU economy and society to meet climate ambitions*, 2021. In dottrina: M. PASSALACQUA, *Green Deal e transizione digitale verso un diritto eventuale*, in M. Passalacqua (a cura), *Diritti e mercati nella transizione ecologica e digitale*, cit, 14 e s.; F. DONATI, *Il Green Deal e la governance europea dell´energia e del clima*, *Riv. Reg. Mercati*, 2022, 13 e s.

5 *Fit for 55* è un insieme di misure pubblicate il 14 luglio 2021, prevede interventi normativi nei settori dell'energia, del clima e dei trasporti Cfr. il sito web del Consiglio europeo, in *https://www.consilium.europa.eu/it/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition/*.

6 REPowerEU è il piano volto ad intervenire nel settore energetico, riducendone il consumo e diversificandone l'approvvigionamento. Cfr. il sito web della Commissione UE, in *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_it.*

7 Il piano *NextGenerationEU* intende costituire uno strumento per consentire all'Unione Europea di assumere prestiti sui mercati finanziari a tassi più favorevoli rispetto a molti Stati membri ridistribuendo gli importi. Con l'obiettivo di raccogliere circa 672,5 miliardi di euro (312,5 sovvenzioni, i restanti 360 miliardi prestiti a tassi agevolati) fino al 2026 alle migliori condizioni finanziarie (5% del PIL dell'UE), la Commissione UE si propone di ricorrere ad una strategia di finanziamento diversificata, determinando il sostegno finanziario a ciascuno Stato sulla base di un contributo finanziario massimo che sarà erogato in funzione del conseguimento dei risultati in riferimento ai traguardi e agli obiettivi del piano per la ripresa e la resilienza. Cfr. Regolamento UE 2021/241, 12 febbraio 2021, *che istituisce il dispositivo per la ripresa e la resilienza*; Commissione UE, *The EU as a borrower – investor relations*, accessibile in *https://ec.europa.eu/info/strategy/eu-budget/eu-borrower-investor-relations_it*; Commissione UE, *NextGenerationEU - Strategia di finanziamento*, 2021, in *https://ec.europa.eu/info/sites/default/files/about_the_european_commission/eu_budget/2021.1966_it_002_21.05.pdf* . In dottrina: F. CAPRIGLIONE, *Covid-19. Quale solidarietà, quale coesione nell'UE?*, in *Riv. trim. dir. econ*., 2020, 167-227; L. CIPRIANI, *Covid-19 e finanza UE. Il recovery fund e le altre misure a confronto come piano di rinascita per l'Europa*, in *Riv. trim. dir. econ*., 2021, 5

per la prossima generazione sono identificati quali obiettivi per lo sviluppo economico del Mercato Unico[8].

Il coordinamento di tale strumento finanziario con altre forme di finanziamento europeo (quali il fondo *InvestEU* ed i fondi strutturali)[9] è volto a produrre effetti trasversali per incidere in maniera efficiente sul mercato europeo.

In questo contesto giuridico ed economico complesso si è avvertita la necessità di tutelare gli interessi economici nazionali degli Stati membri.

Il *Green Deal Industrial Plan* europeo si propone di rafforzare la competitività dell'industria europea a zero emissioni, stimolando lo sviluppo industriale delle imprese UE in tale settore[10].

Tale piano si fonda su quattro concetti: la semplificazione del quadro normativo di riferimento, l'accesso delle imprese ad investimenti e finanziamenti per la produzione di tecnologie pulite in Europa, lo sviluppo di un *know-how* necessario alle imprese per una transizione verde e la cooperazione globale intesa quale apporto del mercato alla transizione verde. Interventi giuridici nell'economia saranno attuati per la loro implementazione.

La Commissione UE intende presentare una disciplina sull'industria a zero emissioni per individuare gli obiettivi di capacità industriale e fornire un quadro normativo idoneo che intervenga sul rilascio di autorizzazioni semplificate e a sostegno dell'espansione delle tecnologie nel Mercato Unico[11]. L'Unione Europea si propone di intervenire in particolare sulla disciplina delle materie prime (per garantire l'accesso a materiali essenziali per la produzione di tecnologie), e del mercato dell'energia elettrica, al fine di ridurre i costi nel Mercato Unico e evitare che la dipendenza dai Paesi esportatori influenzi le scelte politiche degli Stati membri.

Riforme mirate e volte a semplificare gli ordinamenti giuridici nazionali, unitamente a finanziamenti pubblici[12], possono contribuire alla ricerca e sviluppo nell'Unione Europea e attrarre ulteriori investimenti privati necessari per la transizione verde[13]. La Commissione UE intende

---

8 Regolamento UE 2021/241, art. 3. Tali obiettivi sono ricompresi, nell'ordinamento giuridico italiano, nel Piano Nazionale di Ripresa e Resilienza (PNRR), che si sviluppa lungo sei missioni coerenti con i pilastri per la ripresa e resilienza definiti a livello europeo. Le sei missioni sono individuate in: 1 - digitalizzazione, innovazione, competitività e cultura; 2 - rivoluzione verde e transizione ecologica; 3 - infrastrutture per una mobilità sostenibile; 4 - istruzione e ricerca; 5 - inclusione e coesione; 6 – salute. Si v. Piano Nazionale di Ripresa e Resilienza - PNRR, 2021, accessibile in *https://www.governo.it/sites/governo.it/files/PNRR_0.pdf*. Cfr. anche: Italia Domani (https://italiadomani.gov.it/it/home.html). Circa l'attuazione del PNRR si v. il d.l. 31 maggio 2021, n. 77, avente ad oggetto la *Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*, conv. con l. 29 luglio 2021, n. 108. In dottrina: F. BASSANINI, *Le riforme, il "vincolo esterno europeo" e la governance del PNRR: lezioni da un'esperienza del passato*, in *Astrid*, 2021; ID., *Il PNRR e gli investimenti infrastrutturali in Italia*, in *Astrid*, 19 aprile 2021; L. TORCHIA, *L'amministrazione presa sul serio e l'attuazione del PNRR*, in *AIPDA FORUM Next Generation EU,* 1° aprile 2021; M. CLARICH, *Il Piano Nazionale di Ripresa e Resilienza tra diritto europeo e nazionale: un tentativo di inquadramento giuridico*, in *Corriere Giur*., 2021, 8-9, 1025; M. MACCHIA, *La governance del piano di ripresa*, in *Giornale Dir. Amm*., 2021, 733 e s.; C. A. MAURO, *La sharing economy nel Piano Nazionale di Ripresa e Resilienza (PNRR) tra Stato e mercato*, in *Riv. trim. dir. econ.*, 2022, 83 e s.

9 Regolamento UE 2021/523, *che istituisce il programma InvestEU*. Sul programma si v. *https://europa.eu/investeu/home_en*. Circa i fondi strutturali, il riferimento è al Fondo europeo di sviluppo regionale, al Fondo sociale europeo, al Fondo di coesione, al Fondo europeo agricolo per lo sviluppo rurale e al Fondo europeo per gli affari marittimi e la pesca.

10 Commissione UE, *A Green Deal Industrial Plan for the Net-Zero Age*, 1 febbraio 2023.

11 La proposta della Commissione UE è stata discussa dal Consiglio europeo in occasione della riunione straordinaria del 9 febbraio 2023. Si v. il sito del Consiglio europeo accessibile in *https://www.consilium.europa.eu/it/meetings/european-council/2023/02/09/*.

12 Ricorrendo ai finanziamenti derivanti dal Piano *REPowerEU*, dal programma *InvestEU* e dal Fondo per l'innovazione (in cui sono previsti 38 miliardi di euro di sostegno dal 2020 al 2030 per lo sviluppo commerciale di tecnologie innovative a basse emissioni di carbonio, con l'obiettivo di immettere sul mercato soluzioni industriali per decarbonizzare l'Europa e sostenere la sua transizione verso la neutralità climatica. Si v. *https://climate.ec.europa.eu/eu-action/funding-climate-action/innovation-fund/what-innovation-fund_en*).

13 Si v. la strategia europea sulla finanza sostenibile: Commissione UE, *Strategy for Financing the Transition to a Sustainable Economy*, 6 luglio 2021.

contemperare le esigenze connesse al rispetto della disciplina della concorrenza[14] (garantire il corretto funzionamento del mercato interno quale fattore per il benessere dei cittadini, delle imprese e della società dell'UE), semplificando nel contempo i procedimenti per la concessione da parte degli Stati membri degli "aiuti" pubblici per accelerare la transizione verde[15].

La necessità di sviluppare specifiche competenze e professionalità nei settori economici connessi alla transizione ecologica comporta la definizione di specifiche attività formative e interventi sul mercato del lavoro[16].

La cooperazione globale (nell'ambito delle attività dell'Organizzazione Mondiale del Commercio – OMC) nella catena di approvvigionamento come strumento per supportare la transizione verde può rappresentare un valore aggiunto. Accordi di libero scambio e forme di cooperazione possono costituire un canale di dialogo per garantire l'approvvigionamento globale attraverso una base industriale competitiva e diversificata[17].

La Commissione proteggerà inoltre il mercato unico dal commercio sleale nel settore delle tecnologie pulite e utilizzerà i suoi strumenti per garantire che i sussidi esteri non distorcano la concorrenza nel mercato unico, anche nel settore delle tecnologie "green".

## 2. Gli aiuti di Stato come strumento di politica economica volta al perseguimento degli interessi europei

La disciplina sugli aiuti di Stato[18] costituisce un complesso normativo organico ed è tradizionalmente considerato una materia di confronto tra gli interessi dell'Unione Europea e quelli degli Stati membri. Profilo discusso è il rapporto tra la necessità di tutelare il mercato ed il perseguimento di interesse nazionali, in un contesto in cui le deroghe al divieto di aiuti di Stato possono costituire strumento di politica economica europea.

La relazione tra tutela della concorrenza e il governo pubblico dell'economia è evidente ove gli aiuti di Stato sono ritenuti strategici, e quindi legittimi, per la realizzazione di attività volte a creare un impulso all'economia tale da implementare la concorrenza nel Mercato Unico[19].

---

[14] Sul fondamento giuridico della disciplina della concorrenza nell'ordinamento giuridico europeo si v. TFUE, artt. 101-109 ed il protocollo n. 27 sul mercato interno e sulla concorrenza. In dottrina, *ex multis*: B. Raganelli, *Concorrenza, regolamentazione, vigilanza e tutela*, Milano, Cedam, 2019; M. Libertini, *Diritto della concorrenza dell'Unione Europea*, Milano, Giuffrè, 2014; L. F. Pace (a cura di), *Dizionario sistematico del diritto della concorrenza*, Napoli, Jovene, 2013; G. Tesauro, *La tutela della concorrenza tra diritto comunitario e diritto italiano*, in *Econ. Pol. Ind*., 2003.

[15] La Commissione UE si propone di consultare gli Stati membri in merito ad una modifica del quadro temporaneo per gli aiuti di Stato in caso di crisi e transizione e rivedere il regolamento generale di esenzione per categoria alla luce del Green Deal (aumentando le soglie di notifica per il sostegno agli investimenti verdi). Tra le proposte della Commissione è altresì valutata la possibilità di utilizzare dei fondi UE esistenti per finanziare l'innovazione, la fabbricazione e la diffusione delle tecnologie verdi (a medio-lungo termine, maggiori finanziamenti UE per sostenere gli investimenti nella produzione di tecnologie a zero emissioni potranno essere messi a disposizione mediante un fondo per la sovranità europea che la Commissione UE intende proporre. Cfr. Commissione UE, *State aid: Commission consults Member States on proposal for a Temporary Crisis and Transition Framework*, 1° febbraio 2023, in cui si chiarisce come la Commissione UE intenda intervenire sul Regolamento (UE) 17 giugno 2014, n. 651, *che dichiara alcune categorie di aiuti compatibili con il mercato interno in applicazione degli articoli 107 e 108 del trattato*, che consente agli Stati membri di attuare direttamente le misure di aiuto, senza doverle notificare preventivamente alla Commissione per approvazione. Quest'ultima modifica è connessa a favorire la realizzazione degli Importanti Progetti di Comune Interesse Europeo (IPCEI).

[16] La Commissione UE intende proporre l'istituzione di una *Academy* per l'industria a zero emissioni al fine di attuare programmi per migliorare le professionalità esistenti e riconvertirle nelle industrie strategiche.

[17] L'Unione Europea ha sviluppato accordi di facilitazione degli investimenti sostenibili (*Sustainable Investment Facilitation Agreements* - SIFA), in particolare in Africa, per facilitare l'attrazione e l'espansione degli investimenti integrando gli impegni in materia di ambiente e diritti del lavoro.

[18] TFUE, artt. 107-109. Circa la possibilità di configurare aiuti di stato nel finanziamento di attività di ricerca e sviluppo si v.: Commissione UE, *Disciplina degli aiuti di stato a favore della ricerca, sviluppo e Innovazione*, 27 giugno 2014.

[19] A titolo esemplificativo, provvedimenti a favore delle imprese possono ridurre gli ostacoli all'ingresso in un determinato mercato di riferimento o promuovere una politica di infrastrutture a sostegno di aree territoriali da rigenerare o settori economici.

Nel 2022, la Commissione Europea era già intervenuta mediante l'approvazione di nuove linee guida sugli "aiuti di Stato a favore del clima, dell'ambiente e dell'energia"[20].

Nell'attuale contesto economico internazionale i provvedimenti discussi conseguono all'invito di alcuni Stati membri all'Unione Europea di "*bolster its energy and industrial strategic sovereignty*"[21] e costituiscono una risposta europea ai provvedimenti economici posti in essere negli Stati Uniti[22]. Dal punto di vista della politica commerciale europea, un profilo controverso dei provvedimenti statunitensi è rappresentato dal fatto che l'accesso agli incentivi è legato in molti casi a criteri di idoneità legati alla produzione o all'approvvigionamento sul mercato nazionale, circostanza che escluderebbe le imprese europee.

Condizioni di reciprocità tra l'Unione Europea e gli Stati Uniti sono in via di definizione[23] e parrebbero definire obiettivi comuni[24], riconoscendo la rilevanza delle catene di approvvigionamento connesse alle materie prime "critiche"[25].

La necessità di limitare la delocalizzazione all'estero di imprese europee innovative e mantenere attrattiva e competitiva l'industria dell'Unione europea in settori di interesse strategico costituiscono obiettivi essenziali per tutelare l'economia e gli interessi europei[26].

---

20 Commissione UE, *Disciplina in materia di aiuti di Stato a favore del clima, dell'ambiente e dell'energia*, 27 gennaio 2022.

21 Si v. il joint statement tra Bruno Le Maire (Minister of the Economy, Finance and industrial and digital Sovereignty of France) e Robert Habeck (vice-chancellor, Federal Minister of Economic Affairs and Climate action of Germany), 22 novembre 2022, accessibile in *https://presse.economie.gouv.fr/22112022-joint-statement-by-bruno-le-maire-and-robert-habeck-we-call-for-a-renewed-impetus-in-european-industrial-policy/,* in cui si propone l'intento di "*pursue and engage in an ambitious, competitiveness-seeking future-oriented European industrial policy which aims at boosting European strategic sovereignty*".

22 Si v. l'*Inflation Reduction Act - IRA*, sottoscritto il 16 agosto 2022 è il terzo atto legislativo approvato dagli Stati Uniti d'America dalla fine del 2021 con l'obiettivo principale di incidere sulla competitività economica e la produttività industriale degli Stati Uniti. La *Bipartisan Infrastructure Law - BIL*), il *CHIPS & Science Act* e l'*IRA* hanno priorità parzialmente sovrapposte e insieme introducono 2 mila miliardi di dollari in nuove spese federali nei prossimi dieci anni. Il solo IRA prevede investimenti e sussidi per circa 370 miliardi di dollari. Cfr. *https://www.whitehouse.gov/cleanenergy/inflation-reduction-act-guidebook/*. L'Ufficio di bilancio del Congresso degli Stati Uniti (*Congressional Budget Office - CBO*) stima che la legge ridurrà i deficit di bilancio di circa 58 miliardi di dollari nel prossimo decennio, per l'effetto combinato degli aumenti di spesa e delle maggiori entrate. Sul punto, cfr. Congressional Budget Office*, Estimated Budgetary Effects of Public Law 117-169*, accessibile in *https://www.cbo.gov/publication/58455*.

23 Il 27 ottobre 2022, è stata costituita una *task force* UE-USA sull'IRA per approfondire tali profili e risolvere gli elementi più controversi.

24 Si v. il *Joint Statement* tra il Presidente J. Biden e la presidente U. von der Leyen, 10 marzo 2023, accessibile in *https://ec.europa.eu/commission/presscorner/detail/en/statement_23_1613,* in cui si afferma "*The EU-U.S. Task Force on the Inflation Reduction Act has productively deepened our partnership on these common goals, and has taken practical steps forward on identified challenges to align our approaches on strengthening and securing supply chains, manufacturing, and innovation on both sides of the Atlantic*".

25 Si v. il *Joint Statement* tra il Presidente J. Biden e la Presidente U. Von der Leyen, cit., "*we will deepen our cooperation on diversifying critical mineral and battery supply chains, recognizing the substantial opportunities on both sides of the Atlantic to build out these supply chains in a strong, secure, and resilient manner. To that end, we intend to immediately begin negotiations on a targeted critical minerals agreement for the purpose of enabling relevant critical minerals extracted or processed in the European Union to count toward requirements for clean vehicles in the Section 30D clean vehicle tax credit of the Inflation Reduction Act*".

26 Ursula Von der Leyen, *Speech at the European Parliament Plenary on the preparation of the European Council*, 15 dicembre 2022, in cui ha sottolineato le preoccupazioni di effetti distorsivi della concorrenza connessi al pacchetto di sovvenzioni adottato dagli Stati Uniti. In particolare si afferma: "*Just look at the United States. They have recently approved a significant investment plan, which also sets standards for clean-tech sectors, the so-called Inflation Reduction Act. And let us be very clear: First of all, supporting the clean transition is the right thing to do if you do it right – in a transparent manner, in a spirit of cooperation, and in a way that ensures a level playing field. It should be a race against time, not a race against each other. It should be a race to the top, not a race to the bottom. Yet, there is a risk that the Inflation Reduction Act can lead to unfair competition*".

La contestuale proposta europea di garantire l'accesso a forme di finanziamento e trasformare il quadro temporaneo "di crisi" per gli aiuti di Stato in un quadro temporaneo "di crisi e transizione"[27] per facilitare e accelerare il cambiamento "*green*" costituisce espressione dell'esigenza di promuovere e sostenere gli interessi economici anche intervenendo sull'ambito di applicazione delle misure a tutela della concorrenza (ed in particolare degli aiuti di Stato[28]).

La circostanza che non tutti gli Stati membri abbiano la capacità economica per erogare aiuti di Stato e la concentrazione del loro utilizzo in alcuni ordinamenti giuridici comporta il rischio di generare distorsioni nel Mercato Unico[29].

La cooperazione tra Stati membri e Istituzioni dell'Unione Europea costituisce un fattore determinante per garantire l'efficienza delle politiche economiche il cui necessario coordinamento, a livello europeo, può favorirne l'effettività in un contesto in cui gli interessi europei si rapportano con quelli nazionali.

## 3. L'esercizio del "*Golden power*" come strumento di tutela degli interessi economici strategici nazionali

Interventi volti a sostenere il Mercato Unico nell'economia internazionale si pongono così in rapporto all'esercizio di poteri nazionali volti a tutelare un proprio interesse economico ritenuto strategico.

Nell'ordinamento giuridico italiano si è superata la disciplina del *golden share*[30], sostituendo le partecipazioni azionarie munite di prerogative speciali con un potere di intervento generalizzato dello

[27] Il quadro temporaneo di crisi per gli aiuti di Stato, adottato il 23 marzo 2022, consente agli Stati membri di avvalersi della flessibilità prevista dalle norme sugli aiuti di Stato per sostenere l'economia nel contesto della guerra della Russia contro l'Ucraina. Il quadro temporaneo di crisi è stato modificato il 20 luglio 2022 per integrare il pacchetto di preparazione all'inverno, in linea con gli obiettivi del piano *REPowerEU* ed il 28 ottobre 2022 conformemente al regolamento relativo a un intervento di emergenza per far fronte ai prezzi elevati dell'energia (regolamento UE 2022/1854) e alla proposta della Commissione UE relativa a un nuovo regolamento di emergenza per far fronte ai prezzi elevati del gas nell'UE e garantire la sicurezza dell'approvvigionamento in inverno. Cfr. Commissione UE, *Aiuti di Stato: la Commissione adotta un quadro temporaneo di crisi*, 23 marzo 2022

[28] Le misure in discussione rimarrebbero in vigore fino al 31 dicembre 2025.

[29] Commissione UE, *State aid Scoreboard 2021*, 6 settembre 2022, 24 e s., in cui si evidenzia come in termini economici la spesa totale per aiuti di Stato sia preponderante in Germania, Regno Unito (oggi fuori dall'UE) e Francia.

[30] La disciplina del *golden share* era contenuta nel d.l. 31 maggio 1994 n. 322, conv. in l. 30 luglio 1994, n. 474. La Corte di Giustizia UE era intervenuta contestando la compatibilità della disciplina del "golden share" con i principi europei di libera circolazione dei capitali (TFUE, art. 63) e di libertà di stabilimento (TFUE, art. 49). Corte giust. UE, 23 maggio 2000, *Commissione CE* c. *Repubblica italiana*, in C-58/99, in cui si censura la disciplina italiana nella misura in cui, in parallelo al processo di privatizzazione, prevedeva l'individuazione di quelle società (operanti nel settore della difesa, dei trasporti, delle telecomunicazioni, delle fonti di energia e degli altri pubblici servizi) in cui introdurre una clausola di attribuzione di poteri speciali conferiti al Ministro del Tesoro. La previsione è stata ritenuta "potenzialmente in grado di ostacolare o scoraggiare l'esercizio delle libertà fondamentali garantite dal Trattato e di conferire alle autorità italiane un potenziale potere di discriminazione che può essere utilizzato in modo arbitrario". La Corte si è parallelamente espressa sulle normative presenti in Francia (C-483/99), Spagna (C-463/00), Regno Unito (C-98/01) e Germania (C-112/05). Nella medesima logica sono stati ritenuti con conformi all'ordinamento europeo altri interventi normativi, con cui si prevedeva la tutela di società d'interesse nazionale strategico (es. con l. n. 266/2005, si individuava un potere speciale in capo all'azionista pubblico definito *poison pill*, che, in caso di offerta pubblica di acquisto ostile di società partecipate dall'azionista pubblico, permetteva di deliberare un aumento di capitale per accrescere la quota di partecipazione di quest'ultimo e non consentire il tentativo di scalata non concordata).

Stato (denominato "*golden power*") su specifiche operazioni in settori strategici[31] conferendo l'esercizio del relativo potere alla Presidenza del Consiglio dei Ministri.

L'esercizio dei poteri speciali (*golden power*) comporta la facoltà di dettare condizioni all'acquisito di partecipazioni, di porre il veto all'adozione di determinate delibere societarie e di opporsi all'acquisto di partecipazioni.

Criteri europei per definire la compatibilità delle misure adottate a livello nazione sono stati definiti dalla Commissione UE[32]. Una disciplina europea sul controllo degli investimenti esteri nell'Unione Europea è stata adottata solo nel 2019[33], nell'ottica di tutelare "*key technologies*" per motivazioni strategiche da interventi esterni all'Unione Europea[34].

L'attuazione di tale regolamento nell'ordinamento giuridico italiano ha comportato l'introduzione delle definizioni di "infrastrutture critiche", "tecnologie critiche", "fattori produttivi critici", "informazioni critiche" e "rapporti di rilevanza strategica", che costituiscono un elemento essenziale ai fini del corretto inquadramento dell'ambito di applicazione della disciplina[35].

Nel settore della difesa e della sicurezza nazionale, l'attuale ambito di applicazione della disciplina comprende le minaccia effettiva di grave pregiudizio per gli interessi essenziali, e si riferisce all'acquisto, a qualsiasi titolo, di partecipazioni in imprese che svolgono attività di rilevanza strategica, nonché delibere societarie ritenute significative[36].

Un primo profilo da prendere in considerazione risiede nella necessità di superare la concezione tradizionale dell'interesse nazionale, intesa come mera tutela delle prerogative della sovranità statale, in favore di una concezione che possa adattarsi ed evolvere le proprie azioni alle esigenze dettate da un contesto complesso e globalizzato.

---

31 Sulla disciplina italiana dei *golden powers* si v. d.l. 15 marzo 2012, n. 21, *recante norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni*, conv. in l. 11 maggio 2012, n. 56; DPR 25 marzo 2014, n. 85, *Regolamento per l'individuazione degli attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni*; DPR 25 marzo 2014, n. 86, *Procedure in materia di poteri speciali nei settori dell'energia, dei trasporti e delle comunicazioni*; Dpcm 6 giugno 2014, n. 108, *Regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale*; Dpcm 6 agosto 2014, *Individuazione delle modalità organizzative e procedimentali per lo svolgimento delle attività propedeutiche all'esercizio dei poteri speciali*; Dpcm 15 dicembre 2014, *Istituzione del Gruppo di coordinamento delle attività per l'esercizio dei poteri speciali di cui all'articolo 3 del Dpcm 6 agosto 2014*. In dottrina: F. RIGANTI, *I golden powers italiani tra «vecchie» privatizzazioni e «nuova» disciplina emergenziale (artt. 15, 16 e 17, d.l. 8 aprile 2020, n. 23, convertito con modificazioni dalla l. 5 giugno 2020, n. 40; d.l. 15 marzo 2012, n. 21, convertito con modificazioni dalla l. 11 maggio 2012, n. 56)*, in *Nuove Leggi Civ. Comm*., 2020, 867 e s.; R. Angelini, *Stato dell'arte e profili evolutivi dei poteri speciali: al crocevia del golden power*, in *Riv. dir. soc*., 2018, 681-714; A. Sacco Ginevri, *I golden powers dello Stato nei settori strategici dell'economia*, in *Federalismi.*it, 16 novembre 2016; F. Bassan, *Dalla 'Golden share' al 'Golden power': il cambio di paradigma europeo nell'intervento dello Stato sull'economia*, in *Studi sull'integrazione europea*, 2014, 57-80; C. San Mauro, *La disciplina della nuova golden share*, in *Federalismi.it*, 31 ottobre 2012; id., *La disciplina della 'golden share' dopo la sentenza della Corte di Giustizia C-326/07*, in *Concorrenza e mercato*, 2010, 409-432. M. Colangelo, *Regole comunitarie e golden share italiana*, in *Mercato Concorrenza Regole*, 2009, 595-602.

32 Commissione UE, *Comunicazione relativa ad alcuni aspetti giuridici attinenti agli investimenti intracomunitari*, 19 luglio 1997.

33 Regolamento UE 2019/452, *che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione*. In dottrina: E. Chiti, *L'evoluzione del sistema amministrativo europeo*, in *Giorn. Dir. Amm*., 2019, 681 e s.; G. Napolitano, *L'irresistibile ascesa del golden power e la rinascita dello stato doganiere*, in *Giorn. Dir. Amm*., 2019, 549 e s.;

34 Commissione UE, *Reflection paper on harnessing globalisation*, 10 maggio 2017.

35 D.P.C.M. n. 179 del 2020. Sono inoltre individuati i beni e i rapporti rilevanti ai fini dell'esercizio dei poteri speciali nel settore dell'acqua, della salute, nel settore finanziario, nei settori dell'intelligenza artificiale, della robotica, dei semiconduttori, della cybersicurezza, delle nanotecnologie e delle biotecnologie, nei settori delle infrastrutture e delle tecnologie aerospaziali non militari, nel settore dell'approvvigionamento di fattori produttivi e nel settore agroalimentare. Il decreto chiarisce che, fra i beni e i rapporti rilevanti ai fini dell'esercizio dei poteri speciali rientra la piattaforma del Sistema Informativo Elettorale (SIEL).

36 D.l. 15 marzo 2012, n. 21, cit., art. 1. Sul ruolo del Ministero della Difesa e del Ministro dell'Interno cfr.: Dpcm 6 giugno 2014, n. 108.

La nozione di "interesse nazionale" e il suo ambito di applicazione nell'economia devono contemperare esigenze politiche ed economico-finanziarie e acquisire un carattere dinamico[37], anche in considerazione di nuovi mercati connessi a settori e tecnologie emergenti.

Tale necessità comporta di contemperare l'equilibrio tra iniziativa economica privata e interessi pubblici, e richiede professionalità sempre più specifiche e settoriali. Ciò involge la preliminare definizione di rapporti di collaborazione con soggetti pubblici rilevanti (quali le autorità amministrative indipendenti di settore[38], gli enti di ricerca) e la valutazione di profili che hanno carattere giuridico, economico-finanziario e politico.

La costituzione di rapporti collaborativi dinamici nel settore pubblico può supportare la tutela degli interessi economici strategici nazionali, sia nel contesto presente sia in ottica futura.

Tali aspetti paiono richiede l'elaborazione di una cultura strategica comune (attraverso una analisi capace di anticipare i fenomeni macroeconomici e di evoluzione tecnologica), finalizzata a comprendere i mutamenti del contesto globale e tutelare in modo sempre più efficace l'interesse nazionale.

[37] L. Fiorentino, *Verso una cultura del golden power*, in *Golden power*, 2019, 21 e s.;

[38] Tale previsione è stata introdotta al d.l. 15 marzo 2012, n. 21, cit., art. 2-bis, con l'art. 4-bis, c. I, lett. d), d.l. 21 settembre 2019, n. 105, conv. con l. 18 novembre 2019, n. 133.

Pagina bianca

**ISTITUTO DI RICERCA E ANALISI DELLA DIFESA**

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.

L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e cyber security; Giuridica.

L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.

L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche.

L'IRAD si avvale altresì per le attività d'istituto di personale qualificato "ricercatore della Difesa, oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato.

L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore dalla Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.

Pagina bianca

L'*Osservatorio Strategico* è uno studio che raccoglie analisi e report sviluppati dall'Istituto di Ricerca e Analisi della Difesa (IRAD), realizzati da ricercatori specializzati.
Le aree di interesse monitorate nel 2023 sono:

- Balcani e Mar Nero;
- Mashreq, Gran Maghreb, Egitto ed Israele;
- Sahel, Golfo di Guinea, Africa Sub-sahariana e Corno d'Africa;
- Cina;
- Asia meridionale ed orientale e Pacifico;
- Russia, Asia centrale e Caucaso;
- Golfo Persico;
- America Latina;
- Area Euro/Atlantica (USA-NATO-Partners);
- Politiche energetiche;
- Sfide e minacce non convenzionali.

Gli elaborati delle singole aree, articolati in analisi critiche e previsioni, costituiscono il cuore dell'"Osservatorio Strategico"**.**

Pagina bianca

*Stampato dalla Tipografia del*
*Centro Alti Studi per la Difesa*

Pagina bianca

ISBN 979-12-5515-043-5