SLJ STRATEGIC LEADERSHIP JOURNAL

Volume IV – Anno 2024

ISSN 2975-0148 – ISBN 9791255150787

CENTRO ALTI STUDI DIFESA

SCUOLA SUPERIORE UNIVERSITARIA

I NOSTRI VALORI

INNOVAZIONE COME SFIDA

Viviamo l'innovazione con coraggio e curiosità, come una sfida entusiasmante in grado di generare valore nella formazione e nella ricerca per far fronte con successo alla complessità del mondo attuale.

SPIRITO DI SQUADRA E APPARTENENZA

Crediamo nello spirito di squadra e nel senso di appartenenza che, attraverso la lealtà reciproca, la condivisione e l'armonia nelle relazioni, assicurano il benessere individuale e il successo organizzativo.

ECCELLENZA NELLE COMPETENZE

Ci ispiriamo all'eccellenza nel nostro agire quotidiano, impegnandoci a riconoscere con equità le competenze di ciascuno e a potenziarne i talenti e mirando ad essere punto di riferimento per l'offerta formativa e l'attività di ricerca a cui come Istituzione siamo chiamati.

RESPONSABILITÀ AL SERVIZIO DEL PAESE

Fondiamo sull'etica e sull'integrità il nostro operare, in continuità con la tradizione, a favore della cultura di una leadership responsabile al servizio del Paese e della comunità internazionale.

VALORIZZAZIONE DELLE DIFFERENZE

Siamo convinti che un approccio aperto e integrativo, che nell'altro riconosca e valorizzi tutte le peculiarità che lo rendono unico, permetta l'espressione e la crescita delle capacità individuali e costituisca leva strategica per lo sviluppo di network capaci di facilitare il conseguimento degli obiettivi organizzativi ed istituzionali.

Centro Alti Studi Difesa

Scuola Superiore Universitaria

STRATEGIC LEADERSHIP JOURNAL

CHALLENGES FOR GEOPOLITICS AND ORGANIZATIONAL DEVELOPMENT

Volume IV – Dicembre 2024

Centro Alti Studi Difesa – Scuola Superiore Universitaria

Direzione e Redazione Palazzo Salviati
Piazza della Rovere, 83, 00165 – Roma
www.casd.it
Tel 06 4691 23208 – e-mail: irad.usai@casd.difesa.it

ISSN 2975-0148 – ISBN 9791255150787

A cura di
Federico Girotti
Barbara Raimondi

Martedì 26 novembre 2024 si è tenuta presso Palazzo Salviati, sede del CASD, la cerimonia di Apertura dell'Anno Accademico 2024\2025 del Centro Alti Studi Difesa, Scuola Superiore Universitaria, che ha visto gli interventi del Ministro della Difesa, On. Guido Crosetto, del Capo di Stato Maggiore della Difesa, Generale Luciano Portolano, e della Presidente della Scuola Nazionale dell'Amministrazione, prof.ssa Paola Severino, la cui Lectio Magistralis ha affrontato lo "Sviluppo delle Competenze come leva strategica per la Pubblica Amministrazione", elogiando il CASD come centro capace di promuovere le conoscenze necessarie per affrontare le sfide contemporanee. L'auspicio della Presidente Severino è quella di realizzare una salda collaborazione tra la Scuola Nazionale dell'Amministrazione (SNA) e il CASD. Ciò con l'obiettivo di sviluppare percorsi formativi integrativi tra civili e forze armate, che forniscano capacità di leadership per formare una nuova cultura digitale a servizio di tutti.
Dal canto suo, il Ministro della Difesa, ha ribadito l'importanza del CASD nel formare leader capaci di valorizzare le competenze degli specialisti e integrarle nei processi decisionali. L'On. Crosetto ha poi affermato come il progresso si concretizza non nel soddisfacimento dei risultati raggiunti, ma nell'ispirazione derivante da coloro che hanno compiuto ulteriori sviluppi. Egli ha concluso sottolineando la notevole capacità della Russia di influenzare l'opinione pubblica italiana e la nostra limitata capacità di difenderci, riflettendo sulla complessità dei molteplici fronti della guerra ibrida e sulla lunga strada ancora da percorrere: *«In questa strada da fare io penso che il CASD debba diventare sempre più centrale e la cooperazione tra le pubbliche amministrazioni sempre più importante»*.

D I S C U S S I O N I

(Sezione non soggetta a peer-review)

Alessandro Azzoni
Ministro Plenipotenziario
Vice Direttore Generale per gli Affari Politici e Direttore Centrale Sicurezza
Direzione Generale per gli Affari Politici e di Sicurezza
Ministero degli Affari Esteri e della Cooperazione Internazionale

Scendere dalla barca – Strategia e conflitti asimmetrici

"Never get out of the boat…
Unless you were going all the way",
(Apocalypse Now)

Di cosa stiamo parlando?

Il termine "conflitto asimmetrico" è usato per indicare situazioni che, pur presentando punti in comune, sono spesso molto diverse fra loro. Evitando inquadramenti troppo rigidi, mai utili per una comprensione del reale, iniziamo con il dire che di solito si fa distinzione tra tre tipi di asimmetria: asimmetria di potere, asimmetria strategica e asimmetria strutturale.

Il confine tra questi è spesso labile e, nella maggior parte dei casi, si possono individuare più tipologie di asimmetria utilizzate contemporaneamente. Tuttavia, una distinzione può essere utile per l'analisi e la comprensione dello sviluppo di un conflitto. Si parla di diversi tipi di asimmetria, non di tipi diversi di conflitto, anche perché ogni conflitto include quasi sempre più di una tipologia di asimmetria e ciascuna con diversi gradi di intensità.

L'asimmetria di potere si verifica ogni volta che esiste un forte squilibrio…di potere. Per esempio, nella Prima Guerra del Golfo, la coalizione a guida Stati Uniti e l'Iraq rappresentava Stati con governi riconosciuti, eserciti regolari e istituzioni politiche in grado di prendere decisioni e attuarle. Da questo punto di vista la situazione era piuttosto equilibrata. L'asimmetria stava invece nell'enorme differenza di forze militari: una questione di quantità, più che di qualità.

L'asimmetria strategica si verifica invece quando le due parti sono asimmetriche nel loro approccio tattico e/o strategico al conflitto e di solito include anche un forte squilibrio di potere. Esempi tipici sono le guerriglie e i fenomeni di tipo terroristico. Nonostante i numerosi studi sulla guerra asimmetrica, il pensiero

strategico della maggior parte degli studiosi militari occidentali è ancora basato principalmente sulla tecnologia e sulla potenza di fuoco, mentre i combattenti ribelli o i terroristi sono solitamente cellule decentralizzate e leggere, perfettamente in grado di mimetizzarsi nella popolazione prima e dopo aver portato l'attacco. Questo cambia ogni paradigma tattico convenzionale.
Come diceva Henry Kissinger (1923-2023): "Uno dei principi fondamentali della guerriglia è che per vincere basta non perdere; un esercito regolare, invece, per non perdere deve vincere".
L'asimmetria strutturale si verifica invece quando c'è un forte squilibrio di status tra le parti. Quello che rende questo tipo di asimmetria piuttosto peculiare e diverso è che alla radice del conflitto c'è la struttura stessa del rapporto tra gli avversari. In un conflitto caratterizzato da asimmetria strutturale il vero obiettivo della lotta è cambiare la struttura delle relazioni tra gli avversari. Di solito, una delle parti cerca di modificarla, mentre l'altra lotta per evitare qualsiasi cambiamento. Il caso più rappresentativo è quello delle guerre di indipendenza/decolonizzazione, in cui al centro del conflitto c'è il rapporto tra colonizzatori e colonizzati. Non sempre, però, una delle parti è un'istituzione governativa e l'altra un'organizzazione non statale. Ad esempio, l'asimmetria strutturale caratterizza la maggior parte dei conflitti sull'accesso e il controllo sulla terra. I conflitti preistorici tra agricoltori sedentari e pastori nomadi sono stati endemici sin dagli albori della civiltà e dall'invenzione dell'agricoltura e ancora oggi incombono, in un mondo in cui il 45% della popolazione si guadagna da vivere direttamente dalla terra. Sono conflitti che, pur modificandosi ed integrandosi con istanze più o meno contemporanee (dai "marxismi" africani degli anni '60 e '70 del secolo scorso fino agli attuali movimenti fondamentalisti islamici in Sahel), restano quello che sono sempre stati e semmai possono reagire ad altri fattori, dai cambiamenti climatici alle riforme agrarie.
Una caratteristica che contribuisce a differenziare i tre tipi di asimmetrie riguarda il tempo. L'asimmetria di potere è statica ed è improbabile che un Paese debole diventi forte – e viceversa – da un giorno all'altro. L'asimmetria strategica è piuttosto una questione di scelte e obiettivi e quindi, dipendendo dalle decisioni degli attori, in linea di principio può cambiare in un tempo relativamente breve. L'asimmetria strutturale è, contro intuitivamente, dinamica: una riforma agraria può cambiare in un momento il paradigma di base di un conflitto per la terra. Magari non pone fine del tutto alla lotta, in attesa dell'applicazione concreta della riforma, ma lo squilibrio di fondo diminuisce drasticamente.
Insomma, le guerre asimmetriche sono antichissime. Esiste una linea che porta da Masada a Fallujah, pur nelle ovvie differenze, e non si parla di poche centinaia di chilometri dello stesso deserto ma della loro natura di operazioni militari intrinsecamente contro insurrezionali. Forse sono proprio le guerre simmetriche ad avere una storia relativamente più recente e più breve, dalla fine della Guerra dei Trenta anni (Westfalia, 1648) alla fine della Guerra Fredda (Berlino, 1989), naturalmente con le dovute eccezioni.

Qui basta ricordare che già nel 510 a.C., Sun Tzu paragonava l'esercito all'acqua (un elemento che ha una valenza simbolica positiva in tutte le religioni, soprattutto orientali): come l'acqua adegua il suo corso al terreno che incontra, così l'esercito vince adeguandosi all'avversario che combatte. Negli anni Venti e Trenta del secolo scorso, poi, Mao Tse-tung ha analizzato teoricamente e applicato sistematicamente la guerra asimmetrica, prima contro il governo del Kuomintang, poi contro i giapponesi e quindi di nuovo contro Chiang Kai-shek. Mao aveva capito perfettamente un altro aspetto determinante dei conflitti asimmetrici, ovvero che l'asimmetria è sempre in relazione, oltre che con il tempo, con l'intensità. Una decelerazione del conflitto – un passaggio da un'alta a una bassa intensità cinetica – permette di opporre una resistenza armata efficace a un avversario tecnologicamente e operativamente superiore. Guerre asimmetriche e guerre a bassa intensità sono strettamente collegate: minore è l'intensità (e maggiore è la capacità di assorbimento delle perdite umane), minore sarà l'impatto dell'asimmetria, ovvero la prevalenza della parte sulla carta più forte.

Parliamo ora di una variabile legata alle nuove tecnologie. Gli enormi passi avanti della tecnologia militare e soprattutto dei sistemi unmanned negli ultimi due decenni, hanno fornito i mezzi per la "nascita" di nuove asimmetrie e nuovi tipi di intensità. La guerra tecnologica, fino a pochi anni fa – e ancora oggi, basti pensare ai caccia di ultima generazione o ai droni giganti – era appannaggio delle nazioni tecnologicamente avanzate. Oggi, perlomeno nella sua versione tattica, è alla portata non solo di ogni nazione ma di ogni gruppo insurrezionale o terroristico con un minimo di potere economico. Inoltre, le competenze diffuse in rete rendono possibile costruire ordigni biologici, e non solo, all'interno di un laboratorio appena avanzato. Dinamica alquanto emblematica, quella che accade da qualche anno a questa parte, con la vendita di centinaia di droni turchi Bayraktar, cui hanno fatto seguito – a brevissima distanza di tempo (e di luoghi di conflitto) – gli economici Shahed iraniani. I droni marittimi ucraini, a basso costo ma ad altissima resa offensiva su naviglio russo nel Mar Nero, o degli stessi alianti di Hamas lanciati – contro ogni previsione – su territorio israeliano lo scorso 7 ottobre.

I conflitti asimmetrici sono un modo non nuovo di fare la guerra cui, però, non siamo ancora del tutto abituati. Tuttavia, d'ora in avanti tutto sarà asimmetrico e ibrido e la variabile stessa dell'imprevedibilità diventa cifra decisiva della contemporaneità. Si pensi alla prima e alla prossima seconda, Amministrazione Trump.

La parte in possesso di un vantaggio tecnologico e operativo cerca generalmente di accelerare il conflitto per far valere la sua predominanza, quella in svantaggio cerca di abbassarne l'intensità e prolungarne la durata per fiaccare nel tempo la volontà politica della parte più potente.

Variazione sul tema: cosa "ci insegna la storia" dei conflitti strutturalmente asimmetrici?

Inoltriamoci in una digressione sul tema, perché è importante riconoscere gli elementi ricorrenti. Spesso si sente dire: "La storia ci insegna…". Secondo il parere di chi scrive, la storia racconta molto ma non insegna. Sembra necessario, tuttavia, esercitarsi nello studio storico, cimentarsi in quelle che un maestro di libertà nel secolo delle illibertà che fu Karl Popper (1902-1994) chiamava le "congetture e confutazioni", anche solo per procedere per smentite e sottrazioni, evitando la presunzione del sapere e agendo socraticamente anche nel campo delle scienze sociali.

Proprio quell'approccio che forse consente di notare che ci sono schemi ricorrenti, per esempio nella dinamica dei conflitti asimmetrici strutturali, tra una potenza coloniale e un popolo colonizzato, tra un dominatore e un "damné de la terre" di Frantz Fanon (Les Damnés de la terre, 1961). I percorsi che potrebbero portare alla fine del rapporto di dominio e quindi alla fine del conflitto hanno quattro fasi: consapevolezza, confronto, negoziazione e pace sostenibile. Nessuno dice che i singoli cittadini dello stato coloniale non possano essere favorevoli all'autodeterminazione della popolazione colonizzata, ma da un punto di vista oggettivo (strutturale), essi fanno parte del lato dominante e ne traggono vantaggio.

Nella prima fase, le popolazioni o gli individui dominati prendono consapevolezza dell'ingiustizia strutturale che caratterizza la situazione in cui vivono e concepiscono la necessità di reagire al dominio. Un sussulto che, consentite la breve divagazione, forse nel Vecchio Continente non siamo più abituati a vivere.

La crescita della consapevolezza del conflitto e della giustezza della propria causa, e quindi la costruzione dell'identità di gruppo sono componenti fondamentali: senza di loro non può avvenire alcuna mobilitazione. Acquisendo consapevolezza del rapporto di dominio, i dominati vedono sé stessi come un gruppo con interessi/bisogni comuni e con un avversario comune. Ciò favorisce la mobilitazione e l'organizzazione, e la crescita della mobilitazione richiede a sua volta forme di organizzazione più complesse, che rafforzano e ampliano ulteriormente l'organizzazione stessa e così via. Allo stesso tempo, la mobilitazione attira più partecipanti alla lotta, ampliando e approfondendo il livello di consapevolezza e rafforzando l'identità del gruppo.

La crescente consapevolezza dei conflitti latenti, insieme alla crescente mobilitazione, porta solitamente la parte dominata a confrontarsi con quella dominante. Il confronto può avere molteplici forme: resistenza passiva, mobilitazione politica, lotta non violenta, azioni militari o attacchi terroristici. Di solito coesistono più di un tipo di azione, spesso perché esistono ali politiche e militari relativamente indipendenti l'una dall'altra all'interno dello stesso movimento, una che opera apertamente e l'altra in clandestinità. Gli esempi sono moltissimi, dal Sinn Fein e l'IRA alle ali di Hamas.

Questa fase è spesso strettamente intrecciata con la precedente. Forme di scontro possono manifestarsi presto, subito dopo che la parte dominata prende coscienza dell'ingiusto rapporto di dominio. Di fatto, il confronto stesso accelera e radicalizza il processo di consapevolezza, estendendolo a nuovi settori della popolazione e aumentando la convinzione in quelli già consapevoli, dando origine ad un ciclo di rafforzamento. La repressione, cioè la risposta più comune della parte dominante, può indebolire il movimento di insurrezione nel breve termine ma nel lungo periodo molto probabilmente rafforza la risolutezza dell'avversario e favorisce il processo di consapevolezza.

Alla negoziazione si giunge quando le due parti arrivano alla conclusione che il costo della lotta non è più sopportabile, o quando una terza parte riesce a convincerle o a costringerle a negoziare[1]. Di solito, la parte più difficile da convincere è quella dominante, poiché lo status quo è a suo favore e condizione necessaria per arrivare alla fase negoziale è la disponibilità a ridurre lo squilibrio tra le parti. La negoziazione è un modo per far sì che ciascuna parte si confronti con gli obiettivi dell'avversario e riconosca la legittimità di almeno una parte di essi. In particolare, è il lato dominante – ormai non più così dominante, poiché gli squilibri di potere sono diminuiti – che deve adattarsi alla nuova realtà e rinunciare ad alcuni dei propri obiettivi e/o delle proprie prerogative. La consapevolezza del conflitto raggiunge così il suo punto più alto.

Una volta raggiunto un accordo, inizia un nuovo processo: costruire una pace sostenibile. Ciò implica una ristrutturazione dei rapporti tra le parti, ovvero lo smantellamento del patrimonio di odio, pregiudizi, frustrazione e sfiducia reciproca creato da anni di dominazione oppressiva e di violenza e la decostruzione e riorganizzazione delle strutture di governo. Ciò non può accadere immediatamente e richiede un lavoro certosino e una trasformazione culturale. In Sud Africa, la fine dell'apartheid non ha subito portato la pace. Sebbene le strutture più ingiuste e oppressive siano state smantellate in tempi rapidi, la maggior parte delle persone che vivono nelle township non ha ancora visto alcun radicale miglioramento nelle proprie condizioni di vita e le disuguaglianze economiche rimangono spaventose. In casi come questo, la frustrazione delle speranze nutrite dalle fasce più sfavorite della popolazione potrebbe portare ad una ripresa del conflitto, magari con nuove e più radicali rivendicazioni.

Delle quattro fasi del processo, le prime tre sono in un certo senso naturale conseguenza del conflitto asimmetrico, mentre la pace sostenibile è la più problematica. Quasi tutti i conflitti di questo tipo passano almeno una volta attraverso le prime tre fasi, mentre la pace sostenibile può non verificarsi mai. Il pensiero non può non andare al conflitto israelo-palestinese e non solo nella prospettiva di una pace sostenibile.

---

[1] *Un obiettivo che cerco di perseguire da tempo in carriera diplomatica (ma non solo) è la costituzione, la formazione, la crescita e lo schieramento sul campo di un gruppo coeso di mediatori italiani di generazione intermedia, da impiegare sui fronti più sensibili e dotato di pensiero strategico e comprovate capacità negoziali.*

La pace sostenibile non è semplicemente la fine tecnica del conflitto, ma un lungo e impegnativo processo di convalescenza e guarigione, che non può prescindere dalla ricerca onesta della verità su quanto accaduto, dalla giustizia per le vittime dei crimini compiuti e da una conseguente riconciliazione. Senza queste fasi la pace pur raggiunta non sarà davvero solida e sostenibile nel tempo. Tornando all'esempio sudafricano, la Commissione per la verità e la riconciliazione, presieduta dal vescovo Desmond Tutu, è stata un esempio paradigmatico di azione che si muove nella direzione di una pace sostenibile.

Altri esempi di conflitti strutturalmente asimmetrici che hanno portato ad una pace sostenibile sono stati la lotta per l'indipendenza dell'India, la guerra di decolonizzazione in Algeria e la lotta contro la segregazione razziale in Nord America. Nel primo caso, l'India e il Regno Unito sono stati in grado di costruire in tempi relativamente brevi, e mantenere in seguito, relazioni amichevoli e cooperative.

Assai più problematico il caso dell'Algeria e della Francia. Dopo la guerra che vide un attore non statale ma di impianto nazionale come il FLN[2] opporsi allo Stato dominante e ottenere l'indipendenza, il rapporto tra Algeria e Francia ha avuto e continua ad avere alti e bassi e la lotta di liberazione resta tuttora il mito fondante della nazione algerina. Tuttavia, i forti legami tra Francia e Algeria, a livello economico, sociale e culturale, hanno resistito a periodi di relazioni tese e sono addirittura cresciuti nel tempo. Un rapporto che però resta di "amore-odio" e di "azione-reazione" in termini quasi termodinamici, che non può essere esaminato se non ricorrendo anche agli strumenti della psicologia di massa e all'eredità inevitabile di Albert Camus.

Quanto all'ultimo esempio, nonostante tutti i problemi che ancora sussistono, l'elezione di un Presidente afroamericano rappresenta chiaramente un punto di svolta nelle relazioni razziali negli Stati Uniti.

Sono tre casi molto diversi ma con elementi in comune: in tutti e tre il punto di partenza del conflitto è stato il rapporto strutturalmente ineguale tra le parti. La consapevolezza del conflitto è cresciuta fino al momento in cui la parte più forte è stata costretta ad inserire la questione nella propria agenda politica e quindi ad accettare l'eliminazione dello squilibrio strutturale attraverso accordi internazionali o riforme interne.

Particolarmente importanti sono poi i circuiti che coinvolgono le fasi centrali del confronto e della negoziazione. Può infatti accadere che il mancato raggiungimento di un accordo porti a un nuovo confronto più violento, anche perché raramente le decisioni vengono prese da un unico decisore: molto spesso, entrambi i campi hanno più attori, a volte con programmi diversi e alcuni di essi potrebbero trarre vantaggio dal fallimento della negoziazione (le real IRA e i paladini "puri e duri" della Causa emergono in ogni negoziato), ovvero reagire ad un'esclusione (iniziale) dalla medesima. Esistono casi infine in cui alcuni attori terzi peccano di eccesso di dinamismo, come nel pur meritevole tentativo

[2] *Front de Libération Nationale*

di mediazione in Algeria da parte della Comunità di Sant'Egidio nel corso degli anni Novanta.
A volte, la parte che ha più da perdere da un cambiamento dello status quo usa il negoziato per rallentare la transizione verso una pace sostenibile, per esempio prolungando le trattative e, nel frattempo, lasciando che la situazione sul campo cambi a proprio vantaggio, per rendere più difficile (se non del tutto impraticabile) una soluzione nei termini accettabili per la controparte. Ovvero applicando l'antico divide et impera, concedendo privilegi solo a selezionati individui o gruppi dell'altro campo per renderli più disposti ad accettare i suoi termini. Ricordiamo l'esperienza recente ma già dimenticata delle ex primavere arabe, con un fuoco (sociale, politico, generazionale) ancora vivissimo sotto la cenere. Infine, c'è sempre la "strategia della tensione", ovvero mettere in atto azioni tali da suscitare reazioni violente da parte dei gruppi più radicali dell'altra parte e quindi arrivare al congelamento dei negoziati o, nel caso in cui sia già stato raggiunto un accordo provvisorio, al blocco della sua attuazione.

Asimmetria e Controinsurrezione

Dopo tutto ciò che è stato detto, potremmo affermare che i conflitti asimmetrici non presentino niente di nuovo e che forse, in ultima istanza, asimmetria sia semplicemente un sinonimo di strategia e viceversa?
I teorici del conflitto contemporaneo, sia che descrivano guerre asimmetriche o non convenzionali, guerre tra popoli o altri generi del conflitto armato moderno, di solito postulano grandi cambiamenti nel carattere, se non nella natura effettiva, della guerra. Molti di essi, però, nel sottolineare ogni possibile differenza tra la guerra moderna e le guerre passate, di fattoo paragonano un ritratto accurato del conflitto moderno ad uno quasi caricaturale dei conflitti antichi.
Sono caricature perché si basano su una prospettiva eurocentrica[3] della strategia (le guerre combattute tra Paesi europei o occidentali, tutti con culture strategiche simili, nate tra Alessandro, Annibale, Cesare e Napoleone e normalizzate da Clausewitz e Jomini), confrontano fenomeni diversi tra loro e percepiscono il cambiamento sulla base di tali confronti errati, che servono solo a dar vita alle varie mode nel pensiero strategico. La guerra convenzionale deve essere paragonata alla guerra convenzionale, quella che invece convenzionale non è deve essere paragonata con conflitti a lei simili.
Ciò che invece è eterno è la strategia, intesa come capacità di individuare gli obiettivi e i modi per raggiungerli o, per quanto ci riguarda, la minaccia o l'uso della forza per raggiungere tali obiettivi. La strategia non ha una forma

[3] *L'eurocentrismo, o etnocentrismo se vogliamo considerare l'insieme della civiltà occidentale, è spesso il peccato originale delle professioni "umanistiche". Per limitarlo, dovremmo aprirci sempre più al confronto con altre discipline, a partire dalle scienze "esatte", quelle che un diplomatico come Gottfried W. Leibniz definiva basarsi sulla "lingua universale": fisica, matematica, biochimica, ecc. Pensiamo ai contributi di pensiero strategico di personalità come il fisico Andrey Sacharov, la chimica Angela Merkel o lo stesso economista agrario Michail Gorbačëv.*

permanente, sebbene mantenga la sua sostanza e la sua funzione, ed è sempre stata praticata.

Ciò che deve essere chiaro, secondo il parere di chi scrive, è che la strategia può essere interpretata come la generazione e lo sfruttamento dell'asimmetria ai fini della vittoria. La generazione di asimmetria è infatti alla base di gran parte, se non della maggior parte, della teoria strategica. Il controllo del mare o dell'aria non significa altro che la generazione di una grande asimmetria positiva in uno di questi ambiti rispetto al nemico. Allo stesso modo, l'idea stessa di concentrare le proprie forze contro un punto specifico, tema centrale sia in Antoine-Henri Jomini che in Carl von Clausewitz, equivale a generare asimmetria in quel punto, per ottenere gli effetti desiderati.

L'asimmetria è quindi chiaramente, non solo perfettamente compatibile con la guerra convenzionale, ma è in sé una definizione di buona strategia. Durante la Seconda Guerra Mondiale, la guerra convenzionale per eccellenza, gli Alleati finirono per creare grandi asimmetrie nella produzione e nella logistica militare-industriale, sul mare e nell'aria in tutti i Paesi dell'Asse. Al contrario, la Grande Guerra fu per così tanto tempo una "inutile strage" (Papa Benedetto XV, 1917), proprio per lo stallo simmetrico sul fronte, ovvero perché fino al 1918 nessuna delle due parti fu in grado di generare le asimmetrie necessarie. Alla fine, hanno sempre vinto i belligeranti che sono stati in grado di generare le asimmetrie più importanti.

Alcune asimmetrie potrebbero essere più immediate o più efficaci di altre. Per esempio, oggi rischiano di tornare a vincere coloro che da decenni si esercitano in disinformatsija, oltre il confine ucraino e fino al cuore di Washington. Insomma, l'asimmetria efficace come la strategia efficace, è sensibile al contesto.

Dunque l'asimmetria è strategia e la strategia è asimmetria. Per questo, condannare retoricamente (o sanzionare) i nostri avversari, colpevoli di aver generato asimmetria, significa solo dimostrare di essere condizionati dalla comprensione della storia recente attraverso il prisma di uno wishful thinking, ovvero il pio desiderio che i propri nemici siano strateghi scarsi.

Il wishful thinking di solito non porta al successo strategico, come indica chiaramente l'esperienza della "guerra al terrorismo" finita con la "fuga" da Kabul.

È vero: le asimmetrie convenzionali su terra, mare e aria sono molto più facilmente comprensibili rispetto alle asimmetrie non convenzionali come la guerriglia. È proprio sulla ricerca delle asimmetrie (un po' la "nemesi" delle guerre stellari di Reagan e forse proprio perché ha studiato la lezione delle guerre stellari di Reagan) che Putin sembra giocare la sua partita, fin dal dramma ceceno.

Si può comprendere una minaccia e tuttavia essere incapaci di contrastarla. Il Generale tedesco Frido von Senger paragonò l'operare sotto la supremazia aerea alleata a "giocare una partita di scacchi contro un avversario che poteva muovere tre pezzi per volta". Nessuna comprensione della minaccia può aiutare ad

alleviare una situazione se tale comprensione non viene trasformata in piani operativi, sia per le asimmetrie convenzionali quanto per quelle non convenzionali. In effetti, le asimmetrie convenzionali sono solitamente le più pericolose perché di solito i loro effetti politici finali sono maggiori. Da Dario III, a Napoleone e a Hitler, tutti hanno perso il loro impero a causa di nemici che, in definitiva, erano stati in grado di generare un'asimmetria efficace; mentre sono relativamente poche le asimmetrie non convenzionali che hanno avuto effetti storici paragonabili. Uno dei pochi esempi pertinenti, anche se impreciso, è la Rivoluzione americana, ma anche quella guerra fu più "ibrida" che puramente non convenzionale.

L'asimmetria oggi è più comunemente associata all'insurrezione. A differenza della generazione di asimmetrie convenzionali, la teoria contemporanea della controinsurrezione enfatizza piuttosto l'asimmetria dal punto di vista del sostegno della popolazione, attraverso la fornitura di sicurezza e altri servizi, inclusa una governance efficace. Intendiamoci: contro un nemico che sta generando un'asimmetria non convenzionale serve anche la forza, perché una volta che la controinsurrezione, superiore in forza, non riesce a vincere e si ritira dal conflitto, l'unica forza vitale rimasta sarà quella degli insorti.

Anche questo è un pensiero non nuovo. Nel Regno Unito, da sempre all'avanguardia su questi temi, si iniziò a riflettere sul tema sin dalla fine del XIX secolo. Sul piano strategico, nelle "piccole guerre" coloniali le forze regolari sono in svantaggio, mentre mantengono un vantaggio tattico negli scontri armati.

"Poiché la tattica favorisce le truppe regolari mentre la strategia favorisce il nemico, l'obiettivo (…) è affrontare le forze ostili in battaglia aperta, non costringerle a cedere ricorrendo alla strategia".

Forse qualcuno negli Stati Uniti del 1965 avrebbe dovuto leggere Charles Edward Callwell, prima di decidere cosa fare in Vietnam. Forse il crollo dello stesso Impero britannico, o meglio la sua mancata evoluzione in un "Commonwealth delle liberal democrazie", è connesso proprio alla mancanza di un'elaborazione strategica, come quella che pure alcuni grandi statisti britannici avevano cominciato ad abbozzare con la Federalist Society ad inizio Novecento, portando alla nascita di una (pur monca del potere militare e dunque di capacità strategiche) Società delle Nazioni.

Fra i grandi teorici novecenteschi della guerra insurrezionale, Thomas E. Lawrence, Mao Tse-tung, Vo Nguyen Giap ed Ernesto "Che" Guevara, solo Lawrence non teorizzò la necessità di passare ad un certo punto dalla guerriglia alla guerra più o meno convenzionale per la conquista definitiva del potere. Lawrence non lo fece perché non ne aveva bisogno, dato che la sua era sì una "piccola guerra", ma era anche parte di un'operazione convenzionale più ampia comandata dal Generale Edmund Allenby nel quadro della guerra mondiale. In tempi più recenti, i talebani di Helmand sono tornati alle tattiche di guerriglia solo dopo aver subito perdite disastrose in assalti frontali convenzionali alle basi

alleate, con enormi tributi di sangue che avevano generato la perdita di un ampio sostegno locale.
Insomma, tutti i teorici della guerriglia ne hanno identificato i limiti perché alla resa dei conti, "quando un uomo con la pistola incontra un uomo col fucile, quello con la pistola è un uomo morto". Se non si trasforma in soldato convenzionale, il guerrigliero alla fine non vince. Può solo aspettare che il suo avversario ammetta la sconfitta. L'asimmetria non convenzionale è capace di negare la vittoria ad un nemico superiore, ovvero di negare al nemico il controllo della situazione, ma non di vincere in modo definitivo. Negare ad altri il controllo rimane comunque un'arma potente e una strategia basata sull'effetto cumulativo di azioni minori e sulla continua elusività presenta sempre notevoli difficoltà per la parte avversaria.
Non presentare un unico insieme di obiettivi e agire contro e tra i civili in aree geografiche più vaste di quelle del nemico può confondere la controinsurrezione in un labirinto di scelte alternative e potenzialmente contrastanti. Durante la Guerra del Vietnam (pensiamo a quanto decisiva sia stata l'esperienza di tale conflitto nella coscienza collettiva in termini di infodemia e insostenibilità del carico di comunicazione pubblica per un Paese liberaldemocratico), gli Stati Uniti identificarono fino a 22 diversi obiettivi di guerra, con scelte operative che potevano essere favorevoli ad alcuni ma controproducenti per altri. In Afghanistan, per lungo tempo le politiche statunitensi richiedevano che i signori della guerra locali fossero liquidati ai fini della costruzione dello Stato ma allo stesso tempo che fossero preservati per combattere i Talebani.
La generazione di asimmetria attraverso l'uso di tattiche di guerriglia può essere difficile da comprendere appieno e ancor più da sconfiggere per le potenze occidentali, nonostante decenni di tentativi, tuttavia è fondamentalmente lo stesso fenomeno della generazione di asimmetria convenzionale e può essere compreso con gli stessi concetti strategici di base. Il dominio britannico dei mari vinse per oltre un secolo i tentativi francesi di sconfiggerlo e portò allo sviluppo da parte della Francia di una serie di metodi con cui colpire il "governo delle onde" britannico, senza sfidarlo direttamente: dalla guerra di corsa alla jeune école, che pose l'accento sul naviglio minore anziché sulle grandi corazzate.
L'asimmetria non convenzionale prende di mira la strategia del nemico piuttosto che il nemico stesso. Il tempo è un bene prezioso nella strategia e deve essere utilizzato con saggezza, ma la sostanziale sfida intellettuale per la controinsurrezione non è quella del tempo o dell'intensità ma quella dei modi. Esiste infatti una sorta di "questione morale" che uno Stato democratico e liberale si trova ad affrontare se vuole provare a sconfiggere direttamente un'insurrezione. Anzi, i concetti stessi di "controinsurrezione" e "antiterrorismo" possono avere significati completamente diversi a seconda del carattere del governo coinvolto.
La guerra non è solo confronto militare ma è anche – mettendo da parte ogni pur giustissima valutazione etica – un atto politico all'ennesima potenza, tanto da potersi raffigurare come la fine e la negazione filosofica della politica, dato che,

seppur gli altri strumenti del potere politico non perdano rilevanza una volta che inizia lo scontro militare, la loro utilità è decisamente stemperata dall'uso della forza.
Per questo riportiamo la nota citazione di Georges B. Clemenceau (1841-1929): "La guerre! C'est une chose trop grave pour la confier à des militaires".

Conclusione

Nel suo "The utility of force. L'arte della guerra nel mondo contemporaneo" (2005), Rupert Smith scrive: "La pratica della guerra […] consiste nel raggiungere un'asimmetria rispetto all'avversario. Etichettare tutte le guerre come asimmetriche è per me una sorta di eufemismo per non ammettere che il mio avversario non è al mio livello, eppure io non sto vincendo".
L'asimmetria come oggi comunemente usata – per denotare un tipo di guerra apparentemente nuovo e particolare – non è quindi un concetto utile e anzi implica un'arroganza strategica che presuppone che esista un solo modello di guerra: il nostro. Lawrence Freedman ha definito la strategia come "l'arte di creare potere" e, dato che il potere è una qualità necessariamente relazionale – non si può avere potere se non relativamente a qualcun altro – la generazione di asimmetria è la riduzione del potere del nemico nei nostri confronti e/o l'aumento del nostro contro quello del nemico. Etichettare solo un certo tipo di strategie come asimmetriche rischia quindi di oscurare gli enormi e reali vantaggi asimmetrici che le democrazie liberali hanno rispetto a quegli insorti che impiegano concretamente le strategie asimmetriche. Se continuiamo a separare la guerra asimmetrica dalla guerra e dalla strategia convenzionale, impediremo alle potenze occidentali di impiegare pienamente ed efficacemente la loro forza contro sfidanti più deboli, poiché la popolarità dell'asimmetria nella letteratura strategica è un sintomo della nostra scarsa comprensione di che cosa sia davvero la strategia.

LETTURE CONSIGLIATE

- Charles Edward Callwell, *Small Wars: their principles and practice*, 1896
- Karl von Clausewitz, *Della guerra*, 1832
- Valter Coralluzzo, Marina Nuciari, *Conflitti asimmetrici. Un approccio multidisciplinare*, 2006
- Conrad C. Crane, *Cassandra in Oz: counterinsurgency and future war*, 2016
- Lawrence Freedman, *Strategy: a history*, 2013
- Vo Nguyen Giap, *People's War, People's Army: The Viet Cong insurrection. Manual for underdeveloped countries*, 1962
- Andrea Graziosi, *Occidenti e modernità. Vedere un nuovo mondo*, 2023
- Antoine Henry Jomini, *Sommario dell'arte della guerra*, 1838
- Henri Kissinger, *Diplomacy*, 1994

- Thomas Edward Lawrence, *I sette pilastri della saggezza*, 1926
- Karl Popper, *La società aperta e i suoi nemici*, 1945
- Andrew Roberts e David Petraeus, *L'arte della guerra contemporanea: dalla caduta del Nazismo al conflitto in Ucraina*, 2024
- Stefano Ruzza, *Il rapporto tra guerra e asimmetria*
- Rupert Smith, *The utility of force. L'arte della guerra nel mondo contemporaneo*, 2005
- Frido von Senger und Etterlin, *La guerra in Europa. Il racconto di un protagonista*, 1960
- Edgar Snow, *Stella rossa sulla Cina. Storia della rivoluzione cinese*, 1937
- Sun Tzu, *L'arte della guerra*

Cosimo Meneguzzo
is an expert in business and economic analysis, as well as public policy development. He has extensive experience consulting for private manufacturing and service companies, in addition to supporting public entities in policy formulation and implementation. Furthermore, he has founded innovative ventures and collaborated with research institutions and universities. His main publications focus on new technologies and the circular economy.

Fabrizio Minniti
is an expert on international security. As a researcher for the Military Centre for Strategic Studies, he has written reports in the fields of intelligence, international terrorism, nuclear doctrine, European security, and defence policy. He was appointed as an External Consultant for EUBAM-Rafah in Israel, and has worked as a Political Advisor to the DCOM–NATO Resolute Support Mission in Afghanistan.

Cognitive Warfare through fake food and nutrients[1]

A B S T R A C T

La cognitive warfare, potenzialmente intensificata da alimenti e nutrienti contraffatti, rappresenta una minaccia significativa per la salute cognitiva, causando carenze e infiammazioni che possono portare a un declino cognitivo. Questa strategia potrebbe minare la resilienza sociale, soprattutto in Europa occidentale. Un'analisi FMEA è essenziale per identificare i rischi e migliorare la rilevazione, la consapevolezza e la cooperazione. La natura nascosta della cognitive warfare richiede misure proattive per proteggere la sicurezza e la stabilità globale.

Cognitive warfare, potentially intensified by counterfeit foods and nutrients, poses a significant threat to cognitive health, leading to deficiencies, toxic additives, and inflammation, which can cause cognitive decline and impaired decision-making. This strategy could undermine societal resilience, particularly in Western Europe. An FMEA analysis is essential for identifying risks and enhancing detection, awareness, and cooperation. The covert nature of cognitive warfare demands proactive measures to protect global security and stability.

[1] Part of this work has been translated into English with the assistance of ChatGPT, a language model developed by OpenAI. Any errors or inaccuracies in the translated text remain the responsibility of the authors.

Introduction

In recent years, the concept of cognitive warfare has expanded beyond traditional psychological operations to include more subtle and insidious methods. Cognitive warfare integrates various activities with other instruments of power to influence attitudes and behaviors by targeting cognition at various levels, from individuals to entire populations. Its goal is to gain a strategic advantage by altering perceptions of reality, making human cognition a crucial battlefield. This approach exploits vulnerabilities by undermining rational thinking, thereby creating systemic weaknesses. The manipulation of societies through cognitive warfare has become more prevalent, highlighting the importance of defending against such strategies[2].

A declination that has not yet been addressed, but cannot be ruled out a priori, is the manipulation of nutrition through the distribution of fake foods and fake nutrients. This paper explores how cognitive warfare could be waged by compromising the nutritional quality of food, thereby affecting the cognitive health, and functioning of populations. This new technique could be considered under the broader concept of "epistemic warfare"[3]. Epistemic warfare, as described, involves manipulation and control of knowledge to gain strategic advantage. This form of warfare uses the dissemination of misinformation, psychological operations, and the exploitation of cognitive biases to undermine adversaries.

Another aspect to which this specific declination of cognitive warfare can be linked is bioterrorism. Bioterrorism is defined as the deliberate use of biological agents such as bacteria, viruses, toxins, or pathogens to inflict disease or death on humans, animals, or plants with the aim of causing panic, economic damage, or social destabilization. This type of terrorism, which has been used for many centuries and in various contexts, continues to pose a significant threat to public health and national security because biological agents are easily dispersed and can cause high rates of mortality and morbidity, as well as panic and social disruption[4-5].

The major threats associated with bioterrorism include agents such as Bacillus anthracis (anthrax), Variola virus (smallpox), Clostridium botulinum toxins

---

2 NATO Allied Command Transformation, Cognitive Warfare: Strengthening and Defending the Mind, Norfolk, 2023. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

3 PILI G., "Epistemic warfare, as described, involves the manipulation and control of knowledge to gain strategic advantages. This form of warfare leverages the dissemination of misinformation, psychological operations, and the exploitation of cognitive biases to undermine adversaries", in Filosofia Pura della Guerra, Parte III Teoria Pura della Guerra, Cap IV Guerra Epistemica. Aracne Editore, I 2015, Roma

4 Centers for Disease Control and Prevention (CDC), Bioterrorism Agents/Diseases by Category, Atlanta, 2023, https://emergency.cdc.gov/agent/agentlist-category.asp

5 RAND Corporation, Bioterrorism, Santa Monica, 2023, https://www.rand.org/topics/bioterrorism.html.

(botulism), and various hemorrhagic viruses like Ebola[6]. These agents are categorized as "Category A" by the Centers for Disease Control and Prevention (CDC) for their ease of transmission and high potential for mortality and morbidity[7].

It is often argued that the primary risks of bioterrorism arise from the silent spread of biological agents, which can cause epidemics that could quickly overwhelm health response capabilities. It is also argued that the production and release of biological agents does not necessarily require extensive resources or advanced scientific knowledge, making these tools accessible to non-state actors[8-9].

However, it is important to note that healthcare systems in many Western countries are highly complex and resilient. The notion that non-state actors could easily compromise such systems ignores several critical factors. First, access to biological agents and their effective dissemination would likely require significant coordination and expertise beyond the capabilities of many non-state actors. In addition, compromising a healthcare system would require access to sensitive data and the execution of sophisticated cybercrime operations, adding layers of difficulty and reducing the feasibility of such attacks[10].

In addition, Western healthcare systems have robust surveillance and response mechanisms in place to rapidly detect and contain outbreaks. The integration of advanced technologies and stringent security protocols further reduces the likelihood of a successful bioterrorist attack. Therefore, the potential for such attacks that overwhelm health systems to be effectively carried out by non-state actors is likely to be necessarily limited, given the expertise, resources and access required[11].

This perspective is consistent with findings that underscore the significant challenges non-state actors face in carrying out complex bioterrorist attacks, suggesting that while the threat exists, the actual risk may be mitigated by the resilience of Western healthcare infrastructures and their preparedness for such threats[12].

Bioterrorism response requires complex and coordinated preparedness, including epidemiological surveillance, facility preparedness, staff training and public information in order to reduce panic and manage emergencies.

---

6 Viera A.J., Primary Care Approach to Managing Chronic Pain, American Family Physician, 2021, https://www.aafp.org/pubs/afp/issues/2021/1000/p376.html.

7 Centers for Disease Control and Prevention (CDC), Bioterrorism Agents/Diseases by Category, Atlanta, 2023, https://emergency.cdc.gov/agent/agentlist-category.asp.

8 RAND Corporation, Bioterrorism, Santa Monica, 2023, https://www.rand.org/topics/bioterrorism.html.

9 Viera A.J., Primary Care Approach to Managing Chronic Pain, American Family Physician, 2021, https://www.aafp.org/pubs/afp/issues/2021/1000/p376.html

10 RAND Corporation, Bioterrorism, Santa Monica, 2023, https://www.rand.org/topics/bioterrorism.html

11 Centers for Disease Control and Prevention (CDC), Bioterrorism Agents/Diseases by Category, Atlanta, 2023, https://emergency.cdc.gov/agent/agentlist-category.asp.

12 Viera A.J., Primary Care Approach to Managing Chronic Pain, American Family Physician, 2021, https://www.aafp.org/pubs/afp/issues/2021/1000/p376.html

1. The role of nutrition in cognitive health

Nutrition is of fundamental importance to the health of the brain and cognitive function. Essential nutrients like vitamins, minerals, omega-3s and antioxidants support neural development, neurotransmitter function and overall cognitive performance[13]. Diets rich in these nutrients enhance brain function, protect against cognitive decline, and improve mood and mental clarity[14]. It is noteworthy that foods rich in dietary fibers and polyphenols can improve the gut microbiome and, as a result, affect the neurotransmitters through the gut-brain axis, thus helping to prevent or delay neurological disorders[15].

1.1 Counterfeit nutrients and Cognitive Warfare

Fake nutrients and fake foods pose a significant risk to cognitive health. These products may lack essential nutrients, micronutrients, and fiber, or contain harmful substitutes that can affect cognitive processes. For example, counterfeit vitamins may be ineffective or even toxic, leading to nutrient deficiencies that affect brain function. The subtle introduction of counterfeit nutrients could be a covert strategy to undermine the cognitive abilities of a population, leading to widespread confusion, reduced critical thinking and impaired decision-making. In this regard, the achievement of food sovereignty, understood as self-sufficiency and short, traceable supply chains within the European and Western area, might be seen as a paramount objective.

1.1.1 Mechanisms of Cognitive Impact

1. Nutrient Deficiencies: Consuming counterfeit nutrients can result in deficiencies of essential vitamins and minerals, which are crucial for brain health. This can impair cognitive processes such as memory, attention, and problem-solving[16].
2. Toxic Additives: Fake food products might contain harmful additives like heavy metals or industrial chemicals. These toxins can accumulate in the brain, leading to neurological damage and cognitive decline[17].

---

13 Naidoo U., Nutritional Psychiatry: Your Brain on Food, Harvard Health Blog, 2015, https://www.health.harvard.edu/blog/nutritional-psychiatry-your-brain-on-food-201511168626.

14 Age UK, Diet and Brain Health, London, 2024, https://www.ageuk.org.uk/information-advice/health-wellbeing/mind-body/staying-sharp/looking-after-your-thinking-skills/diet-and-brain-health/.

15 Kasprzak-Drozd E., et al., 2021, International Journal of Molecular Sciences, 22(7), Article 3715, https://doi.org/10.3390/ijms22073715.

16 JIN Y., et al., Dietary Patterns and Depressive Symptoms in Adults: A Systematic Review and Meta-Analysis, Nutrition Reviews, 79(6), 693-708, 2021, https://doi.org/10.1093/nutrit/nuaa107

17 PÉREZ-TORRES D., et al., Nutrition in Cognitive Decline: Mechanisms and Clinical Evidence, Nutrients, 14(19), Article 4137, 2022, https://doi.org/10.3390/nu14194137.

3. Disrupted Metabolism: Counterfeit nutrients may not be bioavailable, meaning the body cannot effectively absorb and use them. This can lead to metabolic imbalances, affecting overall brain function and health[18].
4. Chronic Inflammation: Poor-quality diets can increase inflammation in the brain, which is associated with cognitive impairments and mental health disorders. Anti-inflammatory nutrients are crucial for maintaining brain health, and their absence in counterfeit foods can have detrimental effects[19].

1.1.2 Potential for mass disruption

The strategic use of counterfeit food in cognitive warfare could have far-reaching consequences. By affecting the cognitive health of a large population, adversaries could weaken societal resilience and stability. For example, compromising a nation's food supply with counterfeit nutrients could lead to widespread cognitive decline. This could impact education, workforce productivity and national security[20].

1.2 Common nutrient needs in Western Europe

In Western Europe, the nutritional needs of the population vary significantly with age and lifestyle habits. Older adults often require higher intakes of vitamin D, calcium, and omega-3 fatty acids to support bone health, cognitive function, and cardiovascular health[21]. Additionally, younger populations, particularly those with busy lifestyles, may struggle with maintaining adequate levels of vitamins B12 and D, iron, and magnesium due to dietary habits that favor convenience and processed foods[22].

The prevalence of processed and fast foods can lead to deficiencies in essential nutrients, contributing to chronic conditions such as obesity, diabetes, and cardiovascular diseases[23]. Addressing these needs through proper dietary choices and supplementation is crucial for maintaining overall health and cognitive function.

---

[18] KARIMI F., et al., Impact of Nutritional Interventions on Cognitive Decline in Older Adults: A Systematic Review and Meta-Analysis, BMC Geriatrics, 23, Article 4497, 2023, https://doi.org/10.1186/s12877-023-04497-7.

[19] VAUZOUR D., et al., Dietary Polyphenols as Modulators of Brain Functions: Evidence from Pre-Clinical and Clinical Studies, Nutrients, 13(1), Article 199, 2021, https://doi.org/10.3390/nu13010199

[20] NAIDOO U., Nutritional Psychiatry: Your Brain on Food, Harvard Health Blog, 2015, https://www.health.harvard.edu/blog/nutritional-psychiatry-your-brain-on-food-201511168626.

[21] Age UK, Diet and Brain Health, London, 2024, https://www.ageuk.org.uk/information-advice/health-wellbeing/mind-body/staying-sharp/looking-after-your-thinking-skills/diet-and-brain-health/.

[22] Neuro Media, Exploring the Connection Between Food and Cognition, 2024, https://www.neuromedia.ca/exploring-the-connection-food-and-cognition/

[23] JIN Y., et al., Dietary Patterns and Depressive Symptoms in Adults: A Systematic Review and Meta-Analysis, Nutrition Reviews, 79(6), 693-708, 2021, https://doi.org/10.1093/nutrit/nuaa107

The median age of the population could be an important indicator to detect which nutrients may be of greatest importance and which are the greatest risks associated with the use of counterfeit nutrients.

1.2.1 Monitoring fake nutrients

Given the critical role of these nutrients, especially in Western Europe, it is imperative to monitor the presence of counterfeit nutrients that match the most common nutritional needs. Ensuring that vitamins such as B12 and D, iron, calcium, and omega-3 fatty acids are genuine and bioavailable is essential for public health. Robust monitoring systems can help detect and prevent the distribution of fake nutrients, safeguarding the cognitive and physical health of the population[24].

2. Real world examples and Risk-Analysis

While there is no direct evidence linking counterfeit nutrients to state-sponsored cognitive warfare, numerous episodes of food fraud illustrate the potential risks. For example, food scandals involving melamine-contaminated baby formula and counterfeit olive oil highlight how easily food supply chains can be compromised[25]. These incidents were primarily driven by economic gain. However, they demonstrate that food fraud can be used for more malicious purposes.

2.1 FMEA Analysis

We conducted a risk analysis using a Failure Mode and Effects Analysis (FMEA) (*Table 1*) and qualitatively categorized the risks. The FMEA is a method for identifying and preventing potential failures in a process or system, improving safety and quality. It allows for the classification and mitigation of risks, enabling preventive actions to avoid problems and optimize efficiency[26].

---

[24] U.S. Environmental Protection Agency (EPA), Innovative Nutrient Removal Technologies: Report, Washington, D.C., 2021, https://www.epa.gov/system/files/documents/2021-08/innovative-nutrient-removal-technologies-report-082721.pdf.

[25] Age UK, Diet and Brain Health, London, 2024, https://www.ageuk.org.uk/information-advice/health-wellbeing/mind-body/staying-sharp/looking-after-your-thinking-skills/diet-and-brain-health/.

[26] American Society for Quality (ASQ). "Failure Modes and Effects Analysis (FMEA)." Available at: https://asq.org/quality-resources/fmea

Table 1

FMEA: Cognitive Warfare Through Fake Food and Nutrients								
Failure Mode	Potential Effect	Severity (S)	Potential Causes	Occurrence (O)	Current Controls	Detection (D)	RPN	Mitigation Strategy
Distribution of Fake Vitamin D	Cognitive decline, depression, weakened immune system	9	Intentional adulteration, poor regulation	6	Quality checks by health agencies	5	270	Enhance testing protocols, public awareness campaigns
Distribution of Fake Omega-3 Supplements	Cognitive decline, increased risk of dementia	9	Substitution with cheaper oils, mislabeling	6	Random batch testing	4	216	Stricter import controls, better supplier vetting
Distribution of Fake Vitamin B12	Cognitive impairment, memory loss, neurological issues	8	Substitution with ineffective compounds	5	Certification of suppliers	5	200	Increase frequency of inspections, improve public education
Distribution of Fake Iron Supplements	Cognitive fatigue, decreased attention span, anemia	7	Adulteration, substitution with non-bioavailable forms	6	Regulatory oversight	5	210	Implement advanced testing techniques, enhance supplier scrutiny
Distribution of Fake Calcium Supplements	Cognitive issues due to metabolic disturbance, osteoporosis	7	Economic gain, counterfeit products	5	Regulatory inspections	5	175	Improve traceability, stronger penalties for offenders
Fake Processed Foods with High Sugar Content	Increased risk of cognitive decline, memory impairment, inflammation	8	Use of cheap, high sugar fillers	7	Nutritional labeling regulations	4	224	Stricter food labeling laws, public health campaigns

2.1.2 Risk Assessment of Cognitive Warfare through counterfeit food

Assessing the rank or level of risk of a cognitive warfare attack on Western Europe using counterfeit food involves considering several factors. These include the potential severity of the impact, the likelihood of it occurring, and the effectiveness of current detection and mitigation strategie

Factors to Consider:

a. Severity (Impact)
   - Health Impact: Counterfeit nutrients can cause significant cognitive decline, neurological issues, and overall health deterioration.
   - Economic Impact: The spread of counterfeit food can disrupt economies, burden healthcare systems, and reduce workforce productivity.
   - Social Impact: Loss of trust in food systems, public fear, and potential social unrest.

b. Likelihood of Occurrence
   - Existing Precedents: Numerous incidents of food fraud have occurred, indicating that counterfeit food is already a known issue.
   - Ease of Execution: Counterfeit food production can be relatively easy and cost-effective, making it a feasible strategy for adversaries.
   - Current Controls: Although there are regulatory bodies and checks in place, the current controls may not be fully effective in preventing sophisticated counterfeit operations.

c. Detection and Mitigation Effectiveness
   - Monitoring and Testing: Regular testing and monitoring exist but need enhancement to detect and prevent advanced counterfeit methods.
   - Public Awareness: Public awareness is growing, but more education is needed to identify and avoid counterfeit products.
   - Regulatory Framework: The regulatory framework is strong but requires continuous improvement to keep up with evolving threats.

Using a qualitative risk assessment matrix, we can categorize the risk as follows:

Risk Factor	Low (1-3)	Medium (4-6)	High (7-9)
Severity (Impact)			8
Likelihood of Occurrence		6	
Detection and Mitigation		5	

2.1.3 Overall Risk Rank/Grade

- Severity (8/9): The impact on health, economy, and society can be severe due to cognitive decline and other health issues.
- Likelihood (6/9): There is a medium likelihood of occurrence, given the existing incidents of food fraud and the feasibility of execution.
- Detection and Mitigation (5/9): Current measures are moderately effective but need significant improvements.

2.1.4 Calculation of Risk Priority Number (RPN)

The RPN is calculated as: RPN=Severity×Likelihood×Detection

RPN=9×6×5=270

Distribution of Fake Vitamin D seems to be the priority risk to resolve.
Based on the calculated RPN and the qualitative analysis, the rank or level of risk for cognitive warfare with counterfeit food against Western Europe could represent a serious risk, especially if focused on the most needed nutrients. This high-risk level emphasizes the need for increased surveillance, stricter regulations, better public awareness, and international cooperation to effectively mitigate the threat. The strategic manipulation of nutrition could become a powerful tool in cognitive warfare, with far-reaching implications for the health, security, and stability of Western Europe.

3. Chemical and Biological Warfare vs Cognitive Warfare

Chemical and biological warfare involves the use of toxins, pathogens, and chemical agents to inflict injury or death on humans, animals, and plants. Chemical agents, such as nerve or blister agents, and biological agents, typically viruses or bacteria, are designed to incapacitate or rapidly destroy targets. These methods focus on causing direct physical damage and disruption. In contrast, cognitive warfare is a more insidious strategy that targets the mind. Using specific nutrients or counterfeit food, cognitive warfare combines physical, biological, and chemical elements to subtly affect cognitive functions such as memory, decision-making and critical thinking. This sophisticated approach includes psychological operations and misinformation campaigns to weaken societal resilience and create confusion. While chemical and biological attacks are overt and cause immediate damage, cognitive warfare is covert and aims at long-term cognitive degradation and psychological manipulation without immediate visible effects. This complexity makes cognitive warfare a unique and evolving threat in the modern warfare landscape[27].

[27] NATO Joint Warfare Centre, Cognitive Warfare, Stavanger, 2021, https://www.jwc.nato.int/application/files/7216/9804/8564/CognitiveWarfare.pdf.

4. Bioterrorism and Cognitive Warfare

The use of pathogens or other tools aimed at debilitating the health of an adversarial group is a common aspect of both bioterrorism and cognitive warfare[28]. The fundamental difference, however, is that in the latter case the strategy of debilitating the adversary is part of a deeper and more insidious strategy of manipulation. In cognitive warfare, the release of pathogens or counterfeit nutrients aims to weaken cognitive abilities already compromised by disinformation campaigns and thought manipulation.

While bioterrorism has traditionally focused on causing physical harm through the spread of diseases such as anthrax or smallpox, cognitive warfare targets the mental capabilities of a population, making it a more sophisticated and layered threat. Rather than relying solely on the direct physical effects of biological agents, cognitive warfare integrates these attacks into a broader strategy of psychological manipulation that seeks to disrupt and control the target's perception and decision-making processes.

For instance, bioterrorism could involve the intentional release of a pathogen like Bacillus anthracis (anthrax), which the CDC has categorized as a high-priority agent due to its potential for high mortality and its ability to cause public panic[29]. On the other hand, cognitive warfare might employ the same pathogen, not just to cause immediate health crises but to create a prolonged state of fear and confusion, amplifying the effects through coordinated disinformation campaigns that undermine trust in public health institutions.

Moreover, counterfeit nutrients could be strategically introduced into the food supply to cause deficiencies in essential vitamins and minerals, such as omega-3 fatty acids, which are critical for cognitive health. The subtlety of this approach lies in its ability to gradually degrade cognitive function, leading to confusion, impaired decision-making, and increased susceptibility to further manipulation.

This insidious aspect of cognitive warfare highlights the importance of comprehensive strategies that encompass not only immediate medical responses but also long-term psychological and social resilience. Public health systems must be prepared to detect and mitigate not only the biological threats but also the accompanying psychological operations that seek to exploit these physical attacks[30].

In summary, while both bioterrorism and cognitive warfare utilize biological agents to weaken an adversary, cognitive warfare extends this threat into the psychological realm, aiming to erode cognitive capabilities through a combination of direct health impacts and manipulative disinformation tactics.

---

[28] JOHNSON K., Biological Warfare, eMedicineHealth, 2021, https://www.emedicinehealth.com/biological_warfare/article_em.htm.

[29] Centers for Disease Control and Prevention (CDC), Anthrax as a Bioterrorism Weapon, Atlanta, 2023, https://www.cdc.gov/anthrax/bioterrorism/index.html.

[30] Institute of Medicine (US) and National Research Council (US) Committee on Science, Technology, and Law, Biological Threats and Terrorism: Assessing the Science and Response Capabilities, Washington, D.C., 2002, https://www.ncbi.nlm.nih.gov/books/NBK570614/

Conclusion

Exploring cognitive warfare through the lens of nutritional manipulation represents a compelling extension of traditional psychological operations. Cognitive warfare, by its very definition, aims to influence perceptions and behavior on a large scale, and the inclusion of nutritional tactics introduces a novel and alarming dimension. The manipulation of food quality to affect cognitive health is an area that, while hypothetical, cannot be overlooked given the profound implications for public health and societal stability.

Cognitive warfare has traditionally involved psychological manipulation through misinformation, but the inclusion of nutritional manipulation broadens its scope. By targeting the food supply with counterfeit nutrients, adversaries can covertly impair cognitive functions in large populations, securing a long-term strategic advantage. Essential nutrients like vitamins, minerals, and omega-3 fatty acids are crucial for brain health; counterfeit nutrients could lead to widespread deficiencies, impairing memory, attention, and decision-making. Toxic additives in food can cause neurological damage, while non-bioavailable counterfeit nutrients may disrupt metabolism and induce chronic inflammation, further degrading cognitive functions.

This approach shares similarities with bioterrorism but differs in its long-term psychological focus rather than immediate physical harm. Cognitive warfare aims to undermine cognitive capacity over time, creating a prolonged vulnerability. Western Europe, with its reliance on processed foods and specific nutritional needs, is particularly vulnerable to the effects of counterfeit nutrients. Ensuring the authenticity of essential nutrients is vital for maintaining cognitive health and societal stability.

Risk assessment highlights the high threat level posed by cognitive warfare through counterfeit food. Effective detection and mitigation require enhanced surveillance, stricter regulations, and increased public awareness. Western health systems must be robust and prepared to respond to such threats to mitigate risks. Unlike chemical and biological warfare, which causes immediate physical damage, cognitive warfare insidiously targets mental capabilities over time, necessitating comprehensive defense strategies that address both physical and psychological aspects.

Strategically, recommendations include enhanced monitoring and testing for counterfeit nutrients, public awareness campaigns, regulatory improvements to ensure food integrity, and international cooperation to develop unified strategies against cognitive warfare.

The main contribution of the paper is to begin to focus on aspects that have not yet been considered among the possible threats to national security. So far, the term hybrid warfare has been used to include domains that are not strictly and/or exclusively kinetic. Most definitions of hybrid warfare do not take into account the political, economic, social and informational domains of warfare that states can employ on a much larger scale than non-state actors and with very different intentions. It goes far beyond the irregular, terrorist, criminal and

unconventional aspects that make up hybrid warfare. More specifically, operations in the so-called grey zone are included in the concept of non-linear guerrilla warfare. Non-linear warfare (NLW) is based on subverting and dividing the enemy's social and political structure.

NLW have become increasingly prevalent in the 21st century as state and non-state actors seek to gain strategic advantage without resorting to full-scale conventional warfare. This form of non-linear warfare uses an approach in which the actual armed conflict is not the primary objective. Instead, the goal is to create a complex and fluid situation that exploits the opponent's weaknesses by any means necessary.

Non-linear warfare exerts pressure on the target state in order to undermine its cohesion, its internal resilience and the vital functions of a society.

In conclusion, the hypothetical scenario of cognitive warfare through food manipulation is a serious and complex threat. The protection of public health, the food supply chain and the protection of individual cognitive functions from the potential manipulation of the nutritional principles of food are part of a broad concept of national security. The significant food and national security implications of a potentially disruptive approach in this area make it more necessary than ever to adopt a combined civil-military approach within the information and decision-making cycle to counter these new threats.

The integration of counterfeit nutrients into cognitive warfare strategies could have far-reaching implications for public health and economic stability. Proactive measures to improve surveillance, raise public awareness and strengthen regulatory frameworks are essential to prevent this new form of warfare. By understanding and addressing the multifaceted nature of cognitive warfare, Western societies can better prepare for and mitigate the potential risks associated with this insidious threat.

STRATEGIC LEADERSHIP
JOURNAL

CHALLENGES FOR GEOPOLITICS
AND ORGANIZATIONAL DEVELOPMENT

EDITORIALE

Cari lettori, ho il piacere di presentarvi il quarto numero del 2024 della nostra rivista “SLJ”.
Il presente fascicolo segna anche una tappa storica poiché conclude per la prima volta un anno di pubblicazioni completo.
Partiamo, quindi, dall’inizio; la copertina, che vede rappresentata una immagine della cerimonia di apertura dell’anno accademico, evento molto importante per un centro di formazione come il nostro, alla quale hanno partecipato il Ministro della Difesa, On. Guido Crosetto, il Capo di Stato Maggiore della Difesa, Generale Luciano Portolano, e la Presidente della Scuola Nazionale dell’Amministrazione, prof.ssa Paola Severino che ha tenuto una Lectio Magistralis sullo “sviluppo delle competenze come leva strategica per la Pubblica Amministrazione”.
Nella rubrica dedicata alle discussioni proponiamo due articoli che vertono uno sulla “Strategia e conflitti asimmetrici” e l’altro su “Cognitive Warfare”.
Proseguendo nello sfogliare la rivista, nella parte propriamente scientifica, possiamo trovare degli articoli riguardanti la “Space Economy”, la “Geopolitica delle multinazionali”, le possibili interazioni tra “Space e Cyberspace”, tematiche di carattere energetico e di cambiamento climatico e, infine, Europa e unione dei mercati dei capitali.
Il nostro obiettivo si conferma quello di offrire ai Lettori un ventaglio sempre maggiore di spunti di riflessione e di tematiche, che seppur nelle loro specificità, si possono ricondurre alla missione fondamentale del nostro Centro.
Come sempre, a margine di queste poche righe di Editoriale desidero ringraziare tutti gli Autori del presente fascicolo unitamente a coloro che lavorano nella Redazione e a tutti i nostri Lettori e Lettrici auguro: buona lettura!

Il Capo Redattore
Col. AArnn Pil. Loris Tabacchi

INDICE

Ministero della Difesa

Periodico della Difesa
Registrazione Tribunale di Roma n. 88/2023 in data 22.06.2023
Codice Fiscale 97042570586
ISSN 2975-0148 – ISBN 9791255150787

STRATEGIC LEADERSHIP JOURNAL

A R T I C O L I

(Sezione soggetta a peer-review Double Blind)

Marco Stefano Borsarelli
Laureato con lode in Scienze Politiche presso l'Università degli Studi di Torino, titolato IASD con lode (75° edizione), VP EFA Production PM presso Leonardo - Aircraft Division

SPACE ECONOMY: UNA SFIDA ALL'INSEGNA DELLA COLLABORAZIONE

ABSTRACT

Il concetto di space economy indica tutte le attività che implicano l'uso commerciale delle tecnologie spaziali, siano esse collocate all'interno dell'orbita terrestre oppure all'esterno. Il settore spaziale, a lungo dominato dalla presenza delle istituzioni pubbliche, è oggi sempre più interessato da iniziative private e ha visto raddoppiare il proprio fatturato nel corso degli ultimi quindici anni. Una domanda crescente di servizi digitali basati sullo spazio, l'ingresso di nuovi attori, la nascita di nuovi modelli d'impresa, l'aumento dei finanziamenti privati, innovazione e nuove formule di collaborazione fra attori privati e istituzioni pubbliche sono le principali tendenze osservabili attualmente nel settore della space economy.

The concept of space economy denotes all activities involving the commercial use of space technologies, whether they are located within Earth orbit or outside. The space sector, long dominated by the presence of public institutions, is now increasingly affected by private initiatives and it has seen doubled its revenues over the past fifteen years. A growing demand for space-based digital services, the entry of new players, the emergence of new business models, increased private funding, innovation and new formulas for collaboration between private actors and public institutions are the main trends currently observable in the space economy sector.

Introduzione

Negli ultimi decenni, l'umanità ha assistito a una accelerazione nell'esplorazione e nell'utilizzo dello spazio extraterrestre. Questo ha generato una nuova era, quella della *space economy*, in cui l'attività economica è estesa oltre i confini terrestri, abbracciando una vasta gamma di settori, dalle telecomunicazioni all'osservazione della Terra, dalla navigazione satellitare alla ricerca scientifica e oltre. Parallelamente, la proliferazione di tecnologie come l'intelligenza artificiale e Internet sta ridefinendo le modalità di produzione, consumo, comunicazione e interazione sociale. In questo contesto, la *space economy* si erge come modello e *driver* fondamentale per nuove forme di mercato e di collaborazione: l'interazione tra questi due fenomeni ha il potenziale di trasformare radicalmente l'economia globale, generando nuove opportunità di crescita economica, innovazione e sviluppo sostenibile. Tuttavia, per comprendere appieno l'importanza di questo legame e le sue implicazioni, è essenziale analizzare le dinamiche della *space economy* e il suo impatto sugli attori privati e non nei diversi settori che la compongono. Questo articolo propone una analisi della relazione tra la *space economy* e le nuove forme di *business* che sta sviluppando, mettendo in luce come l'utilizzo dello spazio abbia

stimolato l'innovazione tecnologica e la trasformazione economica, richiedendo una struttura normativa dedicata e adeguata a supportare questo nuovo dominio e gli attori ad esso legati, in ottica di rendere il mercato spaziale e gli investimenti effettuati sempre più sostenibili nel tempo e incentivando nuove e più forti forme di collaborazione tra enti pubblici e privati.

Lo Spazio e la *Space Economy*: cenni storici, definizioni e confini

L'economia e i suoi potenziali sviluppi sono sempre stati oggetto di importanti discussioni tra economisti, politici e cittadini. I *trend* dello sviluppo economico sono cambiati nel corso degli anni e quelli che, fino a pochi anni fa, erano considerati inconcepibili o eccessivamente avveniristici per l'immaginazione umana, oggi si sono trasformati in *trend* reali che stanno ottenendo sempre più attenzione da parte dei mercati e dei governi. La *Global Space Economy* costituisce uno dei temi attuali con particolari prospettive di sviluppo.

Una definizione generalmente accettata ormai da tutta la comunità scientifica relativamente al concetto di *space economy* è quella dell'*Organisation for Economic Co-operation and Development* (OECD) del 2014[1], che sancisce come appartenenti al settore economico spaziale tutti gli attori coinvolti nell'applicazione sistematica delle discipline scientifiche per l'esplorazione e l'utilizzo dello spazio[2]. Nel 2021, Erik Kulu affermò che "parlare di economia spaziale significa parlare di come fare ricavi e generare entrate dallo spazio, usando risorse in orbita o oltre la Terra, definendo l'economia spaziale come la nuova industria spaziale extraterrestre"[3]. L'ampio respiro di questa definizione, sufficientemente generica da lasciare spazio a una moltitudine di applicazioni, dimostra come la rilevanza della s*pace economy* sia ormai a un livello di espansione tale da riuscire con difficoltà a rilevarne con precisione i confini ed i settori economici interessati dal fenomeno. Le crisi finanziarie e la necessità di uno sviluppo economico e tecnologico sono fattori che hanno inciso sotto diversi profili allo sviluppo dell'economia spaziale, rendendola elemento determinante per gli Stati.

Unitamente a tali eventi, la competizione globale si sta intensificando, mentre le attività spaziali si espandono e si diversificano di giorno in giorno. Tale circostanza rende altresì complesso determinarne con esattezza il valore economico[4]. Per meglio comprendere questo nuovo ambito di indagine, occorre definirne alcuni elementi essenziali e alcune definizioni necessarie a inquadrare correttamente la tematica. La "corsa allo spazio" inizia nel 1957, quando l'Unione Sovietica lancia il satellite Sputnik 1.

---

1 OECD, *The Space Economy at a Glance 2014*: "*The global space economy, as defined by the OECD Space Forum, comprises the space industry's core activities in space manufacturing and in satellite operations, plus other consumer activities that have been derived over the years from governmental research and development"*.

2 ESA, Eurostat, *Developing a space economy thematic account for Europe - 2023 Edition.*

3 KULU E., *In-space Economy in 2021 – Statistical Overview and Classification of Commercial Entities*, in *72nd International Astronautical Congress (IAC 2021), Dubai, United Arab Emirates*: "*In-space economy means generating revenue in space using assets in orbit or beyond Earth. Inspace economy is the new extraterrestrial space industries. Sometimes called as space-based economy and in narrower de_nitions on-orbit economy, space-for-space economy, low Earth orbit economy, beyond-Earth space economy and it also encompasses cislunar economy, Moon and Mars*".

4 Si veda Commissione Europea, *The future of the European space sector. How to leverage Europe's technological leadership and boost investments for space ventures*, pagg. 21-22 par. 2.1.2 *The traditional and new space market - market segment and sizes*. Si veda anche PricewaterhouseCoopers (PwC*), Main Trends & Challenges in the Space Sector, 2nd Edition* (Dic. 2020).

I primi programmi spaziali, all'epoca ancora fortemente limitati dalla scarsa disponibilità di ingenti somme di denaro necessarie per attuarli, furono esclusivo appannaggio delle due superpotenze mondiali dell'epoca, USA e URSS[5]. Furono pensati, avviati e realizzati principalmente per scopi scientifici e sperimentali, ma anche per dimostrare in chiave strategica militare mondiale le capacità tecnologiche raggiunte dai due Paesi.

Con una velocità fino ad allora non immaginabile, negli anni successivi si susseguirono missioni spaziali che portarono l'uomo sulla Luna, misero in orbita i primi satelliti, inizialmente militari e successivamente commerciali, consentirono all'uomo di effettuare le prime passeggiate nello spazio, lanciarono nello spazio i moduli per la realizzazione di stazioni spaziali orbitanti intorno alla Terra[6]. Tali attività, accompagnate da una efficace campagna mediatica, hanno enfatizzato le enormi potenzialità della ricerca scientifica del nuovo ambiente chiamato "spazio" e le possibili evoluzioni connesse al suo sfruttamento. A partire dagli anni '70 la corsa allo spazio tra USA e URSS finì. Le ragioni furono varie: l'obiettivo più importante tra quelli da raggiungere, ossia la Luna, era stato raggiunto; i rapporti tra le due superpotenze andarono incontro a un periodo di temporanea distensione, consentendo così di ridurre gli investimenti nelle missioni spaziali; infine, altri Paesi iniziarono a sviluppare propri programmi spaziali[7], facendo cadere quindi il principio esclusivo della corsa a due verso lo spazio.

La collaborazione tra USA e URSS si concretizzò il 17 luglio 1975, giorno in cui una navicella sovietica e una americana si agganciarono in orbita, trasformando di fatto la competizione vissuta negli anni '50-'60 come collaborazione e non più come spirito antagonistico tra le parti[8].

Gli effetti della corsa allo spazio si possono vedere ancora oggi: la rivalità tra Stati Uniti e Unione Sovietica, causa di investimenti enormi nelle esplorazioni, consentì scoperte fondamentali in molti campi scientifici, primo tra tutti l'astronomia, oltre a portare all'umanità eccezionali progressi tecnologici.

Questi risultati, che posero le fondamenta delle successive esplorazioni spaziali, hanno effetti importanti sulla nostra vita quotidiana: satelliti artificiali per le telecomunicazioni, sistemi di posizionamento e navigazione, trasmissioni televisive, scambio dati iper-veloce sono solo alcuni esempi delle applicazioni che oggi abbiamo grazie alla competizione avvenuta nel secolo scorso per raggiungere lo spazio.

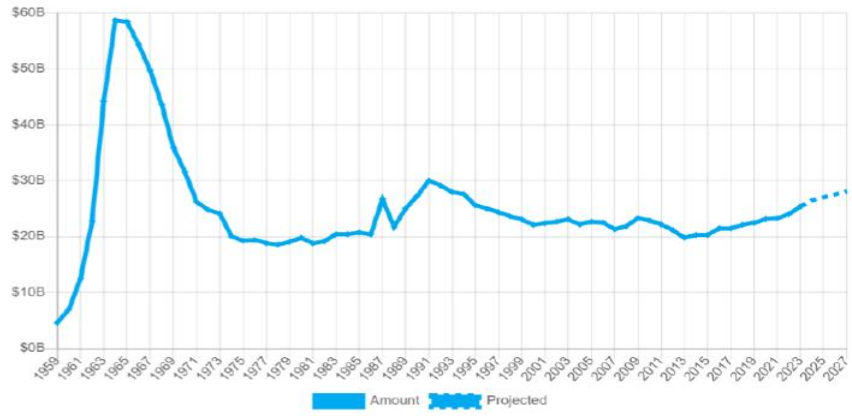
---

5 SPERANDEO P., "*L'impatto dell'evoluzione del comparto spaziale nel settore economico, politico e della sicurezza nazionale*", in *Osservatorio n.181 – 2020*, pagg. 11-21.

6 La MIR, stazione spaziale orbitante sovietica, divenuta di proprietà della Federazione Russa nel 1991, è stata posta in orbita nel 1986. Nel marzo 2001, ormai abbandonata, è stata fatta precipitare in direzione dell'Oceano Pacifico, al largo delle coste dell'Australia e si è disintegrata al rientro nell'atmosfera terrestre (da Enciclopedia Treccani Online).

7 SPERANDEO P., "*L'impatto dell'evoluzione del comparto spaziale nel settore economico, politico e della sicurezza nazionale*", in Osservatorio n.181 – 2020, p. 13.

8 FONZO E. (a cura di), "*La corsa allo spazio tra USA e URSS durante la Guerra Fredda: la storia in Breve*", accessibile in https://www.geopop.it/la-corsa-allo-spazio-tra-usa-e-urss-durante-la-guerra-fredda-la-storia-in-breve/.



Budget della Nasa nel periodo 1959 - 2023[9]

L'assenza di una definizione univoca di "spazio esterno" comporta la necessità di rapportare le differenti nozioni esistenti. Secondo una prospettiva meramente fisica, lo spazio inizia nel punto esatto in cui termina l'atmosfera terrestre[10].
Una definizione tecnica di spazio parte invece dalla *Kàrmàn Line*[11], un limite convenzionale posizionato a 100 chilometri al di sopra del livello del mare[12]. Da un punto di vista teorico, al di sopra di questa linea la densità atmosferica diventa troppo bassa per fornire ai velivoli convenzionali una spinta sufficiente a mantenersi in volo: a queste quote un velivolo convenzionale dovrebbe raggiungere una velocità orbitale per evitare di rientrare nell'atmosfera. Per completezza di trattazione occorre però inquadrare lo spazio anche dal punto di vista giuridico. Il diritto aeronautico e il diritto dello spazio sono sottoposti per ora a due differenti e separati regimi giuridici, in quanto basati su principi fondamentali molto diversi e in alcuni casi opposti tra loro: il diritto aeronautico riconosce l'autorità territoriale, quello spaziale la nega; il primo sancisce una responsabilità limitata dei vettori, il secondo stabilisce la responsabilità illimitata degli Stati. Ad oggi l'ordinamento giuridico internazionale non appare quindi aver definito un regime giuridico integrato del diritto nello spazio[13].
Questo è attualmente disciplinato da cinque trattati e convenzioni, definiti sotto l'egida dell'ONU nel periodo tra il 1967 e il 1979[14]. Tali documenti si fondano sul principio di libera esplorazione dello spazio oltre l'atmosfera e la non possibilità di

[9] Fonte: https://www.planetary.org/space-policy/nasa-budget.
[10] L'atmosfera terrestre è l'involucro di gas che riveste il pianeta Terra, trattenuto al di sopra della superficie terrestre grazia alla forza di gravità; è lo scudo naturale contro gli oggetti celesti (artificiali e non) in caduta dallo spazio, ma anche contro le pericolosissime radiazioni ultraviolette provenienti dal Sole. Agisce anche da contenitore per l'aria, determinante per garantire la vita e per la regolamentazione della temperatura terrestre.
[11] Theodore von Kàrmàn, ingegnere ungherese, fu il primo scienziato a calcolare l'altezza dal livello del mare a cui l'atmosfera diventa troppo rarefatta per consentire il volo grazie al sostentamento dell'aria e alla legge della portanza, a poco meno di 100 chilometri sul livello del mare.
[12] L'ente governativo mondiale per i registri aeronautico e astronautico, la *Fédération Aéronautique Internationale* (FAI) e molte altre organizzazioni utilizzano la linea Kármán come un modo per determinare quando il volo spaziale è stato raggiunto.
[13] GASPARI F., *"La disputa infinita: la delimitazione dei confini tra spazio aereo e spazio cosmico, in Rivista Marittima"*, Luglio-Agosto 2020.
[14] I trattati furono redatti sotto l'egida dello United Nations Office for Outer Space Affairs, per tramite del Committee on the Peaceful Uses of Outer Space (COPUOS).

appropriarsi dello stesso da parte degli Stati esploratori. Una regola del diritto internazionale, basata su consuetudine, sancisce che la più bassa altitudine teorica a cui un satellite può orbitare intorno alla Terra (circa 100 chilometri sul livello del mare) non è soggetta al diritto di sovranità nazionale, ed è governata dal diritto dello spazio: questa regola si basa su una convenzione adottata a livello internazionale che ha lo scopo di delimitare il confine tra atmosfera e spazio lungo la linea di *Kàrmàn*.

La questione, per nulla di facile soluzione, divide da sempre chi si interessa di questa materia a vario titolo: se per alcuni il confine è meramente una questione scientifica, per altri è una problematica di natura politica. Il *Committee on the Peaceful Uses of Outer Space* (COPUOS) ha riconosciuto come unica soluzione al problema la stesura di un accordo internazionale dedicato, con tutte le difficoltà di armonizzazione e accordo tra le parti che esso comporta.

Il regime giuridico applicabile

I primi tentativi di disciplinare la tematica dello spazio risalgono al 1967, anno in cui viene adottato il primo trattato internazionale sul tema dello spazio, preparato e firmato dalle Nazioni Unite.

Il "Trattato sullo spazio extra-atmosferico" (*Outer-Space Treaty*, OST)[15] nasce con il lancio in orbita del primo satellite artificiale (una sfera di metallo del diametro di poco meno di 60 centimetri), creando di fatto una competizione tecnologica tra USA e URSS[16]. Tale situazione di incertezza generò in differenti Stati la necessità di definire un sistema giuridico e normativo dedicato, uniforme e universale, capace di favorire le esplorazioni e lo studio dello spazio da parte di tutti e che definisse regole comuni per l'attività nello spazio extra-atmosferico. Le Nazioni Unite accolsero questa necessità e crearono la Commissione sull'Uso Pacifico dello Spazio Extra-Atmosferico (COPUOS), con l'obiettivo di garantire la fruibilità e l'uso di tutte le scoperte scientifiche derivanti dallo studio dello spazio da parte di tutti[17] ed

---

[15] Nazioni Unite, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including Moon and Other Celestial Bodies*. Il trattato è composto di diciassette articoli, considerati il fondamento del Diritto Internazionale dello Spazio, una vera e propria "*Space Magna Charta*": sul tema si veda ANTONUCCI A., *Compie 59 anni l'era spaziale dell'umanità*, in L'Osservatore Romano, 11 aprile 2020; si veda anche ANDEM M. N., *The 1967 Outer Space Treaty (1967 OST) as the Magna Carta of Contemporary Space Law: A Brief Reflection*, in *Proceedings of the Forty-Seventh Colloquium on the Law of Outer Space*, Vol. 47 (2004), pp. 292-307.

[16] Si tratta dell'evento storico del 4 ottobre 1957, conosciuto come "Crisi dello Sputnik", che diede inizio alla "corsa allo spazio" che ha caratterizzato il periodo '50-'70, provocando notevole preoccupazione agli alleati nel blocco occidentale. Sulla *Space Race*, sulla vicenda dello Sputnik e sulle sue conseguenze a livello politico e strategico esiste una letteratura ampia, ad esempio LANIUS R. D., LOGSDON J. M., SMITH R. W., *Reconsidering Sputnik: Forty Years Since the Soviet Satellite*, Routledge, London-New York, 2014. Sulle vicende aerospaziali sovietiche si veda SIDDIGI A., *Sputnik and the Soviet Space Challenge*, University Press of Florida, Gainesville (FL), 2003. In riferimento alla reazione dell'amministrazione statunitense cfr. DIVINE R. A., *The Sputnik Challenge. Eisenhower's Response to the Soviet Satellite*, Oxford University Press, Oxford, 1993 e LEVINE A. J., *After Sputnik. America, the World, and Cold War Conflicts*, Routledge, London-New York, 2017.

[17] Si v. art. 2, in cui si sancisce che l'esplorazione dello spazio può essere effettuata esclusivamente nell'interesse di tutti i Paesi. Cfr. anche: OST – art. 2: "*Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means*".

esclusivamente per scopi pacifici[18], normando le controversie che sarebbero potute nascere su questo tema[19] e definire un regime di responsabilità degli Stati, per i danni causati da una missione fallita o da oggetti caduti sul pianeta nel caso in cui i lanci siano partiti dal proprio territorio nazionale[20]. I Paesi membri delle Nazioni Unite hanno successivamente concordato e siglato ulteriori quattro trattati volti a disciplinare: le procedure da seguire nel caso in cui gli astronauti debbano affrontare una situazione di emergenza, con pronta assistenza da parte di tutti i Paesi[21]; la responsabilità degli Stati in caso di danni da oggetti precipitati dalla loro orbita[22]; l'obbligo di registrazione di qualsiasi oggetto sia messo in orbita, per una fondamentale tracciabilità degli stessi[23]; fornire chiarimenti in merito allo sfruttamento della Luna e degli altri corpi celesti, ivi compreso il diritto di proprietà degli stessi[24]. Bisogna però sottolineare che questo ultimo trattato è stato il meno fortunato: solo 18 Stati hanno aderito e la maggior parte di questi non è coinvolta in attività spaziali.

I trattati qui sopra elencati rappresentato l'attuale "*Corpus Iuris Spatialis*". Tuttavia, sarebbe un errore considerarli come unica fonte del diritto spaziale: il 5 agosto del 1963, subito dopo la conclusione della grave crisi di Cuba, venne sottoscritto a Mosca dalle tre grandi potenze nucleari (USA, URSS e Regno Unito) il "Trattato per il bando degli esperimenti di armi nucleari nell'atmosfera, nello spazio cosmico e negli spazi subacquei"[25]. Il fatto che da allora non siano stati firmati ulteriori accordi internazionali a livello delle Nazioni Unite evidenzia come questo

---

[18] Si v. art. 4, in cui si prevede il divieto per tutti gli Stati firmatari di posizionare armi nucleari o qualsiasi altro tipo di arma di distruzione di massa nell'orbita terrestre, sulla Luna o su altri corpi celesti. OST – art. 4: "*States Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner"*.

[19] Outer Space Treaty (OST) - art. 1: "*The exploration and use of outer space, including the moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind"*.

[20] OST – art. 6: "*States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. The activities of non-governmental entities in outer space, including the Moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty. When activities are carried on in outer space, including the Moon and other celestial bodies, by an international organization, responsibility for compliance with this Treaty shall be borne both by the international organization and by the States Parties to the Treaty participating in such organization*". V. anche Art. 7: "*Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the moon and other celestial bodies, and each State Party from whose territory or facility an object is launched, is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air or in outer space, including the moon and other celestial bodies*".

[21] Nazioni Unite, "*Agreement on the Rescue of Astronauts, the Return of Astronauts and the return of Objected Launched into Space*", firmato il 19 dicembre 1967.

[22] Nazioni Unite, "*Convention on International Liability for Damage Caused by Space Objects"*, firmato il 29 marzo 1972.

[23] Nazioni Unite, "*Convention on Registration of Objects Launched into Outer Space*", 1974.

[24] Nazioni Unite, "*Agreement Governing The Activities of States on the Moon and Other Celestial Bodies*", firmato il 18 dicembre 1978.

[25] GALA M., *Il paradosso nucleare: Il Limited Test Ban Treaty come primo passo verso la distensione*, Polistampa, Firenze, 2002. Si veda anche MASTNY V., *The 1963 Nuclear Test Ban Treaty: A Missed Opportunity for Detente?*, in *Journal of Cold War Studies* 10 (2008), 1, pp. 3-25.

particolare corpo di leggi sia ancora oggi oggetto di fortissime implicazioni geopolitiche.

Le più recenti risoluzioni, come ad esempio quella specifica per i "*Principles Relevant to the Use of Nuclear Power Sources in Outer Space*" del 1992 e la "*Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries*" del 1996, costituiscono testimonianza degli importanti sforzi che la comunità internazionale sta cercando di portare avanti per recuperare quella unità di intenti che aveva dato vita alle prime fasi delle esplorazioni spaziali, ma difficilmente possono essere considerati come punti cardine nell'evoluzione del diritto spaziale[26]. Al momento della firma dell'OST, i Paesi coinvolti nella stesura del trattato non ritennero necessario dover prevedere la presenza di soggetti privati portatori di interessi a investire e operare nel settore dello spazio e della sua esplorazione: la situazione infatti vedeva l'URSS, dove non era ammesso alcun intervento al di fuori di quello fatto dallo Stato, e gli USA, che in quel periodo non avevano sul loro territorio imprenditori e società interessate a questo ambito di mercato, ma che nella loro lungimiranza avevano ipotizzato un interesse potenziale futuro da parte di investitori privati. Il compromesso venne raggiunto attraverso il riconoscimento della possibilità di svolgere attività esplorativa nello spazio anche agli enti non governativi autorizzati dallo Stato membro del trattato in cui l'ente aveva sede, e sotto la sua continua supervisione[27]. Si sancisce quindi una piena responsabilità a livello internazionale degli Stati firmatari, indipendentemente dal fatto che l'attività di esplorazione sia svolta da enti governativi o non governativi. Occorre evidenziare come, diversamente dagli altri trattati che regolano l'uso e l'accesso alle *res communes* (acque internazionali, spazio aereo, Antartide), l'OST si limita a fare una breve trattazione dei principi, espressi in termini piuttosto generali: ad esempio, il trattato proibisce espressamente le attività con potenziali "conseguenze pericolose", senza però specificare in alcun modo come declinare il termine "pericolose" e come debba essere interpretato tale concetto[28].

---

[26] RUSCHI F., *Ascesa e Declino del Corpus Iuris Spatialis. Un Itinerario di Filosofia del Diritto Internazionale*, in Dirittifondamentali.it, 15 gennaio 2020.

[27] OST – art. 6: "*States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. The activities of non-governmental entities in outer space, including the Moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty*".

[28] OST – art. 9: "…*States Parties to the Treaty shall pursue studies of outer space, including the Moon and other celestial bodies, and conduct exploration of them so as to avoid their harmful contamination and also adverse changes in the environment of the Earth resulting from the introduction of extraterrestrial matter and, where necessary, shall adopt appropriate measures for this purpose. If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State Party to the Treaty which has reason to believe that an activity or experiment planned by another State Party in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, may request consultation concerning the activity or experiment*".

A questo bisogna aggiungere il fatto che, pur essendo la responsabilità delle attività svolte nello spazio da enti pubblici e privati in capo agli Stati, il concetto di *"activities"* indicato nel trattato non è in esso supportato da una chiara definizione, né da un elenco di attività consentite o vietate. Conseguentemente permane una incertezza giuridica circa la materiale applicazione di questi principi e alla futura evoluzione delle attività che potranno essere proposte da aziende private dotate di risorse economiche adeguate.

Questa situazione di incertezza del diritto porta con sé il rischio di blocco degli investimenti in questo campo o, al contrario, di far diventare la nuova corsa allo spazio un assalto ad una *res nullius*, in cui vale l'applicazione del *first come, first served*[29]. Incertezza ribadita peraltro da alcuni tentativi di iniziative di regolamentazione avvenute recentemente, come ad esempio il trattato sulla prevenzione dello spiegamento di armi nello spazio, la minaccia o l'uso della forza contro gli oggetti spaziali[30], promosso da Cina e Russia nel 2008 durante la Conferenza del Disarmo, rimasto in bozza e mai ratificato nonostante vari tentativi di superamento degli argomenti di scontro tra i Paesi interessati[31]. Nel momento storico attuale, in cui stanno emergendo obiettivi sempre più ambiziosi e per certi versi competitivi, il paradosso diventa evidente: la direttiva sulla *space policy*[32] prevede la costruzione di una stazione spaziale in orbita intorno alla Luna, primo passo odierno verso una presenza stabile dell'uomo sulla Luna, propedeutica e funzionale alle future missioni su Marte (previste nel 2030). A livello europeo, l'*European Space Agency* (ESA) ha previsto con un apposito programma di ricerca la presenza dell'uomo su Marte, con un piano di sviluppo molto simile a quello statunitense.

A fronte di questi esempi di accelerazione nella ricerca e nell'esplorazione dello spazio, l'attuale ordinamento giuridico spaziale rischia di risultare non adeguato a rispondere alle esigenze ed a fornire la certezza del diritto necessaria per gli investimenti indispensabili all'attività di R&S. La questione è tornata in auge nel 2015, con la presidenza USA Obama, durante la quale è stato promulgato il cosiddetto "*Space Act*"[33] e successivamente l'*American Space Commerce Free Enterprise Act*[34] durante la presidenza Trump: il primo con l'obiettivo di limitare le barriere allo sviluppo dell'esplorazione spaziale da parte di imprese private con scopi commerciali, a patto che sia sicura e sostenibile, mentre il secondo ha l'obiettivo di rendere più efficaci e trasparenti le procedure di controllo e autorizzazione sotto la gestione del governo statunitense. Quest'ultima in modo particolare, ha al suo interno alcuni punti fondamentali che mettono in discussione i principi tradizionali del diritto aerospaziale validi fino ad ora: lo spazio non viene più classificato come *res communis*[35].

---

[29] RUSCHI F., *Ascesa e Declino del Corpus Iuris Spatialis. Un Itinerario di Filosofia del Diritto Internazionale*, in Dirittifondamentali.it, 15 gennaio 2020, pag. 13.

[30] SU J., *The "Peaceful Purposes" Principle in Outer Space and the Russia–China (PPWT) Proposal*, in *Space policy*, 26 (2010), 2, pp. 81-90.

[31] TRONCHETTI F. - HAO L., *The 2014 Updated Draft PPWT. Hitting the Spot or Missing the Mark?*, in *Space Policy*, 33 (2015), pp. 38-49.

[32] Si veda: US Department of State, *Space Policy Directive – 1*, sottoscritta da Donald Trump l'11/12/2017.

[33] US Congress, *U.S. Commercial Space Launch Competitiveness Act*, 2015.

[34] US Congress, *H.R. 2809 – American Space Commerce Free Enterprise Act, 115th Congress* (2017-2018).

[35] TRONCHETTI F. - HAO L., *The American Space Commerce Free Enterprise Act of 2017: The Latest Step in Regulating the Space Resources Utilization Industry or Something More?*, in *Space Policy*, 47 (2019), 1-6.

Alla luce di quanto sopra, si può quindi concludere che lo sviluppo degli strumenti di diritto per la regolamentazione delle attività di esplorazione e uso dello spazio extra-atmosferico non ha seguito un percorso di crescita costante. Dopo cinquant'anni dall'introduzione dell'OST, l'attuale agenda del COPUOUS non include ancora proposte per un nuovo trattato internazionale o per l'emendamento di quello in vigore, nonostante i suoi principi siano stati formulati per essere adattati, rivisti o espansi sulla base dell'evoluzione della tecnologia, delle nuove opportunità e necessità dell'umanità e del suo progresso.
La libertà di utilizzare lo spazio e i corpi celesti è diretta conseguenza della assenza di sovranità territoriale degli stessi da parte degli Stati, ma allo stesso tempo è sempre più chiara l'esigenza dei Paesi di intervenire il più rapidamente possibile per fornire una maggiore stabilità e certezza del diritto per favorire e incentivare una maggiore collocazione degli investimenti, mirata agli interessi dei pionieri della *Space Economy*, siano essi pubblici o privati. L'enorme quantità di oggetti in orbita, unita all'assenza di un insieme di procedure ben delineato per comunicare a tutti l'occupazione di un'orbita o una sua deviazione e alla creazione di detriti spaziali ormai incontrollata, mostrano un sistema spaziale governato da una generale assenza di regole, nel quale è diventato estremamente importante coordinare una disciplina comune, aggiornata e puntuale sull'utilizzo dello spazio extra-atmosferico. In assenza di un quadro normativo armonizzato condiviso, che preveda anche sanzioni contro gli eventuali autori di gravi violazioni compiute nell'uso dello spazio, insieme alla portata ancora troppo generica delle convenzioni attualmente in vigore, potrebbe in estremo causare comportamenti irresponsabili e pericolosi sia da parte di enti privati interessati agli immensi potenziali ritorni economici, che da parte degli enti pubblici e governativi con potenziali produzioni di norme dedicate e valide a livello nazionale, a tutela di interessi specifici e non generali come previsto dall'OST.
È importante rilevare però che tale normativa ha generato anche comportamenti virtuosi e sostenibili: è recente la volontà di alcune aziende private di stipulare convenzioni in maniera completamente volontaria e auto-disciplinata, con lo scopo di garantire la sicurezza nelle missioni e promuovere un uso responsabile dello spazio extra-atmosferico, attraverso l'adozione di standard internazionali, linee guida dedicate e *best practice* provenienti da mezzo secolo di esplorazioni spaziali[36]. La partecipazione a questo accordo è aperta a tutti gli operatori spaziali, siano essi aziende private o enti governativi: un primo esempio di autoregolamentazione virtuosa, che dovrebbe sempre di più stimolare il dialogo internazionale per raggiungere quel quadro normativo preciso e puntuale in merito all'uso dello spazio, di cui l'umanità non può più fare a meno.

La *Space Economy* in Europa

In un periodo di grandi incertezze, causate dalla situazione geopolitica attuale (conflitto in Ucraina, Medio Oriente, elezioni politiche che porteranno al voto nel corso del 2024 circa la metà della popolazione mondiale per nominare i membri dei consigli e delle istituzioni internazionali più importanti), lo spazio e la sua decisività in termini economici, di ricerca e sviluppo, di essenzialità per il futuro della

[36] Space Safety Coalition (SSC), *Best Practices for the Sustainability of Space Operations*, v. 2.35, Nov. 2023.

sicurezza dei Paesi sono una certezza consolidata[37]. È un fatto ormai impossibile da ignorare da parte dei Governi e di conseguenza ancora più importante deve essere il ruolo dell'Europa nel contesto internazionale, stando di fianco alle grandi potenze "amiche", ma vicino anche ad altre potenze ben più lontane, tutte però caratterizzate da una *road map* ben chiara e definita in materia di spazio extra-atmosferico. Occorre ampliare in Europa la condivisione della necessità di investimenti nelle attività spaziali, che richiedono però un forte intervento da parte del legislatore e delle istituzioni per la regolamentazione di tali attività, al fine di tutelare e invogliare proprio quegli investimenti che diversamente sarebbero a rischio. Le piccole e medie imprese, importantissime nella catena del valore della *space economy*, possono temere infatti che il quadro normativo si aggravi e che ciò possa determinare delle conseguenze insostenibili per il loro equilibrio finanziario, creando di fatto un effetto opposto rispetto al desiderio di incentivazione della economia spaziale in Europa[38]. Lo spazio in Europa è quindi un evidente motore di innovazione: se nei decenni passati era sinonimo esclusivamente di spesa e investimenti pubblici, oggi il settore vede sempre più emergere nuovi attori privati, fortemente attratti dalle nuove opportunità commerciali che derivano dall'esplorazione spaziale e dallo sviluppo.

L'industria spaziale in Europa, inserita come settore strategico all'interno della più ampia industria aerospaziale e della difesa, progetta, sviluppa e costruisce sistemi spaziali, lanciatori, veicoli spaziali e relativi apparati terrestri di supporto e gestione per clienti pubblici e privati. Essa è ormai posta al vertice di una catena di valore legata ai servizi pubblici e privati, commerciali e non. I servizi spaziali ad alto valore aggiunto (Copernicus, Galilelo, *broadcasting* e banda larga diffusa, informazioni geospaziali, etc.) e il loro segmento di utenti terrestri generano benefici socio-economici ormai evidenti e sostengono e supportano lo sviluppo dell'Europa[39].

Le opportunità per i futuri mercati commerciali

La *space economy* può generare rilevanti esternalità positive sia materiali che immateriali.

Nel primo ambito rientrano le capacità di sviluppo di nuove tecnologie ad alta *performance* che diventeranno elementi abilitanti per gli sviluppi di altri settori (nuovi materiali, nuove tecnologie mediche, etc.): creazione di posti lavoro di alto

[37] *Il 23 e il 24 gennaio 2024 si è tenuta la 16th European Space Conference a Bruxelles, il luogo dove gli attori principali delle politiche spaziali si incontrano ogni anno per fare il punto della situazione e verificare insieme gli scenari futuri. L'importanza di questo evento che si è tenuto a Bruxelles è stata dimostrata anche dal livello di partecipazione, che ha visto prima di tutto ben quattro commissari europei (Thierry Breton, Virginijus Sinkevičius, e i vice presidenti Maroš Šefčovič e Josep Borrell Fontelles).*

[38] L'incentivazione all'ingresso delle imprese private nel settore dell'economia dello spazio potrebbe anche essere aumentata se i costi della "non Europa" venissero ridotti: in uno studio del Parlamento Europeo è emerso che l'economia dell'UE potrebbe raggiungere entro il 2032 almeno 2,8 trilioni di euro di ulteriori guadagni, se venissero seguite e applicate le politiche proposte ed elaborate dal Parlamento Europeo in 50 aree specifiche, riducendo le duplicazioni degli investimenti in settori e progetti simili e aumentando le sinergie e le collaborazioni tra Paesi ed Enti. Si veda a tal proposito European Parliamentary Research Service, *Increasing European added value in an age of global challenges. Mapping the cost of non-Europe (2022-2032)*, febbraio 2023; si veda anche BLANDINI A., *Space economy, l'Europa decida quale ruolo giocare sullo scacchiere mondiale*, pubblicato su MilanoFinanza il 30 gennaio 2024, disponibile su https://www.milanofinanza.it/news/space-economy-l-europa-decida-quale-ruolo-giocare-sullo-scacchiere-mondiale-202401292027288 4?refresh_cens.

[39] PROGRI D., *An Overview of the Global Space Economy*, Politecnico di Milano, Master of Science Management Engineering, 2022.

profilo, comunicazioni satellitari e scambio dati veloce, lotta al cambiamento climatico e sicurezza e difesa sono solo alcuni esempi; nell'ambito immateriale è rilevante evidenziare, invece, la spinta intellettuale che viene data alle giovani generazioni, ispirate e incuriosite verso lo studio e l'approfondimento delle materie STEM[40], indispensabili per autoalimentare la ricerca e l'innovazione in questo settore con nuove risorse e nuove idee, oltre che la costruzione di un fondamentale sentimento di speranza per il futuro da parte della società, basato sulle possibili svolte che per l'umanità potrà avere l'uso corretto e consapevole dello spazio[41].

Il passaggio dalla *space economy* alla *new space economy* è strettamente legato all'ideazione e creazione di nuovi servizi satellitari e alla loro integrazione con le infrastrutture e tecnologie di terra, indispensabili per la loro realizzazione e utilizzo. Questa integrazione è un elemento critico per il futuro dei mercati legati alla nuova economia spaziale, che consente di dar loro il carattere di universalità in termini di accessibilità e possibilità di utilizzo[42]. Anche in questa nuova fase, come è stato nei primi 60 anni di corsa allo spazio, un ruolo fondamentale è occupato dagli enti spaziali statali, quali la NASA, l'Agenzia Nazionale Cinese per lo Spazio, l'ESA e l'ASI, queste ultime supportate da importanti gruppi privati come Leonardo e Avio, e dagli istituti di ricerca.

La complessità dell'intero comparto mondiale è ben rappresentata dai numeri che la caratterizzano: oggi risulta formato da 130 agenzie governative, 150 centri di ricerca e circa 10 mila aziende del settore[43]; ecco come forme di collaborazione tra tali soggetti possono favorire procedimenti maggiormente efficienti. La *space economy* sta assumendo sempre più una nuova conformazione, con l'emergere di aziende private e *start-up*, caratterizzate da profili strategici aziendali orientati verso le attività extra-atmosferiche, in maniera indipendente dagli enti spaziali delle nazioni a cui appartengono. Per fare un esempio, l'avvento delle macrocostellazioni di satelliti realizzate da imprese private con elevato grado di verticalità industriale rappresenta una svolta cruciale per la connettività globale e per l'evoluzione tecnologica. Queste reti di satelliti, come quelle sviluppate da aziende quali SpaceX (Starlink) e OneWeb, stanno democratizzando l'accesso a Internet, portando connessioni veloci anche nelle aree più remote del pianeta.

La verticalità industriale, ovvero il controllo interno di quasi tutte le fasi della produzione, dallo sviluppo dei satelliti alla gestione dei lanci e delle infrastrutture di rete, consente a queste aziende di ridurre i costi, migliorare l'efficienza e aumentare la rapidità di adattamento tecnologico. Questo approccio accelera il ritmo dell'innovazione e permette di scalare rapidamente l'infrastruttura per soddisfare la crescente domanda globale di servizi di comunicazione avanzati. Le macrocostellazioni private stanno anche aprendo nuovi scenari per l'osservazione terrestre, il monitoraggio ambientale e la difesa, rendendo il settore aerospaziale più dinamico e competitivo rispetto alle tradizionali agenzie

---

[40] STEM è l'abbreviazione di *Science* (scienza), *Technology* (tecnologia), *Engineering* (ingegneria) e *Mathematics* (matematica). Si veda EU STEM Coalition, atti della "Conference on the Future of STEM in Europe", Bruxelles, 29 febbraio 2024.

[41] MAURO R. - WEINZIERL M. - SARANG M., *Focus – È l'ora della space economy*, settembre 2021, disponibile su: https://www.hbritalia.it/settembre-2021/2021/08/31/news/focus-e-lora-della-space-economy-15103/.

[42] SPERANDEO P., "*L'impatto dell'evoluzione del comparto spaziale nel settore economico, politico e della sicurezza nazionale*", in *Osservatorio n.181 – 2020*, pagg. 19-20.

[43] MALTAURO L., *Space Economy, il grande business da un trilione di dollari*, Accademia Politica su Il Sole 24 Ore, 10 gennaio 2023, disponibile su https://www.econopoly.ilsole24ore.com/2023/01/10/space-economy-miliardi/.

governative, e trasformando lo spazio in un ambiente sempre più accessibile e integrato nelle infrastrutture digitali terrestri[44]. Anche l'Italia ha una lunga tradizione nel mondo delle attività spaziali: è stata la terza nazione al mondo ad aver lanciato in orbita un satellite dopo URSS e USA, ed è uno dei membri fondatori dell'ASI, agenzia di cui oggi è stata confermata essere il terzo paese contributore in Europa, dopo Francia e Germania.
L'ASI è una delle 9 agenzie spaziali con un *budget* annuo di oltre 1 miliardo di dollari e oscilla tra il 6° e il 7° posto al mondo per le spese relative ad attività spaziali in relazione al PIL[45]. Da un punto di vista meramente innovativo/tecnologico, i veicoli spaziali miniaturizzati della classe dei micro e nano-satelliti (*CubeSats*, *PocketQubes*, satelliti su *chip* o qualsiasi altro formato miniaturizzato) rappresentano dei veri e propri cambiamenti negli scenari delle missioni spaziali. Hanno contribuito a "democratizzare" l'accesso allo spazio, rendendolo più facile, veloce, economico e, in ultima analisi, aperto a un gruppo molto più ampio di potenziali utenti e operatori.
I rapidi progressi compiuti nella miniaturizzazione delle tecnologie e dei componenti hanno ovviamente giocato un ruolo cruciale in questa evoluzione del settore spaziale. Oggi, l'uso di formati e metodi di progettazione standardizzati, la semplificazione delle infrastrutture satellitari e la disponibilità di un'ampia gamma di componenti e sistemi pronti all'uso rendono possibile la produzione e la gestione di un veicolo spaziale funzionante a basso costo, nonché di passare da tecnologie spaziali mono-uso a nuovi servizi orbitali che ne estenderanno la vita operativa, mantenendo i satelliti efficienti o addirittura integrandoli e aggiornandoli con nuove capacità e tecnologie mentre sono in orbita, così come la possibilità di integrare sistemi di anticollisione a bordo dei mini-satelliti, e di prevedere a fine vita operativa la capacità di rientro auto-guidato nell'atmosfera terrestre, per la distruzione senza dispersione di frammenti in orbita[46].

La cooperazione tra pubblico e privato come modello organizzativo per lo sviluppo di nuove tecnologie

L'innovazione tecnologica e il progresso digitale sono i *driver* principali della cosiddetta "Industria 4.0": come visto, è composta principalmente da *startup hi-tech* in rapida crescita, che per sostenere e garantire la continuità dei loro progetti necessitano di una grande quantità di capitali, il cui profilo di rischio non è supportato dalle tradizionali istituzioni di finanziamento. L'Europa e l'Italia in particolare, dispongono già di tutte le competenze, le conoscenze e le capacità industriali per essere competitive, che permetteranno loro di sviluppare pienamente il potenziale spaziale da cui trarre tutti i vantaggi economici delineati nei paragrafi precedenti[47].
L'interesse per questo mercato emergente comporta investimenti nello spazio e nella *space economy*, guidando (mediante strumenti di politica industriale) e sostenendo

[44] PIANORSI M. - SAPUTO A., *"Il Futuro è in Orbita"*, ISPI Online (10 gennaio 2022), disponibile su: https://www.ispionline.it/it/pubblicazione/il-futuro-e-orbita-32843/.
[45] Il *budget* nazionale dell'ASI è incrementato anche grazie al PNRR, che ha stanziato circa 2,3 miliardi di euro. Fonte: Dipartimento per la trasformazione digitale, si veda MALTAURO L., *Space Economy, il grande business da un trilione di dollari*, Accademia Politica su Il Sole 24 Ore, 10 gennaio 2023.
[46] NATALUCCI S., *Nanosatelliti cavalieri dello spazio in versione small*, in Spazio2050 – Rivista dell'ASI, ottobre 2022.
[47] MAURO R., *La frontiera della space economy*, in Pandora Rivista, 21 maggio 2021.

tutti gli attori già presenti sul mercato (istituzionali e privati). Parallelamente, deve essere incentivato l'ingresso di nuovi attori rilevanti per il mercato stesso.
Tali considerazioni si inseriscono in un più ampio bilanciamento di interessi tra i necessari investimenti ed i vincoli connessi al ruolo dei soggetti pubblici (si vedano i vincoli al bilancio pubblico derivanti dalla *governance* economica europea alla necessità di garantire il rispetto dei principi dei Trattati UE nei rapporti con il mercato[48]), il tutto sotto un'attenta organizzazione degli investimenti che valuti costi e progetti su cui investire, per facilitare le collaborazioni tra soggetti e favorire così una maggiore efficienza ed efficacia. A tal proposito, occorre ribadire che in Europa il sostegno istituzionale e la spesa pubblica assorbono il volume principale delle capitalizzazioni nel settore dello spazio, ma sono presenti anche investimenti privati che hanno aperto la strada a maggiori flessibilità nell'accesso all'erogazione di fondi: da un lato occorre stimolare la domanda pubblica in maniera sufficiente, dall'altro serve garantire un agile intervento degli investitori privati in grado di ricompensare i rischi iniziali solitamente elevati e le correlate iniziative di innovazione[49].
L'ESA si sta impegnando a garantire l'accesso alle proprie strutture di ricerca, laboratori, infrastrutture e centri operativi di elaborazione dati, agli attori commerciali della nuova *space economy*, così come alle industrie private ormai consolidate, per incentivare la competitività industriale europea[50]. Queste nuove forme di cooperazione e coordinamento, previste e realizzate nell'ambito della rete di *Business Incubation Centre*[51] e dell'iniziativa Cassini[52] a favore dell'imprenditorialità nel settore spaziale, voluta e lanciata dall'UE, in collaborazione con la Banca Europea per gli Investimenti e il Fondo Europeo degli Investimenti, rappresentano soluzioni organizzative di grande importanza che verranno realizzate e attuate tramite operazioni di partenariato con attori industriali

---

48 Il rispetto dei principi UE deve altresì tenere conto anche delle possibili deroghe in materia di "ordine pubblico" e "sicurezza" ed i relativi interessi nazionali. Si veda Parlamento Europeo, "STEP: competitività e della resilienza dell'UE nei settori strategici": la "Piattaforma delle tecnologie strategiche per l'Europa" (STEP) mira a promuovere le tecnologie digitali, quelle a zero emissioni e biotecnologiche, e a rinforzare l'innovazione. Vuole inoltre integrare in maniera più efficace diversi programmi e fondi dell'UE, al fine di convogliare fino a 160 miliardi di euro in nuovi investimenti, insieme agli incentivi della politica di coesione e al dispositivo per la ripresa e la resilienza. La nuova piattaforma dovrebbe sostenere la produzione di tecnologiche cruciali, come ad esempio le biotecnologie e quelle a zero emissioni nette. STEP mira anche ad affrontare la carenza di manodopera e di competenze e a sostenere l'innovazione, per consentire all'industria dell'UE di realizzare la duplice transizione digitale e verde.

49 CONZUTTI A., *La New Space Economy: profili costituzionali dell'integrazione europea in materia spaziale*, DPCE 2021, pagg. 3-4.

50 ESA, *Agenda 2025. Più Spazio per l'Europa*, consultabile su: https://www.asi.it/wpcontent/uploads/2021/05/ESA-Agenda-2025-final_IT.pdf.

51 Per "*business incubator*" si intende uno strumento di sviluppo economico con l'obiettivo di accelerare la crescita e il successo delle nuove imprese, fornendo un supporto sia in termini di risorse che di servizi. L'attività di incubazione garantisce un ambiente in grado di istruire e supportare gli imprenditori durante la fase iniziale di una nuova impresa. Vedere, a tale riguardo, la definizione proposta dalla *National Business Incubation Association*, reperibile all'indirizzo istituzionale dell'associazione: https://www.nbia.org/.

52 Il programma *Cassini* rappresenta la nuova iniziativa della Commissione europea per sostenere imprese innovative, *start-up* e PMI nel settore del *New Space*, nel periodo 2021-2027. Si veda, a questo proposito, Commissione europea, *Cassini Space Entrepreneurship Initiative*, disponibile all'indirizzo https://ec.europa.eu/defence-industryspace/eu-space-policy/space-research-and-innovation/cassini_fr.

sia di grandi che di piccole dimensioni[53]. Dal punto di vista giuridico, la definizione di collaborazioni pubblico-privato comporta adempimenti connessi all'evidenza pubblica che possono incidere negativamente sulle tempistiche dell'attività di ricerca e sviluppo. Il Partenariato Pubblico-Privato (PPP)[54] viene indicato dal Piano Nazionale di Ripresa e Resilienza (PNRR) come strumento giuridico per creare un contesto maggiormente efficiente ed efficace (in termini di risorse finanziarie e di *know how*), per assicurare il raggiungimento degli obiettivi del Piano. Ogni progetto finanziato dal PNRR potrebbe, grazie all'apporto di ulteriori investimenti derivanti dall'iniziativa privata, avere un effetto moltiplicatore per la ripresa[55].

Anche se le complessità connesse alla realizzazione e gestione di forme di PPP costituiscono un ostacolo al loro utilizzo[56], queste forme di collaborazione possono rappresentare nei prossimi anni uno strumento essenziale per l'attuazione del PNRR, per mezzo delle procedure ad iniziativa privata, nei casi in cui la realizzazione degli interventi previsti dal Piano in *partnership* con soggetti privati può rappresentare l'occasione di attrazione di risorse e di competenze, che vadano a migliorare ed efficientare l'azione dell'ente pubblico interessato[57]. Nell'ambito del partenariato pubblico-privato, l'istituto giuridico del *project financing*[58], strumento di derivazione anglosassone, è una forma particolare di PPP ad iniziativa privata finalizzata alla cooperazione tra i poteri pubblici e i privati allo scopo di finanziare, costruire e gestire infrastrutture o fornire servizi di interesse pubblico, che la

---

53 L'Agenzia spaziale adotta, così, un approccio globale di innovazione, associandosi al mondo accademico, ai centri di ricerca, ai centri spaziali nazionali, all'industria e agli investitori privati, compresi i fondi di capitale di rischio, al fine di stimolare un /forte ammodernamento dei settori emergenti delle attività spaziali commerciali.

54 Il PPP è previsto nella Parte IV del Codice dei contratti pubblici di cui al d.lgs. n. 50 del 2016.

55 Piano Nazionale di Ripresa e Resilienza, pagg. 248-249: "in via prudenziale, non si tiene conto esplicitamente della possibilità che i fondi del PNRR vengano utilizzati per sostenere oppure attrarre investimenti privati attraverso il mercato, ad esempio tramite forme di partenariato pubblico-privato, contributi a progetti di investimento, prestiti o garanzie. In tal caso l'impatto sarebbe stato ben maggiore per l'operare di un effetto leva".

56 Si v. come nella disciplina del d.lgs. n. 36 del 2023, l'art. 62, c. XVIII, in cui si prevede che "la progettazione, l'affidamento e l'esecuzione di contratti di partenariato pubblico-privato possono essere svolti da soggetti qualificati per i livelli di cui all'articolo 63, comma 2, lettere b) e c)".

57 L'Organizzazione per la cooperazione e lo sviluppo economici (OCSE) definisce i PPP come accordi contrattuali a lungo termine tra il governo e un partner privato, in base ai quali quest'ultimo presta e finanzia servizi pubblici utilizzando un capitale fisso e condividendo i rischi associati. Quest'ampia definizione mostra che i PPP possono essere progettati per realizzare una vasta gamma di obiettivi in vari settori, come i trasporti, l'edilizia sociale e l'assistenza sanitaria, e possono essere strutturati secondo approcci differenti. Le tre principali categorie di PPP sono le seguenti: a) concessioni, in base alle quali normalmente gli utilizzatori finali del servizio pagano direttamente il partner privato, che non riceve una remunerazione dal settore pubblico, o ne riceve una ridotta; b) joint venture, o PPP istituzionali, in base alle quali il settore pubblico e quello privato diventano entrambi azionisti di una terza società; c) PPP contrattuali, quando il rapporto tra le parti è regolato da un contratto. Si veda su questo tema OCSE, *Principles of Public Governance of Public-Private Partnerships (Princìpi di governance pubblica dei partenariati pubblico-privato)*, 2012. In relazione ai PPP nell'ordinamento giuridico UE si v. Commissione UE, *Comunicazione interpretativa della commissione sull'applicazione del diritto comunitario degli appalti pubblici e delle concessioni ai partenariati pubblico-privati istituzionalizzati (PPPI)*, 5 febbraio 2008. Circa il rapporto tra PPP contrattuale e istituzionalizzato nell'ordinamento italiano si v. il d.lgs. n. 175 del 2016, *Testo unico sulle società partecipate* (per il PPP istituzionalizzato) e il d.lgs. n. 36 del 2023, *Codice dei contratti pubblici* (per il PPP contrattuale).

58 Nell'ordinamento giuridico italiano, si v. d.lgs. n. 36 del 2023, artt. 193-195.

Pubblica Amministrazione possa così usufruire del finanziamento e dell'*expertise* dei soggetti privati[59].
La promozione e il corretto utilizzo del *project financing*, come specifica operazione di finanziamento di progetti diretti alla realizzazione o alla fornitura di servizi nell'interesse pubblico della collettività, rappresentano un tema centrale per la crescita economica e la realizzazione delle infrastrutture in Italia[60]. Risulta evidente l'applicabilità e l'utilità di questo istituto giuridico alle tematiche dello spazio, della *Space Economy* e della digitalizzazione, specialmente in un periodo caratterizzato da scarsa disponibilità di risorse finanziarie pubbliche, diventando quindi uno strumento fondamentale per il finanziamento di progetti di fornitura di servizi per la collettività come quelli spaziali[61].
Data la complessità (tecnica, giuridica ed economica) nell'applicazione di questa tipologia contrattuale, è evidente che l'applicazione dello schema di PPP ai progetti di sviluppo delle tecnologie e servizi satellitari e spaziali dovrà configurarsi progressivamente attraverso l'esperienza e il confronto con le prassi e consuetudini del nuovo mercato emergente, creando e migliorando il modello contrattuale sulla base del principio del *learning by doing*[62], in un contesto giurisprudenziale in cui è richiesta l'applicazione di un istituto che nasce negli ordinamenti di *common law* e che dovrà trovare la sua adeguata applicazione in un ordinamento di *civil law* come quello italiano[63]. La *Space Factory* rappresenta un *asset* strategico per il nostro Paese in questo ambito, rafforzando e potenziando le competenze della filiera industriale nazionale del settore già in forte crescita, come anticipato in precedenza. Potrà quindi essere strumento a supporto di investimenti privati futuri per la realizzazione di costellazioni e mega-costellazioni satellitari[64]. Alla luce di queste considerazioni, è facile quindi prevedere che lo spazio sarà sempre più privato o, più precisamente, sarà sempre più fonte di collaborazione tra enti pubblici, centri di ricerca e società private[65].

La città dell'Aerospazio di Torino come esempio di attività di R&S collaborativa nel settore aerospaziale

L'industria aerospaziale genera da sempre un rilevante contributo economico e strategico nei settori civili e commerciali, della Sicurezza e della Difesa oltreché, come visto nei paragrafi precedenti, dell'emergente *Space Economy*. Nel 2022 ha

---

59 Sul tema del *project financing* si veda anche DRAETTA U. (a cura di), *Il project financing. Caratteristiche e modelli contrattuali*, Milano, Giuffrè, 1997; TULLIO A., *La finanza di progetto: profili civilistici*, Milano, Giuffrè, 2003.

60 SICLARI D., Il ruolo del partenariato pubblico-privato alla luce del PNRR, in Dialoghi di Diritto dell'Economia, aprile 2022.

61 Un utilizzo del PPP più consapevole e maturo da parte delle Amministrazioni e degli operatori del mercato può certamente consentire di cogliere rapidamente nell'interesse del Paese le opportunità presenti nel PNRR sui diversi interventi finanziati (ad es., in materia di digitalizzazione tenendo comunque conto della durata dei progetti del PNRR limitata al 2026.

62 CAMPAGNANO E., *Le nuove forme del partenariato pubblico-privato*, Padova, Cedam, 2020, p. 88.

63 SICLARI D., Il ruolo del partenariato pubblico-privato alla luce del PNRR, in Dialoghi di Diritto dell'Economia, aprile 2022, pagg. 1-4.

64 ASI, Comunicato stampa "Grazie ai fondi del PNRR l'Agenzia Spaziale Italiana affida a diversi contraenti la realizzazione della *Space Factory*", 30 marzo 2023, disponibile su: https://www.asi.it/2023/03/grazie-ai-fondi-del-pnrr-lagenzia-spaziale-italiana-affida-a-diversi-contraenti-la-realizzazione-della-space-factory/.

65 DESIDERIO N., *Copasir: il futuro dello spazio è nella collaborazione pubblico-privato*, luglio 2022, disponibile su https://www.spaceconomy360.it/difesa-cybersecurity/copasir-il-futuro-dello-spazio-e-nella-collaborazione-pubblico-privato/.

generato globalmente un giro d'affari di circa 741 miliardi di dollari, con un profitto di 67 miliardi di dollari e un margine del 9.1%[66], costituendo di fatto un motore fondamentale di occupazione altamente qualificata, sia diretta che indotta. A livello europeo, l'industria dell'aerospazio e difesa ha generato nel 2021 un *turnover* di 238 miliardi di euro, con circa 900.000 addetti[67]. Tuttavia, la particolare natura delle attività di questo settore richiede un continuo e intenso sforzo innovativo per garantire una competitività che comporta investimenti rilevanti, spesso associati ad alti rischi e lunghi periodi di *break-even*.

Mai come in questo decennio il settore dell'aerospazio sta affrontando una serie di sfide tecnologiche e geopolitiche che se da un lato rendono impegnativo mantenere la competitività nel settore, dall'altro incentivano la creazione di nuovi mercati e modelli di business e rappresentano una grande occasione di crescita per il Paese. Ed è proprio quest'ultimo *trend* che ha generato nuove dinamiche di settore e sta mostrando l'emergere di nuove aziende (*start-up* e piccole-medie imprese) che supportano sviluppi di frontiera. In ragione di queste nuove dinamiche e per garantire un percorso di crescita strutturato e sostenibile, la Regione Piemonte ha attivato il Distretto Aerospaziale Piemontese (DAP) e alcuni dei principali referenti industriali del settore aerospaziale (Leonardo, Avio Aero, Thales Alenia Space Italia, Altec) per definire una prima visione condivisa, illustrata in un Piano Strategico Integrato, caratterizzata da una focalizzazione sulla Città dell'Aerospazio, progetto che ha l'obiettivo di costituire un ecosistema in grado di garantire innovazione e sostenibilità, al fine di offrire al Paese la possibilità di implementare il proprio ruolo a livello internazionale nel settore aerospaziale, favorendo al contempo lo sviluppo di una filiera di piccole e medie imprese altamente competitiva e la formazione delle future generazioni di professionisti con competenze di eccellenza.

Uno dei suoi obiettivi strategici risiede proprio nella promozione delle attività spaziali, affinché lo spazio sia sempre più parte integrante dello scenario economico globale, contribuendo sempre più allo sviluppo socio-economico e di posizionamento strategico sulla scena internazionale della *space economy*, attraverso esplorazione planetaria robotica e umana, trasporto e sistemi abitativi spaziali, osservazione della Terra e dell'universo, navigazione satellitare, sistemi e servizi per *in-orbit servicing*, servizi di controllo operativo delle missioni e *processing* di dati scientifici e tecnologici, sia per le intrinseche capacità di produrre innovazione che ai fini della crescita e della competitività. Non solo, ma anche la realizzazione di un ecosistema di *open innovation* aerospaziale (Difesa, Sicurezza, Spazio) che, in collaborazione con università, centri di competenza, centri di ricerca e di sviluppo di *start-up*, rappresenti un *hub* di eccellenza nazionale e un riconoscibile e virtuoso modello internazionale[68], capace di incentivare l'applicazione delle nuove tecnologie digitali (a cominciare dall'intelligenza artificiale), favorendo la transizione digitale oltre che la competitività del sistema locale su competenze distintive.

La Città dell'Aerospazio, pertanto, può offrire significative ricadute sulla competitività del sistema formativo e di ricerca piemontese: l'interazione fra

[66] PricewaterhouseCoopers (PwC), *Global Aerospace & Defence – Annual Industry Perfomance and Outlook*, 2023.

[67] ASD, "*2022 FACT & Figures*".

[68] PASS – Piemonte Aeronautic & Space Strategy, "*Progetto Città dell'Aerospazio & Route Map 2023-2028*", revisione 1 di luglio 2023, con la collaborazione di Leonardo, Altec, Thales Alenia Space, Avio Aero, Distretto Aerospaziale Piemontese e Regione Piemonte.

l'attività di ricerca di base e quella applicata, supportate da una efficace sperimentazione condotta all'interno di laboratori congiunti industria-ateneo, permetterà di promuovere la formazione di risorse qualificate, di sostenere l'attività di formazione professionale e di alta formazione tecnico-scientifica con importanti opportunità occupazionali, tramite contratti di partenariato pubblico-privato tra le aziende e enti accademici (Politecnico di Torino e Università degli Studi di Torino), con l'obiettivo di finanziare la ricerca e lo sviluppo sperimentale congiunto su tematiche di frontiera, orientate allo sviluppo di nuovi prodotti aeronautici e spaziali[69]. Il progetto è ambizioso non solo per i potenziali e importanti vantaggi citati che porterà in futuro, ma anche per l'esperienza nella gestione dei contratti di partenariato, strumenti innovativi di realizzazione di progetti di pubblico interesse, che uniscono risorse, competenze e responsabilità del settore pubblico insieme a quelle del settore privato. In conformità con il codice dei contratti pubblici[70], tali accordi assumono una rilevanza strategica nell'ambito della pianificazione e dell'implementazione di infrastrutture e servizi di pubblica utilità, e presentano una serie di vantaggi che vanno oltre la mera allocazione di risorse finanziarie. In primo luogo, questi contratti permettono all'amministrazione pubblica di accedere a competenze specializzate e risorse finanziarie del settore privato, mitigando eventuali carenze di finanziamento pubblico e promuovendo l'implementazione di progetti di maggiore complessità tecnica ed economica. In secondo luogo, i PPP possono garantire una maggiore efficienza e tempestività nell'esecuzione dei progetti, grazie alla partecipazione del settore privato, notoriamente orientato verso una gestione più snella e dinamica delle risorse. Infine, l'innovazione tecnologica e gestionale apportata dai *partner* privati può portare a soluzioni più avanzate e sostenibili, consentendo all'ente pubblico di soddisfare in maniera più efficace le esigenze della collettività.

---

[69] Il Ministero dell'Università e della Ricerca (MUR), in attuazione dell'Investimento 3.1 "Fondo per la realizzazione di un sistema integrato di infrastrutture di ricerca e innovazione", previsto nell'ambito della Missione 4 ("Istruzione e ricerca") – Componente 2 ("Dalla ricerca all'impresa") del PNRR, ha stabilito di concedere finanziamenti, sotto forma di contributi alla spesa, destinati alla realizzazione o ammodernamento di Infrastrutture Tecnologiche di Innovazione che favoriscano una più stretta integrazione tra imprese e mondo della ricerca, per dispiegare il potenziale di crescita economica del Paese e conferire caratteristiche di resilienza e di sostenibilità – economica e ambientale – ai processi di sviluppo (Avviso n. 3265 del 28 dicembre 2021, di seguito "Avviso"; il Politecnico di Torino ha presentato la una proposta progettuale recante dal titolo "*Knowledge Transfer Innovation Infrastructure for New Aerospace Challenges (IS4Aerospace)*" con un valore complessivo di investimento pari a euro 32.400.000,00; Con Decreto di concessione 153 del 22 giugno 2022, il MUR ha ammesso a finanziamento il progetto presentato dal Politecnico di Torino per un importo complessivo di euro 15.876.000,00 nella forma del contributo alla spesa, a valere sulle risorse previste dal PNRR nell'ambito della Missione 4 "Istruzione e Ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 3.1 "Fondo per la realizzazione di un sistema integrato di infrastrutture di ricerca e innovazione", finanziato dall'Unione Europea *NextGenerationEU*; l'attuazione del progetto avviene attraverso un partenariato pubblico-privato contrattuale ex art. 174, comma 3, del d. lgs. n. 36/2023, avente a oggetto la realizzazione e gestione della relativa infrastruttura tecnologica. Il Politecnico di Torino ha acquisito la disponibilità, mediante diritto di superficie, di un'area idonea alla realizzazione dell'Infrastruttura tecnologica denominata Città dell'Aerospazio e collocata negli ex terreni dell'insediamento Leonardo a Torino, c.so Francia/Marche, da mettere a disposizione degli affidatari della procedura di partenariato pubblico-privato citata; il Politecnico, con Decreto Rettorale n. 1073/2023 del 17.10.2023, ratificato dal C.d.A. nella seduta del 26.10.2023, ha indetto un'unica procedura a evidenza pubblica suddivisa per lotti funzionali (n. 3 lotti), finalizzata all'individuazione degli operatori economici cui affidare, tramite partenariato pubblico-privato contrattuale ex art. 174, comma 3, del d. lgs. n. 36/2023, la realizzazione, lo sviluppo e la gestione, in tutto o in parte, del progetto.

[70] d.lgs. 36 del 2023.

Nonostante i vantaggi evidenziati, l'adozione di PPP non è priva di criticità e rischi: in primo luogo, la complessità intrinseca alla negoziazione e gestione di tali contratti richiede una semplificazione delle procedure amministrative che, soprattutto in relazione a progetti di R&S, comportano la necessità di tempistiche brevi per consentire di sfruttare in maniera efficiente i possibili benefici conseguenti. Pare inoltre necessaria una notevole esperienza e capacità da parte dell'amministrazione pubblica, in termini di competenze legali, finanziarie e di *project management*. La mancanza di capacità o di risorse sufficienti potrebbe compromettere la corretta implementazione e il successo dei progetti. In secondo luogo, l'attribuzione di parte del rischio finanziario al *partner* privato può comportare una dipendenza eccessiva da quest'ultimo, con il rischio di compromettere la flessibilità e l'autonomia decisionale dell'ente pubblico stesso. Inoltre, la ricerca di profitto da parte dei privati potrebbe generare conflitti di interesse o comportamenti opportunistici, specialmente nella gestione dei risultati delle attività di R&D, dei possibili brevetti e del loro utilizzo.
La gestione della proprietà intellettuale e delle informazioni assume rilevanza anche in relazione a componenti che possono comportare ulteriori vincoli di segretezza. Infine, esistono rischi di natura finanziaria legati alla possibile sovrastima dei benefici attesi dai progetti PPP, con conseguente aumento dei costi a lungo termine e potenziali impatti negativi sulle finanze pubbliche. In aggiunta a quanto evidenziato, occorre considerare che la complessità normativa e procedurale è messa in luce dalla molteplicità di leggi, decreti e regolamenti esistenti che disciplinano i PPP in settori specifici quali trasporti, sanità, energia e infrastrutture.
Il d. lgs. 36 del 2023 ha introdotto una serie di disposizioni volte a regolare l'utilizzo dei PPP nel contesto della pubblica amministrazione, stabilendo principi generali, criteri di selezione dei partner privati, modalità di finanziamento e di monitoraggio dei progetti; tuttavia, l'applicazione di queste disposizioni richiede una corretta interpretazione e integrazione con altre normative settoriali e con i principi generali del diritto amministrativo e civile, rendendo il quadro normativo complesso e suscettibile di interpretazioni divergenti[71].
La Città dell'Aerospazio di Torino si trova, quindi, di fronte a una serie di sfide complesse, che derivano sia dal rapido progresso tecnologico nel settore aerospaziale, sia dalle difficoltà normative e procedurali che caratterizzano l'attuale ambiente industriale e della ricerca scientifica. Come detto, se da un lato l'accelerazione dell'innovazione tecnologica richiede una costante adattabilità e un investimento significativo in ricerca e sviluppo per rimanere competitivi a livello globale, dall'altro lato le normative e le procedure spesso rigide e complesse possono rappresentare un ostacolo alla flessibilità e alla velocità necessarie per rispondere prontamente alle esigenze del mercato. In questo contesto, la Città dell'Aerospazio di Torino dovrà bilanciare la necessità di stimolare l'innovazione con la capacità di muoversi efficacemente attraverso un contesto normativo non ancora perfettamente definito ed efficace, promuovendo al contempo un ambiente imprenditoriale dinamico e sostenibile[72].

[71] Presidenza del Consiglio dei Ministri, Dipartimento per la programmazione e il coordinamento della politica economica, "Esternalità e ricadute territoriali, costi e benefici, finanza di progetto – Possibili schemi di Partenariato Pubblico Privato", audizione dell'Unità Tecnica Finanza di Progetto (UTFP) presso il CIPE del 30 ottobre 2007, riportata in "Osservatorio Collegamento Ferroviario Torino-Lione", Quaderno 05.

[72] Si veda in merito l'intervista alla Prof.ssa Fulvia Quagliotti, 13 marzo 2024.

Affrontando queste sfide con determinazione e creatività, Torino può emergere come un polo leader nell'industria aerospaziale, capitalizzando le sue competenze storiche e abbracciando l'innovazione con audacia e spirito imprenditoriale[73].

Conclusioni

La *space economy* emerge come un catalizzatore cruciale e un modello abilitante per la collaborazione tra mondo pubblico e privato, delineando una prospettiva innovativa e dinamica per l'economia globale. Si intravede il profondo intreccio esistente tra lo sviluppo dello spazio e l'evoluzione digitale, cogliendo le implicazioni che tale connessione porta con sé. In sintesi, l'economia dello spazio rappresenta un modello e un *driver* fondamentale per nuovi prodotti e servizi multi-dominio, sviluppati sfruttando le importanti possibilità di ottimizzazione dei costi e sinergia attraverso i contratti PPP, aprendo la strada a una nuova era di possibilità e progresso economico. Tuttavia, per cogliere appieno le opportunità offerte da questa convergenza tra spazio e nuovi mercati, è necessario affrontare le sfide emergenti con determinazione e promuovere una cooperazione ancora più stretta tra tutti gli attori coinvolti pubblici e privati, sia a livello nazionale che internazionale, europeo *in primis*, ma non solo limitato all'Europa. Solo attraverso un impegno collettivo e una visione condivisa si potrà realizzare il pieno potenziale della *space economy*, traghettando la nostra società attuale verso un futuro spaziale sempre più promettente e inclusivo, sempre più strumento di opportunità di crescita e sviluppo globale, e non solo più visto esclusivamente come mezzo per attuare nuove difese e nuove deterrenze tecnologiche militari.

Bibliografia

ANDEM M.N., The 1967 Outer Space Treaty (1967 OST) as the Magna Carta of Contemporary Space Law: A Brief Reflection, in Proceedings of the Forty-Seventh Colloquium on the Law of Outer Space, Vol. 47 (2004).

CAMPAGNANO E., Le nuove forme del partenariato pubblico-privato, Cedam, 2020.

Commissione Europea, The future of the European space sector. How to leverage Europe's technological leadership and boost investments for space ventures, 2019.

CONZUTTI A., La New Space Economy: profili costituzionali dell'integrazione europea in materia spaziale, DPCE 2021.

DRAETTA U. (a cura di), Il project financing. Caratteristiche e modelli contrattuali, Milano, Giuffrè, 1997.

GALA M., Il paradosso nucleare: Il Limited Test Ban Treaty come primo passo verso la distensione, Polistampa, Firenze, 2002.

KULU E., In-space Economy in 2021 – Statistical Overview and Classification of Commercial Entities, in 72nd International Astronautical Congress (IAC 2021).

LANIUS R.D. - LOGSDON J.M. - SMITH R.W., Reconsidering Sputnik: Forty Years Since the Soviet Satellite, Routledge, London-New York, 2014

[73] Regione Piemonte, Piemonteinforma, "Nasce la Città dell'Aerospazio", comunicato stampa del 28.11.2023.

LEVINE A.J., After Sputnik. America, the World, and Cold War Conflicts, Routledge, London-New York, 2017.

MAURO R., Weinzierl M., Sarang M., Focus – È l'ora della space economy, sett. 2021.

NATALUCCI S., Nanosatelliti cavalieri dello spazio in versione small, in Spazio2050 – Rivista dell'ASI, ott. 2022.

OECD Report on Space Economy.

PROGRI D., An Overview of the Global Space Economy, Politecnico di Milano, Master of Science Management Engineering, 2022.

RUSCHI F., Ascesa e Declino del Corpus Iuris spatialis. Un Itinerario di Filosofia del Diritto Internazionale, in Dirittifondamentali.it, 15 gennaio 2020.

SICLARI D., Il ruolo del partenariato pubblico-privato alla luce del PNRR, in Dialoghi di Diritto dell'Economia, aprile 2022.

SIDDIGI A., Sputnik and the Soviet Space Challenge, University Press of Florida, Gainesville (FL), 2003

SPERANDEO P., "L'impatto dell'evoluzione del comparto spaziale nel settore economico, politico e della sicurezza nazionale", in Osservatorio n.181 – 2020.

Su J., The "Peaceful Purposes" Principle in Outer Space and the Russia–China (PPWT) Proposal, in Space policy, 26 (2010), 2.

TRONCHETTI F. - HAO L., The 2014 Updated Draft PPWT. Hitting the Spot or Missing the Mark?, in Space Policy, 33 (2015)

TULLIO A., La finanza di progetto: profili civilistici, Milano, Giuffrè, 2003.

United Nations, United Nations treaties and principles on outer space. Text of treaties and principles governing the activities of States in the exploration and use of outer space, adopted by the United Nations General Assembly, New York, 2002.

Massimo Franchi

Senior Research Fellow all'Università di Modena e Reggio Emilia al Dipartimento di Giurisprudenza e lecturer all'Universidad Nacional de La Plata - Unesco Catedra. All'Università di Parma è membro del Laboratorio di Diritto del Mercato e delle Nuove Tecnologie (DiMeTech). È docente presso ITS Academy Tech&Food. Direttore della "Winter School di Geopolitica" FMS. Ha frequentato il 38° corso COCIM presso il CASD e scrive su Rivista Marittima.

LA GEOPOLITICA DELLE MULTINAZIONALI

ABSTRACT

Le imprese multinazionali, che capitalizzano trilioni di dollari nelle principali borse valori mondiali, rappresentano l'attore principale della globalizzazione. I fatturati sviluppati, il reddito prodotto e la disponibilità di cassa di queste organizzazioni sono superiori a quelli di alcuni Stati con una capacità di influenza, tramite gli investimenti diretti esteri, che si estende oltre i confini nazionali.

Multinational companies, which capitalize trillions of dollars on the main world stock exchanges, represent the main players in globalization. The turnover developed, the income produced, and the cash availability of these organizations are superior to some states with a capacity for influence through foreign direct investments that extend beyond national borders.

Introduzione

Nell'attuale scenario competitivo, le multinazionali esercitano un ruolo strategico ed in grado di influenzare non solo i Paesi di origine, ma anche le aree del globo nelle quali decidono di fare investimenti. Se la caduta del muro di Berlino e dell'equilibrio bipolare che esso esprimeva, avvenuta nel 1989, aveva inizialmente generato una evoluzione verso un nuovo ordine globale, incentrato sugli Stati Uniti d'America ed i loro alleati occidentali, gli scenari mutevoli di un mondo sempre più globalizzato hanno provocato cambiamenti di rotta con l'ascesa di nuovi giocatori globali. Un ordine globale le cui caratteristiche dovrebbero essere sia un corpo di regole accettate da tutti gli Stati che un potere in grado di controllare quando esse vengono meno generando un equilibrio tra legittimità e potere (Kissinger, 2015).

In tale contesto, gli Stati Nazione hanno continuato a perseguire i loro interessi "particolari" ed "originari", pur facendo parte di alleanze ed organizzazioni internazionali. Quello che si è generato è un ambiente iper-competitivo nel quale entità multinazionali hanno continuato ad investire nelle aree del globo ritenute più interessanti e convenienti dal punto di vista fiscale, accrescendo la loro capacità di influenzare i decisori politici e di dettare le agende di governo.

Oltre al mercato in senso lato, si parla oggi di reti di imprese, di comunità, di interdipendenza pubblico privato, di complementarità delle associazioni private con gli enti pubblici, di competizione dei territori, come ben hanno messo in luce i francesi, nella loro visione dell'*intelligence* economica fin dagli anni Novanta del secolo scorso, dal rapporto Martre[1] in avanti. L'impresa è solo una delle istituzioni

[1] Il Rapporto Martre è stato pubblicato nel 1994 su La Documentation Française.

delle moderne società che opera accanto alle cosiddette istituzioni di servizio pubblico (Drucker 2000, 146) la cui estensione in alcuni Paesi è divenuta enorme impiegando milioni di dipendenti. Questa società pluri-istituzionale è però in continua trasformazione secondo una logica aperta ed in espansione riassunta dalla definizione "Business, Government and Many Others".
Si tratta di un "disordine globale" nel quale sono divenute dominanti le minacce ibride che, secondo Hoffman, hanno fuso insieme i due tipi ideali di guerra, regolare ed irregolare (Ilmari, 2021). Certamente, le principali economie globali sono quelle che in maggior misura difendono le loro imprese dando vita a delle vere e proprie "economie di combattimento", indipendentemente dai colori politici dei governi, nelle quali si fondono diversi tipi di interessi, rappresentati dallo stato profondo e dalle organizzazioni private. Per le imprese, l'ottenimento di quote di mercato, il mantenimento dei fatturati e dei margini nascondono comportamenti, offensivi e difensivi, messi in atto per acquisire, analizzare, migliorare, disseminare e scambiare informazioni, trasformandole in attività misurabili economicamente. Tutto questo è accaduto sia in Occidente che Oriente dove l'economia pianificata cinese, con il capitalismo di Stato, ha introiettato le logiche del mercato aprendo vie di comunicazione e trasporto a supporto del loro sistema imprenditoriale, come la "Nuova via della seta"[2]. Un mondo nel quale contano molto anche le percezioni dei consumatori/cittadini che con le loro decisioni di acquisto, spesso guidate dal *marketing* e manipolate dagli strumenti digitali, possono determinare il successo di un prodotto e la conseguente fortuna di un territorio (Franchi, 2020).
Uno scenario nel quale si è modificato il concetto stesso di guerra che deve considerare anche le scalate ostili a società strategiche, l'impiego della disinformazione, l'acquisizione di contratti statali da parte di imprese straniere, ecc. Tutto questo richiama alla guerra economica che rientra sotto l'ombrello delle guerre ibride[3] per le quali tutto è consentito pur di difendere il sistema di benessere che permette lo svolgimento regolare della vita civile in uno Stato-Nazione ed il mantenimento del potere e dell'influenza dello stesso nel mondo. Un concetto ben evidenziato da due Colonnelli cinesi, Qiao Liang and Wang Xiangsui[4], per i quali oltre al confronto diretto e tecnologico esistono anche mezzi alternativi di scontro. Per i due studiosi, la prima regola di una guerra senza restrizioni è che non ci sono regole, nulla è proibito. Nella loro prospettiva la vittoria non va ricercata sul campo di battaglia fisico, una visione tipica nell'approccio occidentale della guerra, ma "*la lotta per la vittoria si svolgerà sul campo di battaglia al di là del campo di battaglia*".
L'obiettivo di questa ricerca è analizzare il mondo delle multinazionali, i loro sistemi di governance, i perimetri giuridici nei quali operano e la scala dei loro ambiti di azione per consentire al lettore di comprendere al meglio la loro capacità di influenzare le agende degli apparati governativi e di trasformare la società.

Le rivoluzioni industriali

La globalizzazione economica, conseguenza naturale delle rivoluzioni industriali, è stata spinta da tre forze principali: il progresso tecnologico, la volontà politica dei diversi Paesi ed il processo di accumulazione capitalistico (Targetti e Fracasso, 2008). Essa ha visto periodi di grandi espansioni intervallati da altri di rallentamento

[2] La Belt and Road Initiative (BRI) è un'iniziativa strategica annunciata per la prima volta dal governo cinese nel 2013.
[3] United States (U.S.) Army Doctrine Publication (ADP) 3-0.
[4] Entrambi Ufficiali dell'Esercito cinese, hanno scritto nel 1999 il libro "Unrestricted Warfare".

e crisi che sono stati misurati dagli studiosi impiegano tre macro-indicatori: i flussi migratori, le esportazioni di merci e gli investimenti diretti esteri (IDE).
La prima Rivoluzione industriale, iniziata dalla fine del 1700 in Inghilterra, prese avvio in un mondo tecnicamente limitato con una tecnologia che non consentiva di sfruttare appieno le economie di scala. Si trattava di un mercato non ancora in grado di raggiungere le piazze lontane, ma che nella sua progressiva crescita, tra espansione dei commerci e guerre mondiali, stava cambiando la società. Da quel momento sarà la fabbrica, con l'avvento delle macchine che consentono di aumentare la produttività, principalmente nel settore tessile, il luogo simbolo del capitalismo (Zamagni, 2000). Con essa, alla produzione si associa il controllo della forza lavoro e la specializzazione delle maestranze. Nel 1776, il filosofo ed economista scozzese Adam Smith pubblicò la celebre opera *"Indagine sulla natura e le cause della ricchezza delle nazioni"* che divenne la base del pensiero capitalista classico influenzando il pensiero economico per i secoli a seguire. In essa vennero trattati, per la prima volta in un corpo unico, i temi del progresso, della capacità produttiva del lavoro, della natura, dell'accumulazione ed impiego di fondi, dei sistemi di economia politica e del ruolo dello Stato nello sviluppo economico.
La seconda rivoluzione industriale, dalla fine dell'Ottocento in poi, si sviluppa negli Stati Uniti ed in Germania, grazie all'alta densità di capitale e di energia necessarie per consentire un processo produttivo continuo (Zamagni, 2000). Essa ha visto porre l'attenzione sulle economie di scala e di diversificazione ed ha riguardato molteplici settori come i trasporti, in particolare le ferrovie, le comunicazioni, la chimica, l'elettricità ed il petrolifero. Le reti ferroviarie, nello specifico, da alcuni considerate un investimento antieconomico, furono fondamentali nello sviluppo degli Stati Uniti d'America.
La terza rivoluzione industriale, dal 1950 in avanti, ha visto ancora gli Stati Uniti d'America e la Germania quali protagonisti. Con essa si è assistito al decentramento ed alla modifica organizzativa della fabbrica, divenuta un luogo anche di alienazione delle persone. Come risposta, le grandi imprese si sono riorganizzate con nuovi approcci ed organigrammi multi-divisionali, espandendo le loro operazioni in tutto il pianeta. I settori interessati da questa ondata sono stati la comunicazione e l'informatica, i trasporti aerei, l'energia atomica e le biotecnologie. Le imprese, alla ricerca della flessibilità, hanno iniziato a dare maggiore autonomia al *management*, anche se gli attori principali di questa rivoluzione sono stati le aziende già consolidate.
La quarta rivoluzione industriale, cominciata agli inizia del XXI secolo, è basata sulle nuove tecnologie come l'Intelligenza Artificiale, IoT, i Big Data, la robotica, la *blockchain*, le biotecnologie e la stampa 3D. Pur presentando indubbi vantaggi per la vita delle persone essa impone una riflessione etica profonda sulle tematiche della potenziale disoccupazione in ampie fasce della popolazione e sulla tutela dei dati che sono divenuti una vera merce di scambio.
Nel dibattito sulle cause principali dello sviluppo, tra i fattori di natura esterna, è indicato il commercio internazionale. Autori come Kuznets[5], Deane[6] e Cole[7] hanno sostenuto che il commercio internazionale ha avuto un ruolo fondamentale nella crescita economica. Infatti, in passato come oggi, nei Paesi in cui lo sviluppo ha raggiunto le dimensioni più rilevanti (Inghilterra, Usa, Germania ed oggi la Cina) il

[5] Simon Smith Kuznets (1901-1985), economista e Premio Nobel per l'economia del 1971.
[6] Phyllis Mary Deane (1918-2012), storica dell'economia e professore emerito.
[7] William Alan (Max) Cole (1926-2004), professore e storico dell'economia.

commercio estero, ossia la possibilità di contare su sbocchi più ampi e differenziati, è stato un fondamentale attore in campo non solo economico, ma anche sociale (Kuznets, 1968).
Ogni rivoluzione industriale, compresa la quarta che dal duemila in avanti ha visto la centralità di internet, del *cloud* con l'integrazione dei sistemi cyber e fisici, ha messo l'accento sull'innovazione, quale fattore chiave per competere. In questo scenario, risulta evidente che solo un sistema Paese che in qualche modo esprima e tuteli le proprie innovazioni, tramite marchi e brevetti, possa sopravvivere e mantenere, nel lungo periodo, un benessere sociale sostenibile che consenta la convivenza tra generazioni.
Joseph Alois Schumpeter[8], noto economista austriaco, sottolineò il ruolo dell'imprenditore innovatore quale motore della crescita. Secondo il celebre studioso, solo l'imprenditore è in grado di operare mutamenti radicali, grazie ad innovazioni continue di prodotto o di processo, impiego di nuove materie prime, apertura dei mercati e cambiamenti organizzativi. Inoltre, con la felice e positiva espressione "distruzione creatrice" egli individuò il processo evolutivo dell'economia capitalistica occidentale (Schumpeter, 2021). Oggi la maggior parte di questo processo creativo è realizzato da imprese multinazionali, le sole in grado di realizzare grandi progetti di innovazione che possono condizionare la società globale. La culla delle imprese multinazionali sono ancora gli Stati Uniti d'America, primo mercato di capitali al mondo, anche se conglomerate globali sono nate e si sono affermate al di fuori del perimetro occidentale, come ad esempio in Cina ed in India.

I sistemi di Corporate Governance
La Corporate Governance rappresenta l'insieme di regole attraverso le quali le imprese sono gestite e controllate nel loro percorso di creazione del valore. L'importanza della *corporate governance* è cresciuta nel tempo ed oggi rappresenta un elemento essenziale non solo per le imprese di grandi dimensioni, il comparto "large", ma anche per le medie organizzazioni. La qualità del sistema di governo è divenuta dunque un *asset* strategico sul quale porre attenzione e dal quale trovare spunti importanti in relazione alle performance aziendali.
Nel dibattito accademico, si riscontrano due definizioni di *corporate governance* classificabili sulla base delle variabili legate ai soggetti che si vogliono tutelare ed al come essi si tutelano, ossia tramite quali meccanismi di governo.
Una buona *governance* dovrebbe considerare la qualità del *management*, i compensi degli amministratori e dei dirigenti, la trasparenza, l'indipendenza dei consiglieri di amministrazione, le informazioni non economiche, il funzionamento del consiglio di amministrazione, la struttura dell'azionariato, il meccanismo di remunerazione ed incentivazione, ecc. Si tratta di un vasto ambito di applicazione basato su fonti normative nazionali – Testo Unico della Finanza T.U.F (D.lgs 58/1998), D.lgs 231/2001, la riforma del diritto societario D.lgs 6/2003, L. 62/2005, L. 262/2005 sulla tutela del risparmio, D.lgs 195/2007, D.lgs 674/2023, ecc. –, internazionali (OCSE-G20 del 2023), autorità di controllo, gestori di mercato e volontà delle singole imprese. Per le società quotate, Borsa Italiana ha proposto un "buon governo delle società quotate" attraverso l'attuazione del Codice Italiano di Corporate

[8] Joseph Alois Schumpeter (Třešt', Moravia, 1883 - Taconic, Connecticut, 1950). Docente a Graz e a Bonn (1925-32), fu ministro delle Finanze della Repubblica austriaca (1919); emigrato negli Stati Uniti, insegnò dal 1932 alla Harvard University. Fonte Enciclopedia Treccani.

Governance (Borsa Italiana 2023), cui hanno aderito a fine 2022 il 95% delle società italiane con azioni sul mercato EXM[9].
La riforma del 2003 ha offerto alle imprese la possibilità di scegliere uno dei tre modelli di amministrazione e controllo: il modello tradizionale, il modello dualistico e quello monistico (D.lgs 6/2003). Il modello tradizionale prevede il consiglio di amministrazione ed il collegio sindacale con attività di controllo dell'amministrazione, il modello dualistico è caratterizzato dalla presenza di un consiglio di sorveglianza e di un consiglio di gestione, mentre nel modello monistico il consiglio ha al suo interno un comitato di controllo.
Nonostante questo importante apparato normativo e la possibilità di aderire volontariamente a "best practices", si sono verificati casi di *corporate governance* fallace con comportamenti poco corretti da parte degli amministratori verso gli Stakeholder e con esternalità negative (Stiglitz, 2015) che hanno impattato sulle entrate fiscali dello Stato italiano, classificabili in tre grandi aree: imposte dirette, imposte indirette e contributi sociali.

Investimenti Diretti Esteri
L'art. 207 del TFUE[10] all'art. 1. indica che "*la politica commerciale comune è fondata su principi uniformi, in particolare per quanto concerne le modificazioni tariffarie, la conclusione di accordi tariffari e commerciali relativi agli scambi di merci e servizi, e gli aspetti commerciali della proprietà intellettuale, gli investimenti esteri diretti, l'uniformazione delle misure di liberalizzazione, la politica di esportazione e le misure di protezione commerciale, tra cui quelle da adottarsi nei casi di dumping e di sovvenzioni. La politica commerciale comune è condotta nel quadro dei principi e obiettivi dell'azione esterna dell'Unione*".
In particolare, il quadro normativo relativo agli Investimenti Diretti Esteri, o Foreign Direct Investment, ha visto in Italia un'evoluzione progressiva nell'arco di un trentennio che ha definito ed esteso, nella sostanza, i poteri speciali dello stato in ambito economico. Dopo l'avvio delle privatizzazioni degli anni '90 del secolo scorso molti Paesi, tra cui l'Italia, introdussero l'istituto giuridico della "golden share" (D.L. n. 332/1994)[11] che prevedeva diritti speciali ai detentori di azioni anche se in possesso di quote minoritarie. A fronte di tali iniziative, la Corte di Giustizia delle Comunità Europee, con la sentenza 6/12/2007 n. C-464/04, indicò una potenziale violazione dei precetti contenuti nel Trattato CE.
In seguito, con il Decreto-Legge convertito con modificazioni dalla L. 11 maggio 2012, n. 56[12], su impulso dell'Unione Europea, sono stati ampliati i poteri nelle acquisizioni, a qualsiasi titolo, "di partecipazioni in imprese che svolgono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale" (art. 1 lettera a) D.L. 21/2012). Inoltre, esso ha previsto il "veto all'adozione di delibere, atti od operazioni dell'assemblea o degli organi di amministrazione di un'impresa di cui alla lettera a), che abbiano per effetto modifiche della titolarità, del controllo o della disponibilità" e l'"opposizione all'acquisto, a qualsiasi titolo, di partecipazioni in un'impresa di cui alla lettera a) da parte di un soggetto diverso dallo Stato italiano, enti pubblici italiani o soggetti da questi controllati" (art. 1 lettera c) D.L. 21/2012). La norma ha evidenziato il concetto di "potenziale influenza dell'acquirente" sulla

9 Euronext Milan.
10 Il trattato sul funzionamento dell'Unione Europea.
11 Decreto-legge 31 maggio 1994, n. 332, convertito con modifiche nella legge 30 luglio 1994, n. 474, ulteriormente modificata dalla legge 24 dicembre 2003, n. 350.
12 In G.U. 14/05/2012, n. 111.

società, in ragione della nuova posizione derivante dall'acquisizione della partecipazione imponendo la notifica della stessa acquisizione, entro dieci giorni, alla Presidenza del Consiglio dei Ministri. Nel caso di società quotate nei mercati regolamentati la notifica era indicata nel superamento della soglia del 3%, con successive notifiche al 5%, al 10% e fino al 50%.

Nel 2017, con la legge 4 dicembre 2017, n. 172[13], recante disposizioni urgenti in materia finanziaria e per esigenze indifferibili, è stato ampliato il perimetro degli interessi strategici ed introdotta, all'art. 13, la cosiddetta "norma antiscorrerie" sulla base delle esperienze francesi ed americane. Essa ha portato l'inserimento, nell'art. 120 del Testo Unico della Finanza, di un nuovo comma 4 nel quale si imponeva agli acquirenti di partecipazioni rilevanti (pari o superiori alle soglie del 10%, 20% e 25%) un obbligo di comunicazione alla CONSOB, al mercato ed alla partecipata quotata avente l'Italia come Stato membro d'origine (Alvaro e altri, 2019).

In seguito, la Ue ha stabilito, con il Regolamento UE 452/2019, "un quadro per il controllo degli investimenti esteri diretti nell'Unione da parte degli Stati membri per motivi di sicurezza o di ordine pubblico e per un meccanismo di cooperazione tra gli Stati membri e tra gli Stati membri e la Commissione con riguardo agli investimenti esteri diretti che possono incidere sulla sicurezza o sull'ordine pubblico. Esso prevede altresì la possibilità che la Commissione emetta pareri su tali investimenti" (art. 1 Regolamento UE 452/2019). Esso ha superato la discrezionalità statale nel controllo degli investimenti esteri, prescrivendo la verifica degli investimenti tra stati membri, nel caso l'investitore non sia controllato da soggetti europei, introducendo obblighi di *screening* anche dopo l'operazione ed ampliando l'attenzione ai settori considerati critici. Nel Regolamento sopra citato, l'investimento diretto estero, è considerato "un investimento di qualsiasi tipo da parte di un investitore estero inteso a stabilire o mantenere legami durevoli e diretti tra l'investitore estero e l'imprenditore o l'impresa cui è messo a disposizione il capitale al fine di esercitare un'attività economica in uno Stato membro, compresi gli investimenti che consentono una partecipazione effettiva alla gestione o al controllo di una società che esercita un'attività economica" (art. 2 Regolamento UE 452/2019). Semplificando, gli IDE sono gli investimenti nel capitale degli operatori economici, costituiti quali imprese, da parte di società di investimento o di altre aziende. Si tratta di investimenti che devono assicurare "un certo grado di controllo" che sia rappresentato da una partecipazione di almeno il 10% dei diritti di voto esprimibili (Franchi, Tagliavini e Regalli, 2020).

Se il Regolamento UE 452/2019 ha portato indubbi vantaggi in tema di coordinamento e trasparenza, occorre anche valutare, secondo uno studio realizzato dall'OCSE[14] nel 2022 con il sostegno finanziario della Commissione, una serie di significative differenze tra i vari sistemi nazionali, in relazione alla copertura settoriale, nelle esenzioni concesse ad alcuni acquirenti, nelle differenze tra i concetti di sicurezza e di ordine pubblico, nelle differenze tra le date e nei termini di notifica, nelle differenze dei termini impiegati per indicare la probabilità dei rischi, nelle differenze tra le soglie di avvio dei controlli e nei poteri relativi alla prese in considerazione delle minacce nei confronti di altri stati membri. Accanto a queste indicazioni si è ravvisato anche l'aumento del grado di burocrazia del sistema tipico di un apparato normativo operante su larga scala.

[13] Di conversione del D.L. 16 ottobre 2017, n. 148.

[14] Relazione dell'OCSE, *Framework for screening Foreign Direct Investment into the EU – Assessing effectiveness and efficiency*, 2022.

Gli IDE evidenziano sia la capacità di un sistema economico di attirare investimenti (IDE passivi), con la rassicurazione istituzionale che essi saranno tutelati e protetti nel medio e lungo periodo consentendo un ritorno agli investitori, che la sua dinamicità nell'operare all'estero (IDE attivi) attraverso stabilimenti produttivi, filiali o acquisizioni di altre aziende. In questa prospettiva, l'internazionalizzazione diventa non il semplice scambio di merci nei mercati internazionali, ma l'essere in grado di andare in territori stranieri, organizzare un complesso industriale e mantenere la continuità imprenditoriale per anni influenzando la società locale.
Gli IDE rappresentano una mano "invisibile", contrapposta a quella "visibile" dell'intervento diretto statale. Una parte della teoria economica che sottolinea la perfezione o in ogni caso la forte efficienza dei meccanismi di auto regolazione del mercato, si basa sull'assunto che la libertà delle forze private in competizione tra loro conduca al migliore risultato di equilibrio e al più elevato livello di sviluppo e ricchezza. Per un certo contesto speculativo, non vi sarebbe spazio per politiche nazionali pubbliche, le quali sono ritenute controproducenti in quanto di ostacolo al raggiungimento naturale dei migliori risultati complessivi. I principali Paesi, tuttavia, possono muoversi sui mercati internazionali tramite schemi che consentono di ottenere risultati di rilievo grazie all'intervento indiretto ed apparentemente invisibile di un'impresa multinazionale.
Secondo le Nazioni Unite, sono oltre 100.000 le multinazionali nel mondo, anche se la testa della classifica è composta principalmente dalle grandi imprese americane. Si ritiene che esse controllino direttamente l'80% del commercio mondiale, un terzo del PIL della Terra e che le 100 multinazionali coperte nel database ADIMA[15], nel 2016, abbiano generato quasi 10 trilioni di dollari di ricavi (c.a. il 20% del PIL mondiale) guadagnando 730 miliardi di profitto e pagando 185 miliardi di dollari di tasse.
Nella classifica Fortune Global 500[16], stilata sulla base del fatturato, si possono trovare le più importanti aziende multinazionali al mondo che nel 2022 aggregavano ricavi per oltre 41 trilioni di dollari. La localizzazione globale di queste imprese, con al primo posto da dieci anni consecutivi il colosso americano Walmart, vede tre aree di polarizzazione, Nord America, Europa e Cina ed una quarta area significativa legata al Medio Oriente e rappresentata da Saudi Aramco, al secondo posto della classifica.
Da punto di vista di Drucker la dimensione aziendale ha un effetto determinante sulla strategia che, a sua volta, ha un impatto decisivo sulla dimensione (Drucker, 2000). Egli ritiene non solo che tra le imprese sussista interdipendenza, ma che la piccola impresa, tipica del tessuto imprenditoriale italiano, abbia bisogno di un *management* e di un'organizzazione che la protegga dalla marginalità e dal fallimento. Una casta di *manager* che nelle grandi imprese multinazionali, spesso con sede legale ubicata nei Paesi a maggiore convenienza fiscale, ha tendenze apolidi in quanto separa il ruolo manageriale globale dal Paese di origine della persona. Dopo la Seconda Guerra Mondiale, la società moderna si è trasformata in una società delle istituzioni (Drucker, 2000) dalle quali dipende il funzionamento della stessa.

Il settore Difesa

[15] Analytical Database on Individual Multinationals and Affiliates.
[16] https://fortune.com

Anche nel settore della difesa, centrale nella Guerra Economica, le imprese multinazionali rivestono un ruolo chiave. Esse sono oggi di grande attualità per i tanti progetti in atto tesi a mantenere competitivo e sicuro l'Occidente. In tale scenario, a competere su scala globale non sono solo gli Stati-Nazione, i blocchi di alleanze, gli enti locali, ma anche le aziende multinazionali ed in particolare quelle dei settori Oil&Gas, infrastrutture e difesa. Storicamente il settore Oil&Gas è stato l'agente di innesco di conflitti armati locali e regionali, soprattutto nel Medio Oriente. Collateralmente all'impiego militare, le imprese del settore difesa hanno dovuto garantire alle forze armate capacità offensive, difensive e vantaggi tecnologici in grado di consentire una superiorità rispetto ai nemici ed alle imprese concorrenti impegnate ad elaborare soluzioni simili o migliori. Il cuore della ricerca e sviluppo militare è posseduto da queste imprese che investono somme elevate dei loro bilanci per applicare nuove tecnologie e migliorare quelle esistenti. Molto spesso, dopo qualche anno, queste innovazioni entrano nel mercato per usi civili e garantiscono benefici in molteplici aspetti della vita delle persone, compreso quello sanitario.

La spesa mondiale per la difesa ha raggiungo, nel 2024, i c.a. 2.500 miliardi di dollari con un incremento di c.a. il 7% rispetto al 2022[17] ed arrivando a c.a. il 2,3% del PIL mondiale. La leadership spetta al continente americano che assorbe il 41% di questi investimenti seguito da Asia ed Oceania con il 33% e dall'Europa con il 24%. I maggiori investitori statali sono gli Stati Uniti, la Cina e la Russia. In particolare, il bilancio difesa degli Stati Uniti, arrivato a 916 mld di dollari nel 2023 è seguito dalla Cina con 296 miliardi di dollari e dalla Russia con 109 miliardi di dollari. Questo terzetto è tallonato dall'India, con 84 miliardi di dollari e dall'Arabia Saudita con 76 miliardi di budget.

Alcuni nomi di imprese del settore difesa sono universalmente noti, come il quintetto di testa tutto americano, composto da Lockheed Martin Corp., Raytheon Technologies (RTX), Northrop Grumman, Boeing e General Dynamics. Invece, per quanto riguarda i gruppi cinesi (SIPRI Top 100) si rilevano alcune sigle che spesso svelano gruppi industriali di dimensioni globali: Norinco (China North Industries Corporation), AVIC (Aviation Industry Corporation of China), CASC (China Aerospace Science and Technology Corporation), CETC (China Electronics Technology Group Corporation), CASIC (China Aerospace Science and Industry Corporation), CSSC (China State Shipbuilding Corporation), CSGC (China South Industries Group Corporation).

La Norinco è una conglomerata cinese che controlla centinaia di imprese operanti nel settore difesa, ma non solo. Infatti, Norinco esprime un ruolo geopolitico rilevante in vaste aree del globo. Essa opera sia nello sviluppo del settore minerario in Mongolia che nella Repubblica Democratica del Congo, tramite la Comika Company. Inoltre, Norinco gestisce pozzi petroliferi in Iraq e vende camion pesanti in Malaysia esprimendo un potenziale qualitativo in grado di sostituire similari prodotti occidentali.

Un altro esempio è la AVIC (Aviation Industry Corporation of China) che opera nel settore della difesa tramite partenariati attivi con il Pakistan, per la nuova generazione del caccia multiruolo leggero FC-1/JF-17, e tramite accordi per la fornitura di componentistica aerea militare alla Russia che sono stati denunciati e sanzionati dagli americani. Per concludere, la CETC (China Electronics Technology Group Corporation), che è specializzata nelle comunicazioni, è anche la terza

[17] Fonte: elaborazioni ASM su dati SIPRI-Stockholm International Peace Research Institute.

industria IT del Paese. L'azienda è concentrata altresì nella produzione di sistemi per il riconoscimento facciale ed è il principale azionista della discussa società Hikvision, le cui telecamere per videosorveglianza diffuse in tutto il mondo sono state oggetto di sanzioni americane e rimosse in alcuni Paesi occidentali (Bureau of Industry and Security, Commerce).
Molte aziende occidentali operanti nel settore difesa dipendono da *supply chain* di fornitura, organizzate a compartimenti stagni, che nel settore aerospaziale arrivano a detenere il 50%/60% del valore di un sistema. Per migliorare la collaborazione con i fornitori, spesso specializzati in un singolo componente e con dimensioni variabili, sono state realizzate piattaforme software in grado di rendere più agile il lavoro, aggiornando e modernizzando in tempo reale i programmi dei mezzi esistenti (Dassault). Questa modalità di gestione dei processi migliora non solo la collaborazione tra aziende e fornitori, ma consente anche un'interazione nella progettazione ed un controllo della produzione e del rispetto dei tempi di fornitura. Anche l'azienda Leonardo rimarca l'importanza della *supply chain* e tra le azioni tese a mitigare le diverse tipologie di rischi, tra cui le frodi o attività illecite da parte di dipendenti e di terzi, indica "la gestione responsabile della catena di fornitura, attraverso la qualifica, la selezione e la gestione dei fornitori, nonché l'adozione di uno strumento di *risk analysis* nell'ambito delle attività di due *diligence* svolte nell'ambito del processo di conferimento degli incarichi a promotori commerciali, consulenti commerciali e lobbisti" (Leonardo S.pA). La tematica della "Supply Chain Resilience" è divenuta nota durante il Covid-19, che ha messo in discussione tutte le logiche produttive "lean" del settore *automotive* basate su *stock* di magazzino molto bassi e fornitori ubicati in tutto il modo. Dopo l'ubriacatura teorica dell'*offshoring*, iniziata negli anni '70 e '80 del Novecento per divenire un fenomeno diffuso anche nel nuovo secolo, si sono verificate delocalizzazioni delle produzioni in aree del globo con costi della manodopera più bassi e minori spese operative (Targetti e Fracasso, 2008) e si è assistito ad un ripensamento sulla lunghezza delle catene di approvvigionamento nelle logiche della prevenzione e protezione. Anche se una delle caratteristiche più importanti di una filiera resiliente è che sia corta, riportarla il più vicino possibile all'Occidente ed all'Italia non è affatto semplice per una questione di tempi, costi e di sistemi produttivi posseduti e controllati da operatori stranieri non disponibili a cedere il loro vantaggio competitivo. In questo scenario, capire come le catene di approvvigionamento della difesa, che ad esempio per i trasporti impiegano comunque tecnologie provenienti dal settore civile, dipendano da infrastrutture sottostanti richiama al tema della cooperazione con i Paesi alleati ed alla protezione delle imprese strategiche, indipendentemente dalle loro dimensioni e dal tipo di assetto proprietario. Inoltre, la vulnerabilità delle catene di approvvigionamento impone un cambiamento di mentalità ed un passaggio alle logiche SCDM[18] attraverso le quali generare un reale mutamento di strategia (Lucas e altri, 2024).

Conclusioni

I conflitti in corso nel globo procedono tra dazi e sanzioni rivolti, per rappresaglia, alle imprese ed ai loro rappresentanti. Queste pratiche rallentano ed ostacolano l'esercizio dei diritti di proprietà ed intralciano il valore dato al tempo da parte degli operatori economici (Stiglitz, 1998).

[18] Supply Chain Disruption Management.

D'altro canto, da secoli gli Stati competono su scala mondiale anche attraverso il commercio e gli investimenti diretti esteri (Constant, 2013). Essi sono molto meno costosi in termini di denaro e di vite umane e molto più redditizi rispetto al costo giornaliero di un conflitto come quello in corso in Ucraina.
La guerra economica pone al centro il controllo statale sulle imprese ritenute strategiche, esercitato in Italia tramite i poteri speciali della cosiddetta "golden power" (dal D.L. 21/2012), preceduta cronologicamente dalla "golden share" che prevedeva diritti speciali ai detentori di azioni anche se in possesso di quote minoritarie (D.L. n. 332/1994).
Accanto ad essi, occorre sottolineare il forte supporto da parte dei governi ai sistemi economici e nella difesa dei campioni nazionali, attuato con veicoli speciali nella forma di società per azioni a controllo pubblico, come ad esempio Cassa Depositi e Prestiti, oppure in Europa tramite AFD (Agenzia di sviluppo francese), BGK (Istituto nazionale di promozione polacco), Bpifrance (Banca pubblica di investimento francese), CDC (Istituto nazionale di promozione francese), InvestNL (Istituto nazionale di promozione olandese), KfW (Istituto nazionale di promozione tedesco) ed ELTIa (Associazione degli investitori a lungo termine con sede a Bruxelles). Quello che si è realizzato in pratica non è un sistema economico al servizio dello sforzo bellico, ma un'arena che vede le imprese multinazionali diventare strumento di combattimento avanzato e tecnologico, più o meno indipendente, in grado di tutelare nei mercati esteri, se indirizzato, gli interessi nazionali. Questa prassi riconosce il fondo sovrano, che dovrebbe esercitare tale diritto solo nel Paese d'origine ispirato dai Principi di Santiago del 2008 e limitato dalle normative nazionali, quale veicolo giuridico utilizzato per conquistare l'avversario che purtroppo, con la cassaforte vuota in seguito alla crisi finanziaria, economica e sociale, è costretto ad aprire le porte ed a vendere i gioielli di famiglia per ripianare i debiti. Nel 2023, il fondo sovrano norvegese NBIM[19], considerato uno dei migliori a livello globale per trasparenza, ha gestito c.a. 1.379 miliardi di dollari in investimenti, con un portafoglio di azioni valutato 1 trilione di dollari e partecipazioni in oltre 9.200 società. Nonostante il parlamento norvegese abbia deciso che il fondo non possa investire in imprese che producono alcuni tipi di armi, tabacco, cannabis, carbone, o che violano alcune norme etiche fondamentali, nel portafoglio internazionale del fondo risultano partecipazioni in Leonardo, Dassault, Saab, General Dynamics, ecc. Dall'analisi dei numeri risulta evidente sia la capacità di influenza che un fondo come quello norvegese può avere nelle imprese partecipate che il ruolo giocato nei mercati finanziari globali.
Una guerra economica, o forse meglio una guerra commerciale, che vede l'attore principale nell'impresa multinazionale. Come sopra indicato questa tipologia di azienda, con fatturati superiori al PIL di molti Paesi del pianeta è in grado di movimentare, grazie allo sviluppo tecnologico, immense somme di denaro in una frazione di secondo e senza lasciare traccia. La mobilità del denaro è diventata un ulteriore fattore in grado di ridimensionare il ruolo delle autorità pubbliche che a fatica riescono ad imporre regole, ad effettuare controlli ed a perseguire i criminali (Franchi e Caruso de Carolis, 2017).
Imprese multinazionali quotate la cui proprietà ed il *management* non sono più riferibili ad uno Stato specifico, con la localizzazione della sede legale che spesso segue i vantaggi fiscali del momento, come l'esenzione fiscale su dividendi e

[19] NBIM, Norges Bank Investment Management. Il nome formale del fondo è Government Pension Fund-Global (GPFG**).**

plusvalenze (PEX[20]) nelle holding olandesi[21] che ha portato molte importanti aziende multinazionali italiane a trasferire nel Paese dei tulipani la sede legale, generando un sistema di concorrenza fiscale a distorsione del mercato comune europeo.

Un problema di tale portata mette in crisi i decisori politici, spesso all'oscuro delle strategie prese dalle aziende multinazionali che sono conosciute quando i loro effetti, come il taglio lineare del personale o la chiusura di uno stabilimento, raggiungono l'opinione pubblica. Questo avviene in Occidente, mentre in Oriente l'impresa multinazionale è controllata direttamente dallo Stato che la trasforma in un vero e proprio mezzo di combattimento per la conquista dei mercati mondiali e per l'ottenimento della leadership tecnologica.

Bibliografia

CONSTANT B., La libertà degli antichi, paragonata a quella dei moderni, Einaudi, Torino 2013.

DRUCKER P. F., Manuale di Management, compiti, responsabilità e me¬todi, Etas, Milano, 2000.

FRANCHI M., Guerra e Commercio, RIVISTA MARITTIMA - ISSN 0035-6964. - 1(2015), pp. 76-82.

FRANCHI M., Guerra Economica e Diplomazia, RIVISTA MARITTIMA - ISSN 0035-6964. - (2020), pp. 36-43.

FRANCHI M., RAINIERI B., Riflessioni sul Management Responsabile, Licosia, Ogliastro Cilento 2019.

GALLI G. – CALIGIURI M., Come si comanda il mondo. Teorie, volti, intrecci, Rubbettino, Soveria Mannelli 2017.

ILMARI K., "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," Parameters 51, no. 3 (2021), doi:10.55540/0031-1723.3084.

LANZALACO L., Le Politiche Istituzionali, Il Mulino, Bologna 2005.

LIANG Q., XIANGSUI W., Unrestricted Warfare: China's Master Plan to Destroy America, Echo Point Books & Media, 2015.

KISSINGER H., Ordine Mondiale, Mondadori, Milano 2015.

KUZNETS S.S., Toward A Theory Of Econ Growth, W.W. Norton and Company, Inc., New York City 1968.

FRANCHI M., CARUSO de CAROLIS A., Guerra Economica, Modelli Decisionali e Intelligence Economico Finanziaria, Licosia Edizioni, Ogliastro Cilento 2017.

FRANCHI M. – TAGLIAVINI G. – REGALLI M., La Difesa della Competitività: Investimenti Diretti Esteri e Intelligence Economica, Società Italiana di Intelligence, Arcavacata di Rende (CS) 2020.

ROMANO S., Atlante delle Crisi Globali, Rizzoli, Milano 2018.

RONZITTI N., Diritto Internazionale, Giappichelli, Torino 2023.

[20] Participation Exemption.

[21] https://www.government.nl/topics/taxation-and-businesses/corporation-tax

SCHUMPETER J.A., The Theory of Economic Development, Routledge, Londra 2021.

SMITH A., Indagine sulla natura e le cause della ricchezza delle nazioni, ISEDI, Torino 1976. L'opera originale venne pubblicata nel 1776.

STIGLITZ J.E., Economia del Settore Pubblico, Hoepli, Milano 2015.

STIGLITZ J.E., Il Ruolo Economico dello Stato, Il Mulino, Bologna 1989.

TARGETTI F. – FRACASSO A., Le Sfide della Globalizzazione, Francesco Brioschi Editore Srl, Milano 2008.

ZAMAGNI V., Dalla Rivoluzione Industriale all'Integrazione Europea. Breve Storia Economica dell'Europa Contemporanea, Il Mulino, Bologna 200.

Documenti

BORSA ITALIA, Relazione 2023 sull'evoluzione della corporate governance delle società quotate" 11° rapporto sull'applicazione del Codice di Autodisciplina, Milano 2023.

CORTE DI GIUSTIZIA EUROPEA, Relazione Speciale. Controllo degli investimenti diretti esteri nell'UE, 2023.

DASSAULT Systèmes, Trasformare la supply chain nella rete del valore. https://www.3ds.com/it/industries/aerospace-defense/transform-supply-chain-value-network

DEPARTMENT OF COMMERCE. BUREAU OF INDUSTRY AND SECURITY. 15 CFR Part 744. [Docket No. 190925-0044] RIN 0694-AH68. https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list

CONSOB, La nuova via della seta e gli investimenti esteri diretti in settori ad alta intensità tecnologica. Il golden power dello Stato italiano e le infrastrutture finanziarie, S. Alvaro, M. Lamandini, A. Police, I. Tarola, 2019.

COPASIR, Relazione sulla tutela degli asset strategici nazionali nei settori bancario e assicurativo, Roma 2020.

FORTUNE, Global 500, 2023.

ISTAT, Rapporto Annuale 2024, Situazione Paese, Roma, 15 maggio 2024.

OECD (Organisation for Economic Cooperation and Development), ADIMA-100, Analytical Database on Individual Multinationals and Affiliates, 2016.

OCSE, Framework for screening Foreign Direct Investment into the EU – Assessing effectiveness and efficiency, 2022.

RAND, Toward Defense Supply Chain Disruption Management. A Research Agenda for Defense Supply Chain Resilience. Rebecca Lucas, Thomas Ekström, Paola Fusaro, Elizabeth Hastings Roer, Lucia Retter, 2024.

SIPRI, Top 100 arms-producing and military services companies in the world, 2022.

SP 500 Dow Jones Indices.

SWF, 2024 Annual Report.

UNCITAD, Foreign direct investment, Economic Trend, 2022,

United States (U.S.) Army Doctrine Publication (ADP) 3-0.

Elisa Leoni
Ph.D. Student at the School Of Advanced Defence Studies (CASD/SSUOS) - University of Turin (UNITO), in Defence & Security Studies, curriculum: Legal studies for innovation

EXPLORING THE INTERCONNECTION BETWEEN SPACE AND CYBERSPACE: THE DUE DILIGENCE PRINCIPLE AS A TOOL OF INTERNATIONAL LAW TO COUNTER CYBERATTACKS ON SPACE SYSTEMS

ABSTRACT

Il presente contributo si propone di esaminare il principio della due diligence come strumento di diritto internazionale per contrastare e condannare gli attacchi cibernetici ai segmenti di terra dei sistemi spaziali. Dopo una panoramica sulla crescente interconnessione tra spazio e cyberspazio, farà seguito un"analisi del principio della due diligence, sia dal punto di vista del diritto internazionale, sia nella sua applicazione al dominio cibernetico. Questo approccio teorico verrà infine applicato al caso di studio relativo all"attacco cibernetico del 24 febbraio 2022, che ha compromesso i servizi di comunicazione satellitare della compagnia americana ViaSat.

This paper advocates for the due diligence principle as a vital tool in International Law to tackle and condemn cyberattacks targeting the ground segments of space systems. It begins by exploring the growing connection between space and cyberspace, before examining how the due diligence principle is understood in International Law. The discussion then shifts to how this principle can be interpreted and applied specifically within the cyber domain. Finally, this framework is used to analyse the February 24, 2022, cyberattack on the satellite communication services of the American company ViaSat.

Introduction

The Russian-Ukrainian war has opened the eyes of the international community to the essential nature of satellite services, not only in the military context but also in our daily lives. Satellites are not only critical infrastructures[1], but also serve as the foundation for numerous other essential systems, creating a potential single point of failure for a wide range of sectors[2]. Space systems are indispensable for both civilian and military applications, supporting activities that are integral to the functioning of modern society. For instance, the financial sector relies on accurate Positioning, Navigation, and Timing (PNT) data to ensure precise timestamping of transactions. The transportation and logistics sectors depend on satellite-based location data for

[1] For instances the European Union classifies space as European Critical Infrastructure in its Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[2] United States General Accounting Office (GAO) Report, CRITICAL INFRASTRUCTURE PROTECTION Commercial Satellite Security Should Be More Fully Addressed, 2002.

tracking shipments, optimising routes, and managing supply chains efficiently. In emergency contexts, satellite communications are vital for ensuring reliable and resilient communication during disaster recovery, search and rescue operations, and emergency response coordination[3]. Space systems also contribute to advancements in entertainment and research, highlighting their multifaceted importance. Moreover, they support military command and control operations and provide internet connectivity to remote and underserved regions around the globe.
Nevertheless, the complexity of these systems often results in inadequate cybersecurity measures, further exacerbated by the lack of comprehensive international policies to strengthen their resilience[4].
What the conflict has also underscored is the direct interconnection between space and cyberspace. This interweaving stems from the fact that, on one hand, there is a domain geographically distant from Earth, namely space, and on the other, a domain capable of overcoming any distance, namely cyberspace. This interconnection entails and will continue to entail an increase in cyber risks and threats directed toward outer space, which will consequently impact activities carried out on Earth. From the International Law perspective, a principle that could limit these threats by preventing and particularly condemning them is the due diligence principle. Unfortunately, its application in cyberspace is not yet considered customary, but assisting in its process of application by highlighting its strengths and weaknesses will certainly help in the development of state practice in this area. Applying the due diligence obligation to real-world events, providing evidence of possible shortcomings arising from this process, and clarifying the application itself is the primary objective of this article, which is organized as follows. Section 1 examines the characteristics and consequences of the interconnection between space and cyberspace. Subsequently, section 2 provides a legal analysis of the due diligence obligation in International Law, tracing its origins and contemporary interpretation by the international community. Subsection 2.1 attempts to apply the principle to the cyber domain, focusing on its legal characteristics. Finally, Section 3 promotes the application of the due diligence principle to the ViaSat cyberattack case study. To achieve this, subsection 3.1 delves into the technical characteristics of the attack, explained in simplified terms, while subsection 3.2 attempts to attribute the alleged violation of the due diligence obligation in cyberspace to the Russian Federation. In the concluding section, the advantages and shortcomings of applying the principle under analysis are discussed based on the elements revealed throughout the examination.

1. The increasing interconnection between space and cyberspace

It can be argued that there is a significant interconnection between space and cyberspace, which may expose satellite technologies to cyber threats. Indeed, as has been declared by the Commander of the U.S. Space Force"s Space Operations Command, Lt. Gen. Stephen Whiting: «Cyberspace is the soft underbelly of our global space networks»[5]. Accordingly, the main threat for space assets it is

[3] BACE B. - YASIR G. - UNAL T., *Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems*, in «*Telecommunications Policy*» 48 (2024) p.2. https://doi.org/10.1016/j.telpol.2024.102739.

[4] VARADHARAJAN V. - SURI N., *Security challenges when space merges with cyberspace*, in «Space Policy», 67 (2024), http://dx.doi.org/10.1016/j.spacepol.2023.101600.

[5] ERWIN S., *Space Force to shore up cybersecurity as threats proliferate*, Space News, 2022, Space Force to shore up cybersecurity as threats proliferate - SpaceNews.

represented by cybers-attacks[6] which with rapidity, unpredictability and easiness, can partially or completely compromise the function of space systems.
This vulnerability was not identified only recently. As demonstrated in the Martinovic and Pavur Manual, over the past 60 years there have been more than a hundred cases of malicious cyberattacks targeting satellites or, more generally, space systems[7]. One notable example occurred in 1998, when a group of hackers managed to take control of the German-American ROSAT X-Ray satellite, instructing it to orient its panels towards the sun provoking irreparable damage to the satellite's optical sensors[8]. In recent years, a notable example is the 2014 cyberattack on a U.S. weather satellite, which caused significant disruption to satellite feeds[9] and impacted various associated websites[10]. Regarding the types of cyberattacks targeting satellite systems, these threats include various methods aimed at different components. Common attacks involve unauthorized attempts to gain command-and-control over satellites, enabling operational disruption. Interception of sensitive data compromises the confidentiality and integrity of communications, while denial-of-service attacks can render systems inoperable, disrupting services[11]. Ransomware attacks block access to critical systems until a ransom is paid, delaying civilian and military operations[12]. Additionally, *spoofing*[13], *jamming*[14] and *hacking* target the link segment, undermining the reliability and security of communications between the space and ground segments. Moreover, the fact that cyberattacks are relatively inexpensive encourages their use by non-state actors who, over the past decades, have increasingly played a prominent role in launching cyberattacks against both States and industries. This growing involvement of non-state actors, often operating with limited resources, but with substantial technical expertise, has amplified the threat landscape, making critical infrastructures particularly vulnerable to disruption and exploitation. For example, the 2007 cyberattacks on Estonia, widely attributed to Russian patriotic hackers, crippled government,

---

6 Cyberattacks are defined by NATO as an act or action initiated in or through cyberspace to cause harmful effects. Source: NCIA | Cyber Security (nato.int).

7 PAVUR J. - MARTINOVIC I., *SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research*, Oxford University, 2020, 2010.10872 (arxiv.org).

8 SUWIJAK C. - LI S., *Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space*, in «Journal of East Asia and International Law» (15/No.1), 2022, p.100.

9 Satellite Feeds: The term "feed" refers to a transmission, often live, carried out by a satellite and aimed at supplying one or more television networks. These technical connections are used to route services or enable live broadcasts from distant locations. Source: http://www.scaistar.com/guide/feed/feed01.htm#:~:text=Si%20definisce%20con%20il%20termine, la%20diretta%20da%20luoghi%20lontani.

10 *Ibidem*.

11 KAVALLIERATOS G. - KATSIKAS S., *An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space*, in «International Journal of Critical Infrastructure Protection», 43 (2023), An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space - ScienceDirect.

12 BACE B. - YASIR G. - UNAL T., *Law in Orbit: International Legal Perspectives*..op. cit. p. 3.

13 Spoofing: A type of cyberattack used to falsify (from the English verb "to spoof") various types of information, such as the sender of a message, in order to deceive the recipient into believing that the messages originate from known, trustworthy, or unsuspected sources. This type of attack typically leverages social engineering techniques. Source: CSIRT, National Cyber Security Agency, Glossario - CSIRT Italia.

14 Jamming is an electronic attack against wireless communications, affecting the availability of the communication medium by producing interference that prevents the effective reception of the signal. Source: CyCon_2024_book.pdf (ccdcoe.org).

financial, and media services for weeks[15], highlighting how non-state actors are considered important players in the cyber domain.
At the international level, NATO has increasingly recognized the importance of cyber and space domains. Regarding cyberspace, NATO designated it as an operational domain at the 2016 *Warsaw Summit*[16] and, in 2021, acknowledged that significant malicious cyber activities might, under certain circumstances, constitute an armed attack warranting the invocation of Article 5 of the *North Atlantic Treaty*[17](on a case-by-case basis)[18]. At the 2023 *Vilnius Summit*, Allies endorsed a concept to enhance cyber defence"s role in deterrence and launched the Virtual Cyber Incident Support Capability (VCISC) to assist Nations in mitigating major cyber incidents[19]. As for space, NATO declared it a new operational domain at the 2019 *London Summit*[20]. In 2021, leaders stated that attacks "to, from, or within space" could trigger Article 5[21]. The 2023 *Vilnius Summit* emphasized integrating space into joint operations and enhancing data sharing[20]. Most recently, *NATO"s 2024 Summit* highlighted its commitment to a commercial space strategy[22] by engaging industry representatives[23].The relevant fact is that NATO has not only shown interest in space and cyberspace as separate domains, but also in the interconnection between them. Indeed, at the *Madrid Summit* held in July 2022, the integration between cyber operations conducted in cyberspace and the real effects produced in the space environment was established[24]. To better explain, during the Summit it was stated that threats originating from cyberspace can pose real risks to both orbital and terrestrial components, seriously endangering business continuity in the space context[25]. In fact, the primary concern arising from this intersection is that cyber-attacks could render space assets unusable. As already mentioned, these assets are especially crucial in the military context, where they play a central role in

---

15 OTTIS R., *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, NATO Cooperative Cyber Defence Centre of Excellence, 2008, Analysis of the 2007 Cyber Attacks against Estonia from the Inf (ccdcoe.org); CZOSSECK C., OTTIS R., TALIHÄRM A.-M., *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*, in «*International Journal of Cyber Warfare and Terrorism (IJCWT)*», Vol.1(1), 2011, pp. 24–34.

16 NATO - Official text: Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016), 09-Jul.-2016.

17 *The North Atlantic Treaty, Washington DC*, April 4, 1949, NATO - Official text: The North Atlantic Treaty, 04-Apr.-1949.

18 NATO - Official text: Brussels Summit Communiqué issued by NATO Heads of State and Government (2021), 14-Jun.-2021.

19 NATO - Official text: Vilnius Summit Communiqué issued by NATO Heads of State and Government (2023), 11-Jul.-2023.

20 NATO - Official text: London Declaration issued by NATO Heads of State and Government (2019), 04-Dec.-2019.

21 See *supra* note DA VEDERE

22 Following the NATO Vilnius Summit in July 2023, allies are developing a commercial space strategy to accelerate military technologies. Based on recommendations from a NATO-industry working group, the strategy aims to leverage commercial space capabilities, improve space situational awareness, and streamline acquisition processes to enhance defense cooperation and security in space. Source: HITCHEN T., *NATO plans first commercial space strategy to spur tech innovation*, Breaking Defence, 2024, NATO plans first commercial space strategy to spur tech innovation - Breaking Defense.

23 *Integrating Commercial Space for Military Applications in Europe: A Challenge and Opportunity*, ESPI, 2024 (para. 5) Integrating Commercial Space for Military Applications in Europe: A Challenge and Opportunity - ESPI.

24 NATO - Official text: Madrid Summit Declaration issued by NATO Heads of State and Government (2022), 29-Jun.-2022.

25 MARTINO L., *Cyber e Spazio: nuovo fronte di difesa integrata*, ISPI, 2022, Cyber e Spazio: nuovo fronte di difesa integrata | ISPI (ispionline.it).

managing the chain of command and control, identifying targets, guiding drones or weapons, and performing numerous other military activities[26].
In addition to the efforts of NATO member States, other initiatives are also worth mentioning: the *European Cybersecurity Skills Framework* (ECSF) developed by ENISA in 2022[27], the *NIST Cybersecurity Framework*, created by the U.S. National Institute of Standards and Technology (NIST)[28] and the *PANDORA-EDIDP Project* an EU-funded cyber defense platform designed for real-time threat hunting, incident response, and information sharing[29]. At this stage of the analysis, it is evident that space assets are crucial for delivering services to both military and civilian sectors. However, the growing interconnection between those two domains has significantly increased the vulnerability of space systems to cyber threats. While cyberattacks discussed in the introduction may not meet the threshold of an "armed attack" under *jus contra bellum*, their disruptive impact raises pressing questions about the capacity of International Law to address these emerging challenges effectively. Specifically, which principles of International Law can effectively prevent and address cyberattacks targeting space systems, particularly the ground segment? The following section examines the principle of due diligence, evaluating its potential as a regulatory framework while critically underling its limitations.

2. The principle of due diligence in International Law

According to Professor Ian Yuying Liu, due diligence is a corollary of State sovereignty[30]. This obligation is not a rule of attribution, but a primary norm derived from the judgment of the International Court of Justice (ICJ) in the *Corfu Channel Case* and, more recently, in *Pulp Mills Case*[31]. Briefly examining the two cases, the

---

[26] To know more about the use of space technologies in the military sector see: NATO Science & Technology Organization. *Science & Technology Trends 2023-2043: Across the Physical, Biological, and Information Domains*. Volume 2: Analysis, 2023, pp. 164-178.

[27] ECSF is a tool aimed at harmonizing cybersecurity education and workforce development across Europe. It defines roles and skills necessary for cybersecurity professionals, helping bridge the gap between the supply (training) and demand (workplace) sides in the EU cybersecurity workforce. Source: European Cybersecurity Skills Framework (ECSF) — ENISA (europa.eu).

[28] The framework provides a set of guidelines to help organizations manage and reduce cybersecurity risks. It is widely adopted globally and structured around five core functions: Identify, Protect, Detect, Respond, and Recover. Source: Cybersecurity Skills and Workforce Frameworks | NIST.

[29] Financed by the European Commission under the European Defence Industrial Development Programme (EDIDP), PANDORA supports collaborative cyber defense among EU member states. The project focuses on strengthening cyber resilience within the EU by providing innovative tools and solutions for better threat management and incident handling. Source: PANDORA-EDIDP.

[30] LIU Y.I., *State Responsibility and Cyberattacks: Defining Due Diligence Obligations*, in «The Indonesian Journal of International and Comparative Law», 2017, p. 199.

[31] As affirmed by Doctor Jack Kenny, due diligence obligations have been addressed in a number of international courts and arbitral awards…See: International Court of Justice, Corfu Channel Case (United Kingdom v. Albania), 9 April 1949, I.C.J. Reports 1949, p. 4, p. 22; International Court of Justice, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), 26 February 2007, I.C.J. Reports 2007, p. 43, para. 430; International Court of Justice, Pulp Mills on the River Uruguay (Argentina v. Uruguay), 20 April 2010, I.C.J. Reports 2010, p. 14, paras 101, 197, 204, 223; International Court of Justice, Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), 16 December 2015, I.C.J. Reports 2015, p. 665, paras 104, 153, 168, 228; International Tribunal for the Law of the Sea, Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (Advisory Opinion), 1 February 2011, ITLOS Reports 2011, paras 110–112, 117–120, 131–132; International Tribunal for the Law of the Sea, Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission, 2 April 2015, ITLOS Reports 2015, paras 125–132, 146–150.

former concerned a dispute between the United Kingdom and Albania centred on an incident that occurred on 22 October 1946. During that time, two British warships struck mines and sustained significant damage while navigating the Corfu Channel within Albanian territorial waters. The Court held Albania responsible under International Law for the explosions and the resulting casualties and damage. It concluded that Albania's responsibility was due to its failure to inform the United Kingdom about the presence of mines in its waters. The Court based this duty to notify on "certain general and well-recognized principles", which include «[E]very State"s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States»[32].

In the more recent *Pulp Mills Case*, the issue presented to the Court concerned Uruguay's responsibility for breaching environmental obligations under a 1975 bilateral Treaty with Argentina[33]. To determine the scope of Uruguay's obligations under this Treaty, particularly regarding the preservation and protection of the San Juan River ecosystem, the Court referred to the customary obligation to prevent transboundary environmental harm, noting: «[T]he principle of prevention, as a customary rule, has its origins in the due diligence that is required of a State in its territory»[34]. Although the status of the no-harm rule was uncertain at the time of the judgment, it is now established that States have a customary International Law obligation to prevent their territory from being knowingly used for actions that violate the rights of other States[35].

Analysing some doctrinal interpretation of the due diligence principle in International Law, it is possible identify contrasting positions. Indeed, as McDonald explains, «there is no "general principle of due diligence" in International Law, a legal requirement to exercise due diligence may be a component part of a primary rule of International Law, but this can only be determined by referring back to the primary rule in question»[36]. Moreover, in relation to the *Corfu Channel* case, McDonald asserts that the Court did not identify a universal source for a general obligation of due diligence, nor did it extend due diligence obligations developed in specific contexts to other areas as if they were universally applicable[37]. In contrast, according to Koivurova, many areas of International Law have developed primary obligations that require States to exercise due diligence. These obligations do not require States to achieve a specific outcome but rather to make efforts to reach the result set out in the obligation[38]. In addition, a research elaborated by *Max Planck Institute for Comparative Public Law and International Law* suggested that due diligence may operate as a primary obligation in various fields, requiring States to take measures to mitigate risks, including those posed by non-state actors[39].

---

32 International Court of Justice, *Corfu Channel* (United Kingdom of Great Britain and Northern Ireland v. Albania), April 9, 1949, ICJ Reports 1949, p. 22.

33 *Statute of the River Uruguay*, a treaty signed by the two States on 26 February 1975, available at the following: Uruguay_River_Statute_1975.pdf (internationalwaterlaw.org)

34 International Court of Justice, *Pulp Mills on the River Uruguay* (Argentina v. Uruguay), 20 April 2010, I.C.J. Reports 2010, p. 14, para. 101.

35 OLLINO A. *Due Diligence Obligations in International Law*, Cambridge University Press: Cambridge, United Kingdom, 2022, p. 54.

36 MCDONALD N., *The Role of Due Diligence in International Law*, in «Cambridge University Press» (2016) p. 1041.

37 OLLINO A. *Due* …op. cit. pp. 54-57; KENNY J. *A general obligation of due diligence in international law*?, European Journal of International Law, 2024.

38 KOIVUROVA T., *Due Diligence*, in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law*, 2010.

39 *Ibidem*.

Moreover, as affirmed by Professor Karine Bannelier-Christakis: «[T]oday, everybody agrees that the *dictum* of the Court expresses a general principle of International Law». In this regard, it is important to clarify that the aim of this paper is not to extrapolate the concept of due diligence from other fields of International Law to determine whether it constitutes a general principle of International Law. Instead, the focus is on understanding the specific characteristics of the obligation under discussion and exploring its application in the context of cyberattacks.
As expressed by many scholars, due diligence is an obligation of conduct and not of a result[40]. According to S. Heathcote: «[S]tates should "deploy their best efforts to achieve [the] desired outcome[…]even if that outcome need not be ensured»[41]. To better understand the difference between a norm of conduct compared to a norm of result it is useful cite the ICJ pronunciation in the Genocide Case: «[I]t is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide so far as possible. A State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance»[42].
Having gained a clearer understanding of the origins and primary characteristics of due diligence in International Law, it is now essential to assess its potential application in the context of cyberspace.

2.1. Due diligence in cyberspace

According to the examination of the Court judgments, it is evident that the obligation is strictly related to the concept of territorial sovereignty, as a consequence, to apply it in cyberspace it is important to clarify if the cyber domain can be considered as a territory under the sovereignty of a State. To answer this question, some academics have affirmed that «[c]yberspace, as an intangible medium, can only exist inside tangible infrastructure […]. It operates via networks of computers, information systems, and telecommunication infrastructures located within a State's territory»[43]. Moreover, based on the interpretation of certain scholars who consider due diligence a general principle of International Law, as derived from ICJ judgments, this principle can consequently be extended to all activities, including those occurred in

---

40 "It is an obligation of conduct, not an obligation of result" stated the International Law Commission in its commentary of Article 7 concerning the due diligence that watercourse States need to exercise. International Law Commission, 'Draft Articles on the Law of the Non-Navigational Uses of International Watercourse sand Commentaries thereto and Resolution on Transboundary Confined Groundwater', Report of the International Law Commission on the Work of its Forty-sixth Session, 1994. In a similar way see also Pulp Mills, supra note 7, paras. 186–187.

41 HEATHCOTE S., *State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility*, in Bannelier K. - Christakis T. - Heathcote S. (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case*, London-New York, Routledge, 2012, p. 308.

42 International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, February 26, 2007, ICJ Reports 2007, para. 430.

43 WINGFIELD T., *The Law of Information Conflict*, U.S. Dep't. of Defense, Dictionary of Military and Associated Terms, 2000.

cyberspace[44]. At the international level, part of the community promotes application of the due diligence principle in cyberspace. Indeed, its legitimate application is cited in Rule13c[45] of the Report of the Group of Governmental Experts (GGE) *On Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*[46] and in Rule number 5[47] of the *Tallinn Manual 1.0*[48]. Rule 13c establishes that «States should not knowingly allow their territory to be used for internationally wrongful acts using Information-Communication-Technologies (ICTs)»[49]. While Rule 5 of the *Tallinn Manual* affirms «a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States»[50].

Many State practices can be referenced to suggest that the due diligence principle could be applicable in cyberspace. One relevant example is the *American International Strategy for Cyberspace*, which includes due diligence in cybersecurity as a new and essential emerging norm in this context, defining it as: «the responsibility of States to protect information infrastructures and secure national systems from damage or misuse». Similarly, Italy asserts that the obligation of due diligence applies to cyberspace. Consequently, it requires States to adopt all reasonable measures concerning activities conducted within cyberspace under their jurisdiction, to prevent, eliminate, or mitigate potentially significant harm to the legally protected interests of another State or the international community. Furthermore, Italy maintains that due diligence is an obligation of conduct, not of

---

44 BANNELIER-CHRISTAKIS K., *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?*, in «Baltic Yearbook of International Law»,14(2014), p. 5.

45 UN Doc A/76/135, July 14, 2021.

46 The constitution of Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security was established by United Nations General Assembly Resolution 73/266. The Group of Experts comprises 25 members representing major UN Member States. The primary goal of the Report, and the ongoing analytical work by the GGE, is to promote "a common understanding and effective implementation of potential cooperative measures to address existing and potential threats in the realm of information security." Although the norms on Responsible State Behaviour are not legally binding, their development reflects a consensus of thoughts and practices supported by numerous states, which in turn fosters the creation of binding customary practices.

47 SCHMITT M., NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge UP, 2013. p. 26.

48 To facilitate the application of international law to the cyber context, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), inspired by the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, established a Governmental Group of Experts (GGE) to draft a manual aimed at assisting in the application of jus ad bellum and jus in bello in the context of cyber warfare. As a result of this initiative, the Tallinn Manual on the International Law Applicable to Cyber Warfare 1.0 and 2.0 was produced, with the most recent edition published in 2017. However, some academics and non-Western states such as China and Russia have raised concerns regarding the drafting of the aforementioned Manual. The primary criticisms focus on the composition of the Group of Experts, which is perceived to be overly representative of a "Western" perspective; nine out of the 23 members were American, while none were from countries like Russia, China, Iran, or Israel. Additionally, there is insufficient analysis of the principle of non-intervention, and the threshold at which a cyber operation can be considered “use of force” has not been definitively established. Moreover, the criteria for attribution are also not thoroughly discussed. Sources: SCHMITT M., *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge UP, 2013; FLECK D., *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manua*l, in «Journal of Conflict and Security Law», 2013, pp. 331-335.

49 Vedi *supra* note 44 p. 10.

50 Vedi *supra* note 46.

result. Therefore, a State that demonstrates its commitment to halting or limiting the execution of illicit cyber activities initiated from or transiting through its territory cannot be held responsible for failing to achieve these goals (cessation or limitation of the illicit activity)[51]. In addition to these three examples, statements from other States can be used to support the opinion that due diligence constitutes a general international obligation for every State not to knowingly allow its territory to be used for internationally wrongful acts involving cyber means. Some of the States that have adopted this approach are: Australia[52], Czech Republic[53], Estonia[54], France[55], Germany[56], Japan[57], the Netherlands[58], Norway[59], Switzerland[60], and Sweden[61].

To conclude the evaluation of the due diligence application in cyberspace, deserved to be mention the position expressed by the Council of the European Union in its *Declaration on a Common Understanding of International Law in Cyberspace*, approved on November 2024. In the annex, and more precisely at its point 3, it is asserted as follows: «Due diligence is a principle of International Law that applies in the cyber context […]. As States have jurisdiction over ICT infrastructure and individuals as referred to in Section 1 above[62], they are required to make efforts that this ICT infrastructure is not used by non-state or State actors for acts contrary to the rights of other States, once they know or ought to have known of such activities. States are required to take all appropriate and reasonably available and feasible measures […] to act against cyber operations that violate rights of another State under International Law. The same duty applies for cyber activities within the territory or ICT infrastructure that they otherwise effectively control»[63].

Having established the origins of the obligation and its hypothetical application in cyberspace, it could be argued that a State's failure to exercise due diligence commit an internationally wrongful act. At the same time, invoking the international responsibility regime for such acts would require determining when a State is considered to have violated the due diligence obligation in the context of cyberspace activities. To do so, is essential referring to the text of the provision and, specifically, to the Rule13c of the GGE Report[64], which best represent the opinion of the international community concerning due diligence application in cyberspace. Reading the text of Rule 13c, it is certain that to invoke international responsibility is first necessary demonstrate that the State from whose territory the cyberattack is

---

51 *Italian Position Paper on International Law and Cyberspace*, 2021, pp. 6-7, italian_position_paper_on_international_law_and_cyberspace.pdf (esteri.it)

52 Australia's International Cyber Engagement Strategy (dfat.gov.au)

53 czech-republic-oewg-pre-draft-suggestions.pdf (un-arm.org)

54 president.ee

55 National position of France (2019) - International cyber law: interactive toolkit

56 on-the-application-of-international-law-in-cyberspace-data.pdf (auswaertiges-amt.de)

57 100200935.pdf (mofa.go.jp)

58 Letter to the parliament on the international legal order in cyberspace | Parliamentary document | Government.nl[59]

59 A-76-136-EN.pdf (un-arm.org)

60 Switzerland's Position Paper on the Application of International Law in Cyberspace • Page 1 • UNIDIR Cyber Policy Portal Database

61 Sidan kan inte hittas - Regeringen.se

62 Section 1 of the Council of the European Union, *Declaration on a Common Understanding of International Law in Cyberspace*, 18 November 2024, Brussels, Press Release No. 1234/24, reads as follow: States exercise territorial jurisdiction over Information and Communications Technology (ICT) infrastructure located in their territory, and persons engaged in cyber activities, within their territory.

63 *Ibidem*.

64 Vedi *supra* note 48.

carried out must be aware about that. Such knowledge can be considered constructive if, under normal circumstances, the State would or should have been aware of the harm coming from its territory or infrastructures under its control and jurisdiction. The concept of constructive knowledge related to due diligence in cyberspace, is well supported by several States, such as Finland, Northway, Romania and Switzerland[65]. However, this perspective does not obligate a State to implement preventive measures with its cyber infrastructure, nor does it require the State to monitor all its infrastructure to stay informed about potential transboundary harm[66]. Indeed, States can interdict a cyberattack only if they are aware about that but, in cyberspace, the time between an attack initiation and conclusion is very limited and the real origin of a cyberattack can be falsified. Indeed, it is easy for both State and non-state actors falsifying the true origin of attacks, using, for example, a simple VPN[67]. Moreover, States frequently use proxies to conduct cyber activities with the intent of denying attribution[68]. To solve this problem, and not incur in a false attribution, the applicant must provide solid, unbiased evidence showing the respondent should have known about the cyberattack. This may include expert testimony on network logs or documentary evidence like press reports. An international tribunal can also appoint its own experts to verify the reliability of such evidence[69].

The second aspect to verify is if the cyberattack is contrary to the rights of another State. Only cyberattacks of a certain level of gravity will engage a State's due diligence obligation. Indeed, the obligation deals with only cyberattacks that amount to an internationally wrongful act[70] and which result in serious adverse consequences for the target State. Under the laws of state responsibility, harm is not a prerequisite for identifying an internationally wrongful act. However, in cases involving due diligence, the existence of damage is essential to confirm a breach of the primary rule[71]. To understand when the "serious injury" trigger the due diligence obligation in cyberspace, could be useful mentioning the definition of "unlawful cyber act" provided in the *Tallin Manual 1.0*. Accordingly, an "unlawful [cyber] act" is defined as any cyber activity originating from one State"s territory that impacts the rights of other States, resulting in a negative outcome[72]. To better understand the level of harm required to trigger the due diligence obligation in cyberspace, it is useful to analyse the various definitions provided by relevant academics and international documents. For instance, the *Tallinn Manual* 1.0 suggests that physical damage to objects or harm to individuals is not always necessary to classify a cyberattack as unlawful[73]. The notion of "serious injury" is assessed retrospectively and does not dictate what actions a State should take during

65 KASTELIC A., *Due diligence in cyberspace* …p.13.

66 TALBOT JENSEN E., *The Tallinn Manual 2.0: Highlights and Insights*, in «Georgetown Journal of International Law 735», Vol. 48 (2017), p. 745.

67 VPN: Virtual Private Network, a virtual private network that ensures privacy, anonymity, and security through a dedicated communication channel created over a public network infrastructure. Source: LOMBARDO S., *VPN: cos'è, come funziona e per cosa viene utilizzata una rete privata virtuale*, Cybersecurity 360, 2022, VPN, cos'è la Virtual Private Network e quali sono i vantaggi (cybersecurity360.it)

68 TALBOT JENSEN E., *The Tallinn Manual 2.0:* …, op. cit., pp. 745-746.

69 LIU Y.I., *State Responsibility* …op. cit., pp. 239-240.

70 Draft articles on Responsibility of States for Internationally Wrongful Acts (ARISWA), 2021, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries - 2001 (un.org)

71 LIU Y.I., *State Responsibility* …op. cit., pp. 242.

72 SCHMITT M., NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual* …op. cit., p. 26.

73 *Ibidem* (Rule 1 and 5).

the attack itself. To support this view, reference can be made to Professor Roscini's definition of cyberattacks, where he noted that those causing physical damage comparable to conventional attacks could amount to the use of force or an armed attack. He also affirmed that cyberattacks targeting National Critical Infrastructure[74] could also meet the threshold of the use of force[75]. In the hypothetical event of a cyber-attack causing this level of damage, the State that suffers the damage is more likely to invoke a violation of Article 2(4) of the UN Charter[76] or the right of self-defence enshrined in article 51 of the UN Charter[77], rather than focusing on the due diligence obligation. Consequently, this high threshold of injury is inappropriate for triggering due diligence in cyberspace, instead, a lower level of damage should also be sufficient to activate (cyber) due diligence. According to the paper elaborated by Professor Liu, a cyberattack is considered "destructive" and results in "serious injury" once it causes significant disruptions to a network's functionality. Due diligence obligations should be triggered as soon as the initial injury incapacitates the network, reaching the threshold of "destructiveness"[78]. To determine whether a cyberattack is "destructive", a relevant and useful definition is the one elaborated in the *Budapest Convention on Cybercrime*[79], which defines system interference as «the serious hindering […] of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data». Considering the network interdependency, cyberattacks could cause consequent harm to society without physical damages. As a consequence, cyberattacks which provoke temporary or permanently loss of network's functionality that provide essential services, like transport, healthcare, communications etc. can trigger due diligence obligation.

For a complete analysis of the concept of "serious injury", it is also important to consider the types of cyberattacks that are deemed to have an insufficient level of injury to trigger the obligation. One of this category is represented by cyber exploitation activities, which are defined as an "unauthorized access to computers, computer systems, or networks, in order to exfiltrate information, but without affecting the functionality of the accessed system or amending/deleting the data

---

74 Vedi *supra* note 1.

75 ROSCINI M., *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, 2014, pp.52-58.

76 Article 2 (4) of the UN Charter reads as follows: «All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations». *Charter Of The United Nations And Statute Of The International Court Of Justice*, San Francisco 1945, https://treaties.un.org/doc/Publication/CTC/uncharter.pdf

77 Article 51 of the UN Charter reads as follows: « Nothing in the present Charter shall impair the inherent right of individual or collective self defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security». *Charter Of The United Nations And Statute Of The International Court Of Justice*, San Francisco 1945, https://treaties.un.org/doc/Publication/CTC/uncharter.pdf

78 LIU Y.I., *State Responsibility* …op. cit., pp. 248.

79 The Budapest Convention on Cybercrime, also known as the Council of Europe Convention on Cybercrime, is the first international treaty designed to address internet and computer crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation between countries. Adopted in 2001, it remains a key instrument for combating cybercrime globally. Too know more about the Budapest Convention see: Budapest Convention - Cybercrime (coe.int).

resident therein"[80]. For the purposes of this paper, since cyber exploitation does not cause a loss of functionality or physical injury, it cannot be classified as a cyberattack that would trigger the due diligence obligation. In addition to the two elements, another requirement needs to be fulfilled to invoke due diligence obligation violation, namely, the "feasibility measures". The "feasibility" of measures for a State will depend on the technical and financial resources at its disposal. Indeed, a State will not breach International Law if it does not successfully end or prevent a cyberattack stemming from its territory which is too complex to be controlled by its capabilities. Furthermore, even in instances where States have the capacity to prevent harmful cyber operations carried out in their territory, they are under no obligation to do so when it would be unreasonable in the circumstances (denial its essential services to hamper the attack). To better understand the types of measures required, it is helpful to examine the non-exhaustive list provided in Rule 13C of the GGE Report. Some of them include: (a) States are expected to take reasonable, proportionate, and effective steps within their capacity to end ongoing activities in their territory, consistent with international and domestic law, although it is not expected that States monitor all ICTs activities within their territory; (b) States aware of, but unable to, address wrongful ICTs acts within their territory may seek assistance from other States or the private sector, adhering to international and domestic laws. Establishing structures for assistance requests can aid implementation. States should act in good faith and not exploit the situation for malicious activities against the requesting State or third States; (c) An affected State should notify the State from which the activity originates. The notified State should acknowledge receipt to facilitate cooperation and make efforts to determine if a wrongful act occurred. Acknowledgement does not indicate agreement with the notification[81].

Having concluded the analysis of the due diligence obligation, it can now be argued that it is possible to apply this obligation in cyberspace. However, as of today, its application still depends on the willingness of States. Moreover, the difficulty in applying and invoking it in the event of a possible violation is objectively significant. The primary critical concern pertains to the unique characteristics of cyberspace, which render more difficult identify the origin of the attacks and consequently attribute the conduct to a State. A clearer definition of the legal characteristics of the due diligence obligation in relation to cyberspace could certainly promote its application, thereby reducing the number of potential cyberattacks, regardless of whom they are directed against. In this sense, it could be interesting to better define the obligations derived from this provision, such as the list indicated in Rule 13c. What is encouraging is the expanding State practice supporting the application of the due diligence principle in cyberspace. A prominent example of this tendency is represented by the Council of the European Union Declaration, which may pave the way for similar approaches by other States.

To further elaborate on this topic, the ViaSat case study serves as an illustrative example that allows for an examination of the application of the due diligence principle in cyberspace, particularly in relation to cyberattacks targeting the ground segment of space systems.

[80] ROSCINI M., *Cyber operations* …op. cit., p.17.
[81] UN Doc A/76/135, 2021, p. 10.

3. ViaSat cyberattack and the application of the due diligence

3.1. Technical characteristics of ViaSat cyberattack

Prior to examining the general characteristics of the cyberattack in question, it is essential to clarify the rationale for specifically applying the due diligence principle to cyberattacks targeting the ground segment. Firstly, cyberattacks are more likely to exploit vulnerabilities in the ground segment, making it a critical focal point for such analysis. Moreover, a comprehensive legal examination of cyberattacks directed at the link or space segments of a space system would also require addressing the application of the due diligence principle in the outer space domain, a topic that would necessitate an entirely separate and extensive study.

Having clarified this, it is appropriate to dedicate some attention to the characteristics of the ground segment of a space asset. The ground segment is essential for communication between satellites and user terminals, encompassing infrastructure such as gateway stations, control systems, and network management facilities like the Network Control Centre (NCC) and the Network Management Centre (NMC), which manage satellite access requests. It also includes earth terminals and user receivers that transform satellite signals into usable data for devices such as modems, antennas, and mobile phones[82]. Command and control systems ensure satellite functionality, and for LEO constellations, numerous globally distributed ground stations are required to maintain communication[83].

The ground segment value chain comprises interconnected processes and stakeholders involved in operating satellite communication infrastructure. It is divided into three blocks: a) Upstream: Includes hardware and software for operations, such as antennas and modems, along with launch facilities and networks connecting ground segment components; b) Midstream: Covers mission support activities like satellite control, signal downlinking, and data retrieval; c) Downstream: Focuses on data processing, storage, and analytics-based services after reception. This segmentation ensures efficient and reliable satellite communication system operations[84].

Having provided some general notions about the function and structure of the ground segment, it is now time to shift attention to the ViaSat cyberattack. On February 24, 2022, Viasat"s KA-SAT network suffered a major disruption caused by a malware-based wiper attack that rendered thousands of end-user terminals inoperative[85]. As clarified by ViaSat in a subsequent press release, the attack specifically targeted a "consumer-oriented partition" of the KA-SAT network, including Tooway, SurfBeam2, and SurfBeam2+ Internet modems, rather than the satellite itself[86]. The consequences of the attack were widespread, affecting users not only in Ukraine but across Europe.

In Ukraine, the attack impacted key users such as the government, military, and security services. The disruption extended beyond Ukrainian borders, affecting

---

82 CASARIL F. - GALLETTA L., *Securing SATCOM user segment: A study on cybersecurity challenges in view of IRIS*, in «Computers & Security» 140 (2024), p. 3. http://dx.doi.org/10.1016/j.cose.2024.103799.

83 PwC, 2020. Market perspectives of ground segment as a service (gsaas).

84 *Ibidem*.

85 Viasat News Blog, 2022. Ka-Sat network cyber-attack overview. KA-SAT Network cyber attack overview - Viasat.

86 *Ibidem*.

around 9,000 users of the French NordNet satellite broadband service[87] and nearly 15,000 customers of BigBlu, a British provider, across Germany, France, Hungary, Greece, Italy, and Poland[88]. Enercon, a German energy company, also experienced operational setbacks, losing remote monitoring and control over its 5,800 wind turbines due to their reliance on the KA-SAT network"s SCADA system[89].
Interestingly, the segment of the network targeted in the attack is owned by ViaSat, a U.S.-based company, but operated by Skylogic, a subsidiary of Eutelsat. The attack unfolded in two distinct stages[90]: a) Denial-of-Service Attack: exploiting vulnerabilities in the authentication mechanisms of Viasat modems, particularly in Ukraine and Germany, to gain unauthorized access to the ground and user segments. This caused a service outage that took several days to fully resolve; b) Network Infiltration: leveraging a separate vulnerability in Skylogic"s VPN appliances to breach the ground network management segment. The attackers moved laterally within the network, disrupting communications for over 15,000 users, including governmental and military entities.
The case study clearly demonstrates the direct interconnection between space and cyberspace, highlighting the critical vulnerabilities that permeate satellite communication systems with respect to cyberspace. It is now possible to try to attribute to the Russian Federation the violation of the due diligence obligation.

3.2. Attempt to attribute to the Russian Federation the breach of the due diligence obligation in relation to ViaSat cyberattack

Before evaluating the alleged violation of the due diligence obligation by the Russian Federation, it is important to examine the international response to the wrongful act in question. A few months after the cyberattack on satellite communication networks, the United States[91], the United Kingdom[92], and the European Union[93] publicly attributed responsibility for the attack to the Russian Federation. The first authority to hold Russia accountable for the February 24 cyberattack was the European Union's High Representative, Josep Borrell, followed by representatives from the United States, the United Kingdom, Canada, and Estonia[94]. Additionally, the United Kingdom's National Cyber Security Centre (NCSC) declared it was "almost certain" that Russia was behind the attack[95]. Furthermore, some U.S. officials claimed that Russian military hackers were responsible for the cyberattack on the satellite service. However, Saloni Sharma,

87 ConnexionFrance, 2022. Thousands in France lose Internet in suspected Russian cyberat tack. Thousands in France lose internet in suspected Russian cyberattack.

88 Techq, 2022. Thousands of Internet users go dark in Europe from 'cyberattack'. Technology News | TechHQ | Latest Technology News & Analysis.

89 ENERCON, 2022. Over 95following disruption to satellite communication. Enercon turbines disrupted by satellite cyber attack - Modern Power Systems.

90 Reversemode, 2022. VIASAT incident: from speculation to technical details. VIASAT incident: from speculation to technical details.

91 BIEIESEKER C., *US and EU Officials Attribute Viasat Cyber Attack to Russia*, Via Satellite, 2022, US and EU Officials Attribute Viasat Cyber Attack to Russia - Via Satellite (satellitetoday.com)

92 VILLANCE C., *UK blames Russia for satellite internet hack at start of war*, BBC News, 2022, UK blames Russia for satellite internet hack at start of war (bbc.com).

93 BIEIESEKER C., *US and EU Officials Attribute* …op. cit.

94 Council of the EU. (May 10, 2022). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union [Press release], Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - Consilium (europa.eu)

95 VILLANCE C., *UK blames Russia for satellite* … op. cit.

spokesperson for the National Security Council, stated: «At this time, we have no attribution to share and are closely examining the issue»[96]. When asked about the responsibility for the cyberattack, Victor Zhora, Deputy Chief of the State Service of Special Communications and Information Protection, Ukraine's main Cybersecurity Agency, responded: «We do not need to attribute it as we have clear evidence that it was organized by Russian hackers to disrupt the connection among customers using this satellite system»[97]. It worths mentioning that after the cyberattacks, Russia fell victim to a hacking operation that resulted in the loss of control over two of its satellites. The Russian Space Research Agency (ROSCOSMOS) commented on this incident, stating: «A cyber operation that caused the loss of contact between its reconnaissance satellites and the ground station is considered an act of war»[98].

In order to understand whether Russia has breached its due diligence obligation, it would be preferable to use as a reference the GGE Report *On Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* rather than the *Tallinn Manual 1.0 or 2.0*. This preference is due to the fact that, first of all, a representative of the Russian Federation is a member of the GGE and secondly, the *Tallinn Manual*s represent a minority of States within the international community while the GGE Report involves many countries located all over the world.

Reporting on Rule 13c: «States should not knowingly allow their territory to be used for international wrongful acts using ICTs»[99]. As better explained in section 2.1, the provision implies that if a State is aware of or is notified in good faith that an internationally wrongful act, conducted with the assistance of ICTs, originates from or transits through its territory, it must take all appropriate and reasonably available and feasible measures to identify and address the situation. Furthermore, Rule 13c prohibits a State from allowing another State or a non-state actor to use ICTs within its territory to commit internationally wrongful acts[100].

In the context of the ViaSat case study, assessing whether the Federation breached its due diligence obligation involves examining whether Russia, upon being aware of the wrongful act originating from or transiting through its territory, took all necessary measures to address the situation. Regarding knowledge of the wrongful act, it is undeniable that Russia was aware of the cyberattack targeting the Ka-Sat network. This assertion is supported by the fact that the cyberattack occurred just hours before the actual invasion by Russian troops into Ukrainian territory. This timing provided a significant advantage to Russian forces by "blinding" the Ukrainian command and control chain. Therefore, it is highly probable that the wrongful act was perpetrated by Russian intelligence services or, alternatively, organized and planned by Russia itself, thus making it fully aware of the cyberattack.

One aspect that remains impossible to verify is the exact origin of the malicious operation, which, in cyberspace, is among the most challenging elements to ascertain. Understanding this would help determine whether the act was carried out

---

96 NAKASHIMA E., *Russian military behind hack of satellite communication devices in Ukraine at war's outset, say*, The Washington Post, 2022, Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say - The Washington Post.

97 *Ibidem*.

98 VÄLJATAGA A., *Cyber vigilantism in support of Ukraine: a legal analysis*, CCDCOE, 2022, p. 3.

99 Vedi *supra* note 48.

100 Vedi *supra* subsection 2.1.

within or outside Russian territory and consequently, ascertain whether it constitutes a cyberattack "transiting or originating" from the Federation, in order to establish a violation of (cyber) due diligence. In the case at hand, assuming the attack was indeed perpetrated by the GRU[101], an entity known to utilize the information technology infrastructure of the Federation's Armed Forces along with their developed information and communication technologies for its cyber activities, it becomes highly probable that the attack originated within the Federation's territory. Given this hypothetical scenario, it can be confidently stated that not only was the Russian Federation fully aware of the wrongful act, but also that it originated from its own territory, thereby fulfilling the criteria outlined by the obligation under examination.

The second element to assess is whether the cyberattacks caused a "serious injury" to the affected State, thereby violating its rights. As discussed in subsection 2.1, a "serious injury" in cyberspace is typically considered to occur when a cyberattack results in the temporary or permanent loss of functionality of networks that provide essential services, such as transportation, healthcare, or communications etc. In this specific scenario, the loss of network functionality is undeniably evident. The ViaSat cyberattack not only disrupted the chain of command and control for Ukrainian troops but also severely impaired the communications of Ukrainian citizens and the government. Furthermore, the attack's effects extended beyond Ukraine's borders, as highlighted in section 3.1. States such as Germany, the United Kingdom, Italy, Poland and France experienced some of the repercussions. Consequently, it is reasonable to conclude that the "serious injury" criterion is fully satisfied in this case study, given the widespread and significant impact of the cyberattack.

Once it is established that the State in question was aware of the wrongful act, that it originated from its territory, and that the attack caused a "serious injury" to the affected State, a breach of the due diligence obligation can be demonstrated by showing that the Federation failed to take the actions required by this obligation. Despite the obligations have been already mentioned in subsection number 2.1, reporting it would be useful to better apply the provision in this peculiar case study. Again, some of the obligations are: a) States must take appropriate steps to stop activities within their territory, but are not required to monitor all ICTs activities; b) If a State cannot address wrongful ICTs acts, it can seek help from other States or the private sector, following laws. Establishing assistance structures can aid implementation. States should act in good faith and avoid exploiting the situation maliciously; c) An affected State should notify the State of origin of the activity, which should acknowledge receipt and cooperate to determine if a wrongful act occurred. Acknowledgment doesn't imply agreement with the notification etc[102].

At present, there is no evidence that the Russian Federation has taken steps to address the damage caused by the attack. If the hypothesized scenario were confirmed—namely, that Russia was aware of the attack's origin within its territory—it could be argued that the Federation failed to fulfil its duty to prevent, counter, or terminate the malicious activity. This would constitute a clear violation of its due diligence obligations. Furthermore, Russia's prominent capabilities in the field of information technology make it difficult to argue that a failure to act could

[101] GRU stands for Main Intelligence Directorate - outlasted the KGB when the Soviet Union collapsed in 1991 and appears to be flourishing today. To know more consult the following link: Why Russia's GRU military intelligence service is so feared (bbc.com)

[102] Vedi *supra* note 80.

be attributed to a lack of capacity. Even if Russia was, hypothetically, unable to mitigate the ongoing damage due to capacity limitations, the principle of due diligence allows for alternative avenues of compliance. For instance, Russia could have sought assistance from other States or international entities to address the situation, thereby avoiding a potential violation of its international obligations. This inaction raises concerns about the Federation's compliance with the principle itself, which obligates states to take reasonable steps to address harmful cyberattacks originating from their territory, regardless of the outcome. In conclusion, it is currently impossible to hold the Federation responsible for violating the obligation as outlined in Rule 13c of the GGE Report *on Responsible State Behaviour in Cyberspace* due to insufficient evidence and information.

Notwithstanding the fact that this specific case study is not a perfect example of the successful application of the due diligence principle in cyberspace, its primary relevance lies in highlighting cyberattacks that exploit the ground segment of a space system. This aspect is critical because it underscores the interconnected nature of space and cyberspace, which amplifies the vulnerabilities of space systems to cyber threats. As previously explained, this interconnection is significant from an international law perspective, as it allows for a focused application of the due diligence principle to a single domain—cyberspace—without necessitating an extensive evaluation of its application across both space and cyberspace. Moreover, what deserves more emphasis in the analysis is the practical application of the due diligence obligation to real-world events. Such exercises are invaluable for identifying the strengths and weaknesses associated with this obligation, thereby encouraging States to develop and promote consistent state practice in this area.

Conclusion

Given the increasing reliance of both civil society and the military sector on space services, it is imperative to mitigate, as much as possible, the vulnerabilities that could adversely affect these services. As demonstrated in this paper, the primary risks to these services currently stem from cyberattacks due to the growing interconnection between space and cyberspace. Moreover, technological advancements in both sectors render space assets simultaneously more vulnerable and resilient to cyberattacks, as technological development can be exploited for both peaceful and malicious purposes.

The due diligence obligation could play a crucial role in blocking and condemning cyberattacks that may partially or entirely, temporarily or permanently, compromise space systems, particularly their ground segments. As discussed throughout the sections of this paper, there are notable shortcomings in the current application of the due diligence obligation in cyberspace to effectively protect space systems. For instance, it may be necessary to further define the specific obligations arising from this principle, such as those outlined in Rule 13c. Adopting a broad and flexible approach to the measures that States can implement to avoid breaching this obligation could prove beneficial. Such an approach would clarify how to correctly apply and adhere to the obligation, thereby facilitating its implementation through national, regional, and international policies. Another issue that requires resolution is the attribution process. As previously emphasized, cyberspace is a domain where States and non-state actors can operate maliciously without being held accountable for their actions. To address this problem, it is essential to develop technical capabilities that facilitate the identification of the original source of an attack. In the invocation process of international responsibility for alleged violations of the due

diligence obligation, the technological process of attribution itself will play a pivotal role. Overcoming this limitation will significantly enhance the legal process of attribution. While in environmental law it is relatively easier to identify the State responsible for a wrongful act which violates due diligence, in cyberspace establishing this link between the conduct and the perpetrator is more challenging, due to the ease with which the source of an attack can be falsified. Once this problem is resolved, the application of the due diligence obligation will become more straightforward. Consequently, this will lead to a substantial reduction in the number of cyberattacks perpetrated by both State and non-state actors.
Finally, a clear process of interpretation and application of the provision is likely to result in an increase in state practice, ultimately leading to the recognition of the due diligence obligation in cyberspace as a customary norm.

Bibliography

BACE B. - YASIR G. - UNAL T., Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems, in «Telecommunications Policy» 48 (2024).

BANNELIER-CHRISTAKIS K., Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?, in «Baltic Yearbook of International Law»,14(2014), p. 5.

BIEIESEKER C., US and EU Officials Attribute Viasat Cyber Attack to Russia, Via Satellite, 2022. BOSCHETTI N., FALCON N., FALCON G., Space Security Lesson Learned from the ViaSat Cyberattack, in «ASCEND», (2022).

BRUMFIELD C., Incident response lessons learned from the Russian attack on Viasat, CSO, 2023,

CASARIL F. - GALLETTA L., Securing SATCOM user segment: A study on cybersecurity challenges in view of IRIS, in «Computers & Security», 140 (2024).

Charter Of The United Nations And Statute Of The International Court Of Justice, San Francisco 1945.

Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No.185, adopted on 23 November 2001, entered into force on 1 July 2004.

Council of the EU. (May 10, 2022). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union [Press release].

CZOSSECK C. - OTTIS R. - TALIHÄRM A.-M., Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security, in «International Journal of Cyber Warfare and Terrorism (IJCWT)», 1(1), (2011).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

DoD Releases, DoD Commercial Space Integration Strategy, 2 April, 2024.

ERWIN S., Space Force to shore up cybersecurity as threats proliferate, Space News, 2022.

FLECK D., Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual, in «Journal of Conflict and Security Law», (2013).

HEATHCOTE S., State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility, in Bannelier K. - Christakis T. - Heathcote S. (eds.), The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case, London-New York, Routledge, 2012, p. 308.

HITCHEN T., NATO plans first commercial space strategy to spur tech innovation, Breaking Defence, 2024.

Integrating Commercial Space for Military Applications in Europe: A Challenge and Opportunity, ESPI, 2024 (para. 5).

International Court of Justice, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), February 26, 2007, ICJ Reports 2007.

International Court of Justice, Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), April 9, 1949, ICJ Reports 1949.

International Court of Justice, Pulp Mills on the River Uruguay (Argentina v. Uruguay), 20 April 2010,I.C.J. Reports 2010.

Italian Position Paper on International Law and Cyberspace, 2021.

KA-SAT Network cyber-attack overview, Via-Sat, 2022.

KAVALLIERATOS G. - KATSIKAS S., An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space, in «International Journal of Critical Infrastructure Protection», 43 (2023).

KENNY J., A general obligation of due diligence in international law?, European Journal of International Law, 2024.

KOIVUROVA T., Due Diligence, in R Wolfrum (ed), Max Planck Encyclopedia of Public International Law, 2010.

LIU Y.I., State Responsibility and Cyberattacks: Defining Due Diligence Obligations, in «The Indonesian Journal of International and Comparative Law», (2017).

LOMBARDO S., VPN: cos"è, come funziona e per cosa viene utilizzata una rete privata virtuale, Cybersecurity 360, 2022.

LYSÉN G., State Responsibility and International Liability of States for Lawful Acts: A Discussion of Principles, Coronet Books Inc., 1997.

MACHEN J., Zero trust" can secure satellite communications against cyberattack, Cybernet, 2019.

MARTINO L., Cyber e Spazio: nuovo fronte di difesa integrata, ISPI, 2022.

MCDONALD N., The Role of Due Diligence in International Law, in «Cambridge University Press» (2016).

MOSCATELLI L., Putin e putinismo in guerra, Salerno Editrice, 2022.

NAKASHIMA E., Russian military behind hack of satellite communication devices in Ukraine at war"s outset, say, The Washington Post, 2022.

NATO - Official text: Brussels Summit Communiqué issued by NATO Heads of State and Government (2021), 14-Jun.-2021.

NATO - Official text: London Declaration issued by NATO Heads of State and Government (2019), 04-Dec.-2019.

NATO - Official text: Madrid Summit Declaration issued by NATO Heads of State and Government (2022), 29-Jun.-2022.

NATO - Official text: Vilnius Summit Communiqué issued by NATO Heads of State and Government (2023), 11-Jul.-2023.

NATO - Official text: Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016), 09-Jul.-2016.

NATO Science & Technology Organization. Science & Technology Trends 2023-2043: Across the Physical, Biological, and Information Domains. Volume 2: Analysis, 2023.

OLLINO A., Due Diligence Obligations in International Law, Cambridge University Press: Cambridge, United Kingdom, 2022.

OTTIS R., Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, NATO Cooperative Cyber Defence Centre of Excellence, 2008.

PAVUR J. - MARTINOVIC I., SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research, Oxford University, 2020.

ROSCINI M., Cyber Operations and the Use of Force in International Law, Oxford: Oxford University Press, 2014, pp.52-58.

SCHMITT M., NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge UP, 2013.

SKINNER B., Military Uses of Outer Space, SSI ISSUE GUIDE: ACCESS TO AND USE OF SPACE BY GLOBAL ACTORS, 2020.

SUWIJAK C. - LI S., Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space, in « Journal of East Asia and International Law » 15, (2022).

TALBOT JENSEN E., The Tallinn Manual 2.0: Highlights and Insights, in « Georgetown Journal of International Law 735», 48(2017).

The North Atlantic Treaty, Washington DC, April 4, 1949, NATO.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, 10 ottobre 1967.

UN Doc A/76/135, July 14, 2021.

United States General Accounting Office (GAO) Report, CRITICAL INFRASTRUCTURE PROTECTION Commercial Satellite Security Should Be More Fully Addressed, 2002.

VÄLJATAGA A., Cyber vigilantism in support of Ukraine: a legal analysis, CCDCOE, 2022.

VARADHARAJAN V. - SURI N., Security challenges when space merges with cyberspace, in «Space Policy», 67 (2024).

VILLANCE C., UK blames Russia for satellite internet hack at start of war, BBC News, 2022.

WINGFIELD T., The Law of Information Conflict, U.S. Dep't. of Defense, Dictionary of Military and Associated Terms, 2000.

Giuseppe Lucci
Laureato in Ingegneria Elettrica presso l'Università degli Studi dell'Aquila, è esperto di infrastrutture critiche. Ha lavorato per Telespazio, Terna, E-distribuzione, etc. Ha completato un Executive MBA presso l'università di Tor Vergata ed il corso di Geopolitica e governo della scuola di LIMES

TRANSIZIONE ENERGETICA – GEOPOLITICA E SICUREZZA DELLE RETI ELETTRICHE

ABSTRACT

La transizione energetica rappresenta un nodo cruciale per affrontare la crisi climatica. L'attuale situazione geopolitica globale ha posto la sicurezza e l'accessibilità economica dell'elettricità in cima all'agenda politica nazionale ed Europea. Lo studio evidenzia i principali aspetti che legano la continuità dell'energia elettrica alla sicurezza nazionale. L'obiettivo è quello di comprendere che il rafforzamento delle infrastrutture elettriche non è più un'opzione, è necessità strategica.

Energy transition is a crucial focal point in addressing climate change. The current global geopolitical situation has placed the security and affordability of electricity at the top of the national and European political agenda. The study highlights key aspects linking electric power flow availability to national security. The aim is to understand that strengthening electrical infrastructure is no longer an option but a strategic need.

Introduzione

Immaginate di aprire le porte di casa vostra e trovare l'inferno. Suona drammatico, vero? Con queste parole, Antonio Guterres, il capo delle Nazioni Unite, ha descritto la situazione del nostro pianeta con un messaggio chiaro: il cambiamento climatico non è più una minaccia lontana, è qui e ora, ma non tutto è perduto. La generazione di energia elettrica attualmente è la maggiore fonte di emissioni di CO_2 a livello globale, ma è anche il settore che sta guidando la transizione energetica verso emissioni nette zero attraverso la rapida diffusione di fonti rinnovabili come il solare e l'eolico.

L'Europa e l'Italia si sono dati degli obiettivi ambiziosi per favorire uno sviluppo della società più sostenibile che per essere traguardati entro la fine di questo decennio implicano la necessità di utilizzare il 25% in meno di combustibili fossili e di triplicare la nostra capacità di produrre energia da fonti rinnovabili.

Per raggiungere questi obiettivi è necessario investire risorse nelle reti elettriche per il trasporto e la distribuzione dell'energia elettrica.

La produzione di elettricità da fonti fossili come il carbone ed il petrolio genera emissioni inquinanti che, da più di un secolo, stanno contribuendo all'aumento della temperatura terrestre, aumento che rende sempre più frequenti gli eventi climatici estremi.

Pertanto, è fondamentale promuovere fonti energetiche pulite e rinnovabili per ridurre questo impatto ambientale.
In questo contesto diventano strategiche le reti per la trasmissione e la distribuzione dell'energia elettrica, che, per soddisfare il crescente fabbisogno di elettrificazione e l'accelerata adozione delle energie rinnovabili necessitano di un significativo ammodernamento e potenziamento.
La realizzazione di nuove linee elettriche è essenziale per collegare grandi progetti di energia eolica e solare fotovoltaica ai centri di consumo, spesso situati a grande distanza dalle aree di produzione (per esempio, le centrali eoliche *offshore*).
Come una gigantesca ragnatela che avvolge il globo, le reti elettriche connettono Paesi e continenti garantendo lo scambio di energia. In pratica è come se potessimo condividere la luce del sole della Spagna con la Norvegia durante le sue lunghe notti invernali!
La rivoluzione verde e la digitalizzazione fanno si che la domanda di energia elettrica cresca esponenzialmente, basti pensare al fabbisogno di energia elettrica richiesto dai *datacenter*, che necessitano di una quantità di energia molto rilevante per il corretto funzionamento dei server.
L'attuale situazione geopolitica globale ha posto la sicurezza e l'accessibilità economica dell'elettricità in cima all'agenda politica nazionale ed Europea, e le reti elettriche, infrastrutture fondamentali per garantire un futuro sostenibile, affrontano oggi sfide senza precedenti.
Ingenti investimenti sono stati introdotti nei prossimi anni per l'ammodernamento delle reti di trasmissione e distribuzione dell'energia elettrica. Questo impegno massivo è necessario soprattutto per garantire la disponibilità e la sicurezza delle forniture di energia elettrica.
Il corretto funzionamento delle reti elettriche costituisce, quindi, un fattore chiave per la sicurezza nazionale poiché l'elettricità alimenta le infrastrutture e i servizi essenziali per il funzionamento del paese. Basti pensare che un'interruzione prolungata della fornitura di energia elettrica, non solo può rendere difficile la vita quotidiana dei cittadini, ma può anche generare effetti devastanti sulla sicurezza, sull'economia e sulla stabilità sociale di un Paese.
L'articolo evidenzia i principali aspetti che legano la continuità dell'energia elettrica alla sicurezza nazionale con l'obiettivo di comprendere che il rafforzamento della resilienza delle nostre infrastrutture elettriche non è più un'opzione, ma costituisce necessità strategica.

Geopolitica delle reti di trasmissione e distribuzione dell'energia elettrica
La transizione energetica sta creando nuovi rapporti di forza e dipendenze a livello globale ridefinendo gli equilibri geopolitici in funzione delle infrastrutture per la trasmissione e la distribuzione dell'energia elettrica e la produzione di energia verde.
Tradizionalmente, la sicurezza energetica si è basata sull'accesso stabile e sicuro ai combustibili fossili, per cui le nazioni con riserve abbondanti di petrolio e gas, come la Russia ed i Paesi del Golfo Persico, hanno esercitato una significativa influenza geopolitica.
Tuttavia, la crescente adozione delle energie rinnovabili sta riducendo questa dipendenza, spostando l'attenzione sulla sicurezza delle infrastrutture energetiche rinnovabili e sulla diversificazione delle fonti di approvvigionamento e generazione.
La necessità di realizzazione di nuovi impianti di produzione di energia elettrica da fonti rinnovabile rende quindi le reti elettriche sempre più strategiche.

Il *blackout* che ha colpito l'Italia nel 2003, causato da problematiche relative all'interconnessione con la Svizzera, ha lasciato al buio 56 milioni di italiani. Questo evidenzia come la sicurezza energetica oggi non dipenda esclusivamente dalla produzione di energia, ma anche dalla capacità di gestire reti interconnesse e resilienti.

La rete elettrica è stata tradizionalmente progettata e costruita per trasmettere l'energia elettrica in modalità *unidirezionale*, producendola generalmente nelle grandi centrali termoelettriche/idroelettriche situate in località remote, e poi trasferendola, attraverso le reti elettriche, ai centri di consumo cittadini/industriali.

La transizione energetica, prevedendo la realizzazione di innumerevoli impianti per la produzione di energia elettrica anche di piccola taglia (piccoli impianti fotovoltaici, per esempio) necessita di una rete elettrica che sia in grado di accogliere anche piccole quantità di energia, e veicolarla presso i potenziali consumatori. Questo significa che le reti elettriche devono veicolare l'energia elettrica in modalità *bidirezionale*: l'elettricità deve essere in grado di effettuare anche il percorso inverso, e questo "dettaglio" pone delle sfide rilevanti, soprattutto per quanto concerne la sicurezza delle reti.

Le reti elettriche nazionali ed internazionali per lo scambio di energia prodotta da fonti di energia rinnovabile sono già diventate cruciali per favorire la transizione energetica, si tratta di una trasformazione ormai irreversibile.

Si pensi, per esempio, all'iniziativa *Supergrid* promossa dall'Unione Europea: si tratta di una serie di progetti infrastrutturali per la Trasmissione dell'energia elettrica, che una volta completati, porterebbero al potenziamento delle interconnessioni della rete europea con altre regioni, come il Nord Africa e il Medio Oriente. In Fig. 1 è schematizzata la rete elettrica interconnessa europea. In viola sono riportate le interconnessioni per il trasporto dell'energia elettrica attraverso i cavi sottomarini, in rosso, verde, giallo e blu gli elettrodotti di Alta ed altissima tensione terrestri (Linee a traliccio e cavi interrati).

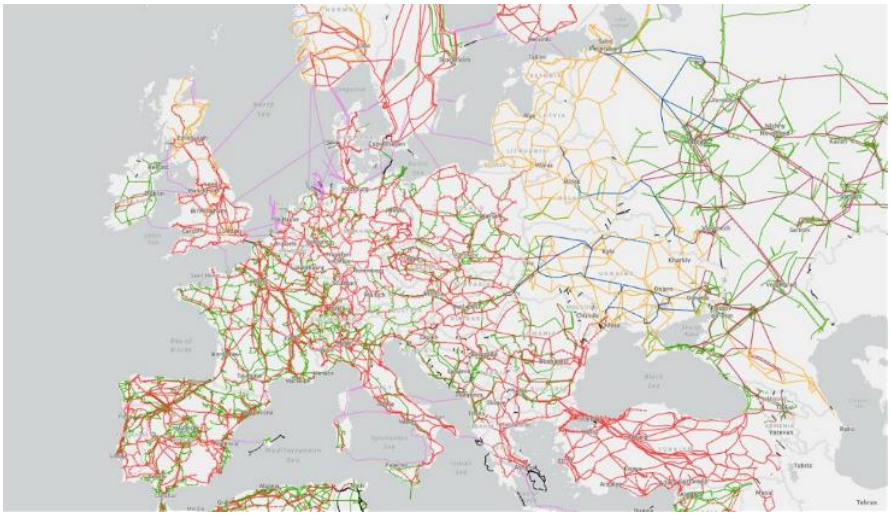


Fig. 1. Reti di interconnessione per la trasmissione dell'energia elettrica in Europa - ENTSO-E https://www.entsoe.eu/data/map/

Anche i cavi sottomarini rientrano a pieno titolo, nella competizione geopolitica. Il loro controllo riflette i cambiamenti e gli equilibri del potere globale, come ci

ricordano spesso gli analisti geopolitici: “Chi controlla i cavi sottomarini, controlla il flusso di informazioni del XXI secolo”.
La Cina, attraverso la sua ambiziosa “Via della Seta Digitale”, sta espandendo globalmente la sua influenza nella costruzione e nella gestione dei cavi sottomarini, soprattutto in Africa e Asia. Questa espansione apporta vantaggi economici e strategici, offrendo alla Cina, potenzialmente, il controllo del flusso di energia e delle informazioni in vaste aree del mondo.
Gli Stati Uniti e i loro alleati, preoccupati per le implicazioni sulla sicurezza nazionale, stanno cercando di contenere l’espansione cinese. Queste tensioni geopolitiche si riflettono in iniziative come l’aumento dei pattugliamenti navali della NATO nel Mar Baltico e nell’Atlantico, e gli sforzi dell’alleanza Quad (USA, Giappone, Australia, India) per rafforzare la resilienza dei cavi nell’Indo-Pacifico.
Un altro aspetto che lega fortemente la transizione energetica alla geopolitica è legato alla disponibilità delle materie prime. Per costruire le batterie serve il cobalto: il 60% di questo prezioso metallo proviene da un unico Paese, la Repubblica Democratica del Congo.
È una situazione che ricorda molto quella che abbiamo vissuto con il petrolio, quando pochi Paesi controllavano gran parte della produzione mondiale. Si sta sostituendo la dipendenza da un tipo di risorsa con un’altra. La buona notizia è che la scienza sta lavorando a soluzioni alternative: i ricercatori stanno sviluppando nuovi tipi di batterie che utilizzano materiali più comuni e accessibili, come il sodio (sì, lo stesso elemento che troviamo nel sale da cucina) ed il grafene. Queste innovazioni potrebbero presto cambiare le carte in tavola, liberandoci dalla dipendenza da alcuni materiali rari.
Stati Uniti e Unione Europea stanno investendo miliardi in ricerca e sviluppo con l’obiettivo del dominio del mercato delle energie pulite, oggi in mano principalmente alla Cina. Questo potrebbe portare ad una polarizzazione tecnologica che andrebbe ad influenzare le politiche energetiche di altri stati, impattando sulla loro sicurezza energetica.
La transizione energetica è come un grande puzzle globale che stiamo ancora imparando a comporre.
Ci saranno vincitori e vinti, proprio come è successo con la rivoluzione industriale due secoli fa. I Paesi che dipendono dall’esportazione di combustibili fossili dovranno reinventarsi, un po’ come fece la Gran Bretagna quando passò dal carbone al petrolio all’inizio del XX secolo.

Sicurezza delle Infrastrutture elettriche
L’elettricità mostra la sua importanza nel momento in cui viene a mancare. I *blackout*, come ombre fugaci o tenebre persistenti, ci ricordano la fragilità della nostra dipendenza energetica.
Blackout come quelli che hanno colpito l’Italia nel 2003 sono rapidi promemoria della vulnerabilità dell’infrastruttura elettrica.
Le reti elettriche per la trasmissione e distribuzione dell’energia elettrica rivestono un ruolo fondamentale nelle dinamiche geopolitiche contemporanee, influenzando numerosi aspetti delle relazioni internazionali. Con la transizione verso le energie rinnovabili e l’integrazione delle reti elettriche, la sicurezza di queste infrastrutture diventa cruciale.
Reti elettriche sicure non solo assicurano una fornitura stabile di energia, ma proteggono anche gli interessi nazionali strategici.

La sicurezza delle infrastrutture elettriche diventa ancor più cruciale in un contesto di crescente interconnessione globale (Fig.1), in quanto, le interconnessioni offrono la possibilità di bilanciare le esigenze energetiche tra diverse regioni, ottimizzando l'uso delle risorse rinnovabili e riducendo la dipendenza dai combustibili fossili. Tuttavia, l'interconnessione aumenta anche il rischio di attacchi informatici su larga scala, con potenziali ripercussioni su più Paesi e, per affrontare queste sfide, è fondamentale sviluppare strategie di sicurezza robuste.

Le vulnerabilità delle reti elettriche sono legate prevalentemente all'obsolescenza dell'infrastruttura, ai rischi ambientali (eventi climatici estremi), alla cybersecurity, agli attacchi fisici.

La transizione energetica sta quindi ridisegnando le dinamiche geopolitiche globali e, per questo, l'attenzione dell'Europa si sta concentrando sulla protezione delle infrastrutture critiche, reti elettriche comprese.

Nel marzo 2023 è stata lanciata una *task force* UE-NATO per rafforzare la resilienza e la protezione delle infrastrutture critiche[1], con un *focus* iniziale su trasporti, energia, infrastrutture digitali e per lo spazio.

L'iniziativa è stata avviata in seguito al sabotaggio del gasdotto Nord Stream avvenuto a settembre 2022.

L'Unione Europea e la NATO condivideranno le *best practices*, con l'obiettivo di migliorare la consapevolezza situazionale, sviluppare principi chiave per migliorare la resilienza, le misure di mitigazione, e le azioni correttive.

Questa sinergia servirà a contrastare coloro che cercano di minare la sicurezza Europea e garantire che le nostre infrastrutture critiche rimangano robuste e affidabili di fronte a minacce in evoluzione.

Un altro aspetto rilevante è lo spionaggio.

L'acquisizione fraudolenta di informazioni strategiche sulle infrastrutture per il trasporto dell'energia porta inevitabilmente ad un indebolimento della sicurezza energetica; a tal proposito, da un'inchiesta realizzata dal giornalista investigativo danese Niels Fastrup, come riportato da diverse fonti giornalistiche internazionali[2], è emerso che la nave scientifica russa *Ammiraglio Vladimirsky*, che fa parte della flotta baltica della marina russa, sia stata sorpresa a navigare in prossimità di impianti eolici *offshore* nei pressi di Inghilterra e Danimarca nel Mar del Nord.

Come si evince dalla rotta della nave, indicata in Fig. 2, dopo una settimana in Scozia, la nave naviga a sud verso il Tamigi in Inghilterra a una velocità massima di circa dieci nodi, ovvero 18 chilometri all'ora.

Qui si trovano, tra l'altro, due grandi parchi eolici *offshore*.

Ancora una volta, la *Ammiraglio Vladimirsky* rallenta attorno ai parchi eolici *offshore*, probabilmente con l'obiettivo di mapparne i fondali.

---

1 European Commission Statement, 16/03/2023 - Launch of the EU-NATO Task Force: Strengthening our resilience and protection of critical infrastructure

2 Fonte DR - https://www.dr.dk/nyheder/indland/moerklagt/afsloering-russiske-spionskibe-forbereder-mulig-sabotage-mod

Fig. 2. Rotta della nave *Ammiraglio Vladimirsky DR* - https://www.dr.dk/nyheder/indland/moerklagt/afsloering-russiske-spionskibe-forbereder-mulig-sabotage-mod

Attacchi informatici (cyber security)

Le reti elettriche, oggi più che mai, sono uno degli obiettivi maggiormente sensibili nel campo della cyber security. L'agenzia internazionale per l'energia (AIE) evidenzia la criticità che gli attacchi informatici sono in aumento nel settore delle infrastrutture elettriche. Nel 2022, l'IEA ha rilevato in media circa 1.100 attacchi informatici settimanali alle infrastrutture appartenenti alla categoria *Utilities* globali, che comprende le reti elettriche[3].

Ci sono evidenze che gli attacchi informatici alle reti elettriche internazionali siano aumentati rapidamente dal 2018, raggiungendo livelli allarmanti nel 2022 in seguito all'invasione dell'Ucraina da parte della Russia. Recenti attacchi informatici nel settore elettrico hanno disabilitato i controlli remoti per i parchi eolici, interrotto la contabilizzazione dell'energia a causa di sistemi IT non disponibili e portato a ricorrenti violazioni di dati che coinvolgono nomi dei clienti, indirizzi, informazioni sui conti bancari e numeri di telefono.

La rivoluzione digitale e la transizione energetica, paradossalmente, tendono a favorire gli attacchi informatici alle reti elettriche. Questo fenomeno è dovuto principalmente all' introduzione innovativa di *smart grids*, ovvero di reti intelligenti che, da un lato, contribuiscono a gestire meglio la domanda e l'offerta di energia rendendo il sistema più efficiente, dall'altro utilizzano sistemi di comunicazione potenzialmente violabili da parte degli *hacker*.

Le *smart grids* usano sensori e tecnologie avanzate per garantire sicurezza ed efficienza nella fornitura di energia. Tuttavia, questa maggiore connessione rende le reti elettriche un bersaglio per gli *hacker*. Tre motivi principali spiegano la vulnerabilità delle reti elettriche agli attacchi informatici: la vasta diffusione delle *smart grids* offre più punti di accesso agli *hacker*, la complessità delle tecnologie usate crea punti deboli, e l'uso di tecnologie vecchie insieme a quelle moderne aumenta le vulnerabilità.

Nel marzo 2022, la rete elettrica indiana è stata vittima di un attacco informatico prolungato.

[3] IEA50 Commentary 01/08/2023 - https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

L'Insikt Group (divisione di ricerca sulle minacce di Recorded Future) ha pubblicato un rapporto rivelando tentativi di attacchi *hacker* a diverse strutture che gestiscono la rete elettrica nel Ladakh, una regione contesa tra India e Cina. Gli analisti dell'Insikt Group, come evidenziato nel report, sono riusciti a confermare che l'attacco informatico si è concentrato sui centri di dispacciamento dell'energia elettrica, ovvero al cuore del sistema di trasmissione dell'energia elettrica indiano; la loro funzione è cruciale per mantenere l'accesso ai sistemi SCADA (Supervisory Control And Data Acquisition), essenziali per il controllo e la supervisione della rete elettrica[4].

Eventi meteo estremi, sabotaggi, incidenti

Oltre alla sicurezza informatica, la resilienza fisica delle reti elettriche è l'altro aspetto decisivo che caratterizza la sicurezza di tali infrastrutture.

Gli eventi climatici estremi, resi più frequenti e intensi dal cambiamento climatico, possono danneggiare in maniera importante le infrastrutture elettriche. Tempeste, uragani e ondate di calore possono causare interruzioni del servizio, mentre le inondazioni possono compromettere le centrali elettriche e le stazioni di trasformazione. Pertanto, è essenziale che le reti siano progettate e manutenute per resistere a questi eventi e riprendersi rapidamente.

L'aumento dei rischi climatici dovuti all'innalzamento delle temperature richiede una maggiore resilienza delle reti elettriche, a causa di eventi meteorologici estremi sempre più frequenti e intensi, come ondate di calore, incendi, cicloni, precipitazioni intense e inondazioni. Questi fenomeni possono causare interruzioni di corrente su larga scala, mettendo a rischio la sicurezza dei sistemi elettrici a livello globale. L'espansione futura delle reti di trasmissione e distribuzione potrebbe aumentare l'esposizione ai cambiamenti climatici, necessitando di maggiori investimenti in manutenzione e aggiornamenti per migliorare la resilienza.

Una strategia per affrontare questi rischi è ridurre la vulnerabilità delle linee aeree di trasmissione e distribuzione che sono particolarmente esposte a incendi, inondazioni e cicloni. Un'alternativa è l'installazione di cavi sotterranei, sebbene ciò comporti costi iniziali più elevati. Tuttavia, anche le reti sotterranee sono vulnerabili alle ondate di calore, che possono causare guasti, specialmente nelle aree urbane. Altri approcci includono l'implementazione di *standard* di progettazione più elevati per i pali e le torri di distribuzione, rafforzandoli con tiranti nelle aree soggette a venti forti e spostando le linee aeree lontano dagli alberi per prevenire danni causati da incendi e venti.

Le tecnologie di telerilevamento, inclusi droni, LiDAR (Laser Imaging Detection and Ranging), immagini aeree e sistemi GIS, sono utili per la gestione della vegetazione, l'ispezione delle infrastrutture, la valutazione dei rischi e il monitoraggio dei danni in tempo reale. Queste tecnologie migliorano la priorità di manutenzione e forniscono dati critici per decisioni ottimizzate. I programmi di risposta alla domanda e le infrastrutture di comunicazione robusta sono essenziali per ridurre lo stress della rete durante eventi imprevisti, permettendo ai clienti di modificare i loro consumi in risposta a cambiamenti di prezzo o incentivi. La digitalizzazione della rete, con componenti automatizzati che permettono un rapido ripristino della fornitura, riduce il numero di clienti colpiti e migliora la sicurezza dei lavoratori.

[4] Recorded Future, China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions

Con l'evento del Nord Stream è emersa più che mai l'esigenza di proteggere le reti elettriche sottomarine. Queste infrastrutture possono essere minacciate da fenomeni naturali che ne influenzano il funzionamento, come incidenti non intenzionali causati da navi o attacchi di squali, ma anche da guerra ibrida, terrorismo, pirateria o azioni belliche condotte da attori statuali e non (si parla di vulnerabilità fisiche).
La domanda di capacità di energia elettrica e di trasmissione dei dati, guidata dall'intelligenza artificiale e dal *cloud computing*, continua a crescere[5], facendo aumentare notevolmente gli investimenti. Allo stesso tempo, i costi di installazione e manutenzione dei cavi sottomarini sono notevoli, basti pensare che le sole riparazioni possono costare diversi milioni di euro per cavo. Questo spinge verso una maggiore cooperazione internazionale nella gestione e protezione di queste risorse vitali, bilanciando gli interessi nazionali con la necessità di una connettività globale sicura e affidabile.

Fig. 3. Cavo sottomarino per la trasmissione dell'energia elettrica - https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Pianificazione della sicurezza delle reti: simulazioni di possibili Scenari futuri
I modelli di simulazione basati sull'analisi di possibili scenari futuri sono essenziali per pianificare una sicurezza energetica resiliente in grado di affrontare sviluppi geopolitici, economici e tecnologici incerti. Quest'approccio permette di esplorare scenari che vanno dal progresso accelerato delle energie rinnovabili con costi in discesa e maggiore indipendenza energetica, fino a situazioni critiche, come un'accesa competizione internazionale per le risorse strategiche.
In uno scenario di rapido sviluppo delle tecnologie di accumulo energetico come le batterie al litio di nuova generazione, i paesi potrebbero ridurre la dipendenza da importazioni di combustibili fossili, rafforzando così la propria autonomia. Al contrario, in uno scenario di crisi potrebbe prevedere una corsa al cobalto e al litio per batterie, innescando tensioni geopolitiche simili a quelle già vissute in passato per il petrolio.
Le simulazioni basate su crisi geopolitiche o cambiamenti normativi permettono di individuare vulnerabilità nelle reti di distribuzione dell'energia. Ad esempio, un aumento della frequenza di attacchi cyber in aree critiche potrebbe mettere in evidenza la necessità di protezioni avanzate nelle infrastrutture favorendo investimenti nella cybersecurity.

[5] International Energy Agency - Electricity Grids and Secure Energy Transitions & International Energy Agency - Word Energy Outlook 2023

Inoltre, in un contesto di crescente instabilità in aree ricche di minerali rari, questi modelli offrono strumenti per pianificare una diversificazione delle fonti di approvvigionamento, mitigando il rischio di dipendenze.
Di seguito vengono proposti tre scenari potenzialmente realistici che potrebbero impattare la sicurezza delle reti di trasmissione e distribuzione dell'energia elettrica:

1. *Competizione per risorse strategiche come il cobalto e il litio*: La crescente domanda di minerali critici come cobalto e litio essenziali per le batterie e le tecnologie di accumulo energetico, è ampiamente documentata. L'Agenzia Internazionale per l'Energia (AIE) conferma come la domanda di questi minerali sia destinata a crescere, generando tensioni geopolitiche, soprattutto per i paesi dipendenti da forniture esterne[6].
2. *Sviluppo accelerato delle tecnologie di accumulo energetico*: Il progresso nelle batterie al litio e altre tecnologie di stoccaggio potrebbe far sì che i costi delle batterie diminuiscano rapidamente grazie ai miglioramenti tecnologici favorendo l'indipendenza energetica di vari paesi e riducendo la dipendenza dalle fonti fossili[7].
3. *Attacchi cibernetici alle infrastrutture critiche*: La necessità di investire in protezioni avanzate è stata evidenziata, per esempio, da recenti attacchi informatici subiti da infrastrutture per la trasmissione dell'energia elettrica nel mondo. La divisione di ricerca sulle minacce cyber di Recorded Future ha pubblicato un rapporto rivelando prove di tentativi di hackerare 21 indirizzi IP associati a 10 componenti della rete elettrica indiana, oltre a 2 infrastrutture portuali[4].

L'approccio della pianificazione delle risorse basata sullo studio di scenari plausibili coniuga la risposta alle minacce con la massimizzazione delle opportunità, contribuendo alla costruzione un sistema energetico più robusto e flessibile per affrontare il futuro.

Conclusione

La transizione energetica è ormai una necessità improrogabile per affrontare la crisi climatica, ma il suo successo dipende dalla nostra capacità di proteggere e adattare le infrastrutture che ne costituiscono il cuore pulsante. Le nostre reti elettriche, vere e proprie arterie della società moderna, si trovano oggi di fronte a sfide senza precedenti. Da un lato devono resistere a eventi meteorologici sempre più estremi, dall'altro devono difendersi da sofisticati attacchi informatici e fisici che potrebbero paralizzare intere nazioni.
La geografia delle energie rinnovabili, inoltre, sta ridisegnando la mappa del potere energetico globale, sostituendo le vecchie dipendenze da petrolio e gas con nuove vulnerabilità legate alle materie prime critiche per la transizione verde.
In questo scenario complesso, la resilienza delle infrastrutture elettriche diventa cruciale quanto la loro sostenibilità: servono reti più intelligenti, capaci non solo di trasportare energia pulita, ma anche di isolare rapidamente i problemi prima che si trasformino in crisi su vasta scala.
La collaborazione internazionale, attraverso iniziative come quelle di UE e NATO diventa fondamentale per costruire una difesa comune contro queste nuove minacce.
Il futuro della nostra sicurezza energetica si gioca quindi su un delicato equilibrio tra innovazione tecnologica, cooperazione geopolitica e protezione delle

[6] International Energy Agency – Global Critical Minerals Outlook 2024
[7] Interna International Energy Agency – Global EV Outlook 2023

infrastrutture: solo gestendo questa complessità potremo garantire che la transizione verso un mondo più sostenibile non ci renda paradossalmente più vulnerabili, ma ci conduca verso un futuro più sicuro e resiliente.
Nei prossimi anni le scelte strategiche dei governi e degli operatori energetici determineranno se le reti elettriche diventeranno un pilastro di stabilità o un potenziale tallone d'Achille della sicurezza nazionale. Diventa quindi molto utile, per avere un quadro più articolato dei rischi e delle opportunità, lo studio di scenari alternativi per i prossimi decenni; scenari basati su modelli predittivi che esplorino come diversi percorsi geopolitici, economici e tecnologici potrebbero influenzare la sicurezza energetica nazionale, europea e globale.

Michael Selis
Laureato presso l'Università di Pisa in "Storia e Civiltà" è attualmente dottorando di interesse nazionale in "Studi europei", curriculum "Storia dell'integrazione europea e dell'idea d'Europa", presso l'Università di Genova e l'Università G. "D'Annunzio" di Chieti-Pescara

ENVIRONMENT, CLIMATE CHANGE AND SECURITY: NATO'S ACTION PLAN AND THE ARCTIC STRATEGY

ABSTRACT

Nel giugno 2022 la NATO ha definito il cambiamento climatico «an overarching challenge of our time» dichiarando di voler divenire «the leading international organization when it comes to under-standing and adapting to the impact of climate change on security». Di conseguenza, l'obiettivo atlantico risulta essere molto ambizioso: da un lato rispettare i punti pre-visti dell'agenda ambientale, mentre, dall'altro, riuscire a mantenere in essere le tre funzioni dell'Alleanza, ossia la difesa collettiva, la gestione delle crisi e la sicurezza dello spazio euro-atlantico. Il seguente paper cerca di analizzare le iniziative intraprese dall'Alleanza negli ultimi anni volte a contrastare il cambiamento climatico e la strategia securitaria che sta adottando in una delle aree maggiormente coinvolte dal fenomeno di cui sopra, ovvero la regione artica.

In June 2022 NATO defined climate change as an «overarching challenge of our time» declaring its desire to become «the leading international organization when it comes to understanding and adapt-ing to the impact of climate change on security». As a result, the Atlantic goal turns out to be very ambitious: on the one hand, to comply with the planned points of the environmental agenda, while on the other hand, to keep in place the three core tasks of the Organization namely, collective defense, crisis management and cooperative security. The following paper seeks to analyze the initiatives undertaken by the Alliance in recent years aimed at combating climate change and the securitarian strategy it is adopting in one of the areas most af-fected by the above phenomenon, namely the Arctic region.

Keywords: NATO Action Plan, Climate Change Agenda, UN 2030 Agenda, Sustainability and Complexity, Integration, Cooperation and Adaptation, Arctic Scenario.

Introduction

Despite the recent significant trust issues between the scientific and political realms and a portion of the citizenry, it's clear that climate change has become a tangible phenomenon. Consequently, major international organizations and numerous countries across the globe are earnestly striving to construct comprehensive global strategies aimed at mitigating CO2 emissions. In her *The Sixth Extinction: An Unnatural History*, Pulitzer Prize winner E. Kolbert (2014) seeks to demonstrate, through precise empirical data, the dramatic consequences that climate change is generating. The main question posed by the American journalist is as simple as it is

dramatic: what future will befall Homo Sapiens? Will it go extinct, as happened to other animal species during the previous Big Five, or will it be able to create cooperative strategies to avoid catastrophe?
The first fact to start with is that a challenge of this magnitude cannot be met using old-fashioned schemes. Nations, taken individually turn out to be dysfunctional and rather anachronistic in this scenario. Consequently, there is a need to abandon the Cold War nationalist/vertical mindset and embark on the path of global/horizontal cooperation (Pitasi, 2021). Because as M. Gorbachev (1988) once said in *Perestrojka*: «We are all passengers aboard one ship, the Earth». The ambitious goal of the NATO agenda, on the other hand, fully demonstrates this: to marry sustainability with complexity.
A mission achievable only through the action of a complex and multilevel organization, which NATO is, precisely. The world is changing and evolving with shocking speed. Decisive challenges await us, which will be rather complex just like the new world we are aiming to build. Since NATO is an organism capable of moving in different areas, its strategic framework is multifaceted. Five assets emerge primarily in the new Atlantic strategy, also reaffirmed during the latest meeting in America on the occasion of the 75th Anniversary of the Alliance (NATO Washington Summit, 9-11, 2024):

A. Donbas war: deactivation of the NATO-Russia Council, strengthening of the NATO-Ukraine Council (2023) and activation of the new NATO Security Assistance and Training for Ukraine (NSATU);
B. Mediterranean Dialogue: consequently, NATO's southern flank enhancement with particular focus on the area of North Africa and the Levant;
C. Open door policy: new admissions of Sweden and Finland (2023-2024); ongoing negotiations for Ukraine;
D. Indo-Pacific: Japan, Australia, South Korea, New Zealand. Paraphrasing former Atlantic Secretary General Jens Stoltenberg: «NATO is a regional Alliance between Europe and North America but the challenges we face are global and our security is interconnected. What happens in the Euro-Atlantic region matters for the Indo-Pacific, and what happens in the Indo-Pacific matters to the Euro-Atlantic» (Stoltenberg Declaration, 12/07/2023). The Main goal point of the Atlantic Indo-Pacific strategy is to contain China and monitor the situation in Taiwan;
E. Climate change: social, to ensure a habitable planet for future generations; geopolitical, with the monitoring of key-areas such as the Arctic region (NATO Vilnius Summit, 2023).

In the following paper I will analyze the fifth point while always keeping in mind, however, the interconnectedness and complementarity of it with the other four mentioned above.

1. Climate Change and Security Action Plan

NATO began to take an interest in environmental issues since the late 1960s when the Committee on the Challenges of Modern Society (CCMS) was launched. It was defined primarily to analyze the effects produced by air and noise pollution (NATO Environment, climate change and security, 2021). Two further steps were taken in the Nineties with the creation of the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and in 2006 with the Science for Peace and Security (SPS). The latter, having resulted from the merger of the Science Committee and the CCMS.

The progressive awareness stemmed both from increased international interest and the Alliance's ambition to move beyond its founding ontology. Another important factor was undoubtedly J. Stoltenberg's election as Secretary General in 2014. Before serving as NATO leader, he was in 2013–2014 the UN Special Envoy for Climate Change, as well as the Prime Minister of Norway from 2005 to 2013. Highly sensitive to the issue, Stoltenberg has given the North Atlantic Council (NAC) a decidedly greener footprint than his predecessors, which will also be very likely continued by the new NATO Secretary General, Mark Rutte, former Prime Minister of the Netherlands from 2010 to 2024. Of course, NATO being a military organization the humanitarian thrust alone cannot suffice, that is why climate change brings with it two sides: the humanitarian and geopolitical aspects. NAC goal is to make them complementary and integral. Climate and security, together, as stated in the fifteenth point of The Security Environment section of the 2010 Strategic Concept and by former Secretary General Stoltenberg at the last COP 28 held in Dubai December 2023.

It is an intriguing challenge that should lead the Alliance not only to reduce emissions, but also to cope with possible climate crises in the most insidious scenarios, with inevitable strengthening of crisis management and responsiveness. The authenticity of these endeavors can be discerned from the construction of the new HQs in Brussels, which stands as a state-of-the-art building meticulously aligned with the stringent sustainability standards.

Work began in October 2010 and was completed in 2017, while, its inauguration, took place in 2018. Huge windows make full use of natural energy by reducing energy consumption, while, by collecting rainwater, the building's sloping wings reduce its consumption (NATO HQs, 2024).

The heart and soul of NATO resides in its HQs; consequently, the renovation of the building is not merely an aesthetic desire, but a clear symbolic message about the new path taken. Of course, the plan is to extend a similar methodology to the numerous infrastructures around the world and to the Armed Forces. On this very last point, Atlantic soldiers are increasingly using solar panels as energy generators instead of diesel power.

Adopting renewables on training or battlegrounds also manifests itself in smart solutions, such as integrating solar panels into equipment to efficiently power electronic devices or using fuel cells and hydrogen battery to store electricity (Matera, 2020).

The Climate Change and Security Action Plan was launched at the Brussels Summit on June 14, 2021. It is a rather ambitious program: to make NATO the international leader in what concerns combating climate change. In content, spirit and modus operandi, the document is in line with the 1992 UN Framework Convention on Climate Change, the 1997 Kyoto Protocols and the 2016 Paris Agreement. The goals, in fact, are the same as the latter:

A. «Holding the increase in the global average temperature to well below 2°C above pre-industrial levels and pursuing efforts to limit the temperature increase to 1.5°C above pre-industrial levels, recognizing that this would significantly reduce the risks and impacts of climate change»;
B. «Increasing the ability to adapt to the adverse impacts of climate change and foster climate resilience and low greenhouse gas emissions development, in a manner that does not threaten food production»;

C. «Making finance flows consistent with a pathway towards low greenhouse gas emissions and climate-resilient development» (United Nations Convention-cadre sur les changements climatiques, 2015).

In addition to the international reference standards, the Action Plan aims to make a decisive contribution to Atlantic security and its three security tasks, which, I remind, are deterrence and defense, crisis prevention and management, and cooperative security (NATO Climate Change and Security Action Plan, 2021). To do this, the Alliance will essentially have to adapt to the new scenario that is being generated due to climate change, improve its awareness in the civilian, military and scientific sectors, and enhance cooperation with major international organizations such as the UN, EU, OSCE, BRICS, etc.

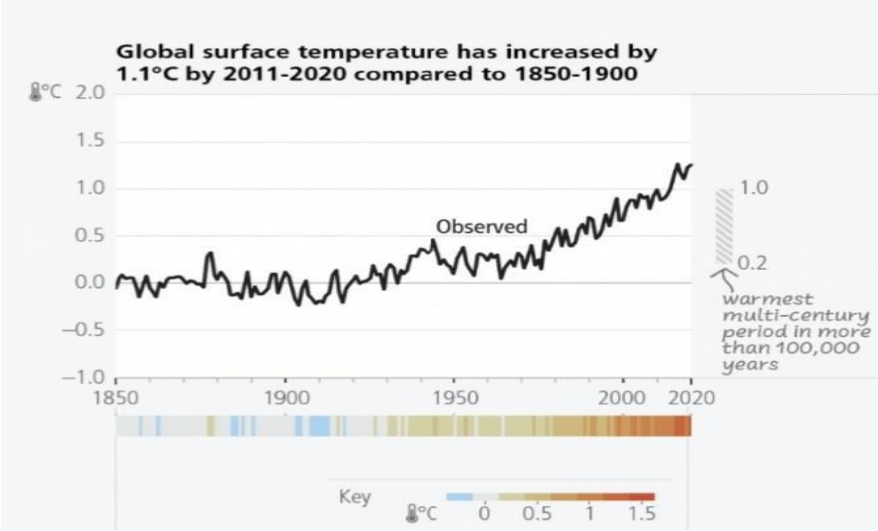
The Alliance's new commitment was confirmed a few months after the summit at the important COP26 in Glasgow (Stoltenberg Declaration, 02/11/2021). To succeed in achieving the coveted Goal 13 of the UN 2030 Agenda, world leaders have drawn up four main work sites to work on:

A. Mitigation, through reduction and/or capture military CO2 emissions;
B. Adaptation to the new environments;
C. Economic financing, with the participation of all member states of the Alliance;
D. Cooperation, as already said, with other international organizations and other nations (Stoltenberg Declaration, 31/10/2021-12/11/2021).

At the summit, Stoltenberg called climate change «a crisis multiplier» (Ivi, 02/11/2021) since it generates – in his opinion and that of a large part of the international community – huge and interconnected issues such as degradation of eco-systems across the globe, melting glaciers, rising sea levels, desertification, increasingly extreme and recurring weather phenomena or the spread of global epidemics etc., linking several social dimensions such as political, human and economic.

The out-emergence of these phenomena is a tragedy even now, but it would become catastrophic if it intensified. Not only for local populations, but also for biodiversity and, therefore, for the survival of many animal species. The data that emerged in the Sixth Assessment Report (AR6) of the Intergovernmental Panel on Climate Change (IPCC) are quite alarming (IPCC, Sixth Assessment Report, 20/03/2023). In the last fifty years there has been an unprecedented increase in temperature (*Graph.1)* compared to the previous 2000 years (considered the same time frame). Not only that, according to the report there has also been «a global mean sea level increase by 0.20 [0.15 to 0.25] meters between 1901 and 2018» (NATO Secretary General's Report, 2023).

If the necessary measures are not taken, the global temperature could reach and exceed the 1.5°C threshold in the coming decades, reaching up to 2°C. Needless to explain what the landfall toward such a scenario would entail. NATO's desire to become the world leader in combating climate change was rebadged during the Madrid Summit on June 29-30, 2022, precisely in the forty-sixth item of 2022 Strategic Concept (NATO Strategic Concept, 2022). It was accompanied by the Climate Change and Security Impact Assessment (CCSIA), a review and integration of the previous Action Plan (NATO CCSIA, 2022).



Graph.1 - IPCC Report.
At: https://report.ipcc.ch/ar6syr/pdf/IPCC_AR6_SYR_LongerReport.pdf.

1.1. Climate Change and Security Impact Assessment (CCSIA)

The nodal points of the new document were outlined by the former Atlantic Secretary Stoltenberg during the first High-Level Dialogue on Climate and Security, which was held during the Spanish Summit (Stoltenberg Declaration, 28/06/2022). As mentioned, the Allies have set themselves the task of reducing Greenhouse Gases (GHG) emissions by 45 percent by 2030 to zero by 2050.

To do so they will have to:

a) embrace an ambitious green energy revolution by effectuating a shift from fossil fuels to sustainable and renewable technologies, exemplified by the widespread adoption of electric military vehicles, and use at the same time new technologies that can make equipment more effective;
b) foster energy source diversification and supplier alternatives to mitigate reliance on a single dominant entity such as China, which holds significant control over the processing of vital materials;
c) encourage cooperation and policy coordination among all member states to prevent the emergence of a fragmented landscape of «incompatible systems»;
d) increase supply and investment in new technologies to lower their high costs;
e) supporting the research.

By helping to keep the global temperature within UN standards, the Alliance could ensure that it could help people living in the most at-risk areas by providing food, energy, water, and other essential services. Not only that, but it could also more easily secure the resilience of its strategic infrastructure and that of the Armed Forces, inasmuch as climate change related phenomena can affect at various levels military operational capabilities and performances. Prevention, preparedness, adaptation, response: these are, and will be in the near future, NATO's four watchwords.

The CCSIA was revised and supplemented in a second edition published in 2023 and containing important advice of NATO's Military Authorities (NATO CCSIA, 2023). After a brief introduction, and an equally brief final conclusion, the heart of

the document lies mainly in the analysis of the methodology to be adopted and the analysis of some key geographic areas.
The first pillar, called Methodology, aims on the one hand to control GHG emissions in the Alliance's various civilian and military infrastructures, while, on the other side, to achieve the ambitious goal of zero emissions by 2050. The overall coordination and analysis of the data collected by the various NATO facilities will then fall to the Brussels HQs and the Emerging Security Challenges Division (NATO Greenhouse Gases Emission Mapping and Analytical Methodology, 2023).
The second pillar of the renew CCSIA, called Regional Assessments and Case Studies, analysis four reference key areas: Europe, North America, Middle East-North Africa/Sahel and High North. The study sheds light on the risks that could emerge in these areas for NATO bases, civilians and the Armed Forces. In Europe, the attention inevitably falls on Naval Air Station Sigonella. This is because Sicily is one of the European areas most exposed to climate change (*Fig.1*).

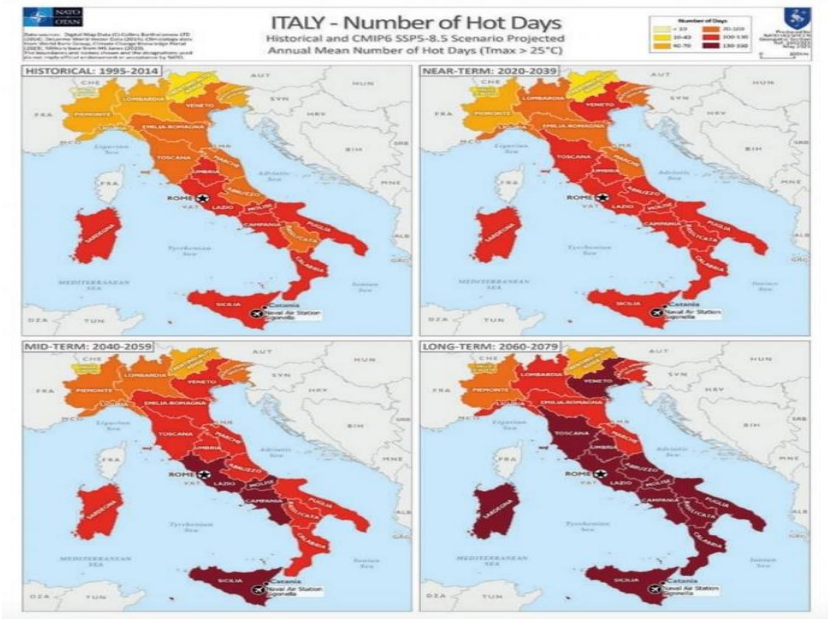


Fig.1 - NATO CCSIA Report: Italian scenario.
At: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230711-climate-security-impact.pdf.

The main danger concerns the obvious increase in heatwaves, which generate numerous problems including, increased land desertification. In North America, storms and hurricanes (level 4-5) will be increasingly frequent. The report employs Naval Station Norfolk in Virginia, recognized as the largest naval base globally, as a pertinent case study. Its protection, consequently, turns out to be of vital importance to the Allies and the United States. In addition to the above two phenomena, the greatest risk is tied to sea level rise, which could severely damage the Naval Station causing serious economic and humanitarian damage. In the third scenario, namely the Middle East (*Fig.2*) and North Africa, desertification is the greatest danger. Heat waves, wildfires, water scarcity to name just three. Leading to depletion of the local economy and instability. Two factors that could generate increased local conflicts, terrorism, and migration.

In addition to the aforementioned documents and the suggested strategy present in the renewed CCSIA, NATO will also utilize precise policy bodies to achieve its goals.
Alongside NATO's Science and Technology Organization and Science for Peace and Security, the Allies established a new Climate Change and Security Centre of Excellence in Canada at the end of 2023. This not only demonstrates Ottawa's centrality within the NAC, but also shows how determined NATO is to pursue environmental policy.

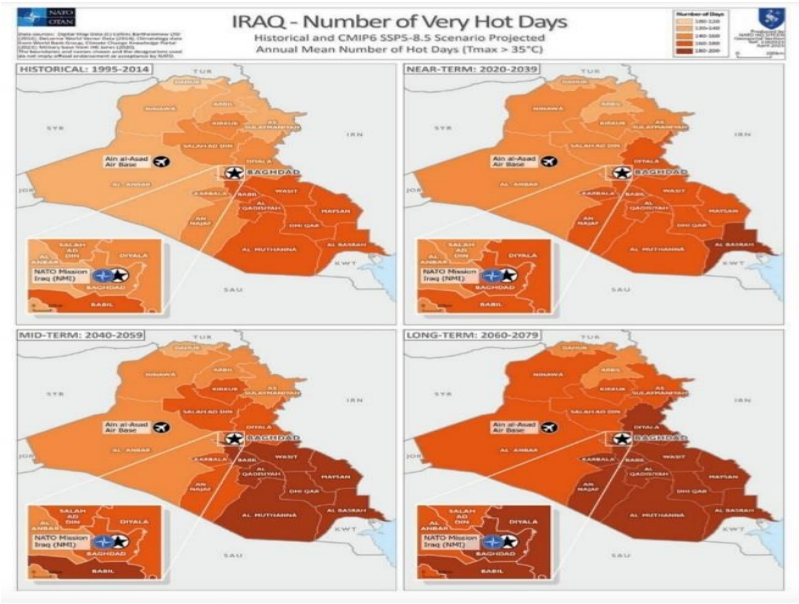


Fig.2 - NATO CCSIA Report: Iraqi scenario.
At: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230711-climate-security-impact.pdf.

The purpose of the new Center will be to provide scientific support and geostrategic expertise so as to further refine the working methodology. Naturally, for NATO to achieve the objectives we have analyzed so far, documents, speeches or Centers of Excellences, will not be enough.
Real coordination will be needed to harmonize the policies of the individual member states of the Alliance. It is crucial, therefore, for NATO, as well as the EU, to coordinate a genuine Transatlantic climate agenda among its members to ensure a cohesive and effective approach.
While cooperation will be essential for developing common strategies that address both climate challenges and security needs, it is equally fundamental to overcome endemic nationalism by strengthening, in the European case for example, external constraints (juridical, political, economic) to better coordinate the national policies of member states and harmonize the transnational and national dimensions.
The lack of a common European Defence market generates, for example, an enormous waste of public funds and increases GHG emissions creating an impasse in the process of European integration in its most delicate pillar: the Common Foreign and Security Policy (CFSP) that Europe can no longer afford to neglect.

2. The Arctic scenario: an introduction

As mentioned before, the fourth area of reference analysed in CCSIA is the Arctic region. Consequently, in the following pages, attention will be paid on the role and strategy that NATO intends to adopt in this area.

As per the findings of the IPCC report, the Arctic region has experienced two to three times more pronounced global warming in comparison to the average warming observed in other geographical areas.

Consequently, this area has acquired paramount strategic significance, entailing not only the potential access to essential resources, but also control over prospective trade routes.

The gradual opening of the Northwest Passage and the Northeast Passage for extended periods guarantees unimpeded navigation for ice-class vessels. If this trend persists, it could lead to a restructuring of global maritime choke points, resulting in an inevitable diminishment of the significance of Malacca, Suez, and Panama (*Fig.3*).

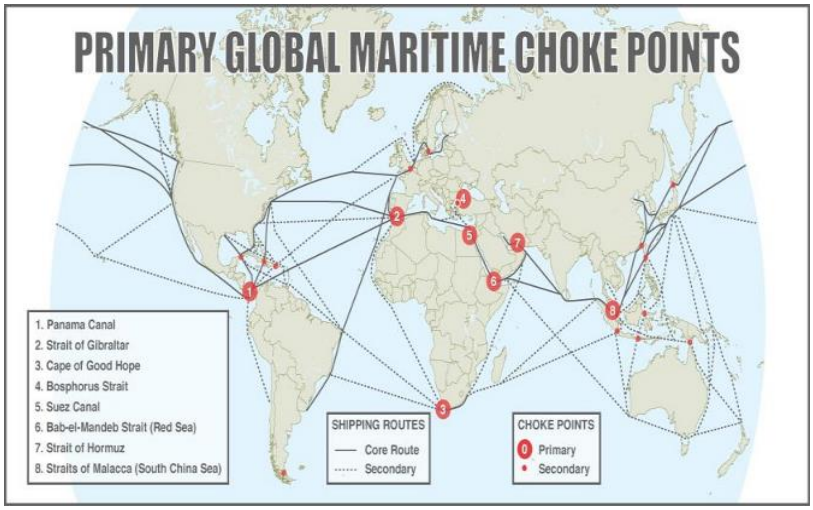


Fig.3 - Global Maritime Choke Points.
Map created by G. Lauriat. At: https://www.ajot.com/premium/ajot-global-maritime-choke-points.

Environmentally, on the other hand, the shrinking of the polar ice pack, the Arctic ice sheet and permafrost are likely to create disastrous consequences for the environment (release of stored carbon), land (biomes such as taiga and tundra), the 4 million inhabitants, animals (terrestrial and marine) and ecosystems.

The "Great game" in the Arctic has in our time, and net of the complexities of globalization, four big players: Russia, China, America and NATO. All these actors, except China and Nato, are in the Arctic Council (AC), which recently resumed his work after a one-year suspension in response to the Russian invasion of Ukraine. The fact that 7 of its members (the eighth being Russia) are also members of the Atlantic Alliance, makes NATO a relevant player in the Arctic scenario as well. The latest accessions of Sweden and Finland turn out, therefore, to be a highly strategic and functional move.

They represent, in fact, together with Norway and Denmark the European anti-Russian shield in the region. Obviously within the NAC America will be, with

Canada in the guise of junior partner, the guardian of the North (Lavorio, 2023), while the EU, UK, Japan and India, on the other hand, could be the external players. Now, in order to try to navigate the complexity of the Arctic scenario, it would be very important in this second part of the paper to analyze some aspects: a) the Arctic Legislature (Charron, 2020); b) the complexity for Arctic countries of combining the globalist dimension with the defense of their national interests; c) the relationship between Nato and Russia; d) finally, the political representation of the inhabitants in the CA (six Indigenous Permanent Participants), which invites the international community to assume its responsibilities as a super partes arbiter of the region.

2.1. The four-way game

If back in 1867 the purchase of Russian Alaska for $7.2 million by the U.S. was branded by the American media and Congress as the "Seward's Folly" (by U.S. Secretary of State William Seward), today, otherwise, it is regarded as one of the most forward-looking political moves ever made (History.com Editors, 2010). Given the evolving landscape, one can readily conceive that the operation is not recalled within Kremlin circles as the "Seward's Folly" but rather, if anything, as an undertaking associated with Alexander II, the reigning Tsar during the sale.

If one wanted to lapse into historical metaphysics, one could explain this deal through Manifest Destiny, which has always been the theological guideline of American politics.

Being a nation directly chosen by God, every foreign policy decision is relegated to determinism, that is, subject directly to divine will. Returning to more secular discourse, however, there is no question that Alaska has become a key asset of American Arctic policy today.

It enables the U.S. to be present in the Arctic game and thus to obstruct, should it so desire, both the Northwest Passage and the Northeast Passage (*Fig.4*).

Currently, the Arctic is at once both a global common and a contested area.

The resolution of this oxymoron lies in delineating who are the owners (if any) of this huge geographic space.

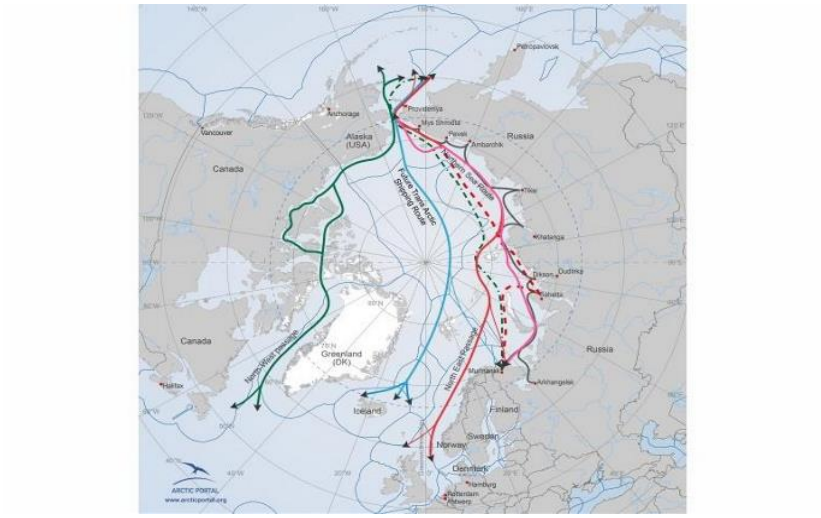


Fig.4 - Arctic Sea Routes and EEZs. At: ArcticPortal.org.

NATO's first task will be to dilute the vanities and nationalist ambitions of the seven Atlantic nations in the CA, as said before the United States, Finland, Denmark – Greenland and the Faroe Islands – Sweden, Iceland, and especially Norway and Canada).
The second task will be to restore relations with the Kremlin, which claims to itself the paternity of much of the region (one need only recall the flag raised on August 1, 2007, on the seafloor of the North Pole, as a testament to this assertion.).
The Arctic, on the other hand, generates 14 percent of GDP and 25 percent of total Russian exports (Lavorio, 2023) while also hosting 13% and 30% of undiscovered oil and natural gas, respectively (Cinciripini, 2023).
This is why Moscow has been adopting, since long time actually, a policy aimed at militarizing the area. At stake is not only the control of the valuable Northern Sea Route, but also a total redefinition of its anthropological nature.
Russia has always been a land power. By virtue of this specificity, it has consistently suffered over time from thalassocrat empires such as the United Kingdom in the 19th century and America today.
In this light, one can understand the aims Joseph Stalin had in Greece and Turkey in the postwar period and President Vladimir Putin's military interventions in North Africa and the Levant.
Consequently, the unlocking of the Northern Sea Route and the Northeast Passage presents Russia with an exceptional opportunity to initiate a profound maritime transformation.
The new routes would, moreover, guarantee maritime domination of the North in all its aspects (legislative, military, economic, cultural). This could cause, as mentioned, a shift in the hierarchy of shipping lanes of considerable magnitude bringing immense resources to the fragile Russian economy.
On the other hand, whenever major sea routes have changed, political geography has also undergone upheavals.
Consider, in this sense, the Italian Maritime Republics, which saw their influence gradually lost during the second half of the 15th century.
The Italic realities discovered that they were suddenly too "small" to match up with the great transatlantic empires: the Portuguese and Spanish at first, the Dutch, English and French later. At that time, the Atlantic became the center and the Mediterranean the periphery.
Similarly, even the Atlantic today is losing its influence on the Pacific, which for several decades has become the heart of world trade. Shanghai and Singapore, i.e., the two largest ports in the world, are, in fact, not in the West, but in the East.
The opening of the new northern routes may not necessarily generate such upheavals; however, it is undoubtedly-but it will be of considerable importance in world trade. Think of the aforementioned Northwest Passage.
To get from Shanghai to New York the fastest route at present is through the Panama Canal.
If the passage were to be opened, it could potentially reduce travel time by approximately seven days, yielding significant economic advantages and fostering increased trade between the two continental coastlines.
To undertake a solid peaceful-diplomatic process with Moscow, NATO will first have to, as mentioned above, try to sterilize, or at least countian, the nationalistic ambitions of some of its member countries. Above all, the downsizing of Norwegian and Canadian aims trying, at the same time, to create a multilateral strategy with the United States to prevent them from moving unilaterally in the region.

These two aspects are linked, however, to another diriment issue: the role of China. Indeed, the three-way game mentioned above (NATO-America and Russia) has become a four-way game for several years now. After all, how should one interpret the assertion in the Chinese White Paper of being a «neighboring state to the Arctic»?

China's interest extends beyond augmenting its soft power within the region; it also encompasses the bolstering of its hard power. For instance, Beijing is allocating significant resources to the construction of icebreaker ships as part of its endeavors. The three ships, while incomparable to the 50 or so Russian ships. (Dall'Asta, 2023) and the approximately 35 in NATO space (of which as many as 7 belong to Canada and 5 to America (Volpe, 2020), demonstrate a growing activism in the region. «Jin Beiji guojia» for short: «State near the Arctic».

In addition to the quantitative data inherent in its fleet, there is also the economic and scientific investment in the territory. And it is here, that the Chinese presence manifests itself most vigorously.

In addition to the economic collaboration with Greenland (with billions of investments in rare earth mining and the construction of strategic infrastructure), Beijing is planning the Polar Silk Road, a mammoth project integrative and complementary to the Belt and Road Initiative (Santoro, 2020).

The goal, in a clear neo-imperial fashion, is to create a land-based counter-globalization that can counter the maritime dominance of the U.S. Navy by decentralizing two of the world's most important choke points in Malacca and Suez. China seeks to enter the Arctic through two spaces: Greenland and Russia. In the second space, mainly through the Power of Siberia project. Thus, the media and international support given by President Xi Jinping to Putin, regarding the Ukraine conflict, is part of a broader foreign policy strategy.

On the other hand, Putin needs Chinese support in order not to remain internationally isolated and to exploit Chinese technology, used for the extraction of liquefied natural gas in the Jamal Peninsula, to his vantage point.

It will be extremely important for Russia to strike a balance in the dialectic of interests with Beijing.

Otherwise, the risk of becoming a mere junior partner of the Chinese colossus could increase considerably. For these precise reasons, Moscow seeks to limit China's push into the Arctic and guard its northern pearl, namely the Northern Sea Route.

China's adeptness lies in its ability to effectively allocate economic benefits to the countries bordering the region. Notably, the key to American success during the twentieth century rested on ensuring remarkable prosperity across its Western domain.

The Pax Americana has not only guaranteed military protection, but also a way of life that has been synonymous with stability for most European states. If China really intends to build an alternative Chinese Pax to that of the United States, then it will have to focus more on its soft power.

Pure power, devoid of an enticing narrative vision, often culminates as a self-contained objective. How many empires have fallen because they were dedicated to military might alone? So many. Conversely, how many empires have succeeded in combining dominance and consensus? Very few.

The United States, notably, stands as a paradigmatic example of this rare combination. «Flagg, fangst og forskning» (Flag, hunt and search) one might say, paraphrasing geologist Adolf Noel (Petroni, 2019). To which China will inevitably

have to add wealth, development, and respect for the environment and animal species.
The purpose is not solely to guarantee stability and prosperity for the indigenous inhabitants, but also to serve as an illuminating symbol for the global community. This vision, fundamentally inclined towards environmental sustainability rather than mere assertive might, seamlessly aligns with the principles of the UN Sustainable Development Agenda.

2.2. Who owns the Arctic and who is in charge?

Let us proceed to establish a coherent geographical and legal framework. Initially, it is essential to acknowledge that the seabed of the North Pole is not under the sovereignty of any specific state, thereby precluding any legitimate claim of ownership.
According to the UN Convention on Law of the Sea, nations can claim sovereignty within, and no more than, 200 nautical miles (Il Post, 2013) away from their territorial shores. Resources found beyond this perimeter, therefore, are considered by the UN (Part 11, Section 2, Article 136 et seq.) to be common heritage of mankind (United Nations Convention on the Law of the Sea, 1982).
The three UN bodies charged with regulating legal disputes are the Commission on the Limits of the Continental Shelf, the International Seabed Authority and the International Tribunal for the Law of the Sea (Cardile, 2022). Given that there exists not a clear-cut dichotomy between the Atlantic bloc and Russia but, as mentioned before, a rather contentious debate even within the Western bloc, the scenario becomes notably intricate.
An example of infighting may have been the so-called whiskey war, which took place between Ottawa and Copenhagen over the islet of Hans, located in the middle of the Kennedy Channel in the Nares Strait (Basile, 2022).
After 40 years of irreverent mutual actions, on June 14, 2022, the Foreign Ministers of the two nations, Denmark's Jeppe Kofod and Canada's Melanie Joly, finally agreed to divide the islet into two equal parts.
Another diriment dispute within the NATO bloc is between Canada and the U.S. over the Beaufort Sea, located in Alaska and the Yukon, and more generally over the Northwest Passage.
Canada considers it a violation of its sovereignty for U.S. ships to navigate the channel (Borzi, 2021), differently, the United States sees free maritime movement as an integral part of its founding ideology and a necessary policy for the defense of its national interests. This issue between Ottawa and Washington is not to be underestimated. Although they are natural allies, Canada has in recent decades developed a special sensitivity verse the region, whose history and tradition enrich its national identity. Hers is a sentiment mirroring that of Russia. If Moscow dominates the eastern Arctic by virtue of its geographical extent, Ottawa feels, for the same reasons, the rightful owner of the western part. Both passages, on the other hand, are guarded jealously by the two nations.
Anyone who wants to pass the Northeast, now and in the future, must/will have to seek permission from Russia, and anyone who wants to pass to the Northwest must/will have to seek permission from Canada.
These two nations will not, however, be the only ones to be consulted. The Western side will also be guarded by Denmark-Greenland, while, the Eastern side, by Norway. Finally, there is, of course, the United States patrolling the Bering Strait,

aka the gateway of the Arctic with the GIUK Gap. No one, in fact, will ever be able to sail freely without their greenlight.

As a result of these climate upheavals, the United States however is beginning to perceive the Arctic not only as a resource, but also as a threat. For these very reasons, Washington is unlikely to agree to restrict its navigation in the North, much to the chagrin of the governments of the aforementioned nations and the Inuit, who in turn claim, further complicating the situation, authorship of the Western Passage. When it comes to contentions involving the Russian entity, a notably prominent one is the ongoing dispute concerning the Barents Sea, which harbors extensive hydrocarbon reserves.

The relationship between Russia and Norway has been strained notably due to the cited conflict in Ukraine. Escalating tensions are becoming palpable, such as those observed in the Svalbard Islands.

In the summer of 2022, Oslo impeded the passage of Russian cargo vessels en route to Barentsburg, a settlement situated on the island of Spitsbergen, the largest in the archipelago. While the incident was subsequently resolved through diplomatic means, the potential for heightened friction in the relations between Russia, Norway, and the Arctic nations within the NATO bloc remains a tangible concern. In this archipelago, the stakes extend beyond mere sea routes and natural resources; they encompass the burgeoning realm of mass tourism, which is anticipated to burgeon further in the forthcoming decades.

As mentioned above, the Alliance will have to be able to dilute these hotbeds of crisis in the North. The danger, should it fail to do so, would be to see increasingly fierce clashes over illegal extensions of EEZs and continental platforms. The increasing condemnations among Arctic states, in short, are not at all reassuring when analyzed in a 30-to 50-year perspective.

Even though the Arctic represents only 6 percent of the Earth's surface, its immense reserves of hydrocarbons, metals and precious stones represent, if relegated only to a power perspective, a real threat to global security (Ferragamo, 2020). Therefore, foresight will have to become the key word from here on out. Foresight in having to move away from nationalist visions that are symbols of an ancient time.

Once again, the United Nations finds itself confronted with a significant responsibility.

The incursion into the Donbas region, and the Palestinian conflict, has starkly exposed the pragmatic efficacy of this international body. Often regarded as the world's arbitrator, its authority, unfortunately, lacks the ability to curtail ongoing conflicts.

On the other hand, NATO possesses the capability to intervene and halt conflicts. However, its leadership and juridical authority is predominantly acknowledged within the Western sphere, failing to garner universal recognition. The aspirations for a global cooperative vision espoused across the various revisions of the Strategic Concept, spanning from the 1990s to the present, must be set aside due to their inherent infeasibility. Giants such as China, India, Russia, or Saudi Arabia and Iran, prominent players in the Eastern and Middle East realm, do not accord any acknowledgment to NATO's leadership.

The 2030 climate agenda could, therefore, be a golden opportunity to connect in a multilateral way these shores, but also to connect the South American continent and Africa in a vision aimed at preserving our planet and mitigate-prevent the international conflicts.

In this sense, the contribution of the United Nations and the European Union, but also of the BRICS and other international organizations and non-state actors, will become necessary.
The EU, for example, has been actively involved in combatting climate change for many years, particularly by issuing various documents on the connections between climate, security, and the military. This is aimed at aligning the policies of all 27 member nations and implementing an efficient public policy to educate European citizens. Let's examine the Strategic Compass (2022) released by the EU External Action Service (EEAS) or Mario Draghi's most recent Report (The future of European competitiveness, 2024). Both the former Italian Prime Minister Draghi and European Commission President Ursula von der Leyen stress the crucial significance of the green transition in boosting the Union's global competitiveness. The two documents also seek to equip the EU with a cohesive approach to confront the vast challenges posed by climate change on a worldwide scale. The Draghi report specifically urges European countries to enhance their CFSP in order to effectively address the intricate climate challenges of the future.
Nations are also urged to boost funding and collaborative research efforts in innovation and artificial intelligence, as well as to revamp the energy market to reduce prices, which remain significantly elevated compared to countries like China and the US.
When it comes to the Arctic situation, Europeans are trying to strengthen their cooperation not only to ensure respect for local populations, environment, and preserving the territory and endangered species, in alignment with UN and NATO agendas, but also to seek energy independence from Moscow.
To achieve these goals, however, both NATO and the EU will have to try to contain internal nationalistic drives and put aside ideological politics by taking a more forward-looking attitude toward the outside world. Diplomatic relations with Russia have undergone a worrying decline in recent years, which risks definitively undermining thirty years of courageous multilateral cooperation. Even the mutual distrust that exists between a part of the Western world and China recalls a vertical bipolar mindset that is not very functional in the horizontal globalized world of 2024 and also the peace of the Arctic. Now, if NATO and EU could reduce economic and geopolitical tensions with China, with an approach by all the actors free from mutual ideologies and suspicions, it would be more difficult to do so with Russia, whose invasion of Ukraine created a watershed in bilateral relations with the West. Here, the issue turns out to be extremely delicate because a possible "Korean" solution of the Ukraine conflict would risk causing enormous damage to an invaded nation and at the same time throwing away two dramatic years of conflict, with money invested and, above all, human lives tragically wasted on both sides.
Having made this fundamental premise, it is also clear that détente with Moscow must become a matter of primary importance for the Euro-Atlantic community, not only to end the Ukrainian conflict but also to prevent international chaos and hypothetical conflicts from arising in the Arctic region as well.

Conclusions

As reported in this work, NATO involvement in climate change unfolds along two distinct and complex avenues: the humanitarian and the geopolitical. These trajectories are intricately interlinked and aptly exemplify the evolving character of the Alliance.

It mirrors a composite, multidimensional, and worldwide entity: one that encompasses humanitarian aspects alongside the robust, reflecting a defensive stance while concurrently embodying dynamism and initiative. These are the foundational pillars of an encompassing reach that has truly transcended the global expanse.

With a membership comprising 32 states, the NAC symbolizes an ambitious and diverse collective. Simultaneously, it manifests outside (at the public opinion) an almost monolithic unity when addressing global concerns, such as the Arctic strategy, the Ukrainian conflict, counterterrorism efforts against Islamic extremism, and the complex dynamics of Chinese neocontainment. The challenge for NATO, therefore, will have to be to succeed in marrying its core geopolitical strategy, which is essential for maintaining the deterrence policy and defend the Euro-Atlantic space, with a more, as already said, forward-looking and diplomatic vision, less ideologized and static, that can help improve relations with China and break the current and dramatic glacis with Russia.

Bibliography Abbreviations

CASD	CENTRO ALTI STUDI PER LA DIFESA
EU	EUROPEAN UNION
HCE	HISTORY.COM EDITORS
IRAD	ISTITUTO DI RICERCA E ANALISI DELLA DIFESA
IPCC	THE INTERGOVERNMENTAL PANEL ON CLIMATE CHANGE
NATO	NORTH ATLANTIC TREATY
UN	UNITED NATIONS
USCG	UNITED STATES COAST GUARD

Bibliography

BASILE M., *Artico, finisce la "guerra del whisky" per l'isolotto Hans: Danimarca e Canada danno l'esempio*, in «La Repubblica», June 15, 2022, n.p. https://www.repubblica.it/esteri/2022/06/15/news/artico_guerra_del_whisky_danimarca_canada-353995379/.

BORZI L., *Sovranità nell'Artico (parte III): rivendicazioni territoriali tra gli Stati artici*, in Centro Studi Italia-Canada, May 3, 2021. https://www.centrostudi-italiacanada.it/articles/sovranita-artico-rivendicazioni-territoriali.

CARDILE G., *Spazio, fondali e Artico: Patrimonio comune dell'umanità? Analogie e differenze nel loro sfruttamento*, in AMIStaDeS, s.d., 2022. https://www.amistades.info/post/spazio-fondali-artico-patrimonio-analogie-differenze-sfruttamento.

CASD - IRAD, *73ª Sessione di Studio – 2º Gruppo di lavoro dell'Istituto Alti Studi per la Difesa*, in Ministero della Difesa, 2022.

CHARRON A., *NATO and The Geopolitical Future of the Arctic*, in Arctic Portal.org. The Arctic Gateway, n.d., 2020. https://arcticyearbook.com/arctic-yearbook/2020/2020-briefing-notes/363-nato-and-the-geopolitical-future-of-the-arctic.

CINCIRIPINI L., *The Arctic within EU Strategies: A Renewed Centrality*, in Istituto Affari Internazionali (IAI), July 28, 2023. https://www.iai.it/sites/default/files/iaicom2337.pdf.

DALL'ASTA G., *La Russia continua a investire sui rompighiaccio*, in Osservatorio Artico, February 3, 2023. https://www.osservatorioartico.it/russia-rompighiaccio/.

Di chi è il Polo? (2013), in «Il Post», December 12, 2013. https://www.ilpost.it/2013/12/12/polo-nord-canada/.

EU, *A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security*, 2022. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

EU, *The future of European competitiveness. Part A-B*, 2024. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en; https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf.

FERRAGAMO S., *La dimensione geo-strategica dell'Artico*, in AMIStaDeS, n.d., 2020. https://www.amistades.info/post/la-dimensione-geo-strategica-dell-artico.

GORBACHEV M. S., *Perestroika: New Thinking for Our Country and the World*, New York,1988.

HARARI J. N., *Homo deus. Breve storia del futuro*, Milan, 2018.

HCE, *U.S. purchase of Alaska ridiculed as "Seward's Folly"*, in HISTORY, March 3, 2010. https://www.history.com/this-day-in-history/sewards-folly.

IPCC, *Synthesis Report of the IPCC Sixth Assessment Report (AR6)*, 2023. https://www.ipcc.ch/report/ar6/syr/.

https://www.difesa.it/assets/allegati/38313/ricerca_ar_smm_18_galiuto_web.pdf.

KOLBERT E., *La Sesta Estinzione. Una storia innaturale*, Vicenza, 2014.

LAVORIO A., *Guardiani del Nord. Gli Stati Uniti e la geopolitica della crisi climatica nell'Artico*. Milan, 2023.

MATTERA D., *Cambiamento climatico e sicurezza. Così la Nato si adatta al futuro (con le Università)*, in Formiche, September 29, 2020. https://formiche.net/2020/09/nato-stoltenberg-nato2030-cambiamento-climatico/.

NATO, https://www.nato.int/.

Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, 2010.

Climate Change and Security Action Plan, 2021.

Remarks by NATO Secretary General Jens Stoltenberg at the high-level roundtable "Climate, Peace and Stability: Weathering Risk Through COP and Beyond" in Glasgow, UK, 2021.

Secretary General attends United Nations "COP26" Climate Change Conference, 2021.

Climate Change and Security Impact Assessment, 2022.

Strategic Concept, 2022.

Opening speech by NATO Secretary General Jens Stoltenberg at the High-Level Dialogue on Climate and Security, NATO Public Forum, 2022.

Climate Change and Security Impact Assessment. Second Edition, 2023.

Greenhouse Gases Emission Mapping and Analytical Methodology, 2023.

Mediterranean Dialogue, 2023.

Opening remarks by NATO Secretary General Jens Stoltenberg at the meeting of the North Atlantic Council at the level of Heads of State and Government, with Sweden, Indo-Pacific Partners, and the EU, 2023.

Remarks by NATO Secretary General Jens Stoltenberg at the UN Climate Change Conference (COP28) in Dubai, 2023.

Steps up work on climate change and security, 2023.

Vilnius Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023, 2023.

Environment, climate change and security, 2024.

HQs, 2024.

Washington Summit Declaration issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. 10 July 2024, 2024.

PETRONI F., *Centralità e fragilità strategica dell'Artico*, in «Limes», n. 1, 2019, pp. 29-40.

PITASI A., (Collaboration with DIB N.B., FERONE E., & PETROCCIA S.), *The Hypercitizen World Game: Writings on the Emerging Global Order*, Paris, 2021.

SANTORO F., *La Polar Silk Road: un riflesso dell'ambizione di Pechino nella conquista della leadership globale*, in Centro Studi Internazionali (CeSI), January 15, 2020. https://www.cesi-italia.org/it/articoli/la-polar-silk-road-un-riflesso-dellambizione-di-pechino-nella-conquista-della-leadership-globale.

UN, https://www.un.org/en/.

Convention on the Law of the Sea, 1982.

Framework Convention on Climate Change, 1992.

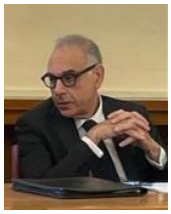
Kyoto Protocol to the United Nations Framework Convention on Climate Change, 1997.

Convention-cadre sur les changements climatiques […], 2015.

The Glasgow Climate Pact, 2022.

USCG, *Major icebreakers of the world*, May 1, 2017. https://www.history.uscg.mil/research/bibliography-collections/units/cutters/icebreakers/.

VOLPE M., *La Cina e l'Artico*, in *Osservatorio Artico*, August 24, 2020. https://www.osservatorioartico.it/la-cina-e-lartico.



Gianfranco Trovatore
Docente di Istituzioni di diritto privato nell'Università di Catania e di Diritto dei mercati finanziari nell'Università Federico II di Napoli. È stato direttore di ricerca presso il CEMISS. Attualmente è membro del Consiglio direttivo di ELEC Italia (European League for Economic Cooperation).

UNIONE DEI MERCATI DEI CAPITALI E AUTONOMIA STRATEGICA EUROPEA

ABSTRACT

L'articolo descrive caratteristiche, finalità e criticità del progetto di Capital Markets Union (CMU). Tra le principali criticità nella realizzazione del pro-getto, risalta la permanente difformità dei sistemi fiscali e delle normative nazionali nei settori finanziario, fiscale e pensionistico. In un contesto geo-politico complesso come l'attuale, individuare le priorità e implementare la CMU è ormai indispensabile per rafforzare l'autonomia strategica dell'UE.

Parole chiave: CMU, Unione europea, Mercato unico europeo, Competiti-vità, ESMA, Draghi

The article describes the Capital Markets Union (CMU) project, which aims to overcome the fragmentation of European financial markets. Among the main challenges highlighted in the article are the persistent disparities in tax systems and national regulations in the financial, fiscal, and pension sec-tors. However, CMU is more critical than ever to strengthen the EU's strate-gic autonomy in a complex geopolitical landscape.

Keywords: CMU, European Union, European single market, Competitive-ness, ESMA, Draghi

SOMMARIO: 1. Origini, scopi e criticità del progetto di Capital Markets Union — 2. La frammentazione del mercato finanziario europeo come problema geopolitico — 3. Le cinque priorità della Capital Markets Union — 4. Conclusioni.

1. Origini scopi e criticità del progetto di *Capital Markets Union*

L'espansione e la maggiore coesione dei mercati finanziari è tra gli obiettivi prioritari dell'UE, tanto più se si considera il divario tra la crescita dell'economia europea in confronto a quella statunitense[1] e che "*i mercati degli strumenti di capitale in Europa corrispondono a meno della metà dei loro omologhi statunitensi, e i mercati del debito a meno di un terzo*"[2].

Da queste premesse trae spunto il progetto di *Capital Markets Union* (CMU), che sullo slancio del *Piano di investimenti per l'Europa* del 26 novembre 2014 (noto

[1] Secondo le stime pubblicate dal FONDO MONETARIO INTERNAZIONALE (FMI) nel proprio *World Economic Outlook: Policy Pivot, Rising Threats* di ottobre 2024, reperibile in https://www.imf.org/-/media/Files/Publications/WEO/2024/October/English/text.ashx, la crescita prevista per il 2024 negli Stati Uniti è stata rivista al rialzo al 2,8%, mentre nell'area euro si prevede che il PIL cresca di appena lo 0,8%.

[2] COMMISSIONE EUROPEA, *Piano di azione per la creazione dell'Unione dei mercati dei capitali*, 2015, p. 3.

anche come "*Piano Juncker*") si delinea a partire dal 2015 nel *Libro Verde* della Commissione Europea "*Costruire un'Unione dei mercati dei capitali*" del 18 febbraio 2015 e dal "*Piano di azione per la creazione dell'Unione dei mercati dei capitali*" del 30 settembre 2015[3]. In entrambi i documenti si prefigurava il superamento della frammentazione dei mercati finanziari a beneficio della competitività delle imprese all'interno dell'UE, sottolineandosi a tal fine la necessità di "*individuare e rimuovere gli ostacoli alla circolazione dei capitali tra investitori e operatori che necessitano di finanziamenti, siano essi ostacoli a carattere nazionale o transfrontaliero*"[4] e che, invece, "*nonostante i progressi compiuti, oggi i mercati dei capitali rimangono ancora segmentati e sono in genere organizzati su base nazionale*"[5].

Un ulteriore documento alla base del progetto è il *Final Report of the High Level Forum on the Capital Markets Union* del giugno 2020, nel quale si sottolinea, tra l'altro, l'importanza di promuovere una più incisiva campagna di educazione finanziaria a livello euro-unitario e nazionale[6]. Ulteriori piani d'azione ed iniziative legislative sono stati promossi negli anni più recenti dalla Commissione UE, ma l'obiettivo di una piena integrazione finanziaria è ancora ben lontano dall'essere raggiunto[7].

Creare un vero Mercato Unico dei capitali tra i Paesi membri dell'UE implica, anzitutto, la rimozione di tutte le barriere agli investimenti *cross border* ed un *single rulebook* per i servizi finanziari che trovi applicazione uniforme in tutti gli ordinamenti sui molteplici ed interconnessi piani della stabilità finanziaria, della prestazione dei servizi d'investimento e della protezione di consumatori e investitori.

Dal 2015 ai giorni nostri il dibattito da parte degli *stakeholders* si è ampiamente sviluppato; e tuttavia, sulla scorta di una precisa volontà politica di procedere alla

---

[3] Il *Libro Verde e* il *Piano di azione* sono reperibili in italiano, rispettivamente, in https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015DC0063&from=EN e https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015DC0468. In argomento sia consentito rinviare a. TROVATORE G. - SAVASTA F., *Il progetto della Capital Markets Union e l'art.47 della Costituzione brevi note sul valore del risparmio*, in «Federalismi.it», 7/2021, p. 248 ss., reperibile in https://www.sipotra.it/wp-content/uploads/2021/03/Il-progetto-della-Capital-Markets-Union-e-l%E2%80%99art.-47-della-Costituzione-brevi-note-sul-valore-del-risparmio.pdf. Si veda anche BANCA CENTRALE EUROPEA (BCE), *Building a Capital Markets Union – Eurosystem contribution to the European Commission's Green Paper*, 2015; EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA), *Esma response to the Commission Green Paper on Building a Capital Markets Union*, 13 Maggio 2015; PANETTA F., *The European Banking and Capital Markets Unions: Challenges and Risks*, Roma 2015, p. 108; COMMISSIONE EUROPEA, *Q & A on the Green Paper on building a Capital Markets Union*, 18 Febbraio 2015, p. 109; BROGI M., *Shadow banking, banking union and capital markets union*, in «Law and economics yearly review», volume 3, parte 2, 2014; QUAGLIA L. - HOWARTH D. - LIEBE M., *The Political Economy of Capital Markets Union in Europe*, in «Journal of Common Market Studies», volume 54, Issue S1, September 2016, pp. 185-203; SAPIR A. – VÉRON N. - WOLFF G. B., *Making a reality of Europe's Capital Markets Union*, 7, 2018, reperibile in https://www.bruegel.org/sites/default/files/wp-content/uploads/2018/04/pc-07-2018.pdf.

[4] COMMISSIONE EUROPEA, *Libro Verde…*, op cit., p. 4.

[5] *Ibidem*

[6] https://finance.ec.europa.eu/publications/high-level-forum-capital-markets-union_en

[7] In particolare, a partire dal 2021 la Commissione UE ha adottato proposte legislative in materia di punto di accesso unico per gli investitori (ESAP), fondi di investimento europei a lungo termine, gestori di fondi di investimento alternativi, infrastrutture del mercato europeo, insolvenza, quotazione delle piccole e medie imprese. Essa ha al contempo avviato il riesame del regolamento c.d. "MiFIR" e della direttiva c.d. "MiFID II" sui mercati degli strumenti finanziari.

Capital Markets Union con un approccio graduale, in questi anni non sono stati fatti molti passi avanti per superare effettivamente la frammentazione dei mercati.
La lentezza nel processo di realizzazione della *Capital Markets Union* non ha soltanto compromesso le prospettive di attrarre il capitale privato nel finanziamento di progetti infrastrutturali e di ricerca tecnologica, ma secondo quanto dichiarato di recente dalla Presidente della BCE ha financo comportato un deflusso finanziario netto dall'area euro di circa 250 miliardi (circa l'1,8% del PIL europeo) per andare prevalentemente nel mercato statunitense[8].
Tra le principali criticità del processo di realizzazione della CMU va segnalata l'esistenza di regolamentazioni nazionali molto diverse tra loro per quanto riguarda i mercati dei capitali, le procedure fallimentari, la *corporate governance* e la fiscalità. Sul piano del regime fiscale, in particolare, permangono diffuse resistenze da parte degli Stati membri alla cessione di ulteriori spazi di sovranità economica.
Altro profilo di criticità è l'estrema frammentazione delle infrastrutture finanziarie: piattaforme di *trading*, sistemi di gestione accentrata e di regolamento sono caratterizzati da standard tecnici non sempre compatibili, il che rende particolarmente arduo interconnettere i mercati nazionali e limita il raggiungimento di economie di scala nella prestazione dei servizi.
Non meno rilevante è la percezione di alcuni governi nazionali che una maggiore integrazione dei mercati dei capitali amplifichi il rischio di propagazione transfrontaliera delle crisi finanziarie che possono generarsi al livello nazionale, soprattutto quelle legate alla crescita del debito sovrano di alcuni Paesi membri[9].
Sulla scorta dell'attuale congiuntura geopolitica e dei propositi manifestati dalla neo-eletta *leadership* statunitense, il progetto della CMU si ripropone oggi all'attenzione del *policymakers*: di questo rinnovato interesse sono espressione, tra l'altro, i due Rapporti commissionati dall'UE sui temi del mercato interno e della competitività.
Mercato unico dei capitali, crescita degli scambi di merci e di servizi nel contesto di una rafforzata competitività economica, difesa comune, piano energetico e trasformazione digitale non sono progetti a sé stante ma tappe intermedie verso il conseguimento di un preciso obiettivo principale: l'autonomia strategica europea.
Affinché si tratti di una strategia credibile, il perseguimento di tale autonomia presuppone anzitutto il superamento della frammentazione che, come detto, tutt'oggi caratterizza lo scenario economico-finanziario europeo.

2. La frammentazione del mercato finanziario europeo come problema geopolitico

Il freno principale alla crescita economica dell'UE è la frammentazione del mercato finanziario: un *venture capitalist* che intenda finanziarsi nel mercato azionario statunitense avrebbe la possibilità di raccogliere, in media, un multiplo delle risorse finanziarie suscettibili di essere raccolte se egli si rivolgesse, invece, al mercato finanziario europeo[10].
Ciò si riverbera, all'evidenza, nell'insufficiente apporto di capitali privati allo sviluppo tecnologico e infrastrutturale dell'area europea. Da qui la valenza

[8] https://finanza.lastampa.it/News/2024/02/23/bce-lagarde-dati-salari-incoraggianti-ma-serve-maggiore-fiducia/MTMxXzIwMjQtMDItMjNfVExC

[9] Per un'analisi economica delle modalità di trasmissione degli shock macroeconomici al sistema bancario, v. BUCH C. M. - EICKMEIER S. - PRIETO E., *Macroeconomic Factors and Microlevel Bank Behavior*, in «Journal of Money, Credit and Banking», Volume 46, Issue 4, 2014, pp. 567-836.

[10] Cfr., in tal senso, l'intervista a Markus Kerber sul quotidiano *la Repubblica* del 10 settembre 2024, p. 4.

geopolitica della frammentazione finanziaria: l'inadeguato apporto del capitale privato ha comportato finora uno sforzo compensativo in tal senso da parte del capitale pubblico, il quale tuttavia di per sé non basta a finanziare investimenti aggiuntivi che, secondo il c.d. "Rapporto Draghi" sulla competitività[11], sono nell'ordine degli 800 miliardi di euro all'anno per molti anni a venire; tanto più se si considera l'elevato indebitamento attuale di numerosi Paesi e l'esigenza di non mettere ancora più in crisi gli standard europei di equità e pace sociale.
Né il sistema bancario né le risorse speciali, anche a fondo perduto, stanziate per la competitività (come la *Next Generation EU*) e neppure i fondi in partenariato pubblico/privato gestiti dalla Banca Europea degli Investimenti sono in grado di assicurare i finanziamenti necessari per realizzare gli obiettivi strategici dell'UE. Nel sistema bancario, infatti, requisiti di capitale sempre più stringenti inducono le banche a concedere prestiti soltanto a fronte di garanzie adeguate, che, tuttavia, per i progetti di più ampio respiro non sempre possono essere messi a disposizione dalle imprese. Secondo una recente *survey* della BCE, in particolare, l'erogazione del credito alle PMI permane molto restrittivo nonostante il *trend* decrescente del costo del denaro, registrandosi un aumento netto della quota di domande respinte per i prestiti alle PMI (percentuale netta del 7%) rispetto ai prestiti alle grandi imprese (3%)[12].
L'accesso alle risorse speciali erogate nell'ambito di *partnership* pubblico/privato ed il loro conseguente impiego, tanto più se a fondo perduto, sono subordinati a lunghe procedure di approvazione; e non va trascurato che, una volta erogati i finanziamenti, la possibilità di utilizzarli con agilità per fronteggiare improvvisi cambiamenti dello scenario economico e nuove esigenze di mercato trova ostacolo nel fatto che si tratta quasi sempre di finanziamenti vincolati a progetti specifici[13].
Anche il Rapporto sul mercato unico europeo "*Much more than a market – Speed, Security, Solidarity. Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*" (c.d. "Rapporto Letta")[14] sottolinea, in tal senso, che occorre canalizzare il risparmio privato nell'economia reale dell'UE.
Due le soluzioni di recente prospettate, rispettivamente, dai ministri dell'Economia di Francia e Germania al fine di superare l'*impasse* che impedisce al risparmio privato di confluire in massa nel capitale di rischio a supporto degli investimenti[15]: la prima soluzione – diacronica e su base volontaria - consisterebbe nell'iniziale

[11] Il Rapporto Draghi sulla competitività è reperibile in https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf
Le analisi di dettaglio e le raccomandazioni del medesimo Rapporto sono reperibili in https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf

[12] BCE, *The euro area bank lending survey - Third quarter of 2024*, p. 10, reperibile in https://www.ecb.europa.eu/stats/ecb_surveys/bank_lending_survey/pdf/ecb.blssurvey2024q3~f30e9a3fd6.en.pdf

[13] In materia di aiuti di Stato alle imprese e per un'analisi approfondita delle questioni irrisolte, v. per tutti, ROSSANO D. - MESSINA P., *Aiuti di Stato alle imprese e garanzie pubbliche*, in M. PELLEGRINI (a cura di), *Diritto pubblico dell'economia*, Padova 2023, pp. 524-526 ss.

[14] Il Rapporto Letta sul mercato unico europeo è reperibile in https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

[15] DE CHIARA A., *Eurogruppo: le reazioni all'appello francese sull'Unione del mercato dei capitali*, reperibile in https://www.euroeconomie.it/blog-detail/post/223421/eurogruppo:-le-reazioni-all%27appello-francese-sull%27unione-del-mercato-dei-capitali

unificazione del mercato dei capitali da parte di un gruppo ristretto di Paesi (perlopiù i Paesi fondatori dell'UE) che offrano titoli di debito comune con adeguato trattamento fiscale; la seconda soluzione consisterebbe nel trasformare sincronicamente l'intera Unione Europea modificandone l'assetto complessivo in senso federalista, anche qui con emissione di titoli di debito comune, ma ciò richiederebbe un'unanimità allo stato difficile da realizzare.
La realizzazione della *Capital Markets Union* quale presupposto della capacità dell'Unione di incidere effettivamente sulle sfide geopolitiche in atto nel contesto globale è al centro del Rapporto Draghi, là dove si rimarca l'esigenza di estendere il più possibile il voto a maggioranza qualificata in seno al Consiglio dell'UE e di elaborare forme incisive di sblocco dell'azione unionale nei casi di stallo dovuti a divergenze di natura politica. È a rischio il progetto europeo nel suo complesso qualora, anche in ambito finanziario, non si giunga in tempi ragionevolmente brevi ad un approccio unificato che consenta all'UE di perseguire un'autonoma politica estera, economica e di difesa.

3. Le cinque priorità della *Capital Markets Union*

All'inizio del 2024 *l'European League for Economic Cooperation* (ELEC) ha pubblicato un *position paper* che declina cinque proposte per i decisori politici corrispondenti ad altrettante priorità della *Capital Markets Union*[16].
Un primo punto è l'armonizzazione delle regole che governano le procedure fiscali, quelle d'insolvenza e la *governance* societaria, in ciò riprendendo lo spunto a suo tempo formulato dal Fondo Monetario Internazionale[17].
Ciò faciliterebbe i flussi di capitali transfrontalieri e l'escussione delle garanzie, supportando le banche a liberarsi dei *non performing loan* (NPL). Gli NPL, infatti, compromettono la capacità delle banche di concedere nuovi prestiti, rallentando al contempo la redditività bancaria.
Occorre in tal senso rafforzare e completare le misure finora adottate nell'UE per supportare le banche nella riduzione degli NPL e cioè la creazione di veicoli *ad hoc* per gestire crediti deteriorati e il rafforzamento del mercato secondario di tali asset[18].
Una seconda priorità per dotare l'economia dell'UE di un mercato dei capitali proporzionato alla complessità e alla forza della sua economia consiste nel creare le condizioni ottimali affinché le cartolarizzazioni possano effettivamente diventare un complemento al finanziamento bancario.
In quanto processo attraverso il quale un'entità trasferisce un insieme di attività illiquide (ad esempio, prestiti o mutui) a un veicolo speciale (*Special Purpose Vehicle* o SPV) che emette titoli negoziabili per raccogliere liquidità sul mercato, la cartolarizzazione è stata utilizzata ampiamente per affrontare il problema degli NPL, in particolare in Italia, dove strumenti come le GACS (Garanzie sulla Cartolarizzazione delle Sofferenze) hanno facilitato il trasferimento dei crediti deteriorati al mercato. In UE la cartolarizzazione è disciplinata dal Regolamento UE

---

16 ELEC, *Why EU Capital Markets Union has become a "must have" and how to get there*, reperibile in https://eleclece.eu/wp-content/uploads/2024/02/ELEC-position-paper-Why-EU-Capital-Markets-Union-has-become-a-must-have-and-how-to-get-there-February-2024-v2.pdf

17 Cfr. FMI, *A Capital Market Union for Europe*, in *Staff Discussion Notes*, 2019/7, reperibile in https://www.imf.org/-/media/Files/Publications/SDN/2019/SDNEA2019007.ashx

18 La rilevanza del tema degli NPL è sottolineata, in particolare, dalla Commissione UE nel proprio *Action Plan* del 2020: *Tackling Non-performing loans in the aftermath of the COVID-19 pandemic*, reperibile in https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0822; v. anche KARADIMA M. – LOURI H., *Non-performing loans in the euro area: Does bank market power matter?*, in «International Review of Financial Analysis», 2020, vol. 72(C).

2017/2402 (Regolamento sulla Cartolarizzazione Semplice, Trasparente e Standardizzata - STS), che tuttavia non ha portato ad un utilizzo di tali strumenti così diffuso come negli USA, mentre invece essi consentirebbero di sfruttare le migliori caratteristiche del sistema bancario (ovvero l'allocazione del credito e la valutazione del rischio) e quelle del mercato dei capitali (ovvero il sostegno al rischio nel medio e lungo termine)[19].
Prioritario è anche il reperimento di capitale di rischio che attinga al risparmio delle famiglie, il quale andrebbe indirizzato verso attività finanziarie più remunerative, a rischio e a lungo termine, nel quadro di una più intensa attività di educazione finanziaria e attraverso incentivi di natura anche fiscale.
Indirizzare i risparmi a lungo termine verso *assets* a rischio più elevato è decisivo al fine di stimolare gli investimenti più rischiosi ma potenzialmente più redditizi come quelli diretti allo sviluppo di nuove tecnologie.
Una quarta priorità, strettamente collegata alla precedente, consiste nella riforma delle istituzioni europee preposte alla tutela del risparmio e nella semplificazione del quadro normativo a partire dalla creazione di un testo unico che disciplini uniformemente il mercato finanziario europeo[20].
In tal senso, occorrerebbe potenziare e ampliare il ruolo e la struttura dell'ESMA sulla falsariga di quanto già avvenuto per la supervisione bancaria, in cui le decisioni centralizzate a livello europeo procedano di pari passo con la loro esecuzione decentrata a livello nazionale.
Imprescindibile è infine l'impiego dell'intelligenza artificiale nell'analisi dei *Big Data* per migliorare l'allocazione del capitale mappando e valutando con precisione i rischi finanziari la domanda di finanziamento.
Nell'ordinamento europeo il fenomeno è stato regolamentato recentemente nel c.d. *AI Act*[21], il quale contempera l'esigenza di non inibire lo sviluppo delle applicazioni di intelligenza artificiale con la necessità di un approccio *risk-based* che diversifichi le forme di tutela dall'uso improprio dei sistemi di AI, combinando il principio di precauzione e il principio di prevenzione.
Nella medesima prospettiva si pongono la proposta di Direttiva UE del 28 settembre 2022[22] e in Italia il disegno di legge sull'intelligenza artificiale presentato in Parlamento il 20 maggio 2024[23].

Conclusioni

È prematuro fare previsioni sul tempo che ci vorrà per realizzare integralmente una vera CMU; ma non è difficile prevedere, in sintonia con quanto osserva il Rapporto Draghi, che a fare la differenza sarà la decisione, del tutto politica, di emissione su larga scala di strumenti finanziari di debito comune e la capacità di canalizzare il risparmio delle famiglie in investimenti produttivi.

---

19 In questo senso, v. ELEC, *op. cit*., p. 6.

20 Così, in particolare, il Rapporto Draghi (Sez. A) che a p. 65 pone a confronto la quantità di regole adottate nell'UE e negli USA, sottolineando come "*around 3,500 pieces of legislation were enacted and around 2,000 resolutions were passed in the US at the federal level over the past three Congress mandates (2019-2024). During the same period, around 13,000 acts were passed by the EU*".

21 Regolamento(UE) 2024/1689 del 13 giugno 2024 reperibile in https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401689

22 Proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale COM/2022/496, reperibile in https://eur-lex.europa.eu/legal-content/IT/HIS/?uri=CELEX:52022PC0496

23 Reperibile in https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm

Non meno importante, specialmente per la peculiare conformazione dell'economia italiana, è salvaguardare – anzi potenziare – a livello europeo il ruolo della piccola e media impresa.

Il sottile equilibrio tra salvaguardia dell'equità sociale e sviluppo economico-finanziario è arduo da mantenere, soprattutto in epoca di riforme radicali come quelle prospettate; ma giustamente scriveva Albert Einstein al malato figlio Eduard che "*Das Leben ist wie ein Fahrrad. Man muß sich vorwärts bewegen, um das Gleichgewicht nicht zu verlieren*"[24].

[24] "La vita [dell'Unione Europea] è come una bicicletta. Si deve avanzare, per non perdere l'equilibrio".

C O N F E R E N C E R E P O R T

(Sezione non soggetta a peer-review)

Luce Gatteschi
Doppia Laurea Triennale in Scienze Politiche presso le università di SciencesPo Toulouse e Universidad Complutense de Madrid; Master's Degree in European Affairs presso SciencesPo Toulouse; Master in Sicurezza Economica, Geopolitica e Intelligence presso SIOI e Master in Studi Diplomatici presso ISPI.

Federico Girotti
Dottore in Economia e Laureando Magistrale in Scienze della Pace e della Cooperazione Internazionale presso Università Pontificia Lateranense

Barbara Raimondi
Dottoressa in Scienze per l'Investigazione e la Sicurezza e Laureanda in Scienze Strategiche presso l'Università degli Studi di Torino

NESSI 2024

Dal 24 al 26 Settembre 2024, Palazzo Salviati, sede del Centro Alti Studi per la Difesa (CASD), ha ospitato l'incontro annuale del Network of European Strategic Studies Institutions (NESSI).
Quest'anno l'evento si è svolto in Italia poiché la Presidenza del Network per il 2024 è affidata all'Istituto di Ricerca e Analisi della Difesa del CASD.
Il NESSI si pone l'obiettivo di promuovere la reciproca conoscenza, la fiducia e il dialogo tra centri di ricerca strategica europei, incoraggiando lo sviluppo di una cultura strategica comune che rispetti le diversità.
All'incontro hanno partecipato autorevoli personalità ed esperti analisti nel campo della difesa e della sicurezza europea, provenienti da alcuni dei Paesi membri, che hanno condiviso le proprie prospettive sulle sfide strategiche per l'Europa in un contesto sempre più instabile, segnato da molteplici minacce alla sicurezza globale e regionale e da tensioni all'interno della politica europea e nei rapporti con la NATO.
Il Generale di Divisione Stefano Mannino, Presidente del CASD, ha aperto i lavori affermando quanto la protezione della stabilità internazionale, della pace, della dignità umana e la salvaguardia dei diritti umani siano gli aspetti prioritari della politica nazionale militare e strategica. Riferendosi alle attuali crisi globali, come la guerra in Ucraina e l'*escalation* di tensioni nella Striscia di Gaza, Mannino ha sottolineato che: "*rafforzare la cooperazione internazionale e il dialogo devono essere considerate delle priorità della politica europea in favore di un rinnovamento della centralità politica e geopolitica*".
A seguire, la Dott.ssa Nicoletta Pirozzi, responsabile del programma "UE, Politica e Istituzioni" dello IAI, ha presentato "Rompere i Tabù sulla difesa Europea" proponendo un rinnovamento della Bussola Strategica ed

evidenziando la necessità di una comune, rapida e più matura visione dell'Unione Europea e dei suoi strumenti, in particolare sul tema della difesa. Propone cinque sfide che possono aiutare a definire la difesa europea e assumere rilevanza nella prossima legislatura.
La Dott.ssa Andreea Tudor dell'"Institute for Political Studies of Defence and Military History" presso il Ministero della Difesa della Romania ha sollevato il quesito: "Come può l'Unione Europea contribuire alla deterrenza e alla difesa comune? È necessaria una revisione della Bussola Strategica o delle relazioni UE-NATO?", avviando un approfondimento sulle clausole di difesa collettiva – l'art. 42, par. 7 del Trattato sull'Unione Europea e l'art. 5 del trattato NATO. Tudor ha evidenziato la necessità di una riflessione strategica sull'autonomia europea in ambito difensivo.
Il Professor António Luís Beja Eugénio dell'"Instituto da Difesa Nacional" sito in Portogallo, ha focalizzato il suo intervento sulla digitalizzazione delle Forze Armate europee come componente cruciale della sovranità in un contesto di rapida crescita informativa. Ha proposto il concetto di "Trinità Digitale", un modello che richiama la Trinità di Clausewitz e offre una cornice moderna per affrontare le questioni di sicurezza militare a livello europeo.
Il Colonnello Zdeněk Petráš, proveniente dal "Centre for Security and Military Strategic Studies, University of Defence" in Repubblica Ceca, ha posto la domanda "Come può l'Europa rafforzare la propria stabilità nella sicurezza e nella difesa?" suggerendo come l'attuale guerra in Ucraina impone una revisione della Bussola Strategica Europea per adattarla alle nuove realtà geopolitiche.
Nella seconda parte del dibattito, l'attenzione si è spostata sugli errori dell'*intelligence* in relazione agli eventi del 7 ottobre 2023 in Israele. Il professor Michel Wyss dell'Accademia Militare delle Forze Armate Svizzere presso l'ETH di Zurigo ha analizzato i fattori che hanno contribuito al fallimento dell'*intelligence* israeliana nel prevedere l'attacco di Hamas e ha delineato possibili riforme per migliorare i processi di sicurezza nazionale in Israele.
La dottoranda Margherita Iagulli del CASD ha trattato invece lo sviluppo della difesa comune europea, soffermandosi sull'evoluzione del progetto e sulle prospettive future. Ha approfondito gli aspetti tecnici delle politiche istituzionali e industriali, con particolare attenzione alla regolamentazione del mercato europeo e alle sfide di medio-lungo termine, come il necessario equilibrio tra le politiche nazionali e la costruzione di una difesa comune.
Successivamente, si è passati al tema "Spanish Geostrategic Vision: Looking towards the South", moderato dal Colonnello Ignacio Fuente Cobo, che ha sottolineato le sfide globali attuali, come la competizione tra Cina e Stati Uniti, e le loro ripercussioni verso il Sud globale. Tra i temi discussi, l'immigrazione dal continente africano, la minaccia terroristica nel Sahel e la presenza della Russia in Africa, considerati come fattori di destabilizzazione per l'Europa che NATO e UE devono affrontare.
Philippe Perchoch, dell'"Institut de Recherche Stratégique de l'Ecole Militaire" (IRSEM), ha illustrato le sfide della sicurezza europea, evidenziando il ruolo strategico dei Paesi Baltici e la loro risposta alla minaccia russa. Ha sottolineato come, grazie a una politica estera orientata al rafforzamento dei legami con NATO e Stati Uniti, i Paesi Baltici abbiano ottenuto il sostegno dell'Alleanza in cambio della loro partecipazione a missioni internazionali. Di fronte a minacce come cyber-attacchi ed espansionismo russo, i Baltici hanno incrementato le proprie difese e sostenuto l'integrazione della sicurezza europea con un

approccio orientato alla cooperazione tra UE e NATO, fondamentale per proteggere settori cruciali come energia e democrazia.
Justinas Juozaitis dell'Accademia Militare di Lituania ha poi spostato il *focus* sul supporto europeo all'Ucraina dal punto di vista del fianco orientale della NATO. Sono state discusse le priorità della sicurezza europea e, in particolare, le strategie della Lituania per contrastare la minaccia russa, come il finanziamento dell'industria della difesa, il miglioramento della mobilità militare e il sostegno costante all'Ucraina. La sessione si è conclusa con un'analisi dei limiti politici ed economici attuali e delle iniziative a disposizione dell'UE per garantire la coesione europea.
Marcin Terlikowski del "Polish Institute of International Affairs" ha esplorato invece gli scenari di *escalation* nell'Indo-Pacifico, focalizzandosi sulle vulnerabilità delle catene di approvvigionamento europee in un contesto di tensioni con Russia e Cina. Ha evidenziato la necessità di una maggiore autonomia e resilienza europea a fronte di un minore impegno degli Stati Uniti in Europa e della cooperazione sempre più stretta tra Russia e Cina, vista come una minaccia per l'equilibrio globale.
Gunther Hauser dell'"Institute for Strategy and Security Policy, Austrian National Defence Academy", ha discusso l'approccio globale dell'Europa per affrontare le sfide internazionali in materia di sicurezza e difesa, enfatizzando l'importanza dei rapporti multilaterali con paesi emergenti, tra cui diversi membri del BRICS.
Infine, i professori Robin Allers e Paal Sigurd Hilde del "Norwegian Institute for Defence Studies" hanno analizzato la sicurezza europea e il conflitto in Ucraina dal punto di vista del fianco settentrionale, illustrando i motivi che hanno portato i Paesi scandinavi ad allinearsi sotto l'ombrello difensivo della NATO dopo l'invasione russa e le prospettive future per le relazioni tra Norvegia e Unione Europea.
La seconda giornata del NESSI ha rappresentato un'importante occasione di riflessione e pianificazione per il futuro del Network, con l'obiettivo di consolidare la collaborazione e il dialogo tra i principali attori nel settore della difesa e della sicurezza in Europa. La giornata è stata arricchita dall'intervento del Professor Andrea Bernardi, del CASD, che ha presentato: "Wargaming at CASD". Sono state così ripercorse le origini del *wargaming*, dai primi giochi risalenti al V secolo a.C. in Grecia fino all'introduzione degli scacchi nel VI secolo d.C. in India e la loro successiva diffusione in Persia ed Europa. Ha poi evidenziato come il periodo più florido per lo sviluppo di queste simulazioni sia stato la Guerra Fredda, durante la quale il *wargaming* divenne uno strumento fondamentale per la pianificazione strategica delle grandi potenze. Il CASD, ha spiegato Bernardi, si concentra su *war games* di livello strategico, volti a sviluppare capacità analitiche e a preparare i partecipanti alla gestione di scenari complessi. Il *war game* presentato simula un confronto tra le potenze locali e le influenze di Russia e Cina nella regione. Il professor Bernardi ha concluso sottolineando i rischi legati all'uso di tali giochi strategici, tra cui la difficoltà di rappresentare scenari realistici, come dimostrato dall'esempio dell'invasione russa in Ucraina. Tuttavia, queste simulazioni hanno contribuito a delineare una risposta occidentale coordinata, confermando il valore strategico del *wargaming* nella gestione delle crisi.
Nell'evento conclusivo, i partecipanti hanno discusso il futuro del NESSI e designato Bucarest come sede per il prossimo incontro nel 2025. Questa scelta

rappresenta un impegno concreto del Network nel consolidare la cooperazione strategica tra i Paesi membri e nell'affrontare con unità le sfide comuni, ribadendo l'importanza di un dialogo sempre più integrato e mirato a costruire una cultura di difesa comune europea.

Luce Gatteschi
Doppia Laurea Triennale in Scienze Politiche presso le università di SciencesPo Toulouse e Universidad Complutense de Madrid; Master's Degree in European Affairs presso SciencesPo Toulouse; Master in Sicurezza Economica, Geopolitica e Intelligence presso SIOI e Master in Studi Diplomatici presso ISPI.

Federico Girotti
Dottore in Economia e Laureando Magistrale in Scienze della Pace e della Cooperazione Internazionale presso Università Pontificia Lateranense

Barbara Raimondi
Dottoressa in Scienze per l'Investigazione e la Sicurezza e Laureanda in Scienze Strategiche presso l'Università degli Studi di Torino

CONFERENZA "IL TRICOLORE NEL MARE: DAL MEDITERRANEO ALL'ARTICO" – 29 OTTOBRE 2024

Il 29 ottobre 2024 si è tenuta presso il Centro Alti Studi per la Difesa (CASD) una conferenza intitolata "Il Tricolore nel Mare: dal Mediterraneo all'Artico". L'evento, organizzato grazie alla collaborazione tra il CASD, la Società Italiana di Intelligence (SOCINT), l'Osservatorio Nazionale Tutela Mare (ONTM), l'Università della Calabria e Limes, si è proposto di approfondire le sfide marittime che l'Italia e l'Europa devono affrontare nei contesti del Mediterraneo e della regione artica. La conferenza, moderata da Giorgio Rutelli, Vicedirettore di Adnkronos, ha visto la partecipazione di un prestigioso panel di esperti.

Interventi Principali
La conferenza è stata aperta da intervento del Generale di Brigata Aerea Danilo Morando, sostituto del Generale Stefano Mannino, Presidente del CASD. L'introduzione ha sottolineato l'importanza strategica della dimensione marittima per la sicurezza nazionale e la prosperità economica dell'Italia.

Sicurezza Marittima e Sfide Strategiche
L'Ammiraglio Giuseppe Berutti Bergotto, Sottocapo di Stato Maggiore della Marina Militare Italiana, ha evidenziato la rilevanza globale delle rotte marittime, ricordando che il 90% del commercio mondiale e una parte considerevole del traffico internet dipendono dalle vie marittime. Il Mediterraneo, che ospita il 20% del traffico commerciale mondiale, rappresenta un collegamento cruciale tra l'Indo-Pacifico e l'Atlantico ed è soggetto a

crescenti pressioni da parte di attori non statali e tensioni geopolitiche. L'Ammiraglio ha enfatizzato la creazione del "Polo Nazionale della Dimensione Subacquea" come centro per integrare la ricerca e la tecnologia italiane al fine di potenziare applicazioni sia militari che civili. Le riflessioni di Berutti hanno incluso le minacce in evoluzione alla sicurezza marittima, come l'aumento della presenza navale russa e i conflitti regionali in Nord Africa che influenzano le rotte commerciali. Dinamiche che hanno portato a una riduzione del 40% dell'attività di *import-export* attraverso il Mar Rosso, con conseguenti aumenti dei prezzi per i consumatori e maggiori emissioni di CO2 a causa della logistica deviata.
Giorgio Rutelli ha enfatizzato l'importanza strategica del Mediterraneo, evidenziando quanto rischino le navi occidentali non protette, spesso attaccate nel Mar Rosso, mentre quelle russe e cinesi non subiscano assalti grazie ad accordi approvati dall'Iran. Ha sottolineato come ciò rappresenti un costo significativo per l'Italia, ribadendo il ruolo cruciale del Paese come *hub* per le comunicazioni e l'energia verso l'Africa e il Medio Oriente.

Intelligenza, Innovazione e Artico
Mario Caligiuri, Presidente di SOCINT, ha sottolineato il ruolo cruciale dell'*intelligence* come fondamento per la preparazione futura, affermando che il XXI secolo è caratterizzato da strategie guidate dall'*intelligence*. Ha messo in luce le vulnerabilità dell'Italia in ambito demografico e nel sistema educativo, fattori che indeboliscono la resilienza sociale e la vitalità economica. Tuttavia, ha evidenziato i punti di forza del Paese, come l'innovazione, la cultura e la posizione strategica nel Mediterraneo, rimarcando la necessità di rafforzare la sicurezza portuale e valorizzare l'eredità marittima. Caligiuri ha inoltre menzionato il recente protocollo d'intesa tra SOCINT e ONTM, volto a consolidare la cooperazione nell'analisi e nella gestione delle sfide marittime.
Ferdinando Sanfelice di Monteforte, Presidente dell'Osservatorio di Intelligence sull'Artico, ha spostato l'attenzione sugli interessi italiani nell'Artico, sia storici che contemporanei. Ha richiamato le esplorazioni italiane del XV secolo, come quelle di Pietro Guerini e ha discusso le motivazioni economiche e strategiche legate all'impegno nell'Artico. Al tempo stesso ha avvertito sulla realtà dell'approccio militarizzato della Russia nel Passaggio a Nord-Est, confrontandolo con lo sviluppo del Passaggio a Nord-Ovest da parte del Canada, che, nonostante le sfide logistiche, rappresenta un'opportunità per l'Italia di diversificare le rotte commerciali.

Il Mediterraneo come Hub Strategico
Roberto Minerdo, Presidente di ONTM, ha esplorato l'importanza dei cavi sottomarini nel Mediterraneo, essenziali per la distribuzione energetica e la trasmissione dei dati. Ha sottolineato il ruolo dell'Italia come hub energetico, rafforzato da progetti come il gasdotto EastMed e il TAP in Puglia, divenuti cruciali a seguito della crisi energetica europea scaturita dal conflitto tra Russia e Ucraina. La resilienza e la posizione strategica delle infrastrutture sottomarine sono fondamentali per mantenere la sicurezza energetica e la stabilità economica.
Laura Canali, cartografa di Limes, ha offerto una panoramica geopolitica, evidenziando come il Mediterraneo non benefici di Zone Economiche Esclusive (ZEE) uniformi, al contrario di altre regioni marittime. Ciò crea tensioni

diplomatiche complesse, in particolare con la dichiarazione unilaterale di una ZEE da parte dell'Algeria, complicando la sovranità marittima italiana e richiedendo strategie negoziali robuste. La situazione nel Mediterraneo si complica ulteriormente a causa dell'Alleanza militare tra Russia e Algeria, con quest'ultima fortemente dipendente da Mosca per le forniture di armi, a cui si aggiunge l'instabilità persistente in Paesi quali lo Yemen e la Libia. Di fronte a questa trasformazione geopolitica, la questione che emerge riguarda come confrontarsi con una "nuova identità" del Mediterraneo, non più percepito come stabile ma caratterizzato da una dinamica continuamente mutevole.

Interventi Regionali e Prospettive Storiche

Pasquale Ciacciarelli, Assessore alle Politiche del Mare della Regione Lazio, ha presentato un quadro della situazione marittima regionale, con un *focus* sui porti di Civitavecchia e Gaeta. Ha sottolineato come il Lazio si configuri come un *hub* turistico e commerciale nel Mediterraneo, illustrando il piano di sviluppo delle infrastrutture portuali e turistiche, condividendo riflessioni sulla necessità di riforme che potenzino la capacità regionale.

Andrea Manciulli, VP European and NATO relations di Fincantieri e Presidente fondazione Fincantieri, ha approfondito la prospettiva storica del Mediterraneo come snodo strategico. Ha ricordato come, fino al Medioevo, il Mediterraneo fosse il fulcro degli scambi commerciali e culturali, collegato alla Via della Seta. La caduta della Pax Mongolica e le incursioni barbariche portarono al declino della via terrestre, costringendo l'Occidente a esplorare nuove rotte marittime e scoprire nuovi continenti, inaugurando l'era atlantica. Manciulli ha sottolineato come il progetto cinese della "Nuova Via della Seta" rappresenti una sfida all'ordine atlantico, ribadendo che la centralità del Mediterraneo può essere sia un motore di progresso in tempi di pace che una fonte di instabilità in tempi di conflitto.

Complessità Artiche e Iniziative Future

Emanuela Somalvico, Direttrice dell'Osservatorio di Intelligence sull'Artico, ha delineato i molteplici rischi presenti nella regione artica, dai virus emergenti a causa del disgelo alle manovre geopolitiche di attori statali e non statali. L'approccio olistico dell'Osservatorio include valutazioni dei rischi riguardanti l'impatto ambientale, gli investimenti infrastrutturali e la sicurezza dei dati. La Direttrice ha, infine, ribadito l'importanza della cooperazione internazionale e di una posizione unitaria italiana per tutelare gli interessi nazionali.

Conclusioni e Osservazioni Finali

Nella parte conclusiva, Federico Ottavio Pescetto, Direttore Generale di ONTM, ha riaffermato l'importanza parallela delle regioni mediterranee e artiche per il futuro strategico dell'Italia. Entrambe richiedono uguale attenzione per garantire che l'influenza e la prontezza italiane siano in linea con le trasformazioni globali. Pescetto ha sollecitato investimenti in personale specializzato e tecnologie innovative per mantenere la competitività italiana.

La conferenza ha rappresentato una piattaforma cruciale per promuovere il dialogo e l'allineamento strategico tra i settori militari, accademici e geopolitici italiani, aprendo la strada a future collaborazioni.

Federico Girotti

Dottore in Economia e Laureando Magistrale in Scienze della Pace e della Cooperazione Internazionale presso Università Pontificia Lateranense

ANALISI DELLE ELEZIONI PRESIDENZIALI USA 2024

Relatore: Professoressa Daniela Giannetti, Università di Bologna

La conferenza, tenutasi al Centro Alti Studi per la Difesa il 14 novembre 2024, dalla Prof.ssa Daniela Giannetti, ordinaria di Scienza Politica presso l'Alma Mater Studiorum – Università di Bologna, ha offerto un'analisi approfondita delle recenti elezioni presidenziali statunitensi. La discussione ha riguardato il sistema elettorale, l'analisi dei risultati e le implicazioni politiche per gli Stati Uniti e per l'Europa. Sono stati evidenziati i principali fattori che hanno caratterizzato queste elezioni, tra cui la crescente polarizzazione politica, il ruolo degli "*swing states*" e l'impatto della disinformazione.

La prima parte del seminario si è concentrata sull'analisi del sistema elettorale statunitense, descrivendo in modo dettagliato i meccanismi del voto e i risultati ottenuti nell'ultima elezione presidenziale. La professoressa ha evidenziato come Donald Trump sia riuscito a ottenere sia il voto popolare che il Collegio Elettorale, un risultato relativamente raro, poiché in molte elezioni i vincitori del voto popolare non corrispondono ai risultati del Collegio Elettorale. È stato poi sottolineato il ruolo cruciale degli "*swing states*", come la Pennsylvania, dove i Repubblicani sono riusciti a prevalere seppur con un margine ridotto. Al tempo stesso, Giannetti ha osservato che le grandi città tendono ad essere più favorevoli ai Democratici, mentre le aree rurali sono generalmente più inclini a votare per i Repubblicani. La percentuale di partecipazione elettorale è stata molto elevata, con una significativa diversificazione nei gruppi demografici e sociologici. In particolare, Trump ha ottenuto un ampio consenso tra le fasce di età più avanzate, ma anche tra i giovani e in alcune minoranze etniche, tra cui gli ispanici, che tradizionalmente tendono a votare Democratico.

Un tema centrale della discussione è stato il fenomeno della crescente polarizzazione negli Stati Uniti, con gli elettori che tendono a percepire l'opposizione politica come un "nemico" piuttosto che un interlocutore con cui negoziare. La disinformazione e la propaganda interna hanno avuto un impatto determinante, alimentando narrazioni che hanno esacerbato le divisioni

politiche, soprattutto su temi sensibili come l'aborto e altre questioni culturali. La professoressa ha esaminato diversi dati economici, evidenziando il miglioramento dell'occupazione e la riduzione dell'inflazione durante la presidenza Biden. Nonostante tali dati positivi, la percezione dell'economia è rimasta negativa, fattore usato a proprio favore nella campagna elettorale di Trump, così come la preoccupazioni legate all'immigrazione illegale, l'aumento percepito della criminalità e altri aspetti supportati da dati, ma strumentalizzati spesso in modo opposto alle evidenze statistiche.

La conferenza si è conclusa con una riflessione sul futuro della democrazia americana e sulle sue implicazioni globali. Giannetti ha posto così una domanda provocatoria riguardo a quale sarà il futuro dell'Unione Europea in relazione agli *shock* esterni che potrebbero derivare dalla politica estera di Trump, suggerendo che la risposta dell'UE potrebbe richiedere un ripensamento delle proprie politiche di difesa e cooperazione internazionale.

R E C E N S I O N I

Laura SOLIDORO

DALLA DOMINICALITÀ AL NEOPROPRIETARISMO. STORIA E NARRAZIONI DI UN PERCORSO

Ed. Giappichelli, Torino 2023, «Teoria e Storia del Diritto» vol. 2, pp. 152;
ISBN 979-1221102581

La proprietà ed il diritto di proprietà sono, forse da sempre, uno dei grandi temi d'indagine. Così da Crisippo a Panezio, passando per Blackstone, fino a Marx ed oltre, i giuristi e, insieme a loro, i filosofi del diritto nonché gli storici del diritto, si sono interrogati non solo su cosa sia la proprietà ma anche sulla funzione che il diritto debba attribuire alla stessa, giungendo spesso a conclusioni diametralmente opposte. In breve, il concetto di proprietà nel corso dei secoli, anzi dei millenni (se si osserva anche il "diritto" dei popoli del Vicino Oriente Antico), ha mostrato una incredibile complessità, in quanto le funzioni della proprietà sono, nello spazio-tempo, mutate. Orbene il libro di Laura Solidoro, che è il secondo volume della collana "Teoria e Storia del Diritto", indaga, partendo proprio dalle radici romanistiche - ecco il lemma "dominicalità" - tale percorso in chiave squisitamente storico-giuridica.

Nel fare ciò l'Autrice suddivide il percorso di ricerca in due ampi capitoli: un primo intitolato "Il decorso della proprietà" (pp. 1-75) ed un secondo "Uno sguardo alla storia: la "proprietà obbliga" (pp. 77-145).

L'A. sottolinea come la vigente concezione europea della proprietà sia ancorata al concetto romanistico della dominicalità (ricordandoci che le radici giuridiche europee sono i pilastri del diritto romano), ma guardando anche all'esperienza giuridica della Common Law (in cui *ownership* e *property* costituiscono una sorta di ambigua distinzione lessicale). Oggi il diritto europeo vede la proprietà come un *quid* da tutelare da parte degli ordinamenti giuridici nazionali.

Su questo scenario, così complesso, che nei secoli si è arricchito di riflessioni filosofiche ed ideologiche, si inserisce il "neoproprietarismo", sorto negli anni ottanta del secolo scorso, frutto a sua volta del liberalismo, in cui la proprietà viene considerata come assoluta e pertanto viene collocata in relazione alla sfera della libertà. Tuttavia, come osserva l'A., la proprietà completamente assoluta e priva di funzione sociale non è mai realmente esista, nemmeno nell'ordinamento giuridico romano che poneva dei limiti - per es. in tema di *decus urbis* - pur sostenendo sempre la tutela processuale della proprietà intesa come diritto da difendere. Soprattutto per lo storico del diritto romano molto interessante appare il secondo capitolo, in cui l'A. tratteggia con maestria gli aspetti romanistici della proprietà romana, che era organizzata giuridicamente sul concetto di limite. Proprio i "limiti" che l'ordinamento giuridico romano pose nel tempo alla

proprietà, pur non abdicando mai alla difesa del diritto di proprietà, possono oggi essere "rispolverati" dal giurista contemporaneo in chiave anti-neoproprietaristica. Ancora una volta i Romani ci forniscono "lezioni dal passato".
Dunque, l'Autrice offre al lettore un percorso storico-giuridico di primissimo livello, articolando la problematica con chiarezza espositiva e narrativa e induce così a riflettere e a considerare un'esegesi delle attuali normative (art. 295 del TCE, poi il Trattato di Lisbona del 2009 aderente alla CEDU, nonché i pronunciamenti della Corte EDU) che tutelano il diritto di proprietà ponendolo in connessione con l'economia di mercato, in cui vige il principio del garantismo concorrenziale.
In estrema sintesi, la monografia di Laura Solidoro rappresenta un momento di chiarezza sia per lo storico del diritto che per il giurista, ma anche per coloro che si dedicano alle "radici" dei diritti europei.

Danilo Ceccarelli Morolli

Francesco ANGHELONE - Andrea UNGARI

ATLANTE GEOPOLITICO DEL MEDITERRANEO 2024

10a edizione

Edizioni Bordeaux, Roma 2024, pp. 570;
ISBN 979-1259632333

L'Atlante geopolitico del Mediterraneo curato da Francesco Anghelone e Andrea Ungari, giunto alla sua decima edizione, si impone all'attenzione del lettore e del cultore di geopolitica *in primis* per una rinnovata e aggiornata veste grafica che ne agevola ancor di più la lettura e parimenti per l'interesse dei contenuti che esprime.

Il libro è impreziosito da una *Prefazione* del prof. Paolo De Nardis (Direttore dell'Osservatorio sul Mediterraneo dell'Istituto di Studi Politici "S. Pio V", pp. 7-9) e da una *Introduzione* del prof. Gianluigi Rossi (emerito di Storia dei trattati e Politica *internazionale* dell'Università "Sapienza di Roma" nonché maestro di molte generazioni di studiosi, pp. 11-13).

Questo corposo atlante presenta una interessante "prima parte", intitolata "approfondimenti", in cui vengono editi tre saggi che fungono da *ouverture*, non priva di riflessioni, su ciò che poi il lettore troverà nel volume a livello di dati; gli scritti in questione sono i seguenti: «*La dimensione mediterranea della politica estera italiana fra Atlantico ed Europa (1949-1969)*» redatta da Bruna Bagnato (pp. 23-45); «*La politica estera italiana ed il "Mediterraneo Allargato" dalla crisi del centro-sinistra ad oggi*», stilata da Antonio Varsori (47-71), ed infine, «*La politica estera italiana e il Medio Oriente negli anni della Repubblica*» vergato da Luca Riccardi (pp.73-101). Nella seconda parte dell'opera si trovano una serie ordinata e ben fatta di "schede" dei Paesi del Mediterraneo. Interessante rilevare che i curatori abbiano incluso tra i "Paesi" anche l'Autorità Nazionale Palestinese; questo potrebbe destare delle critiche.

Infine, l'Atlante contiene anche una interessante terza parte, costituita da altri tre contributi, in forma di approfondimento specifico: «*Italia e Tunisia: sfide e criticità nel più ampio contesto internazionale*» di Mario Savina (pp. 519-526); «*La proiezione futura dei rapporti energetici tra Algeria e Italia*» di Laura Ponte (pp. 527-535); «*NATO e UE al cospetto della crisi libica: dall'apice al tramonto del 'crisis managment' occidentale?*» (536-545) di Stefano Marcuzzi.

Conclude il volume un'utile bibliografia sui singoli Paesi (pp. 549-564) a cui seguono le note biografiche di tutti gli Autori che hanno preso parte a tale progetto (pp. 567-570).

Ne risulta un volume agile nella lettura ma denso di dati che suscitano inevitabili riflessioni nel lettore — sia per il neofita che quello più esperto in relazioni internazionali o in geopolitica — per cui si può certamente asserire che il

presente lavoro si conferma essere uno strumento prezioso di studio e di ricerca. In esso, si delinea anche la politica estera italiana sul Mediterraneo e con essa *de facto* il concetto non solo di "Mediterraneo Allargato", ma anche, come qualcuno ha asserito, di Mediterraneo "allungato" poiché idealmente l'Atlante traccia una linea ideale da Nord a Sud.
Il risultato complessivo di questa decima edizione dell'Atlante è oltremodo apprezzabile non solo per la sua scientifica utilità ma anche per la facilità di consultazione, imponendosi così nel panorama degli strumenti, in lingua Italiana, non solo didattici ma anche di ricerca per la sfera geopolitica, continuando in tal modo nel solco di una tradizione "annalistica ed enciclopedica" che, per la geopolitica, possiamo far risalire al celebre *Annuaire de l'Afrique du Nord* (edito dal 1952 al 2003).

Danilo Ceccarelli Morolli

STRATEGIC LEADERSHIP JOURNAL
Challenges for Geopolitics and Organizational Development

CODICE ETICO

"STRATEGIC LEADERSHIP JOURNAL. Challenges for Geopolitics and Organizational Development" (di seguito SLJ) è una rivista peer-reviewed che si ispira al codice etico delle pubblicazioni elaborato dal COPE (Commitee on Publication Ethics). Pertanto assume tutte le decisioni necessarie contro eventuali frodi che si possano verificare nel corso della pub- blicazione di un lavoro sulla rivista stessa. Le parti coinvolte - Organi istituzionali, Referee e Autori - devono conoscere e condividere i seguenti requisiti etici.

DOVERI DEGLI ORGANI ISTITUZIONALI DI SLJ

1. Compete alla Direzione, con il supporto del Comitato Scientifico e del Comitato Editoriale, la scelta finale degli articoli che saranno pubblicati in SLJ, effettuata tra i contributi pervenuti in Redazione, sulla base delle risultanze della peer-review.
2. La scelta viene effettuata esclusivamente sulla base del contenuto scientifico e intellettuale e senza discriminazioni di razza, genere, orientamento sessuale, religione, origine etnica, cittadinanza, orientamento politico degli autori.
3. Gli articoli scelti verranno sottoposti alla valutazione di Revisori e la loro accettazione è subordinata all'esecuzione di eventuali modifiche richieste e al parere conclusivo della Direzione.
4. Il Direttore Scientifico e i componenti del Comitato Scientifico e del Comitato Editoriale si impegnano a non rivelare informazioni sugli articoli proposti dagli autori e pervenuti in Redazione, nonché sugli esiti dei referaggi, verso terzi estranei alla composizione degli organi di SLJ.
5. Le comunicazioni concernenti il contributo elaborato possono intercorrere con l'autore o con i valutatori ai soli fini del referaggio.
6. Il Direttore Scientifico, i componenti del Comitato Scientifico, del Comitato Editoriale e i valutatori si impegnano a non usare in ricerche proprie, senza esplicito consenso dell'autore, i contenuti di un articolo proposto per la pubblicazione/ revisione.
7. Se alcuno degli organi di SLJ rileva o riceve segnalazioni in merito a eventuali conflitti di interessi o plagio in un articolo pubblicato ne darà tempestiva comunicazione alla Direzione.
8. SLJ rende noto nel proprio colophon i nomi del Direttore Responsabile e dei componenti del Comitato Scientifico, del Comitato Editoriale e della Redazione.

REFEREE

1. Gli articoli pubblicati sono soggetti alla valutazione dei referee secondo il sistema di peer-review c.d. "double-blind" (I revisori non conoscono gli autori e gli autori non sanno chi sono i revisori).
2. Attraverso la procedura di peer-review (double blind) i referee assistono gli Organi di SLJ nell'assumere decisioni sugli articoli proposti ed inoltre possono suggerire all'autore emendamenti tesi a migliorare il proprio contributo.
3. Qualora i referee non si sentano adeguati al compito proposto o sappiano di non poter procedere alla lettura dei lavori nei tempi richiesti sono tenuti a comunicarlo tempestivamente alla Redazione.
4. Ciascun contributo pubblicato in SLJ è sottoposto al giudizio di referee.
5. I referee sono selezionati dalla Direzione o dal Comitato Scientifico o dal Comitato Editoriale - in considerazione del settore scientifico-disciplinare cui risulta riferibile il saggio da valutare - tra professori, ricercatori e studiosi, in ruolo o in quiescenza, ovvero esperti particolarmente qualificati nelle singole materie o discipline.
6. Il giudizio del referee viene comunicato all'autore in forma anonima.
7. Il contenuto dei referaggi è riservato, fatto salvo per le informazioni e comunicazioni eventualmente richieste dai competenti organi di valutazione del sistema universitario nazionale.
8. Il referaggio deve avere ad oggetto il contenuto dell'articolo, i risultati raggiunti, il metodo seguito, la chiarezza dell'esposizione.
9. I referee segnalano alla Redazione eventuali sostanziali somiglianze o sovrapposizioni del testo ricevuto con altre opere a loro note.
10. I referee si impegnano a considerare riservate tutte le informazioni o indicazioni ottenute durante il processo di peer-review e a non discutere i testi con altre persone senza esplicita autorizzazione della Direzione.

11. Le revisioni dei referee devono essere ispirate da criteri di oggettività e imparzialità, in un'ottica di critica costruttiva. Il feedback che forniscono deve essere d'aiuto agli autori per migliorare la qualità del manoscritto, fatta salva la possibilità di giudicare non pubblicabile l'articolo stesso.
12. In considerazione del particolare prestigio o rilevanza di taluni autori, il Direttore Responsabile e il Direttore Scientifico possono, dopo essersi consultati, decidere di pubblicare un articolo senza che questo sia stato sottoposto a referaggio. In tal caso, l'articolo sarà edito con la dicitura "su invito della Direzione".

AUTORI

1. Gli articoli devono essere frutto di ricerche originali degli autori. Dagli articoli deve potersi ricavare il metodo seguito e i risultati raggiunti.
2. Se l'articolo è il frutto del contributo di più autori, essi vanno tutti riconosciuti quali coautori e l'articolo, qualora pubblicato, recherà tutti i nominativi dei singoli autori.
3. Gli autori non devono inviare a SLJ articoli nella sostanza uguali ad altri già pubblicati da loro stessi o da altri.
4. Gli autori, nell'inviare i loro contributi per la pubblicazione in SLJ, si impegnano a non sottoporre gli stessi ad altre riviste ai fini di pubblicazione in Italia e all'estero.
5. Gli autori devono citare ogni fonte, propria o altrui, che sia automaticamente rilevante rispetto al lavoro. Ogni genere di dato, formulazione, figura o idea presa da altri deve essere appropriatamente citata e non può mai essere spacciata come propria.
6. Nel caso in cui gli autori riscontrino un errore all'interno di un manoscritto inviato in valutazione, devono immediatamente informare la Redazione e richiedere eventuali correzioni o la ritrattazione di precedenti affermazioni.
7. Nella redazione degli articoli da proporre per la pubblicazione, gli autori devono attenersi a quanto previsto nelle Norme redazionali consultabili al seguente link:
https://www.difesa.it/smd/casd/im/irad/pubblicazioni-irad/index/35995.html

ELENCO REFEREE

Dr. Antinori Arjie, Dr. Artoni Maurizio, Dr.ssa Astarita Claudia, Prof. Bagarani Massimo, Dr. Baggiani Gregorio, Dr. Baldelli Pietro, Dr. Balduccini Mauro, Dr. Batacchi Pietro, Dr. Beccaro Andrea, Prof. Bernardi Andrea, Prof. Battistelli Fabrizio, Dr.ssa Boldrini Chiara, Dr. Bongioanni Carlo, Dr.ssa Bonomo Silvia, Dott. Borsani Davide, Dr. Bressan Matteo, Dr. Bruschi Luigi, Dr.ssa Carallo Gemma, Dr. Catalano Claudio, Dr.ssa Citossi Francesca, Dr.ssa Ciampi Annalisa, Dr. Cochi Marco, Dr.ssa Coco Antonella, Prof. Colacino Nicola, Dr. Colantonio Antonio, Dr. Coticchia Fabrizio, Dr.ssa Di Chio Raffaella, Dr. Di Leo Alessio, Dr. Di Liddo Marco, Dr. Dian Matteo, Dr. Donelli Federico, Prof.ssa Eboli Valeria, Dr. Fasola Nicolò, Dr. Felician Beccari Stefano, Dr.ssa Feola Annamaria, Dr. Fontana Simone, Prof. Foresti Gian Luca, Dr. Frappi Carlo, Prof. Gaspari Francesco, Prof. Gennaro Alessandro, Dr.ssa Gravina Rossana, Dr. Grazioso Andrea, Prof.ssa Icolari Maria Assunta, Dr. Indeo Fabio, Prof.ssa Irrera Daniela, Prof. La Bella Simone, Dr.ssa La Regina Veronica, Dr.ssa La Rosa Anna, Dr. Locatelli Andrea, Prof. Lombardi Marco, Dr. Macrì Paolo, Dr. Marcovina Marco, Dr. Marcuzzi Stefano, Dr. Marone, Francesco, Dr. Marrone Alessandro, Dr. Marsili Marco, Dr.ssa Martini Francesca, Prof. Martini Matteo, Dr. Mastrolia Nunziante, Dr.ssa Mauro Marlene, Prof.ssa Melcangi Alessia, Dr. Mele Stefano, Prof. Merlo Alessio, Dr. Napolitano Paolo, Dr. Negri Michele, Dr.ssa Nocerino Wanda, Dr.ssa Palloni Elena, Dr. Pasquazzi Simone, Dr. Pastori Gianluca, Dr. Pedde Nicola, Prof. Peluso Pasquale, Prof. Pezzimenti Rocco, Dr. Pezzoli Carlo, Dr. Pignatti Matteo, Dr.ssa Pistoia Emanuela, Dr. Pompei Alessandro, Dr. Rizzolo Ivan, Prof.ssa Rossi Marzia, Dr.ssa Rutigliano Stefania, Dr. Ruzza Stefano, Dr. Stilo Alessio, Dr. Striuli Lorenzo, Dr.ssa Trenta Elisabetta, Dr.ssa Triggiano Annalisa, Prof. Ugolini Francesco, Prof. Ursi Riccardo, Prof. Vagnini Alessandro, Prof. Valentini Tommaso, Dr. Vasaturo Giulio, Dr. Veca Mario, Dr. Vergura Silvano, Dr. Verzotto Davide, Dr. Viola Paolo, Dr. Zacchei Alessandro, Dr.ssa Zawadzka Sylwia.

ALCUNE INFORMAZIONI UTILI

Al fine di proporre un articolo per la pubblicazione in SLJ, è necessario:

- inviare il file (Word o Pages) del testo al seguente indirizzo di posta elettronica: redazione.slj@gmail.com;
- accludere, con file separato, un breve *abstract* del proprio curriculum (massimo 6 righe);
- accludere, con file separati, eventuali immagini, corredate da apposita didascalia.

Gli articoli sono soggetti a *Peer Review - Double Blind*.

Nel redigere l'articolo, gli Autori sono pregati di seguire le regole metodologico-redazionali (*desiderata*), consultabili al seguente link:
https://www.difesa.it/smd/casd/im/irad/pubblicazioni-irad/index/35995.html

***

Coloro i quali desiderino ricevere SLJ in formato pdf al proprio indirizzo e-mail possono indicare il nominativo e l'indirizzo di posta elettronica alla presente casella, così da poter essere inseriti nella "mailing list": *redazione.slj@gmail.com*

***

In order to submit a paper for SLJ, it is necessary to:

- Send the Word or Pages file to the following email address: redazione.slj@gmail.com;
- Attach, as a separate file, a brief abstract of your curriculum (maximum 6 lines);
- Attach any images separately, accompanied by a suitable caption.

Authors submitting articles are hereby informed that their paper will undergo *Peer Review - Double Blind*.

Authors are kindly requested to adhere to the following methodological and editorial guidelines (desiderata), downloadable from the following link:
https://www.difesa.it/smd/casd/im/irad/pubblicazioni-irad/index/35995.html

***

Readers who wish to receive a PDF of the SLJ at their own email address are kindly requested to subscribe to the following mailing list: *redazione.slj@gmail.com*

Stampato dalla Tipografia del
Centro Alti Studi Difesa

CENTRO ALTI STUDI DIFESA

SCUOLA SUPERIORE UNIVERSITARIA

LA NOSTRA MISSION

Sviluppare una leadership etica, equa e responsabile al servizio della comunità, nazionale e internazionale, attraverso una formazione d'eccellenza che potenzi talenti e competenze, valorizzi le differenze e costruisca nuova conoscenza mediante la ricerca e l'innovazione.

LA NOSTRA VISION

Costituire un punto di riferimento nel panorama nazionale e internazionale e divenire snodo vitale nella rete delle relazioni strategiche, per far fronte con successo al complesso scenario del mondo attuale.

STRATEGIC LEADERSHIP
JOURNAL

9 791255 150787