ALEXIS

TESTI PER IL DIALOGO EURO MEDITERRANEO

"Egitto 1975. Posa tubi" - ARCHIVIO STORICO ENI

Estate 2025
www.geodi.unint.eu

INDICE DEI CONTENUTI

01 EDITORIALE

02 ATTI DI CONVEGNO

03 RECENSIONI E SCHEDE

Alexis. Testi per il dialogo giuridico euro-mediterraneo

ISSN 2420-966X - Trimestrale
Testata registrata presso il Tribunale di Roma n. 414/09

Rivista del centro studi GEODI – Geopolitica e diritto comparato
Università degli Studi internazionali di Roma – UNINT
via Cristoforo Colombo, 200 – 00147, Roma
Tel. (39) 06510777258
www.unint.eu
geodi@unint.eu

Gli articoli della sezione Saggi e della sezione Osservatorio Costituzionale sull'Occidente
sono sottoposti a doppio referaggio anonimo.
I contributi delle altre sezioni sono sottoposti a referaggio interno.

Editoriale

La curvatura tecnica del potere: diritto e geopolitica nell'era dell'esponenzialità

Ciro Sbailò
Professore ordinario di Diritto pubblico comparato - Università degli Studi Internazionali di Roma (UNINT)

Il percorso che conduce a questo numero speciale prende avvio nella cornice della Call for Papers lanciata da GEODI per le giornate del 14 e 15 ottobre 2024, la cui struttura scientifica e tematica è stata curata da Andrea De Petris e Giuseppe Terranova: un giurista e un geografo, a testimonianza della necessità – oggi ineludibile – di leggere insieme tecnica, spazio e norma. L'intento era interrogare lo scarto crescente tra l'accelerazione tecnologica che ridisegna la guerra e la lentezza con cui diritto e politica riescono a seguirne il ritmo. La tesi di fondo, richiamata nel documento preparatorio, è che la divergenza tra l'andamento esponenziale delle tecniche belliche e l'andamento lineare delle categorie giuridiche che dovrebbero governarle produce una zona di rischio sistemico: un differenziale epistemico che indebolisce la capacità decisionale e rende urgente una ricognizione comune tra diritto comparato, geopolitica e riflessione epistemologica, anche al fine di orientare – o almeno supportare – la decisione politica.

Il 14 ottobre, nella sede del Centro GEODI, si è svolta la sessione dedicata ai contributi selezionati tramite Call. Giovani studiosi e ricercatori sono stati chiamati a confrontarsi, sotto la presidenza di Paolo Passaglia, su questioni che non appartengono più a piani separati ma convergono nello stesso campo di forze: l'esponenzialità tecnologica, i nuovi problemi costituzionali, la cyber war, il dual use, la trasformazione della sovranità, la geografia invisibile

dei cavi marini, il rapporto fra decisione politica e pressione tecnica. È in quella giornata che sono emerse le linee teoriche che definiscono l'identità stessa della nostra attività di ricerca: una sintassi in cui diritto e geopolitica non dialogano, ma si implicano.

Il 15 ottobre, nell'Aula Magna dell'Ateneo, questa trama concettuale ha trovato la sua proiezione pubblica con il convegno "Diritto comparato e geopolitica di fronte alle sfide della politica estera e di sicurezza europea". La giornata, presieduta da Giuseppe Pisicchio e costruita anch'essa sulla linea scientifica definita da De Petris e Terranova, è stata aperta da una mia introduzione che ha ricollocato i lavori del giorno precedente nella crisi più ampia dell'ordine europeo. Le relazioni di Jorge Lozano Miralles, Paolo Passaglia e Paola Piciacchia hanno mostrato come il diritto non sia un orizzonte neutrale rispetto alla guerra tecnologica, ma una struttura che ne subisce la pressione e ne riflette le asimmetrie.

Lo Spazio GEODI, con gli interventi di Matteo Costola, Gaia Natarelli, Giovanna Spanò e Vanni Nicolì, ha confermato la capacità delle nuove generazioni di ricerca di muoversi in un ambiente concettuale non lineare, dove istituzioni e tecnica non possono più essere pensate come ambiti distinti. La conclusione della giornata è stata affidata alla senatrice Stefania Craxi, Presidente della Terza Commissione Affari Esteri e Difesa del Senato, che ha restituito al dibattito la sua piena dimensione politica: la sicurezza, oggi, non è una politica pubblica, ma la condizione stessa della continuità democratica nello spazio europeo. I lavori della seconda giornata sono disponibili sul canale YouTube della UNINT, su geodi.unint.eu e su radioradicale.it.

I saggi raccolti in questo fascicolo costituiscono il deposito teorico elaborato il 14 ottobre e il riferimento del dibattito del giorno successivo. Andrea Cafiero ridisegna la geografia dei conflitti contemporanei intrecciando territorio e informazione. Fabio Di Nunno affronta il nodo dei sistemi d'arma autonomi indicando nella responsabilità il punto critico dell'automazione bellica. Matteo Fulgenzi mostra come il dominio digitale costituisca il nuovo teatro invisibile del potere. Francesca Martini illumina gli spazi sottomarini, oggi decisivi per la sovranità tecnologica. Andrea Ruffo indaga la pressione della cyber war sulle categorie costituzionali. Mario Schirripa analizza la logica delle guerre ibride come ecosistema cognitivo. Francesco Severa interpreta la difesa europea attraverso la nozione di grande spazio, evidenziando il rapporto fra forma geopolitica e struttura istituzionale.

Questi contributi mostrano che la tecnica non accompagna la politica, la precede; che la guerra non interrompe l'ordine, lo rivela; che il diritto non fotografa il mondo, ma lo interpreta e lo orienta. Le giornate del 14 e del 15 ottobre hanno dato voce a questa consapevolezza, trasformando un insieme di interventi in una lettura unitaria del nuovo ambiente strategico europeo.

Atti di convegno

Lo Stato della Guerra: la propaganda islamista ‘radicale’, tra Tecnica, Tradizione e (geo)Politica

Giovanna Spanò
Assegnista di ricerca in Diritto Pubblico Comparato presso l’Università di Pisa e PhD in “Legal and Social Sciences – Fundamental Rights in the Global Society”

“The State of War: ‘radical’ Islamist propaganda, between Technique, Tradition and (geo)Politics”

Abstract

‘Jihadist’ propaganda has exploited new technological tools in a rather effective and competent way: for instance, reiterating narratives on the polarity between a “unique community and the unbelievers”, at the same recalling old ideas and stereotypes about a violent and aggressive Islamic State. Thus, the contribution aims at discussing the use of technology as a ‘retrospective’ technique through three main pillars: proselytism, takfirism, (warfare) holism.

Keywords: Islamic State – radicalism – on-line propaganda – mis-disinformation – jihadism

Introduzione

Le narrazioni sul "mito dello scontro" si basano sovente su una vistosa distorsione di topoi 'tradizionali', la cui diffusione assume, poi, proporzioni incontrollate per via della comunicazione digitale. La propaganda 'jihadista' ha fruito di nuovi mezzi e 'tecniche' in modo sapiente e competente: si pensi alla contrapposizione tra "comunità prescelta e infedeli", che perpetra scientemente l'idea di uno Stato islamico violento e aggressore. Il presente contributo mira, allora, a discutere un concetto di 'capacità' esponenziale della Tecnologia, in chiave 'retrospettiva', e attraverso tre concetti principali: il proselitismo, il takfirismo, l'olismo (bellico). Rispetto al primo punto, si indagherà l'importanza della (e la differenza nella) propaganda on-line, nonché della chiamata alle 'armi' tra le esperienze transnazionali e quella statalizzata per eccellenza, qual è Daesh. In ciò, come si spiegherà, pare delinearsi anche un 'modello' misto tra 'misinformazione' e disinformazione. Per il secondo, valorizzando il 'discorso' politico, emergeranno alcune riflessioni su una attuale 'Casa della Guerra'. Infine, il terzo si presenta quale breve sintesi dei precedenti: la rivendicazione dell'Islam come ordre inglobant[1]; una guerra 'olistica' che non solo sposta il luogo della belligeranza oltre ogni 'confine' fisico, ma lo articola pure in 'assetto' (geo-)politico. Ciò, provando a intercettare anche l'an e il quomodo di una (possibile) comunicazione tra la tematica in esame e una prospettiva comparata, nei 'termini' dei discorsi a seguire.

1. In limine: una prospettiva (meso-)comparata

Come è stato notato, "in molte discussioni complesse relative alla politica e alla religione, spesso è la posizione intermedia che tende ad essere la più accurata"[2]. Se non altro, almeno rispetto alla complessità che l'attivismo islamico (e islamista) siano in grado di (in)generare. Discendente, questo, quasi automaticamente anche dalla pluralità delle interpretazioni rappresentate nella 'militanza'. Due ulteriori premesse, dunque: l'indagine si collocherà, appunto, in medias res, con tutte le sfumature semantiche del caso. Sono note, infatti, le conseguenze e gli effetti della Tecnologia sul e nel mondo contemporaneo; gli sviluppi inaugurati si presentano, inoltre, tanto vari quante sono le discipline che si occupano di indagarne manifestazioni e fenomeni. Qui, è utile altresì esplorare come la tematica intrecci il diritto comparato, quante e quali tipologie di relazioni essa sia in grado di sollecitare. Le interdipendenze appaiono, in realtà, numerose e tra le altre si segnalano a livello:

I. Di metodo. Per esempio, la trasformazione – talvolta, vera e propria novazione – della categoria della 'Tradizione'. Si pensi alla trasmutazione (se non trasfigurazione) subita dal diritto islamico fin nella contemporaneità; oppure cosa possa costituire la šarīʿa e cosa rappresentino i variegati fenomeni jihadisti,

[1] O. Roy, L'échec de l'Islam politique, Paris, 1992, 29.

[2] A. Deen, Foreword, in S. Al-Ansari, U. Hasan (eds.), Tackling Terror: A Response to Takfiri Terrorist Theology, London, 7.

1.nonché da cosa gemmi quest'ultima qualificazione. Insomma, per sintetizzare, ciò che attiene, in 'senso' generale, ai rapporti tra Rule of Tradition e Rule of Politics[3].
II. Macro. Rileverebbe, certamente, anche una comparazione sulle e tra le Tradizioni – plurali e anche costituzionali – nonché, un focus, a titolo esemplificativo, circa l'idea/le di (e sullo) Stato.
III. Meso. Questo 'livello' di lettura potrebbe richiamare, anzitutto, i processi di ibridazione: di discorsi, pratiche e modelli.
IV. Micro. Quale ambito che si collega, invece, al ruolo e all'egemonia della politica: nella tradizione, nella religione, nei sistemi.

Pur considerando tutte queste variabili, in questa sede ci si concentrerà sul livello meso – in medias res, non a caso. Giacché, in fondo, si tratta di ri-guardare, primariamente, il lessico: nuovi termini da una parte e l'impiego della Tradizione – rectius delle categorie tradizionali – dall'altra; i patterns del modello, giuridico e discorsivo, tra continuità e discontinuità; lo spazio di 'senso' nel e del lessico, della geografia e della geopolitica, tra vecchi e nuovi mondi; la legge e il diritto, anche come legis-latio ovvero, quale processo "di auto-affermazione dell'identità culturale di una comunità [che] per sua stessa natura si dispiega nel futuro secondo un andamento cumulativo e, almeno teoricamente, illimitato"[4]. E a proposito di futuro, la tecnologia, per definizione, richiama qualcosa di avveniristico, proiettato oltre; una 'capacità' esponenziale, spiegava Kurzweil, basata anche sulla Legge dei Ritorni[5] e con cui la crescita lineare della regolazione giuridica – la legis-latio – deve (affannosamente e ricorsivamente) confrontarsi. Rispetto al tema qui in esame, viene senz'altro in luce una potenza, sì incrementale, delle tecnologie, soprattutto nuove e plurime, ma ciò che varia è la Tecnica, quale strumento, metodo e poi metodologia. In particolare – a proposito di legge dei ritorni – la componente di utopia retrospettiva, qui non come 'passatismo', ma come diversa declinazione della contemporaneità, più che modernità, ampiamente superata. La propaganda 'jihadista' ha infatti (ri)proposto l'idea di uno Stato della guerra per eccellenza – quello 'islamico', la cui definizione è già problematica in sé – nonché di uno stato di guerra permanente, estremizzando (ed esacerbando) dicotomie e

---

[3] Per un inquadramento generale tra sistemi, modelli e metodi, cfr., soprattutto, F. CASTRO, G.M. PICCINELLI (ed.), Il modello islamico, Torino, Giappichelli, 2007; C. SBAILÒ, Diritto Pubblico dell'islam mediterraneo. Linee evolutive degli ordinamenti nordafricani contemporanei: Marocco, Algeria, Tunisia, Libia, Egitto, Padova, Cedam, 2022; M. OLIVIERO, I Paesi del mondo islamico, in P. CARROZZA, A. DI GIOVINE, G.F. FERRARI (eds.), Diritto costituzionale comparato, Bari, Laterza, 2009; V.M. DONINI, D. SCOLART, La sharì'a e il mondo contemporaneo. Sistemi giuridici dei paesi islamici, Roma, Carocci, 2020; M. CAMPANINI, Oltre la democrazia. Temi e problemi del pensiero politico islamico, Sesto San Giovanni, Mimesis, 2014. Se si vuole, inoltre, G. SPANÒ, Un modello islamico? Sistemi e paradigmi macro-comparati, oltre la Rule of (Traditional) Law, Torino, Giappichelli, 2024.
[4] G. Anello, Shari'a Costituzionale. Repertorio Codicistico, Contrattualismo Musulmano, Ermeneutica Giuridico-Cognitiva: contributo per una lettura liberale dell'art. 2 della Costituzione egiziana, in Rivista AIC, 3/2016, 22.
[5] R. Kurzweil, The Law of Accelerating Returns, in C. Teuscher, (ed.), Alan Turing: Life and Legacy of a Great Thinker, Berlin-Heidelberg, 2004, 381-416.

polarità. Eppure, proprio dal punto di vista dell'ibridazione, la questione può essere letta attraverso i suoi complessi livelli. I quali, non a caso, da una prospettiva comparatistica, intrecciano i processi di (e il discorso sulla) ibridazione medesima, quasi per definizione. Trattando i due argomenti congiuntamente, si aggiunge una ulteriore premessa, ovvero quella della necessaria decostruzione del tema, tra differenti tecniche – metodi e strumenti –, paradigmi da rivisitare, una Tradizione e una (geo)Politica da risignificare. Più che di ibridazione, potrebbe forse parlarsi di 'ibridismo', quale, letteralmente, "coesistenza di elementi o caratteri eterogenei"[6] e "mescolanza disarmonica"[7].

Una sorta di stratificazione dissociata e disfunzionale[8].

2. Tra spazi e luoghi: alcuni percorsi

Quale chiave di lettura, quale 'retrospezione', quale utopia?

Per ciò che concerne l'analisi proposta, tre direttrici sembrano utili per tracciarne almeno i confini: il proselitismo, il takfirismo, l'olismo.
Già rispetto alla prima, emergono chiaramente alcune complessità. Sicuramente, le contaminazioni e il 'dialogo' tra Rule of History e Rule of Tradition; quest'ultima come 'sistema' adattivo e di per sé ibridato, nonché necessariamente 'stratificato', tra passato e contemporaneità. Tuttavia, mentre le fonti classiche sono accessibili a un numero significativamente ristretto di persone, il proselitismo – in certi casi, propaganda – online si serve volutamente (e ormai frequentemente) di lingue veicolari, che unite a una capacità espansiva del 'virtuale' sono in grado di raggiungere un pubblico indefinito e vastissimo. A ciò si accompagna, spesso, proprio una forma di ibridazione lessicale, di nuovo, a metà tra passato – tradizione – e contemporaneità. Si pensi, in modo paradigmatico, alla Tv fondata dal Califfato nel 2015, chiamata Khilafah Live[9] o ai Mujatweets[10] che combinano gli strumenti (e il linguaggio) dell'informazione 'di massa' a richiami ben precisi e identificativi, a tratti anche identitari. L'egemonia 'pura' della Tradizione ri-espande il proprio spazio di senso, però, quando dal mero proselitismo si passa a una chiamata alle 'armi'. Qui, basti ancora richiamare la copertina della rivista Dabiq del Califfato di Al-Baghdadi che riporta come titolo in inglese 'from Hijrah to

[6] https://www.treccani.it/vocabolario/ibridismo/.
[7] Ivi.
[8] "We could consider the (dys)functionalities due to the (in)compatibility of the systems' components, and differentiate between synergetic mixes and dissociated ones; or, maybe, devise a measuring scale of (dys)functionality to grade them", I. Castellucci, How Mixed Must a Mixed System Be?, in Electronic Journal of Comparative Law, May 2008, 14.
[9] S. Acampa, Applicazione delle tecniche di content analysis ai magazine di propaganda dello stato islamico: la chiamata alle armi di Rumiyah, in Rivista di Criminologia, Vittimologia e Sicurezza, Vol. XII, n. 2, Maggio-Agosto 2018, 50.
[10] H.J. Ingram, Three Traits of the Islamic State's Information Warfare, in The RUSI Journal, 159:6, 2014, 5.

Khilafah'[11]. In questo caso, non si usano equivalenti, ma si impiega un certo lessico, comprensibile a chi sa ascoltarlo. Un linguaggio 'tradizionale' che si fa transnazionale: vi è un primo layer di significato (religioso) e un meta-significato politico, che si basa su paradigmi, concetti e categorie 'tradizionali'. Nella già nota complessità di un Islam 'militante'[12] e dell'altrettanto sfaccettata 'jihadosfera', risulta problematico altresì rinvenire un'uniformità dei e nei fenomeni. Infatti, può cogliersi una prima (seppur superficiale) differenza sia nel proselitismo, sia nella chiamata alle 'armi' tra le esperienze transnazionali e quella 'territorialmente' delimitata di Daesh. Di nuovo a partire dalle riviste ufficiali, ad esempio, alcuni studi hanno rilevato come quella qaidista si concentri specificamente sull'incoraggiare all'azione i lone actors in Occidente, come guida pratica più che come articolazione di una visione religiosa, militare e politica. Al contrario, quella dell'Isis ha avuto portata più ampia, esponendo il fondamento legittimo, da un punto di vista tradizionale, del Califfato e incoraggiando tutti (e tutte)[13] a compiere l'egira verso il ri-costituito Stato islamico[14]. Questo si riflette poi, da una parte, sul peso della 'dottrina' nel proselitismo, nonché, appunto, sull'idea di ordine – anche ordinamento – sciaraitico. L'Isis ha infatti privilegiato una giustificazione dottrinale e religiosa del proprio operato[15] – al di là di una banalizzante 'folklorizzazione'[16]– mentre la propaganda qaidista ha guardato primariamente agli strumenti 'pratici', alle tecniche e ai metodi. Per chi abbia familiarità con le teorizzazioni qutbiane[17], è come se, rovesciandole, il primo guardasse a una fase proto-organizzativa di uno Stato islamico e alle sue basi, per l'affermazione dell'Islam come dichiarazione universale di libertà (dalla sottomissione ad altri uomini, in favore di Dio unico Sovrano), mentre la seconda alla finale, concreta, azione dell'avanguardia. Rispetto a questo, vi è una ulteriore, cruciale differenza: il qaidismo non ha preteso di

---

[11] Si segnala, a questo proposito, l'approfondita analisi di H.K. Gambhir, Dabiq: the strategic messaging of the Islamic State, August 15, 2014, www.Understandingwar.org, 7 ss.

[12] Per tutti, cfr., J.L. Esposito, Voices of resurgent Islam, New York-Oxford, 1983, Political Islam: Revolution, Radicalism, or Reform, Cairo, 1997; A.S. Moussali, Moderate and radical Islamic fundamentalism the quest for modernity, legitimacy and the Islamic State, Florida, 1999.

[13] Cfr., R. Pepicelli, Ğihād e donne: evoluzioni storiche e risignificazioni semantiche e teologiche in età contemporanea, in P. Manduchi, N. Melis (eds.), Ğihād: definizioni e riletture di un termine abusato, Milano, 2019, 139 ss.

[14] Cfr., H.K. Gambhir, op. cit., 1-2, in cui si nota "Begun in 2010, al-qaeda's English-language magazine Inspire does articulate religious justification. However, Inspire specifically focuses on encouraging lone-wolf Western-based terrorists to attack the West. Inspire serves more as a how-to guide for individual attacks than an articulation of an overall religious, military, and political vision. By contrast, ISIS's Dabiq series is farther-reaching, laying out the religious underpinning of the Caliphate and encouraging all believing Muslims to support ISIS and emigrate from their homes to the Islamic State".

[15] Sul punto, ad esempio, C. Bunzel, From Paper State to Caliphate: The Ideology of the Islamic State, The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper, No. 19, March 2015, passim, ma soprattutto 7 ss.

[16] "Lo Stato Islamico è uno di questi oggetti orientalizzati, folklorizzati e ricostituiti, sia nello spazio politico-mediatico sia in quello scientifico, per fungere da confine tra due mondi", M. Sakhi, Territorializzazione dello Stato Islamico e alcuni frammenti di utopia nel ğihād in Siria e Iraq, in P. Manduchi, N. Melis (eds.), op. cit., 236, enfasi aggiunta.

[17] Maʿālim fī al-ṭarīq, trad. ingl., di A.B. Al-Mehri, Milestone, Birmingham, 2006, tra le altre opere. Essa riguarda la creazione di un movimento, di una avanguardia che preparasse una rivoluzione al fine di stabilire un ordine islamico legittimo.

spingersi fino alla costituzione di uno Stato, quindi Daesh, in un certo senso, è tornato alle origini, alle radici, dell'utopia per eccellenza. Come spiegato, infatti, gli attacchi qaedisti dal 2001 in poi "avrebbero determinato un radicale ri-orientamento e una riconfigurazione dell'ideale jihadista 'tradizionale' a favore dell'opzione globale, a quel tempo ancora minoritaria. In questo senso, il qaidismo rappresenterebbe una sorta di 'anomalia' piuttosto che l'essenza di un fenomeno jihadista che, pur adottando orientamenti transnazionali, si era fino ad allora pensato 'localizzato' o 'nazionale'"[18].

A proposito di legis-latio, è più o meno nello stesso torno di tempo, non a caso, che nasce la categoria di radicalizzazione, come distinta e (ontologicamente) diversa dal terrorismo. Al riguardo, Sedgwick notava come la frequenza dell'impiego del termine sia aumentata esponenzialmente – appunto – in un dato, specifico, periodo, suggerendone un nesso con l'emersione del terrorismo c.d. "home grown" in Europa occidentale[19]. Evidentemente, la legis-latio ha accelerato il passo per adattarsi alla complessità dei fenomeni 'politici' e 'sociali'. Ciò è evidente anche dalla prospettiva delle scelte normative di diversi sistemi europei, che in taluni casi si sono rivelate finanche discriminatorie nei confronti delle comunità musulmane, quali "gruppi a rischio", nonché oggetto di particolare attenzione o di essenzializzazione. In realtà, il confine tra 'terrorismo' e radicalizzazione come categoria a sé stante non è sempre risultato netto, sia per la mancanza di strumenti – di una 'tecnica' normativa idonea – sia per l'assenza di metodi strutturati ed efficaci. Difatti, in alcuni sistemi il drafting normativo ha risentito di una certa 'urgenza' dettata dall'emergenza[20]. Pur non potendo dar conto, in questa sede, di un quadro tanto composito e sfaccettato[21], l'Ungheria e la Francia – casi che verrebbero comparati, diciamo, 'per differenza', giacché la prima presenta un pattern repressivo, mentre la seconda di tipo misto, combinando un approccio preventivo/repressivo – sono giunte al medesimo risultato di tracciare un'equazione quasi perfetta tra radicalismo e Islam. In Ungheria, in presenza di un'aperta promozione di doppi standards, il 'jihadismo' è risultato centrale e cruciale in materia di (de-)radicalizzazione,

---

[18] P. Maggiolini, Ğihād e jihadismo. Lotta e progettualità nella storia della violenza politica di matrice islamica, in P. Manduchi, N. Melis (eds.), op. cit., 223.

[19] "The greatest increase in frequency of use of ''radicalization'' in the press was between 2005 and 2007, timing that strongly suggests that the term's current popularity derives from the emergence of ''home-grown'' terrorism in Western Europe, notably the London bombings in July 2005". Allora, "the best solution for researchers is probably to abandon the idea that ''radical'' or ''radicalization'' are absolute concepts, and to recognize the essentially relative nature of the term 'radical'", M. Sedgwick, The Concept of Radicalization as a Source of Confusion, in Terrorism and Political Violence, 22(4), 2010, 479-480; 491.

[20] Così, a titolo esemplificativo, nel caso italiano. Sia consentito rimandare a G. Spanò, De-radicalisation in Italy: is 'emergency' a strategy per se?, in SI, DPCE online, 59 (2), 2023, 2055 ss.

[21] Cfr., V. Federico, S. Sassi, Countering radicalisation in Europe and beyond. Does the law matter?, Ibidem, 1975 ss; L. Vidino, J. Brandon, Europe's experience in countering radicalisation: approaches and challenges, in Journal of Policing, Intelligence and Counter Terrorism, 7:2, 2012. Inoltre, cfr., De-Radicalisation in Europe and Beyond: Detect, Resolve, Reintegrate, D.Rad Project, D.4.2, V. Federico, A. Rosanò, G. Spanò, Comparative Report, De-radicalisation and Integration Legal and Policy Framework, dradproject.com/?publications=d4-2-comparative-report-de-radicalisation- and-integration-legal-and-policy-framework.

mentre i movimenti di estrema destra – rafforzati dalle narrazioni del governo stesso – sono stati volontariamente sottovalutati e anzi scientemente ignorati[22]. Anche in Francia, attenzione 'esclusiva' è stata tributata per molto tempo al radicalismo religioso, sebbene fosse stato sottolineata (anche a livello di pubblico discorso) la rilevanza, a tal fine, dei soli 'movimenti' islamisti, quale forma di attivismo politico antidemocratico e antirepubblicano, e non già dell'Islam di per sé[23]. Allo stesso modo, a livello di policies, si sono registrate sia strategie nazionali specificamente rivolte a fronteggiare la radicalizzazione come categoria in sé, sia quali politiche incluse nel più ampio genus degli interventi in materia di antiterrorismo[24]. La maggior parte delle politiche legate alla deradicalizzazione, di nuovo, ha considerano il 'jihadismo' come principale minaccia, non attribuendo pari importanza all'estremismo politico (ad esempio, i gruppi di alt- e far right), o ai fattori di radicalizzazione legati a posizioni etnico-identitarie, al nazionalismo o al suprematismo. Non sorprende, allora, che tra gli ambiti di policies percepiti dai decisori politici come maggiormente rilevanti sia figurata la religione, in generale, e l'Islam, in particolare. Ad esempio, in Austria, Francia, Germania, Italia e intersecando la materia dell'immigrazione – come dato strettamente correlato – di nuovo, in Austria e in Germania, nonché in Finlandia e in Polonia[25].

Infine, come accennato nell'introduzione, può essere offerta un'altra riflessione a partire da qualità e contenuto della 'tradizione', nel suo significato di 'informazione trasmessa' seppur nella contemporaneità e con gli 'strumenti' della modernità. Torna in gioco, come una sorta di chiusura del cerchio, una ibridazione, un 'modello' misto tra 'misinformazione' e disinformazione. Quindi tra i due poli ideali – non necessariamente anche opposti – tra mis- e disinformazione (informazione 'non affidabile/volutamente falsa'), sono enucleabili due ulteriori 'percorsi' analitici: l'uno relativo alla contro-informazione, anche in senso 'giornalistico' per così dire, l'altro a proposito della disintermediazione[26]. Per il primo, cioè, l'obiettivo principale è parso il capovolgimento 'radicale' della prospettiva, ovvero la presentazione di una versione e visione 'estremamente' alternativa della realtà[27]. L'Isis, per esempio, ha ingaggiato un'opera

---

[22] Cfr., tra gli altri, i dati aggiornati al 2021, R. Fazekas, De-radicalisation and Integration: Legal and Policy Framework in Hungary, , https://dradproject.com/?publications=de-radicalisation-and-integration-legal-and-policy-framework-in-hungary.

[23] Allo stesso modo, come supra, cfr., S.W. Sawyer, R. Zinigrad, De-radicalisation and Integration: Legal & Policy Framework in France, https://dradproject.com/?publications=de-radicalisation-and-integration-legal-and-policy-framework-in-france.

[24] Cfr., V. Federico, M. Moulin-Stozek, G. Spanò, De-radicalisation and Integration Policies and best practices at the European and cross-border level, D.4.3, https://dradproject.com/?publications=de-radicalisation-and-integration-policies-and-best-practices-at-the-european-and-cross-border-level.

[25] Ivi.

[26] Sul punto, cfr., S. Pasta, Una lettura della "Jihadosfera". L'importanza del Web e dei legami deboli nell'educazione al terrorismo, in F. Antonacci, M.B. Gambacorti-Passerini, F. Oggionni (eds.), Educazione e terrorismo. Posizionamenti pedagogici, Milano, 2019, 27.

[27] Ivi.

certosina e sofisticata di propaganda globale con multiple finalità: tra le altre, come detto, quella di legittimare la propria autorità, nonché di proporre, al contempo, una counter-narrative personale, 'personalizzata' e un "do-it-yourself ethos"[28]. Per il secondo, come è stato notato, questo processo può essere inserito in quello più ampio della crisi dell'autorialità provocata dal digitale[29] – ma pure di una autorità, potrebbe aggiungersi. D'altronde, ancora, il principio di autorità è stato considerato una delle più potenti "armi della persuasione"[30]: ed è qui, allora che il proselitismo si fa Tecnica, quindi metodologia e arte della persuasione medesima, plasmando una nuova (forma di) autorità 'radicalmente' alternativa[31]. Tale circostanza ha coinvolto, a cascata, anche i c.dd. processi di de-mediazione, o dis-intermediazione nella e della comunicazione[32]. Gli strumenti – la tecnologia – e i canali – il metodo – risultano potenzialmente liberi e illimitati[33]. Se, come osservato, una ideologia è già insita in tutti i discorsi per definizione, Murgia ricorda pure che il lettore è a sua volta un costruttore attivo di significato[34]. Un'altra questione legata al radicalismo, alle tecnologie, al lessico, alla propaganda, è proprio la difficoltà di rinvenire un parametro standardizzato in grado di definire tutti i tipi di estremismi, a partire dalla scelta di parole chiave o "narrazioni", così come di enucleare una tassonomia idonea a ricomprenderne le variegate tipologie[35].

---

[28] L'espressione sembra particolarmente efficace, sebbene impiegata per altro contest. Cfr. T. Lemieux, J. Brachman, J. Levitt, J. Wood, Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model, in Terrorism and Political Violence, 1(1), 2014, 3.

[29] Ivi.

[30] R.B. Cialdini, Influence: The Psychology of Persuasion, New York, 1984.

[31] Discorso rovesciato può essere portato avanti dal punto di vista del controllo, da parte del potere costituito, dell'arena digitale medesima. Ad esempio, sul punto e per il Maghreb, si rimanda a un recente studio di F. Tamburini, The "Authentic Islam" on the Internet: The Official Websites of the Ministries of Religious Affairs in Algeria, Morocco, and Tunisia, in Journal of Asian and African Studies, November 18, 2024.

[32] S. Pasta, op. cit., 27.

[33] Infatti, "to some, social media as a source of news and information sharing, is an alternative to what is what is deemed as the "censored, biased mainstream media", N. Chelvachandran, H. Jahankhani, A study on keyword analytics as a precursor to machine learning to evaluate radicalisation on social media, 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019, 1.

[34] P. Murgia, La narrazione delǧihād sulla stampa italiana, in P. Manduchi, N. Melis (eds.), op. cit., 272.

[35] R. Denaux, J. M. Gómez-Pérez, Textual Analysis for Radicalisation Narratives Aligned with Social Sciences Perspectives, in Text2Story ECIR, 2019, 39-45; 3. Cfr., inoltre, I. Tanoli, S. Pais, J. Cordeiro, M.L. Jamil, Detection of Radicalisation and Extremism Online: A Survey, 2022. È stato notato, poi, a proposito di 'strumenti', come "there are many tools to extract information from online sources, but there is a lack of a specific and specialised tool for online radicalisation, and this is a problem for Law Enforcement Agencies, Probation Services, Intelligence Services and also for researchers", D. Camacho, I. Gilpérez-López, A. Gonzalez-Pardo, A. Ortigosa, C. Urruela, RiskTrack: a new approach for risk assessment of radicalisation based on social media data, CEUR Workshop Proceedings, 2016. Inoltre, "to successfully progress a profiling methodology utilising the analysis of data generated on social media, psychological and social models must also be utilised to correlate data with behaviours", N. Chelvachandran, H. Jahankhani, op. cit., 1. Cfr. anche A. Almansoori, M. Alshamsi, S. Abdallah, S. A. Salloum, Analysis of cybercrime on social media platforms and its challenges, in Proceedings of the International Conference on Artificial Intelligence

Alcuni studi sui contenuti dei social media legati a vario titolo a forme di militanza islamica o islamista mostrano, inoltre, che il posizionamento più o meno "radicale" possa mutare al variare degli argomenti: il discorso "potenzialmente" violento verrebbe quindi diffuso su base relativa anziché in termini generali[36]. Inoltre, potrebbero sorgere sfide aggiuntive, se consapevoli della presenza di un "vasto ecosistema di sottoculture parallelo ai social media mainstream"[37], in cui, peraltro, il linguaggio 'testuale' non è sempre dirimente o rilevante. Uno studio condotto sui siti "Chan" – collettori di sostenitori o movimenti di alt e far-right – ha infatti mostrato come non soltanto la violenza venisse sovente trivializzata, ma le parole (anche "chiave") e il lessico non erano sufficienti per rilevare contenuti estremisti o violenti. La tecnica – gli strumenti, il metodo – si basava su contenuti e messaggi 'scoraggianti' o poco chiari per i neofiti – quindi difficilmente intercettabili o comprensibili per chi fosse "esterno" all'ambiente o un utente "non competente" – e si affidava per lo più anche a mezzi visivi, giacché "le immagini [erano] le più prolifiche nel diffondere messaggi d'odio"[38]. Inoltre, per la maggior parte di queste (non soltanto "Meme" in senso 'tecnico') l'interpretazione appariva anche ostica al di fuori di quell'ecosistema o sottocultura, nonché i contenuti prima facie inoffensivi e apparentemente 'innocenti'[39]. Valorizzando il discorso, gli strumenti e i metodi, si giunge così alla seconda direttrice: il takfirismo. Letteralmente, il termine si compone, ancora, di un misto tra Rule of History e Rule of Tradition, giacché intercetta da una parte, l'accusa di miscredenza[40], dall'altra una sorta di separatismo dettato da richiami a un 'autentico' Islam, in contrapposizione a regimi empi e corrotti. Per ricongiungere i discorsi – al plurale – l'ibridazione si riconferma quale dato cruciale. Infatti, come è stato affermato, la semiosfera del Califfato contemporaneo è proprio uno spazio di ibridazione"[41] per eccellenza, che trasforma, 'trasfigura' le culture,

---

and Computer Vision (AICV), 2021.

[36] Denaux e Gómez-Pérez, tra gli altri, hanno analizzato diversi contenuti relativi ad argomenti diversificati– dalla discordia tra gruppi, agli obblighi morali, dalla promozione dell'ideologia di gruppo, all'idealizzazione dei membri più radicali – con l'obiettivo di rilevare cambiamenti nelle e delle narrazioni. Gli Autori hanno esaminato diversi ambiti e ambienti 'digitali': per esempio, lo "Young Muslim Digest", l'Al-Risalah del Fronte Nusra, Dabiq, pubblicato dall'Isis (2014-2016) e Rumiyah, rivista pubblicata dall'ISIS dal 2016, cfr., R. Denaux, J. M. Gómez-Pérez, op. cit.

[37] B. Crawford, F. Keen, G. Suarez-Tangil, Memes, radicalisation, and the promotion of violence on chan sites, in Proceedings of the international AAAI conference on web and social media, (15), 2021, 982.

[38] Ibidem, 984.

[39] Ibidem, 986.

[40] Cfr., O. Al-Ghazzi, Modernity as a False Deity: Takfiri Anachronism in the Islamic State Group's Media Strategy, in Journal of the European Institute for Communication and Culture, Vol. 25, Issue 4, 2018; J. Kadivar, Exploring Takfir, Its Origins and Contemporary Use: The Case of Takfiri Approach in Daesh's Media, in Contemporary Review of the Middle East, 2020. Si veda anche la voce Takfir, in The Oxford Dictionary of Islam, https://www.oxfordreference.com/display/10.1093/acref/9780195125580.001.0001/acref-9780195125580-e-2319?rskey=fwPSI7&result=2301.

[41] P. Calefato, a-Gro-ba. Senso dell'altro e ibridazione, in Versus, n. 100-101, Il senso dell'altro. Culture, generi, rappresentazioni: forme di mediazione interculturale, 11-20, Milano, 2006.

rendendole ‘altre’ da sé[42]. L’enfasi aggiunta sull’aggettivo mira a sottolineare come i c.dd movimenti takfiristi abbiano fatto ampio ricorso a meccanismi – tecniche – di alterizzazione, a scapito, oltretutto, della Tradizione. Rispetto a quest’ultima, infatti, emergono due ulteriori elementi: lo Stato islamico, per così dire, ‘classico’ e le categorie della Guerra e dell’Islam, come spazi di senso, anche geografico, tra ‘dentro’ e ‘fuori’.
Avendo riguardo allo Stato islamico e il suo attributo a-territoriale[43], il nuovo ricostituito Califfato di questo si è massimamente servito, trascendendo la dimensione dello Stato nazione, arrivando ovunque e potendo accogliere chiunque volesse farne o diventarne parte[44]. Qui, oltre ai già citati richiami qutbiani, può notarsi anche un rovesciamento di prospettiva, giacché proprio i confini (nazionali, statuali) sono primariamente considerati dei costrutti del kufr, della miscredenza[45]. In relazione alle categorie della Casa della Guerra e della Casa dell’Islam, invece, esse sono state risignificate, seppur tradizionalmente abbiano conosciuto diverse sfumature e sfaccettature intermedie – per tutte, si pensi al ‘luogo’ in cui vigeva un patto di non belligeranza, emblema di un contrattualismo islamico[46]. Pur non essendo intese nella

---

[42] Ibidem. Per esempio, in consonanza, l’anacronismo takfiri dell’Is è stato considerate strettamente collegato a ‘tattiche’ testuali e visuali miste, con un approccio ‘presentista’ e ibrido nei confronti delle fonti classiche, O. Al-Ghazzi, op. cit, passim.

[43] Anche la prospettiva rispetto al ‘territorio’, però, può mutare, giacché: “l’istituzione dello Stato Islamico nel contesto siriano si basa su un processo che chiamiamo ‘situazione di riterritorializzazione’. In effetti, la serie di eventi rivoluzionari ha portato a due processi: il primo è quello della deterritorializzazione, che si riferisce a una lotta [...] contro le strutture statali e contro i tentativi da parte dello Stato di riguadagnare una forma di sovranità moderna, cioè un monopolio della violenza fisica [...] Il secondo processo è quello di riterritorializzazione, che si riferisce a pratiche e poteri che mirano a rifondare, in primo luogo, l’ordine statale moderno tramite il monopolio della violenza fisica e il raggiungimento della continuità territoriale tra le aree occupate”, cfr., M. Sakhi, Territorializzazione dello Stato Islamico e alcuni frammenti di utopia nel ǧihād in Siria e Iraq, in P. Manduchi, N. Melis (eds.), op. cit., 236, 243.

[44]Cfr., A. Ricci, Lo Stato Islamico: sfida globale all’ordine geopolitico mondiale, in Rivista Trimestrale di Scienza dell’Amministrazione, 3/2018, il quale, oltre a definire l’Isis come un elemento di disordine geopolitico, sottolinea che “lo Stato Islamico prescinde dalla geografia. Usa il territorio in via funzionale alla sua reale presenza. Ma, al contrario degli Stati nazionali, può esistere al di là di esso. Si propone come soluzione globale e sovranazionale scardinando quei confini che l’Occidente ha tentato di imporre come elemento di certezza di esistenza degli Stati e di garanzia dell’ordine nelle relazioni internazionali. E che, nella forma del terrorismo jihadista o del Califfato che controlla un territorio, rappresenta una costante sfida all’ordine mondiale. Oggi come ieri e domani come ieri”, 10, 15.

[45] H.J. Ingram, op. cit., 6. L’Autore individua i tre tratti in reach, relevance, resonance e un “multidimensional, multi-platform approach that simultaneously targets ‘friends and foes’”, idoneo a rafforzarli, ibidem, 4.

[46] dār al-ḥarb: zona di Guerra, territorio nemico, i paesi non musulmani, dār al-islām: il territorio musulmano opposto al dar al harb, cfr., N. Melis, Rassegna di studi sul ǧihād, in P. Manduchi, N. Melis (eds.), op. cit., 18; K.A. El Fadl, Legal Debates on Muslim Minorities: Between Rejection and Accommodation, in The Journal of Religious Ethics, vol. 22, no. 1, 1994, Islamic Law and Muslim Minorities: The Juristic Discourse on Muslim Minorities from the Second/Eighth to the Eleventh/Seventeenth Centuries, in Islamic Law and Society, vol. 1, no. 2, 1994; M.M. Ahmad, The Notions of Dār Al-Ḥarb and Dār Al-Islām in Islamic Jurisprudence with Special Reference to the Ḥanafī School, in Islamic Studies, vol. 47, no. 1, 2008; P. Manoucher, M. Sommer, Dar Al-Islam: The Evolution of Muslim Territoriality and Its Implications for Conflict Resolution in the Middle East, in International Journal of Middle East Studies, vol. 11, no. 1, 1980.

giurisprudenza classica come categorie assiomatiche, o dogmatiche, per il Califfato di Al-Baghdadi, la petizione (di 'principi' e) di superiorità religiosa ha ri-costruito i 'confini' dell'appartenenza, anche al di là di una macro-distinzion tra Amico e Nemico. Inoltre, anche lo spazio di 'senso' geografico è apparso trasformato, giacché l'Isis ha combattuto idealmente "la sistematizzazione di una singola geografia, di cui ha fatto le spese quella tipica del califfato, come espressione politico-spaziale della umma"[47]. Ma proprio parte della comunià è rientrata paradossalmente tra i miscredenti combattuti dal Califfato, che 'sistematicamente' – come metodo[48], tecnica – ha ignorato le più basilari distinzioni tra musulmani/non musulmani, Casa dell'Islam, casa della Guerra. Rientrano ugualmente tra i nemici illustri attori dell'Islam politico e popolare: dalla Fratellanza musulmana ad Hamas, tra gli altri, nonché in generale gli sciiti o alcune minoranze. Tornando ricorsivamente alle ibridazioni, pur agendo per la riproposizione di uno Stato islamico globale, l'Isis ha, in realtà, "ri-territorializzato"[49] uno spazio di senso islamico, per cui dirimente sarebbe determinare "non tanto il limite geografico-territoriale, dunque il confine, quanto piuttosto l'aspirazione a varcare quei confini naturali e statuali"[50]. Non per coincidenza, nella prima apparizione pubblica, Al-Baghdadi affermò che "[il] mondo è stato diviso in due campi e due trincee, senza la presenza di un terzo campo: quello dell'Islam e della fede, e il campo del kufr [miscredenza] e dell'ipocrisia'". Non una polarità, come spiegata da Sbailò, tra politica e religione[51], ma una polarizzazione in senso stretto[52]. Ed estremo.

Tra Amici e Nemici, geografie[53], e spazi meta-territoriali, si arriva, infine, alla terza direttrice, ovvero l'olismo dello Stato della Guerra. Essa appare quale sintesi dei precedenti punti: la rivendicazione dell'Islam come ordre inglobant e una guerra 'totale' che ponendosi oltre i confini (e i luoghi) fisici ridisegna anche nuovi 'assetti' (geo-)politici. Essa appare, perciò, un prodotto 'puro' della contemporaneità, in cui la retrospezione sembrerebbe, in fondo, irrilevante di per sé: si rinviene, cioè, un'utopia nel telos, nell'ideale, ma i metodi e gli strumenti – la tecnica – sono modernissimi e attuali. Così come l'"avanguardia' è composta, per

---

[47] A.M. Cossiga, L'occidente, lo stato islamico e la scrittura dello spazio, in M. Amorosi, A.M. Cossiga, M. Emanuele, N. Ferrigni, A. Leto, M. Melani, G. Natalizia, A. Ricci, M. Ritucci, M. Spalletta, G. Vargiu, M. Zandri (eds.), Il terrore che voleva farsi Stato. Storie sull'ISIS, Eurilink, 2016, 249.

[48] "The assertion of takfir has become a method for Daesh to discredit its opponents, such as Shi'a Muslims and other Muslim groups", J. Kadivar, op. cit., 14.

[49] Cfr., supra, nota 42.

[50] A. Ricci, Radicalismo islamico, jihad e geografia dell'incertezza in Bollettino della Società Geografica Italiana, 8, 2015, citato in M. Morazzoni, G.G. Zavettieri, Geografia della paura e comunità virtuale. Il caso di IS e la narrazione del terrore, in AGEI - Geotema, 59, 2019, 134.

[51] Cfr., C. Sbailò, op. cit., soprattutto 13 ss.

[52] "This polarity is a constant theme in IS's IO, and the group often uses statements from its opponents in its own IO messaging in order to reinforce this approach", H.J. Ingram, op. cit., 6.

[53] Cfr, a proposito anche del 'territorio' e dello spazio, nonché di una loro ri-definizione, F. Selvini, G.G. Zavettieri, Helmet cam: lo Stato Islamico e la messa in scena del territorio, in Semestrale di Studi e Ricerche di Geografia XXXI, 2, 2019.

dirlo stavolta in termini schmittiani, da un 'partigiano' globale superiore alla legge, un Kosmopartisan[54]. Lo stesso Schmitt, d'altro canto, profeticamente affermava: "Ma cosa accadrebbe se il partigiano si adattasse al suo nuovo ambiente tecnico-industriale, e imparasse a utilizzare i nuovi mezzi sviluppando una nuova forma?" [...] Chi può impedire [...] che nascano nuove forme impreviste di inimicizia?"[55]. E, nota de Benoist, nell'epoca postmoderna, quella della fine della logica territoriale, la figura medesima del partigiano, alla quale Schmitt attribuiva carattere "tellurico", si deterritorializza definitivamente[56]. Si considerano superate le distinzioni tra belligeranti e neutrali, civili e combattenti e non combattenti, obiettivi legittimi o illegittimi[57].

Una guerra totale.

3. Alcune osservazioni in cerca di un metodo

Ancora non per coincidenza, si è parlato di fine della geografia[58], di geografia della paura[59], di open source jihad[60], che giocando con la semantica, dà l'idea di assenza di appartenenza e di proprietà, delle idee e dei mezzi insieme, di 'estrema' orizzontalità. Cambiano anche le questioni e la loro problematizzazione, da 'ordinare' in uno spazio 'indisciplinato' e geopoliticamente risignificato da un'"era dell'entropia"[61]. Già più di venti anni fa, si discuteva anche della paura di avere paura[62], mentre più recentemente di perdita del sense of place[63]. Fisiologico e finanche necessario, allora, uno spaesamento 'critico' dei giuristi: è essenziale rivedere gli 'spazi', oltreché analizzare una dialettica tra parametri tradizionali e perimetri globali, costantemente in divenire e dai confini sempre cangianti.

D'altronde, tradizionalmente, la guerra è complessa.

---

[54] A. de Benoist, Carl Schmitt Today: Terrorism, 'Just' War, and the State of Emergency, London, 2013, 57.

[55] Ibidem, 55.

[56] Ivi.

[57] Ivi.

[58] S. Graham, The end of geography or the explosion of place? Conceptualizing space, place and information technology, in Progress in Human Geography, 22, 2, 1998.

[59] M. Morazzoni, G.G. Zavettieri, op. cit.

[60] Ibidem, 136.

[61] R.L. Schweller, Entropy and the trajectory of world politics: why polarity has become less meaningful, in Cambridge Review of International Affairs, Volume 23, Number 1, March 2010, che proprio nell'Introduzione alla sua analisi precisa come "there is something about the current international system, its chaos and randomness, that suggests entropy", 145.

[62] F. Bonsignori, T. Greco (eds.), Un solo mondo, un solo diritto?, Pisa, 2007.

[63]E. Dell'Agnese, Bon Voyage, Torino, 2018, citata M. Morazzoni, G.G. Zavettieri, op. cit., 143.

Solo nel diritto islamico, si parla in modo differente di ḥarb, fitna, qitāl, futūḥāt[64]. Di fatto, anche jihadismo è un termine politicamente orientato[65], sebbene poi selettivamente riappropriato e di cui Esposito non mancava di sottolinearne, già diversi anni addietro, un connotato del tutto "unholy"[66]. Non si tratterebbe, cioè, di 'sacralizzazione dell'odio', come spesso si legge, ma forse di considerare la religione anche un indicant (geo)politico.

In chiusura, allora, si tornerà al diritto comparato, in cerca di un metodo. Se, come rilevato "la forma di dominio territoriale sta diventando obsoleta e oggi è più redditizio colonizzare le menti o controllare i mercati anziché annettere territori"[67], è l'ibridazione dei connotati del conflitto, più che il conflitto in sé, a rendersi transnazionale e totale. Oppure, al di là delle suggestioni di McLuhan[68] – che ormai sembrano parlare di molti mondi fa – una inedita forma di crittotipo globale.

---

[64] Cfr., di nuovo, N. Melis, Rassegna di studi sul ǧihād, in P. Manduchi, N. Melis (eds.), op. cit.

[65] Per esempio, si veda M. Sedgwick, Jihadism, Narrow and Wide: The Dangers of Loose Use of an Important Term, in Perspectives on Terrorism, vol. 9, n. 2, 2015.

[66] J.L. Esposito, Unholy War: Terror in the Name of Islam, Oxford, 2003.

[67] A. de Benoist, op. cit., 60-61.

[68] Nota la formulazione dell'espressione "Villaggio Globale", da parte di M. McLuhan, B. Powers, Il villaggio globale. XXI secolo: trasformazioni nella vita e nei media, Milano, 1996; cfr., inoltre, M. McLuhan, Gli strumenti del comunicare, Milano, 1967 e del medesimo Autore con Q. Fiore, War and Peace in the Global Village, New York, 1968.

FONTI PRINCIPALI

- S. Acampa, “Applicazione delle tecniche di content analysis ai magazine di propaganda dello Stato islamico: la chiamata alle armi di Rumiyah”, Rivista di Criminologia, Vittimologia e Sicurezza, Vol. XII, n. 2, Maggio-Agosto 2018.

- O. Al-Ghazzi, “Modernity as a False Deity: Takfiri Anachronism in the Islamic State Group’s Media Strategy”, Journal of the European Institute for Communication and Culture, Vol. 25, Issue 4, 2018.

- A. Almansoori, M. Alshamsi, S. Abdallah, S. A. Salloum, “Analysis of cybercrime on social media platforms and its challenges”, in Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV), 2021.

- G. Anello, “Shari’a Costituzionale. Repertorio codicistico, contrattualismo musulmano, ermeneutica giuridico-cognitiva: contributo per una lettura liberale dell’art. 2 della Costituzione egiziana”, Rivista AIC, 3/2016.

- M. M. Ahmad, “The Notions of Dār Al-Ḥarb and Dār Al-Islām in Islamic Jurisprudence with Special Reference to the Ḥanafī School”, Islamic Studies, Vol. 47, No. 1, 2008.

- F. Bonsignori, T. Greco (eds.), Un solo mondo, un solo diritto?, Pisa University Press, Pisa, 2007.

- C. Bunzel, “From Paper State to Caliphate: The Ideology of the Islamic State”, The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper, No. 19, March 2015.

- P. Calefato, “a-Gro-ba. Senso dell'altro e ibridazione”, Versus, n. 100–101, Milano, 2006.

- M. Campanini, Oltre la democrazia. Temi e problemi del pensiero politico islamico, Mimesis, Sesto San Giovanni, 2014.

- D. Camacho, I. Gilperez-Lopez, A. Gonzalez-Pardo, A. Ortigosa, C. Urruela, “RiskTrack: A New Approach for Risk Assessment of Radicalisation Based on Social Media Data”, CEUR Workshop Proceedings, 2016.

- F. Castro, G. M. Piccinelli (eds.), Il modello islamico, Giappichelli, Torino, 2007.

- N. Chelvachandran, H. Jahankhani, “A Study on Keyword Analytics as a Precursor to Machine Learning to Evaluate Radicalisation on Social Media”, IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019.

- R. B. Cialdini, Influence: The Psychology of Persuasion, HarperCollins, New York, 1984.

- A. M. Cossiga, “L’occidente, lo Stato islamico e la scrittura dello spazio”, in M. Amorosi et al. (eds.), Il terrore che voleva farsi Stato. Storie sull’ISIS, Eurilink, Roma, 2016.

- B. Crawford, F. Keen, G. Suarez-Tangil, “Memes, Radicalisation, and the Promotion of Violence on Chan Sites”, Proceedings of the International AAAI Conference on Web and Social Media, Vol. 15, 2021.

- A. Deen, “Foreword”, in S. Al-Ansari, U. Hasan (eds.), Tackling Terror: A Response to Takfiri Terrorist Theology, London, 2016.

- R. Denaux, J. M. Gómez-Pérez, “Textual Analysis for Radicalisation Narratives Aligned with Social Sciences Perspectives”, Text2Story ECIR, 2019.

- V. M. Donini, D. Scolart, La shari‘a e il mondo contemporaneo. Sistemi giuridici dei paesi islamici, Carocci, Roma, 2020.

- E. Dell’Agnese, Bon Voyage, Einaudi, Torino, 2018.

- K. A. El Fadl, “Legal Debates on Muslim Minorities: Between Rejection and Accommodation”, The Journal of Religious Ethics, Vol. 22, No. 1, 1994.

- J. L. Esposito, Unholy War: Terror in the Name of Islam, Oxford University Press, Oxford, 2003.

- J. L. Esposito, Voices of Resurgent Islam, Oxford University Press, New York–Oxford, 1983.

- J. L. Esposito, Political Islam: Revolution, Radicalism, or Reform, American University in Cairo Press, Cairo, 1997.

- R. Fazekas, “De-radicalisation and Integration: Legal and Policy Framework in Hungary”, D.Rad Project, 2021, https://dradproject.com/?publications=de-radicalisation-and-integration-legal-and-policy-framework-in-hungary.

- V. Federico, S. Sassi, “Countering Radicalisation in Europe and Beyond. Does the Law Matter?”, in D.Rad Project Comparative Report, 2021.

- V. Federico, M. Moulin-Stozek, G. Spanò, “De-radicalisation and Integration Policies and Best Practices at the European and Cross-border Level”, D.Rad Project, 2021.

- H. K. Gambhir, “Dabiq: The Strategic Messaging of the Islamic State”, Institute for the Study of War, Washington, 2014.

- S. Graham, “The End of Geography or the Explosion of Place? Conceptualizing Space, Place and Information Technology”, Progress in Human Geography, Vol. 22, No. 2, 1998.

- R. Kurzweil, “The Law of Accelerating Returns”, in C. Teuscher (ed.), Alan Turing: Life and Legacy of a Great Thinker, Springer, Berlin–Heidelberg, 2004.

- T. Lemieux, J. Brachman, J. Levitt, J. Wood, “Inspire Magazine: A Critical Analysis of its Significance and Potential Impact”, Terrorism and Political Violence, Vol. 1, No. 1, 2014.

- M. McLuhan, Gli strumenti del comunicare, Garzanti, Milano, 1967.

- M. McLuhan, Q. Fiore, War and Peace in the Global Village, Bantam Books, New York, 1968.

- M. McLuhan, B. Powers, Il villaggio globale. XXI secolo: trasformazioni nella vita e nei media, Feltrinelli, Milano, 1996.

- N. Melis, “Rassegna di studi sul ǧihād”, in P. Manduchi, N. Melis (eds.), Ǧihād: definizioni e riletture di un termine abusato, FrancoAngeli, Milano, 2019.

- A. Moussali, Moderate and Radical Islamic Fundamentalism: The Quest for Modernity, Legitimacy and the Islamic State, University Press of Florida, Gainesville, 1999.

- A. Moussali, Moderate and Radical Islamic Fundamentalism: The Quest for Modernity, Legitimacy and the Islamic State, University Press of Florida, Gainesville, 1999.

- P. Maggiolini, "Ǧihād e jihadismo. Lotta e progettualità nella storia della violenza politica di matrice islamica", in P. Manduchi, N. Melis (eds.), Ǧihād: definizioni e riletture di un termine abusato, FrancoAngeli, Milano, 2019.

- P. Manoucher, M. Sommer, "Dar Al-Islam: The Evolution of Muslim Territoriality and Its Implications for Conflict Resolution in the Middle East", International Journal of Middle East Studies, Vol. 11, No. 1, 1980.

- V. Morazzoni, G. G. Zavettieri, "Geografia della paura e comunità virtuale. Il caso di IS e la narrazione del terrore", AGEI – Geotema, 59, 2019.

- P. Murgia, "La narrazione del ǧihād sulla stampa italiana", in P. Manduchi, N. Melis (eds.), Ǧihād: definizioni e riletture di un termine abusato, FrancoAngeli, Milano, 2019.

- M. Oliviero, "I Paesi del mondo islamico", in P. Carrozza, A. Di Giovine, G. F. Ferrari (eds.), Diritto costituzionale comparato, Laterza, Bari, 2009.

- S. Pasta, "Una lettura della 'Jihadosfera'. L'importanza del Web e dei legami deboli nell'educazione al terrorismo", in F. Antonacci, M. B. Gambacorti-Passerini, F. Oggionni (eds.), Educazione e terrorismo. Posizionamenti pedagogici, FrancoAngeli, Milano, 2019.

- R. Pepicelli, "Ǧihād e donne: evoluzioni storiche e risignificazioni semantiche e teologiche in età contemporanea", in P. Manduchi, N. Melis (eds.), Ǧihād: definizioni e riletture di un termine abusato, FrancoAngeli, Milano, 2019.

- O. Roy, L'échec de l'Islam politique, Seuil, Paris, 1992.

- M. Sakhi, "Territorializzazione dello Stato Islamico e alcuni frammenti di utopia nel ǧihād in Siria e Iraq", in P. Manduchi, N. Melis (eds.), Ǧihād: definizioni e riletture di un termine abusato, FrancoAngeli, Milano, 2019.

- H. J. Ingram, "Three Traits of the Islamic State's Information Warfare", The RUSI Journal, Vol. 159, No. 6, 2014.

- M. Sedgwick, “The Concept of Radicalization as a Source of Confusion”, Terrorism and Political Violence, Vol. 22, No. 4, 2010.

- M. Sedgwick, “Jihadism, Narrow and Wide: The Dangers of Loose Use of an Important Term”, Perspectives on Terrorism, Vol. 9, No. 2, 2015.

- F. Selvini, G. G. Zavettieri, “Helmet cam: lo Stato Islamico e la messa in scena del territorio”, Semestrale di Studi e Ricerche di Geografia, Vol. XXXI, No. 2, 2019.

- C. Sbailò, Diritto pubblico dell’Islam mediterraneo. Linee evolutive degli ordinamenti nordafricani contemporanei: Marocco, Algeria, Tunisia, Libia, Egitto, Cedam, Padova, 2022

- A. de Benoist, Carl Schmitt Today: Terrorism, “Just” War, and the State of Emergency, Arktos, London, 2013.

- J. Kadivar, “Exploring Takfir, Its Origins and Contemporary Use: The Case of Takfiri Approach in Daesh’s Media”, Contemporary Review of the Middle East, 2020.

- A. Ricci, “Lo Stato Islamico: sfida globale all’ordine geopolitico mondiale”, Rivista Trimestrale di Scienza dell’Amministrazione, 3/2018.

- A. Ricci, “Radicalismo islamico, jihad e geografia dell’incertezza”, Bollettino della Società Geografica Italiana, 8, 2015.

- G. Spanò, “De-radicalisation in Italy: is ‘emergency’ a strategy per se?”, DPCE Online, Vol. 59, No. 2, 2023.

- G. Spanò, Un modello islamico? Sistemi e paradigmi macro-comparati, oltre la Rule of (Traditional) Law, Giappichelli, Torino, 2024.

- R. L. Schweller, “Entropy and the Trajectory of World Politics: Why Polarity Has Become Less Meaningful”, Cambridge Review of International Affairs, Vol. 23, No. 1, 2010.

- F. Tamburini, “The ‘Authentic Islam’ on the Internet: The Official Websites of the Ministries of Religious Affairs in Algeria, Morocco, and Tunisia”, Journal of Asian and African Studies, November 18, 2024.

Atti di convegno

La teoria geopolitica e i conflitti del III millennio: il possibile ruolo dell'Unione Europea

Andrea Cafiero
PhD, Cultore della materia- Università di Viterbo e della Tuscia
Docente - Master di II livello in Geopolitica della Sicurezza presso l'Università degli Studi di Roma Niccolò Cusano

"Geopolitical theory and conflicts in the third millennium: the potential role of the European Union"

Abstract

From the conflicts of the 1990s, such as the Gulf War and the Balkan Wars, to the Russian-Ukrainian conflict and the Arab-Israeli conflict, the theories of eminent geopolitical scholars seem to be increasingly coming to fruition. Brzezinski, who decades before the start of the war in Donbass, identified Ukraine as a geostrategic pivot that the US should defend from Russian interests. Spykman, who focused on the need to influence and control the Rimland, i.e. the strip of territory comprising the European coastline, the Middle East and the Asian area surrounding the Heartland. Mackinder defined the Heartland as roughly corresponding to the territory of Russia, which would guarantee domination of the "World Island" (Asia, Europe and Africa) to whoever took control of it. In this context, we are witnessing increasingly rapid technological advances and the use of drones, laser weapons, cyber attacks, etc. Control of airspace and military superiority in the sky are increasingly decisive, as the Italian Douhet hypothesised a century ago, making air dominance of primary importance. One wonders what role the European Union, still lacking a common defence, could play in what could turn out to be a decisive clash between what are defined as autocracies and liberal democracies for dominance over the "World Island".

Keyword: Geopolitics – European defense – Heartland–Rimland – Global power rivalry

1. Lo scenario internazionale

Per analizzare lo scenario internazionale, si può fare riferimento a una teoria che, nonostante risalga a un periodo passato, appare oggi più attuale di quanto lo fosse al momento della sua elaborazione. Si tratta della teoria del potere regionale e multipolare, il cui principale teorico è Samuel B. Cohen. Questo geografo americano, nel 1963, criticò le visioni geopolitiche rigide e globalistiche legate alla strategia del containment, da cui derivò la cosiddetta dottrina del domino, utilizzata per giustificare l'intervento americano in Vietnam. Cohen sosteneva che ogni elemento geopolitico della cintura di containment sovietica avesse una propria individualità e che, di conseguenza, la conquista di uno di essi non avrebbe provocato il collasso dell'intero sistema per effetto domino. Egli riteneva che gli Stati Uniti dovessero ridurre il loro impegno nelle aree continentali del Rimland (le terre periferiche dell'Eurasia, tra cui l'Europa costiera, il Medio Oriente e l'Asia monsonica) e adottare una strategia basata su forze mobili di intervento rapido da utilizzare solo in caso di aggressione a parti essenziali del sistema antisovietico. Durante la Guerra Fredda, Cohen suddivise il mondo in due grandi regioni geostrategiche: il mondo commerciale marittimo e quello continentale euroasiatico, a loro volta articolati in regioni geopolitiche dominate da Stati catalizzatori regionali, come la Germania per l'Europa. Tuttavia, a causa della rigidità del sistema bipolare dell'epoca, queste concezioni regionali e multipolari non poterono svilupparsi pienamente (Cohen, 1963).

Oggi, con il superamento di quel sistema, queste idee si stanno affermando, rispecchiandosi nelle attuali visioni del nuovo disordine internazionale. In particolare, la distinzione proposta da Cohen tra le regioni geopolitiche del mondo continentale appare ancora più attuale, con l'Heartland, dominato dalla Russia e comprendente l'Europa Orientale, e l'Asia orientale, sotto l'influenza della Cina. Riguardo al mondo marittimo, le regioni più rilevanti sarebbero quella anglo-americana e quella dell'Europa marittima. Tuttavia, si osserva una crescente collaborazione tra i due principali Stati catalizzatori del mondo continentale, Russia e Cina, accomunati da regimi autocratici, definiti tali dal mondo occidentale.

Conflitti attuali come quello in Ucraina, le tensioni in Medio Oriente e l'area di Taiwan richiamano la teoria del potere peninsulare, elaborata da Nicholas Spykman. Secondo Spykman, la geografia è un elemento determinante per la politica nazionale, in quanto stabile e immutabile. Egli identificava il Rimland come la zona cruciale per il confronto tra potenze marittime e continentali: chi controlla quest'area ottiene il dominio su mare e terra. Il Rimland è la fascia marittima e costiera che circonda l'Eurasia, essa si divide in 3 zone: zona della costa europea; zona del Medio Oriente; zona asiatica (Spykman, 1942). Il conflitto israelo-palestinese, esteso al poi all'Iran, al Libano e alla Siria, nonché le recenti tensioni nel Mar Rosso, legate all'attività dei ribelli Houthi e alle operazioni navali occidentali, sembrerebbero confermare questa teoria. Per altro, la recente caduta del regime di Assad in Siria rappresenta un poderoso colpo all'influenza russa sul Rimland mediorientale. La Russia ha perso, in questo modo, il suo più importante alleato sul Mediterraneo, una

perdita geostrategica non da poco, che potrebbe tramutarsi un duro colpo all'influenza geopolitica russa sui mari e, quindi, sulla capacità di competere per il potere marittimo con le altri grandi potenze, potere marittimo fondamentale per la conquista dell'egemonia geopolitica (Mahan, 1890).

Tutte queste elaborazioni si rifanno alla teoria di Halford Mackinder, geografo inglese che analizzò le opportunità e le minacce geopolitiche del suo tempo, soprattutto in relazione al confronto tra Gran Bretagna, Germania e Stati Uniti. Mackinder è noto per la sua teoria dell'Heartland, descritta nell'articolo "The Geographical Pivot of History". Egli distingueva tra potenze marittime e continentali, sottolineando che il nucleo centrale della Terra, l'Heartland, ricco di risorse e circondato da due cinture periferiche (una interna e una esterna), rappresentava il fulcro del potere globale. La conquista dell'Heartland da parte di una potenza marittima, secondo Mackinder, avrebbe garantito il dominio sull'"Isola Mondo" (Europa, Asia e Africa) (Mackinder, 1904). Nel contesto attuale, oltre al conflitto geoeconomico in corso rappresentato dal sistema sanzionatorio messo in atto contro la Russia e dal congelamento dei beni russi all'estero, i recenti attacchi ucraini a lungo raggio in territorio russo effettuati con armi occidentali, nonché l'invasione dell'Oblast di Kursk da parte delle forze di terra ucraine, sembrerebbero configurarsi come un tentativo di colpire il "cuore della Terra", in risposta all'invasione russa del territorio ucraino iniziata a febbraio del 2022. Un evento senza precedenti dai tempi dell'invasione nazista dell'Unione Sovietica.

2. Egemonia e Nuovo Ordine Mondiale

Il pensiero di Francis Fukuyama si inserisce in un insieme di teorie definite "endismi" (dal termine inglese end, ovvero "fine"), che proclamano la conclusione di un'epoca o di un fenomeno. Secondo l'autore statunitense, la vittoria del capitalismo sul comunismo al termine della Guerra Fredda avrebbe sancito la fine della storia in senso hegeliano. Per Fukuyama, la storia avrebbe raggiunto il suo stadio finale con l'affermazione della liberal-democrazia e del libero mercato. L'idea centrale è che non vi siano più alternative al modello liberale e democratico occidentale, e che il progresso umano conduca verso una pace duratura (Fukuyama, 1992). Tuttavia, questa visione è stata ampiamente criticata per il suo marcato occidentalismo, che esclude le prospettive di culture come quella asiatica, contrarie a omologarsi ai valori occidentali. Inoltre, i conflitti etnico-identitari e gli effetti controversi dell'affermazione dell'identità islamica contraddicono l'ottimismo di Fukuyama, benché la globalizzazione abbia spinto molte parti del mondo, pur con difficoltà e velocità differenti, verso modelli economici occidentali.

Alla visione ottimistica di Fukuyama si contrappone quella pessimistica di Samuel Huntington. Per Huntington, il mondo non si sta avviando verso una pace duratura, ma piuttosto verso nuovi conflitti, non più tra Stati, bensì tra civiltà. I motivi dei conflitti non sarebbero più economici o politici, ma culturali. Huntington sostiene che le differenze tra civiltà, profonde e irriducibili, siano destinate a causare divisioni e

che, in futuro, avranno un impatto ancora maggiore sui conflitti. Inoltre, la diffusione della tecnologia e dell'informazione, pur riducendo le distanze fisiche, ha intensificato le tensioni culturali, veicolando immagini della ricchezza occidentale che alimentano sentimenti di rivalsa nei più poveri. Spesso, la religione assume un ruolo centrale in questi conflitti, influenzando anche le dinamiche politiche. Huntington individua sette grandi civiltà: occidentale, confuciana, giapponese, musulmana, induista, slava-ortodossa e latino-americana. Tra queste, l'unica minaccia al predominio occidentale sarebbe rappresentata da una possibile alleanza tra la civiltà confuciana e quella islamica, ipotesi che però non si è concretizzata (Huntington, 1996).

Infine, Zbigniew Brzezinski riprende le teorie di Halford Mackinder, rielaborandole in funzione della supremazia americana. Per Brzezinski, la supremazia degli Stati Uniti nel mondo è un fatto storico eccezionale che deve essere mantenuto, non tramite la coercizione, ma attraverso la forza attrattiva. Per farlo, gli Stati Uniti devono concentrare la propria attenzione sull'Eurasia, che Mackinder identificava come l'Heartland. Brzezinski individua cinque attori geostrategici principali (Francia, Germania, Russia, Giappone e Cina), capaci di influire al di fuori dei propri territori, e cinque perni geostrategici (Ucraina, Azerbaijan, Turchia, Iran e Corea del Sud), che, pur essendo vulnerabili, rappresentano aree chiave da proteggere contro le mire degli attori geostrategici. Secondo Brzezinski, gli Stati Uniti dovrebbero prevenire la rottura dell'asse franco-tedesco, che, con il contributo di Ucraina e Polonia, potrebbe contrastare le ambizioni della Russia. Per quest'ultima, in crisi dopo la Guerra Fredda, Brzezinski propone una sua integrazione nell'Europa, trasformandola da impero a Stato nazionale. Lo studioso auspica inoltre un rafforzamento dei rapporti con la Turchia e un riavvicinamento con l'Iran, considerato un alleato strategico nell'area del Golfo. Nell'Estremo Oriente, Brzezinski suggerisce una maggiore collaborazione con il Giappone e ritiene inevitabile un confronto con la Cina (Brzezinski, 1998). Le sue riflessioni rappresentano un tentativo di ridefinire il ruolo degli Stati Uniti nel mondo post-Guerra Fredda e di comprendere come influenzare le dinamiche dell'Eurasia, considerata, fin dai tempi di Mackinder, il centro geopolitico globale.

Soffermandoci su questa ultima teoria, appare evidente come sia chiaro che l'Occidente abbia una chiara necessità di contenimento della Cina e, soprattutto, di mutamento dell'assetto politico costituzionale russo. In tal senso, ci si chiede se lo scontro fra autocrazie e democrazie liberali in corso sia per il dominio sull' "Isola Mondo" oppure una sfida sulla definizione ultima della fine della Storia e dell'ultimo uomo, come la intendeva Fukuyama: ci si domanda se le autocrazie e i loro alleati siano semplicemente le ultime resistenze a quel naturale "progresso mondiale" verso la democrazia liberale. In questo senso, lo scontro di civiltà immaginato da Huntington non sarebbe più per il dominio sull'ecumene ma, piuttosto, per stabilire se la Storia sia davvero finita o meno con il sistema politico democratico-liberale.

3. Il possibile ruolo dell'Unione Europea

La vicenda della mancata costruzione della Difesa Comune Europea è particolarmente significativa. Robert Schuman e Jean Monnet, con il sostegno del segretario di Stato americano Dean Acheson, nutrivano la convinzione che, sulla scia del successo della Comunità europea del carbone e dell'acciaio, un progetto di integrazione militare potesse fungere da catalizzatore per una piena integrazione politica. Tuttavia, questa idea non si concretizzò, rendendo superfluo speculare su come sarebbe potuta evolvere. Nonostante ciò, risulta interessante paragonare questa vicenda all'Unione economica e monetaria (UEM) (Colamedici, 2020). Semplificando le complesse questioni sottese a questa materia, che non rientrano nell'analisi presente, è possibile isolare alcuni aspetti chiarificatori. La UEM, realizzata seguendo le tappe indicate nel cosiddetto "rapporto Delors", fu progettata per promuovere una crescita economica sostenibile e un elevato livello di occupazione attraverso adeguate politiche economiche e monetarie (Colamedici, 2020). Essa rappresenta il risultato di un'integrazione economica progressiva, non è dunque fine a sé stessa. Da questa impostazione derivano precise implicazioni logiche. L'unità monetaria mira a favorire una crescita economica sostenibile, obiettivo da raggiungere tramite politiche economiche e monetarie appropriate, implicando una maggiore integrazione politica (Rakić e Verbeken, 2020).

Tuttavia, su questo punto apparentemente chiaro emergono opinioni contrastanti. Da una parte, alcuni sostengono che l'unità politica sia indispensabile, poiché una moneta unica gestita da Stati nazionali con interessi divergenti non sarebbe in grado di svolgere le sue funzioni. Dall'altra, studiosi come Emanuele Severino ritengono che questa conclusione sia arbitraria, nonostante la premessa di una necessaria gestione unitaria della moneta sia corretta. Secondo Severino, la longevità della cooperazione economica europea senza unità politica dimostra che lo Stato ha smesso di essere politico per diventare essenzialmente economico (Severino, 2018).

Una terza prospettiva, proposta da Giorgio Agamben, offre un'interpretazione diversa. Ispirandosi al pensiero di Kojève, Agamben osserva che l'Europa, insistendo su una base esclusivamente economica e trascurando elementi politici come forme di vita, cultura e religione, rivela la sua fragilità, in primo luogo proprio sul piano economico (Agamben 2018). Analogamente all'unione monetaria, neanche la difesa comune può essere fine a sé stessa. Come insegnava Jean Monnet, i risultati si ottengono concentrandosi su obiettivi specifici e ben definiti, capaci di determinare il resto (Monnet, 1988).

In questo senso, una difesa europea efficace, a metà strada tra politica estera e cooperazione industriale, potrebbe costituire un punto di svolta per l'integrazione politica. Essa potrebbe portare alla creazione di una comunità di Stati "indipendenti nell'interdipendenza", che considerano l'integrazione il fulcro della sovranità, non la sua negazione. Una tale comunità politica sarebbe in grado di elaborare e perseguire una grande

strategia, ovvero un quadro guida che permetta di affrontare le incertezze del contesto internazionale complesso. Senza questa capacità di visione strategica, e la sua espressione diretta nella politica estera, il rischio sarebbe di adottare politiche inefficaci o inadeguate rispetto al mutare delle sfide globali (Ortmann e Whittaker, 2019).

Un'Europa, quindi, dinamica e rappresentativa, capace di pianificare e agire in armonia con i propri Stati membri e partner esterni, dovrebbe rispondere con continuità strategica e autonomia alle sfide del presente e del futuro. Per diventare un baricentro geopolitico e una comunità di sicurezza nel Mediterraneo, l'Unione europea dovrà però affrontare un percorso complesso in un contesto segnato da nuove forme di globalizzazione e localismi rinnovati (Colombo, 2010), con confini e ordinamenti sempre più fragili, minacce emergenti e conflitti antichi ancora irrisolti, l'Europa appare oggi sospesa tra un passato che cerca di lasciarsi alle spalle e un futuro ancora da definire (Kissinger, 2018).

Eppure, delle eccellenze europee condivise in ambito di difesa e di tecnologia bellica si possono già apprezzare. In tal senso, l'Eurofighter (F-2000A) è un caccia multiruolo (swing-role) di quarta generazione, progettato principalmente come caccia intercettatore. Questo velivolo offre capacità operative eccezionali e garantisce un'efficacia su vasta scala nel settore della difesa aerea. Il Typhoon è tuttora considerato l'aereo più avanzato sviluppato in Europa, grazie al contributo fornito da Germania, Italia, Spagna e Regno Unito durante la sua fase di sviluppo.

L'F2000 è un velivolo bimotore supersonico, estremamente agile, qualità ottenuta grazie all'uso di materiali innovativi, processi industriali avanzati e tecniche di assemblaggio d'avanguardia. È largamente impiegato in Europa, soprattutto per le tecnologie integrate nel cockpit del pilota, tra cui un eccellente sistema radar che consente funzionalità avanzate nelle missioni aria-aria e aria-terra. Un'altra caratteristica essenziale per un velivolo intercettatore come l'F2000 è la capacità di individuare e tracciare simultaneamente bersagli multipli, anche in ambienti congestionati. Inoltre, l'Eurofighter può eludere, contrastare e sopravvivere a minacce elettromagnetiche in costante evoluzione.

Lo sviluppo dell'Eurofighter ebbe inizio nel 1983 grazie a una collaborazione multinazionale tra Regno Unito, Germania, Francia, Italia e Spagna. Tuttavia, nel 1984, la Francia abbandonò il progetto poiché il consorzio non accolse la richiesta francese di detenere il 50% del controllo sul progetto. La cooperazione internazionale portò alla realizzazione del primo prototipo nel 1994, anno del suo primo volo. Nel 1998 l'aereo ricevette il nome ufficiale di Typhoon, e nello stesso anno furono firmati i primi contratti di produzione.

La fine della Guerra Fredda, un evento di rilevanza globale, modificò le richieste in termini di quantità di caccia multiruolo necessari. L'F2000 entrò ufficialmente in servizio nel 2003. Operativo in tutto il mondo, l'Eurofighter Typhoon ha dimostrato prestazioni operative eccezionali dall'Europa al Sud Atlantico fino al Medio Oriente. Lo sviluppo di un caccia di superiorità aerea così efficiente ha certamente dotato l'Unione Europea, nel suo complesso, di un mezzo valido per conseguire quello che si può definire come "potere aereo", sempre più importante per conseguire una più vasta egemonia bellica e per la conquista del dominio dell'aria, sempre più determinante in guerra (Douhet, 1921) (come può essere osservato in vari conflitti, con particolare riferimento a quello arabo-israeliano).

Il livello attuale di cooperazione instauratosi tra gli Stati membri dell'Unione europea non ha ancora raggiunto l'obiettivo principale: la creazione di una forza di primo intervento realmente europea, in grado di reagire prontamente e di essere dispiegata rapidamente in caso di necessità (Hakansson, 2021). A tal proposito, si ricorda che l'articolo 42, comma 7, del Trattato sull'Unione europea (TUE) prevede che, nel caso in cui uno Stato membro subisca un'aggressione armata sul proprio territorio, gli altri Stati membri sono obbligati a prestargli aiuto e assistenza con tutti i mezzi a loro disposizione, in conformità con l'articolo 51 della Carta delle Nazioni Unite (cosiddetta clausola di assistenza reciproca).

Sebbene i Trattati dell'Unione europea consentano teoricamente la creazione di una forza militare comune – il comma 2 dell'articolo 42 TUE stabilisce infatti che il Consiglio europeo, deliberando all'unanimità, può istituire una "difesa comune" – fino ad oggi si è preferito agire al di fuori dei Trattati per sviluppare un primo nucleo di esercito europeo. Un esempio di tale iniziativa è rappresentato dall'Eurocorps (in italiano Eurocorpo), una forza multinazionale a livello di Corpo d'Armata, operativa dal 1993 grazie a un accordo franco-tedesco successivamente esteso ad altri Paesi con un trattato del 1999 (Vellano, 2021). L'Eurocorps ha il suo quartier generale a Strasburgo e una sede aggiuntiva a Mülheim (Germania), dove è basata la Brigata franco-tedesca. Attualmente, comprende sei Framework Nations (Francia, Germania, Spagna, Belgio, Polonia e Lussemburgo) e sei Associate Members (Italia, Grecia, Romania, Turchia e, dal 2021, Austria).

Pur mantenendo una propria autonomia, l'Eurocorps è già a disposizione dell'Unione europea. Dal vertice di Colonia del 1999, ha intensificato i legami con le istituzioni europee, come dimostrano la firma di una "lettera d'intenti" con lo Stato Maggiore dell'Unione europea nel 2016 e la partecipazione a missioni di formazione (EUTM). Tuttavia, l'Eurocorps non può essere considerato una forza di primo intervento europea, poiché non è formalmente integrato nella Politica di Sicurezza e Difesa Comune, e la partecipazione degli Stati membri resta limitata. Sarebbe auspicabile che gli Associate Members, tra cui l'Italia, assumessero maggiori responsabilità, per ottenere il rango di Framework Members (Vellano, 2021).

L'Eurocorps svolge compiti rilevanti, tra cui garantire la sicurezza del Parlamento europeo a Strasburgo, ed è stato impiegato in missioni in Bosnia-Erzegovina (1998), Kosovo (2000), Afghanistan (2004-2005 e 2012), Mali (2015) e Repubblica Centrafricana (2016), le ultime due tuttora in corso. La natura multinazionale dell'Eurocorps è evidente in ogni struttura, sezione o unità, i cui membri indossano lo stesso berretto, fatta eccezione per i capi ramo, che sono associati a una specifica nazione (Vellano, 2021).

L'Eurocorps non va confuso con gli EU Battlegroups, anche se nel 2016-2017 ha assunto temporaneamente questa funzione. Gli EU Battlegroups sono battaglioni di circa 1.500 uomini, composti da contingenti nazionali messi a disposizione per specifiche missioni decise dal Consiglio europeo. Possono operare fino a 6.000 km da Bruxelles, raggiungendo la capacità operativa iniziale entro 10 giorni dalla decisione. Pur essendo operativi dal 2007, non sono mai stati impiegati in missioni concrete e, a differenza dell'Eurocorps, consistono in contingenti che rimangono sotto controllo nazionale (Vellano, 2021).

Nonostante le difficoltà e le incertezze, vi sono alcuni segnali positivi, in particolare nelle missioni militari e civili condotte all'estero sotto l'egida dell'Unione europea, mirate al mantenimento della pace, inclusi interventi di peace-keeping e peacebuilding. Gli EU Battlegroups possono rappresentare, ritornando al pensiero di Cohen, un embrione di future forze mobili di intervento rapido europee operative ed efficienti.

Conclusioni

Il Presidente francese Emmanuel Macron, in una recente riunione della Comunità Politica Europea, ha affrontato molti degli argomenti trattati nel presente lavoro[1]. Sebbene possa risultare difficile affermare che i conflitti che infiammano lo scenario internazionale odierno rappresentino uno scontro definitivo per il dominio sull' "Isola Mondo" di mackinderiana memoria, se non altro per un eccessivo catastrofismo, essi potrebbero essere invece analizzati nella prospettiva di resistenza conservatrice a quel processo di democratizzazione globale che dovrebbe portare alla "fine della storia" come intesa da Fukuyama. Difatti, a partire dalla caduta del Muro di Berlino, seppur con andamenti altalenanti, la tendenza alla democratizzazione su scala globale non è mai cessata. In questo contesto, le autocrazie sembrerebbero aver alzato il livello della competizione, al fine di rassicurare le proprie popolazioni in merito alla proprie capacità e cercare di preservare la propria esistenza, nonostante le forze disaggreganti, o centrifughe, presenti al loro interno e in grado di mettere a rischio l'integrità dello Stato o del potere politico attuale (Hartshorne, 1950).

Inoltre, l'Unione Europea ha senz'altro interesse, come affermato da Macron, a ostacolare l'espansionismo russo e a provvedere alla propria sicurezza, senza delegare la propria geopolitica agli Stati Uniti d'America che, però, provvedono alla difesa degli Stati europei con basi, mezzi e uomini fin dalla fine della II Guerra Mondiale. Se è vero che la rinnovata aggressività delle autocrazie (la Russia nei confronti dell'Ucraina, la Cina

nei confronti di Taiwan) potrebbe essere considerata di reazione alla progressiva diffusione della democrazia liberale e al "contagio" che questa potrebbe provocare nella società russa e in quella cinese, nonché in quelle dei loro partner internazionali, l'Unione Europea, e l'Europa in generale, hanno la necessità di poter affrancarsi, quando necessario, dalle posizioni degli Stati Uniti potendo, al contempo, provvedere autonomamente alla propria difesa.

---

[1] "Siamo pronti a difendere l'interesse degli europei? È l'unica domanda che ci viene posta. E io credo che questa debba essere la nostra priorità. E quindi, non si tratta di un transatlantismo ingenuo, né di mettere in discussione le nostre alleanze, né di un nazionalismo ristretto che non ci consentirebbe di affrontare la sfida rappresentata da Cina e Stati Uniti d'America. Questo è un momento storico per noi, europei, decisivo. In fondo, la domanda che ci viene posta è: vogliamo leggere la Storia scritta da altri — le guerre avviate da Vladimir Putin, le elezioni americane, le scelte tecnologiche o commerciali fatte dai cinesi — o vogliamo scrivere noi stessi la Storia? Io credo che abbiamo la forza per farlo. Le nostre economie sono forti, i nostri paesi dispongono di sistemi di difesa sofisticati e rappresentiamo qualcosa. L'Unione europea è composta da 449 milioni di abitanti con i suoi 27 paesi, mentre la Comunità politica europea ne conta più di 742 milioni. Se decidiamo di essere consapevoli di ciò che rappresentiamo a livello geopolitico e commerciale, siamo una potenza straordinaria. Non esiste nessun mercato di 742 milioni di abitanti altrettanto unito per storia, interessi e valori come noi, attorno a questo tavolo; nessuno. Se ci svegliamo e decidiamo di non scomparire geopoliticamente e di non essere il mercato di aggiustamento delle altre potenze, economicamente e commercialmente. Per me, questo è il momento di agire, di difendere i nostri interessi allo stesso tempo nazionali ed europei, di credere nella nostra sovranità e nella nostra autonomia strategica, e di affermare che non vogliamo essere semplicemente clienti, delegando ad altri la nostra economia, le nostre scelte tecnologiche o la nostra sicurezza, ma vogliamo affrontare pienamente la questione della pace sul nostro territorio, della nostra prosperità e di altri modelli democratici. Per me, queste sono le 3 sfide della comunità politica europea che dobbiamo discutere insieme. Il nostro interesse è che la Russia non vinca questa guerra, indipendentemente da ciò che pensano qui o altrove. Perché, se vince, significherebbe che alle nostre frontiere ci sarebbe una potenza imperiale a cui si dice: "Potete essere espansionisti". Non vedo come qualcuno possa sentirsi tranquillo attorno a questo tavolo se lasciamo che ciò accada. Allo stesso modo, credo sia molto importante fare tutto il possibile per costruire un accordo tra Armenia e Azerbaigian, e spero che il trattato di pace possa essere firmato. In fondo, la nostra pace e la nostra sicurezza dipendono dal fatto che noi europei sappiamo affermare: "Non vogliamo più imperialismo e non vogliamo più revisionismo dei confini sul nostro continente". Questo messaggio è fondamentale e risponde davvero a un interesse. Oltre a ciò, c'è da costruire la nostra Europa della difesa, fare dell'Europa uno spazio di sicurezza. L'Unione europea ha già fatto enormi progressi in questi anni, ma c'è ancora molto da fare per finanziare e costruire. La NATO ha, ovviamente, un ruolo centrale e noi, europei, vogliamo svolgere il nostro ruolo all'interno dell'Alleanza. Questo pilastro europeo della NATO non sottrae nulla all'Alleanza, ma il fatto che vi sia stato un risveglio strategico che noi dobbiamo oggi assumere è fondamentale: noi europei non dobbiamo delegare per sempre la nostra sicurezza agli americani. Credo sia importante anche trasmettere il messaggio che siamo ormai fornitori di soluzioni di sicurezza. E come si può vedere, che si tratti della nostra sicurezza, della nostra difesa, della nostra economia, del nostro modello di prosperità o della nostra democrazia, dobbiamo costruire un'agenda positiva estremamente ambiziosa se diventiamo consapevoli di cosa rappresenta la grande Europa attorno a questo tavolo, una potenza geopolitica senza eguali. Semplicemente, finora non ci siamo assunti appieno il ruolo di potenza indipendente. Pensiamo che sia necessario delegare la nostra politica estera agli Stati Uniti, il nostro modello di crescita ai nostri clienti cinesi, la nostra innovazione tecnologica agli americani. Non è la scelta migliore. Penso che possiamo riprendere il controllo, se decidiamo, nel prossimo decennio, di costruire, non solo all'interno dell'Unione europea, ma qui. In fondo, è semplice: il mondo è fatto di erbivori e carnivori. Se decidiamo di restare erbivori, i carnivori vinceranno e saremo un mercato per loro. Penso che, perlomeno, sarebbe meglio scegliere di essere onnivori. Non voglio essere aggressivo, voglio solo che siamo in grado

Sia per una necessità di tipo prettamente geografico: alcune politiche troppo audaci degli Stati Uniti d'America potrebbero causare rischi o danni di vario tipo ai partners occidentali, anche data la maggiore vicinanza e integrazione territoriale con le aree di tensione o di conflitto; sia per una necessità relativa alla geopolitica e alle relazioni internazionali europee: dopo la fine della Seconda Guerra Mondiale l'Europa non ha più avuto un ruolo geopolitico indipendente dagli USA, questa ambizione potrebbe essersi rinnovata anche grazie al processo di integrazione europea che rende gli Stati europei paragonabili alle grandi potenze del panorama globale per popolazione, reddito, tecnologia, capacità bellica, soft power, ecc. Inoltre, l'Unione Europea e l'Europa hanno la necessità di poter essere in grado di difendere autonomamente il proprio territorio e di attaccare quando minacciate, anche in prospettiva di un'escalation delle tensioni con le grandi autocrazie rivali delle democrazie liberali. A tal fine, appare urgente l'implementazione di forze mobili di intervento rapido, simili a quelle ipotizzate da Cohen per gli USA durante la Guerra Fredda, in grado di inaugurare una reale Difesa Comune Europea. Inoltre, l'implementazione della Difesa Comune Europea potrebbe rappresentare un concreto passo verso un piena e completa integrazione politica.

---

di difenderci su ciascuno di questi fronti. Ma non ho intenzione di lasciare che l'Europa diventi un teatro magnifico abitato da erbivori che i carnivori, secondo la loro agenda, verranno a divorare. Assumiamo questa responsabilità. Ecco perché credo molto in questo formato. È una questione di volontà comune e di capacità di prendere coscienza di ciò che siamo."

BIBLIOGRAFIA FINALE

- G. Agamben, “L’impero latino”, Quodlibet, 12 giugno 2018;
- Z. Brzezinski, “Grand Chessboard: American Primacy And Its Geostrategic Imperatives”, Basic Books, New York, 1998;
- S. B. Cohen, “Geography and politics in a divided world”, Random House, New York, 1963;
- J. Colamedici, “La difesa comune Prospettive di integrazione europea”, Jura Gentium, XVII, 2, 2020;
- A. Colombo, “La disunità del mondo. Dopo il secolo globale”, Feltrinelli, Milano, 2010;
- G. Douhet, “Il dominio dell’aria”, Ministero della Guerra, Roma, 1921;
- F. Fukuyama, “The End of History and the Last Man”, Free Press, New York, 1992;
- C. Hakansson, “The European Commission’s new role in EU Security and Defence Cooperation: the case of the European Defence Fund”, European Security, 2021
- S. P. Huntington, “The Clash of Civilizations and the Remaking of World Order”, Simon & Schuster, New York, 1996;
- R. Hartshorne, “The Functional Approach in Political Geography”, Annals of the Association of American Geographers, Vol. 40, No. 2, 1950;
- H. A. Kissinger, “Ordine mondiale”, Mondadori, Milano, 2018;
- H. T. Mackinder, “The Geographical Pivot of History”, The Geographical Journal, Vol. XXIII, n. 4, London, 1904;
- A. T. Mahan, “The Influence of Sea Power upon History”, Little, Brown & Company, Boston, 1890.
- J. Monnet, “Cittadino d’Europa: 75 anni di storia mondiale”, Rusconi, Milano, 1978;

- S. Ortmann, N. Whittaker, “Geopolitics and Grand Strategy”, in J. Baylis, J.J. Wirtz, C.S. Gray, “Strategy in the Contemporary World”, Oxford, Oxford University Press, 2019;

- D. Rakić, D. Verbeken, “Storia dell'Unione economica e monetaria”, Parlamento Europeo, Note tematiche sull’Unione europea, 01/2020;

- E. Severino, “Il tramonto della politica”, Milano, Rizzoli, 2018;

- N. J. Spykman, “America's Strategy in World Politics: The United States and the Balance of Power”, Harcourt & Brace, San Diego, 1942

- M. Vellano, “La costruzione di una leadership mondiale dell’Unione europea attraverso il rafforzamento della sua politica di sicurezza e di difesa comune”, I Post di AISDUE, III, 2021.

Atti di convegno

La regolamentazione internazionale dell'uso delle armi autonome: sfide e prospettive

Fabio Di Nunno
Senior Researcher, Project Manager e giornalista

"Regulating the use of autonomous weapons at the international level: challenges and prospects"

Abstract

Technological innovation and automation also affects the military sector, with autonomous weapons systems that select and strike targets based on sensor processing rather than human input, while the development of Artificial Intelligence (AI) opens up further scenarios and challenges to the democratic control and accountability of the armed forces.

Keywords: autonomous weapons systems - Artificial Intelligence - democratic control - armed forces.

Introduzione

L'innovazione tecnologica e l'automazione riguarda anche il settore militare, con sistemi d'arma autonomi, in inglese Autonomous Weapon Systems (AWS), o sistemi d'arma autonomi, in inglese Lethal Autonomous Weapon Systems (LAWS), che rappresentano una categoria di armamenti che selezionano e colpiscono bersagli basandosi sull'elaborazione di sensori anziché su input umani.[1] D'altronde, sistemi autonomi sono stati sviluppati da tempo e sono utilizzati negli ambiti più vari, dall'agricoltura all'esplorazione spaziale. Pensiamo ai robot, dotati di sensori che interagiscono con il mondo circostante, per poi attivare comportamenti reattivi attraverso la propria capacità di elaborazione che emula alcuni aspetti della cognizione umana, finanche alle autovetture a guida autonoma e ai problemi etici che pongono nel caso di un potenziale incidente.[2] Con lo sviluppo dell'Intelligenza Artificiale (IA), questa capacità di cognizione ed elaborazione aumenta in modo esponenziale, aprendo ulteriori scenari nell'ambito militare, con lo sviluppo di nuovi sistemi d'arma e nuove sfide al controllo democratico e all'accountability delle forze armate, laddove questi sistemi d'arma, proprio grazie all'implementazione di algoritmi di IA, possono assumere decisioni autonome e condurre operazioni militari senza un controllo umano diretto. Infatti, la crescente autonomia di sistemi d'arma autonomi letali sta modificando la logica dei conflitti contemporanei, sollevando conseguenti interrogativi etici e giuridici.

Alcuni studi hanno identificato nei droni armati, Unmanned Aerial Vehicles (UAV), i precursori delle armi autonome letali,[3] laddove il drone warfare, la guerra dei droni, nei suoi elementi essenziali di killing lists e

---

[1] È possibile identificare le seguenti tipologie di sistemi d'arma autonomi. I sistemi terrestri autonomi, che ricomprendono i veicoli terrestri autonomi che operano su terreno, dotati di armamenti letali, utilizzati in missioni di sorveglianza, pattugliamento o combattimento senza la necessità di un equipaggio umano a bordo. I sistemi navali autonomi, che ricomprendono imbarcazioni con capacità letali senza equipaggio umano a bordo, utilizzate in missioni di pattugliamento marittimo, protezione delle rotte navali, ricerca, attacco, ecc. I sistemi di difesa aerea autonoma, che ricomprendono quei sistemi che identificano e neutralizzano autonomamente delle minacce aeree senza un intervento umano diretto, con capacità di riconoscimento e decisione basate su algoritmi. I robot terrestri autonomi, che possiedono una capacità di movimento su terreno e che svolgono operazioni militari, quali ricognizioni, disinnesco di ordigni esplosivi, missioni offensive, ecc. I sistemi sottomarini autonomi, che ricomprendono quei veicoli sottomarini privi di equipaggio umano a bordo che operano senza l'intervento diretto dell'uomo. I sistemi di sciame, detti anche swarm di robot, cioè quei gruppi di robot o droni che operano in modo coordinato, utilizzati principalmente per compiti distribuiti e collaborativi. I sistemi di armi autonome letali, in grado di assumere decisioni autonome in merito all'identificazione e all'attacco di obiettivi. I sistemi di supporto logistico autonomi, che comprendono veicoli o droni utilizzati per attività logistiche, quali il trasporto di materiali, munizioni, medicinali, ecc., senza il coinvolgimento diretto dell'uomo.

[2] Cfr. G. Contissa, F. Lagioia, G. Sartor, La Manopola Etica: I veicoli autonomi eticamente personalizzabili e il diritto, "Sistemi intelligenti", 29(3), 2017, pp. 601-614.

[3] Cfr. P. L. Bergen & D. Rothenberg, Drone Wars: Transforming Conflict, Law, and Policy, New York, Cambridge University Press, 2014; G. Chamayou, Teoria del drone. Principi filosofici del diritto di uccidere, Roma, DeriveApprodi, 2015; F. Farruggia (a cura di), Dai droni alle armi autonome. Lasciare l'Apocalisse alle macchine?, Franco Angeli, Milano, 2023.

analisi delle forme di vita, condotte dagli Stati Uniti d'America nella sua guerra al terrore all'inizio del XXI secolo, attuavano una «fusione dell'analisi geo-spaziale con quella della rete sociale»[4] per monitorare le attività umane e così stabilirne le identità da colpire. Allorquando l'obiettivo veniva individuato sulla base di una probabilità statistica e sociologica e non dalla provata affiliazione a gruppi terroristici sorsero i primi problemi etici, laddove si realizzava un'estensione, nel tempo e nello spazio, dell'uso della forza da parte degli Stati e del loro diritto di uccidere, che oltrepassa i confini tra gli Stati, senza rispettare il principio d'integrità territoriale, mettendo in dubbio l'eticità stessa di una guerra di droni. Infatti, come è stato osservato, l'impatto della guerra dei droni sul diritto umanitario è tutto da valutare, con l'uso sempre più frequente di robot, laddove il principio di umanità è ridotto ad un algoritmo.[5] Vero è che la guerra classica è solo un ricordo, mentre le tecnologie informatiche sono ormai costantemente utilizzate nei conflitti armati e, anzi, oggi sono sia uno strumento che un obiettivo di guerra, tanto da parlare di cyberwarfare. La guerra cibernetica presenta pericoli e problemi di difficile soluzione, anche dal punto di vista giuridico, poiché vengono meno le distinzioni del diritto internazionale, come quelle tra civile e militare, neutrale e belligerante, prigioniero e combattente.[6] Tuttavia, è indubbio che nell'ultimo decennio lo sviluppo di armi più propriamente autonome, cioè capaci di selezionare e di attaccare gli obiettivi senza interventi da parte di un operatore umano, ha aperto scenari militari nuovi,[7] sui quali la dottrina si sta interrogando nell'ultimo decennio.[8] Nello specifico, è stato osservato che «il grado di autonomia di questi dispositivi è variabile: di

---

[4] G. Chamayou, Teoria del drone. Principi filosofici del diritto di uccidere, DeriveApprodi, Roma, 2014, p. 43.

[5] Cfr. F. Ruschi, Il volo del drone. Verso una guerra post-umana?, in "Jura Gentium", 1, 2016, pp. 12-38.

[6] Cfr. S. Pietropaoli, Un altro modo di fare la guerra. La cyberwar come problema giuridico, in "Ars interpretandi, Rivista di ermeneutica giuridica", 1/2023, pp. 61-76.

[7] Cfr. M. Artoni (a cura di), L'impiego dell'intelligenza artificiale – Una trasformazione inevitabile. Evoluzione e stato dell'arte, Centro Alti Studi per la Difesa (CASD) – Istituto di Ricerca e Analisi della Difesa (IRAD), 2022; C. Catalano (a cura di), Evoluzione e stato dell'arte dello "SWARMING" e la sua relazione con le Multi-Domain Operations (MDOs): progressi tecnologici, ambiti di applicazione, punti di forza, vulnerabilità, opportunità, minacce, Centro Alti Studi per la Difesa (CASD) – Istituto di Ricerca e Analisi della Difesa (IRAD), 2022; P. Ceola, Macchine Guerriere Autonome, Filosofia, anno LXV, Mimesis Edizioni, Milano-Udine, 2020, pp. 51-62; Id. e C. R. Gaza, Non-human Warfare. Robot e cyborg tra postmoderno e postumano, Collana SISM, 4, Torino, Società Italiana di Storia Militare, 2013; E. ElMasry, Army of the Future: Artificial Intelligence and Its Impact on Operations, JCSP-PCEMI 44, Canadian Forces College, 2018; M. Galeotti, The Weaponization of Everything. A Field Guide to the New Way of War, New Haven, Yale University Press, 2023; Id., Il modello Osint in ambito militare: dinamiche di open/closed access nel trattamento dell'informazione a fini strategici, Rivista di Digital Politics, 3(2), 2023, pp. 413-442; A. Iaria, Da autonomi a completamente autonomi: l'applicazione dell'Intelligenza Artificiale nei sistemi d'arma autonomi (LAWS), Rassegna della Giustizia Militare: Rivista della Giustizia e della Procedura Penale Militare, 6, 2018, 24-32; J. Smith, Autonomous Weapon Systems: A Comprehensive Survey, Journal of Military Ethics, 19(3), 2020, pp. 245-263.

[8] Cfr. D. Amoroso, Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains, Edizioni Scientifiche Italiane e Nomos Verlag, Napoli, 2021; IRIAD – Istituto di Ricerche Internazionali Archivio Disarmo, LAWS: Lethal Autonomous Weapon Systems: La questione delle armi letali autonome e le possibili azioni italiane ed europee per un accordo internazionale, IRIAD Review – Studi sulla pace e sui conflitti, 7-8, 2020,

regola essi sono guidati e controllati a distanza, ma possono in alcuni casi prendere l'iniziativa, specialmente quando il controllo a distanza non sia disponibile o quando sia necessaria una reazione rapida».[9] D'altronde, «l'evoluzione tecnologica va certamente nel senso di una loro crescente autonomia, che giunge in alcuni casi alla capacità di attivarsi autonomamente nel perseguimento, e in alcuni casi nella stessa individuazione, di obiettivi contro i quali esercitare forza letale».[10] Finora, non è stata sviluppata una disciplina precisa sull'uso delle armi autonome, mentre il Parlamento europeo è l'unica istituzione ad essersi espressa chiaramente contro l'uso di armi letali autonome.[11] Sebbene, dunque, il dibattito non sia nuovo, [12] solo di recente la Comunità Interazionale, conscia dei pericoli insiti nello sviluppo di sistemi d'arma autonomi, ha iniziato ad interrogarsi sul tema ed ha intrapreso un'iniziativa volta alla regolamentazione dei sistemi d'arma autonomi in seno alle Nazioni Unite.

1. La Risoluzione dell'Assemblea generale delle Nazioni Unite sui Sistemi di armi letali autonome

L'Assemblea generale delle Nazioni Unite (ONU), nell'ottobre del 2023, ha approvato una risoluzione[13] nella quale riconosce i rischi delle nuove applicazioni tecnologiche nel dominio militare e la rimozione del controllo umano sull'uso della forza, che la comunità internazionale deve affrontare, dal punto di vista umanitario, giuridico, di sicurezza, tecnologico ed etico. Gli Stati si sono detti preoccupati per le possibili conseguenze negative e l'impatto dei sistemi d'arma autonomi sulla sicurezza globale e sulla stabilità regionale e internazionale, compreso il rischio di una corsa agli armamenti, che abbasserebbe la soglia per i conflitti e la proliferazione, anche per gli attori non statali. L'Assemblea generale ha sottolineato l'urgente necessità che la

---

pp. 1-161; A. Krishnan, Killer robots. Legality and ethicality of autonomous weapons, Farnha, Ashgate Publishing Limited, 2009; M. Leonard, L'era della non-pace. Perchè la connettività porta al conflitto, Milano, Bocconi University Press, 2023; M. M. Maas, How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons. Contemporary Security Policy, 40(3), 2019, pp. 285-311; F. Sabry, Armi autonome. In che modo l'intelligenza artificiale prenderà il sopravvento sulla corsa agli armamenti, Abu Dhabi, 1BK One Billion Knowledgeable, 2021; M. Sacchi, La guerra delle macchine. Hacker, droni e androidi: perché i conflitti ad alta tecnologia potrebbero essere ingannevoli e terribilmente fatali, Milano, Algama Editore, 2020.

[9] G. Sartor, L'intelligenza artificiale e il diritto, Giappichelli, Torino, 2022, p. 99.

[10]Ibid.

[11] Il Parlamento europeo, in una risoluzione dedicata ai droni, si è espresso contro le armi autonome letali, chiedendo all'Alto Rappresentante dell'Unione per la politica estera e di sicurezza comune, agli Stati membri e al Consiglio, che però è il solo ad avere la competenza ad esprimere la posizione dell'Unione europea in relazione al dibattito internazionale volto a vietare lo sviluppo, la produzione e l'impiego di armi autonome letali. Cfr. Risoluzione del Parlamento europeo sull'utilizzo di droni armati, 27 febbraio 2014 (2014/2567(RSP)).

[12] P. Asaro, On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making, International Review of the Red Cross, 94(886), 2012, pp. 687-709.

[13] Lethal autonomous weapons systems, General Assembly Resolution 78/241, 13 October 2023.

comunità internazionale affronti le sfide e le preoccupazioni sollevate dai sistemi d'arma autonomi, in particolare attraverso il Gruppo di esperti governativi sulle tecnologie emergenti nel settore dei sistemi d'arma autonomi letali, nonché la necessità che si continui ad approfondire la propria comprensione della questione. Ecco che l'Assemblea generale ha chiesto al Segretario generale delle Nazioni Unire, Antonio Guterres, di raccogliere i pareri degli Stati membri e degli Stati osservatori sui sistemi di armi letali autonome, su come affrontare le sfide e le preoccupazioni correlate, secondo prospettive umanitarie, giuridiche, di sicurezza, tecnologiche ed etiche e sul ruolo degli esseri umani nell'uso della forza, e di presentare una relazione.[13] Il successivo rapporto del Segretario Generale[14] ha ribadito i rischi dei sistemi di armi letali autonome, ma ha anche considerato un vuoto nel diritto internazionale, auspicando una regolamentazione entro il 2026. Gli Stati hanno osservato che i rapidi processi tecnologici, tra cui l'intelligenza artificiale, potrebbero anche porre sfide per la pace e la sicurezza internazionale e sollevare interrogativi sul ruolo degli esseri umani in guerra. Gli Stati hanno ritenuto che le sfide poste dai sistemi di armi letali autonome richiedessero un'attenzione particolare.

2. Definizioni e caratterizzazioni

Gli Stati hanno osservato che al momento non esiste una definizione concordata a livello internazionale di

---

[13] L'Italia ha co-sponsorizzato la risoluzione 78/241 dell'Assemblea generale. Dal 2013 l'Italia partecipa attivamente al dibattito internazionale sui sistemi d'arma autonomi letali, avviato sotto l'egida della Convenzione sulla proibizione o limitazione dell'uso di alcune armi convenzionali che possono essere considerate eccessivamente dannose o aventi effetti indiscriminati, dapprima nell'ambito di riunioni informali di esperti e poi come partecipante allo stesso Gruppo di esperti governativi sui sistemi d'arma autonomi letali. Secondo l'Italia, la Convenzione su alcune armi convenzionali è di gran lunga il forum più adatto per affrontare le questioni attuali ed emergenti relative allo sviluppo e all'uso di sistemi d'arma. Un gran numero di parti ha aderito alla Convenzione, tra cui gli Stati che sono i principali sviluppatori e produttori di applicazioni militari dell'intelligenza artificiale. Inoltre, consente la combinazione di competenze diplomatiche, legali e militari, anche attraverso rappresentanti non solo degli Stati parti ma anche di organizzazioni internazionali, istituzioni specializzate e organizzazioni della società civile. La Convenzione è anche il forum migliore per esaminare la compatibilità di un sistema d'arma con il diritto internazionale umanitario. Oltre a questi principi, l'articolo 35 del Protocollo addizionale alle Convenzioni di Ginevra del 12 agosto 1949, relativo alla protezione delle vittime dei conflitti armati internazionali (Protocollo I), ribadisce che i metodi e i mezzi della guerra non sono illimitati, un concetto reso operativo dall'articolo 36, che impone agli Stati parti l'obbligo di garantire che non vengano utilizzate armi illegali. Sebbene non si tratti di un vuoto giuridico, l'Italia ritiene che sia necessario sviluppare ulteriormente un quadro normativo e operativo che disciplini i sistemi d'arma autonomi. L'elemento umano è, secondo l'Italia, cruciale per l'intero ciclo di vita dei sistemi di armi letali autonome, vale a dire per la loro progettazione, sviluppo, produzione, distribuzione e utilizzo. Se l'obiettivo fosse garantire la conformità al diritto internazionale umanitario, allora dovrebbe essere mantenuto un livello appropriato di giudizio e controllo umano, in modo da garantire la responsabilità ai sensi del diritto internazionale umanitario. Solo un essere umano può essere ritenuto responsabile ai sensi del diritto internazionale umanitario, mai una macchina.

[14] Lethal autonomous weapons systems, Report of the Secretary-General of the United Nations, 1 July 2024.

sistemi di armi autonome o sistemi di armi letali autonome, ma che un accordo su una definizione o una caratterizzazione generale potrebbe essere utile. Ciononostante, diversi Stati hanno ritenuto che si possano iniziare le negoziazioni su uno strumento giuridicamente vincolante. Diversi Stati hanno sottolineato l'importanza del grado di intervento umano in particolare nell'identificazione, classificazione, intercettazione e coinvolgimento di un obiettivo. Hanno sottolineato che l'apporto umano nominale, ovvero gli input o le azioni che non influenzano materialmente le funzioni autonome di selezione o coinvolgimento dell'obiettivo, non è sufficiente. Gli Stati hanno offerto diverse definizioni operative e caratterizzazioni dei sistemi di armi letali autonome. Alcuni hanno attinto alla definizione del Comitato Internazionale della Croce Rossa,[15] secondo la quale la definizione di sistema di armi autonome si riferisce a un sistema di armi progettato per selezionare e ingaggiare uno o più bersagli senza la necessità di un intervento umano dopo l'attivazione. È stato espresso il punto di vista secondo cui una caratteristica dei sistemi di armi letali autonome potrebbe includere l'intelligenza artificiale nella selezione del bersaglio e nell'uso della forza. Diversi Stati hanno suggerito che certi sistemi di difesa antiaerea e missilistica autonomi o automatici non dovrebbero essere considerati sistemi di armi letali autonome, data la loro natura difensiva e la natura deterministica, piuttosto che probabilistica, degli algoritmi utilizzati da quei sistemi per il rilevamento e l'ingaggio di bersagli. D'altronde, tali sistemi vengono utilizzati da decenni senza controversie legali. Molti Stati hanno sottolineato l'importanza di mantenere il controllo umano dell'uso della forza, durante l'intero ciclo di vita di un sistema d'arma, ma in particolare durante l'uso. Il controllo umano[16] è particolarmente importante per garantire la conformità al diritto internazionale, in particolare al diritto internazionale umanitario,[17] nonché la responsabilità e la rendicontazione.[18]

Gli Stati hanno preso in considerazione gli elementi necessari del controllo umano, tra cui il mantenimento da parte degli esseri umani:

- Informazioni sufficienti, anche sulle capacità del sistema d'arma e sul contesto operativo, per garantire la conformità al diritto internazionale.

---

[15] Cfr. International Committee of the Red Cross (ICRC), Autonomous weapon systems: Technical, military, legal and humanitarian aspects. CCW Expert meeting, Geneva, 2014, <https://www.icrc.org/en/document/report-icrcmeeting-autonomous-weapon-systems-26-28-march-2014>; Id. Views of the International Committee of the Red Cross on autonomousweapon system, paper subm itted to the Informal meeting of experts on lethal autonomous weapons systems of the Convention on Certain Conventional Weapons (CCW), ICRC, Geneva, 11 April 2016; Id. Position on Autonomous Weapons Systems, ICRC, Geneva, 12 May 2021.

[16] Cfr. V. Boulanin, N. Davison, N. Goussac, & M. P. Carlsson, Limits on autonomy in weapon systems. Identifying Practical Elements of Human Control, SIPRI Stockholm International Peace Research Institute, 2020.

[17] V. Boulanin, L. Bruun & N. Goussac, Autonomous weapon systems and International Humanitarian Law: Identifying limits and the required type and degree of human-machine interaction, SIPRI Stockholm International Peace Research Institute, 2017.

[18] La cosiddetta Explainable AI (XAI) affronta proprio la questione di dotare i sistemi della IA di una di caratteristiche affinché l'operatore sia messo in grado di comprendere il perché di una decisione assunta da un'arma autonoma.

- La capacità di esercitare il proprio giudizio nella misura richiesta dalle norme internazionali di diritto umanitario.
- La capacità di limitare i tipi di attività e gli obiettivi.
- La capacità di porre limitazioni alla durata, all'ambito geografico e alla scala di utilizzo.
- La capacità di ridefinire o modificare l'obiettivo o le missioni del sistema.
- La possibilità di interrompere o disattivare il sistema.

Gli Stati hanno suggerito varie misure attraverso le quali si potrebbe raggiungere il grado richiesto di controllo umano, tra cui:

- La creazione di un'interfaccia intuitiva per l'interazione uomo-macchina.
- Delle procedure per garantire che i sistemi di armi letali autonome siano stati testati, valutati, convalidati e verificati.
- Delle revisioni legali sufficienti dei sistemi di armi letali autonome.
- Una formazione adeguata per tutti gli esseri umani che interagiscono con sistemi di armi letali autonome.
- La garanzia della prevedibilità, dell'affidabilità e dell'illustrazione logica dei sistemi di armi letali autonome.

3. Sfide, preoccupazioni e potenziali benefici dei sistemi di armi letali autonome

Gli Stati hanno osservato che i sistemi di armi letali autonome sollevano una serie di preoccupazioni, tra cui quelle umanitarie, sui diritti umani, giuridiche, di sicurezza, tecnologiche ed etiche. Hanno chiesto che tali preoccupazioni siano affrontate in modo esaustivo. Diversi Stati hanno osservato che i sistemi di armi letali autonome pongono sfide al rispetto del diritto internazionale, in particolare del diritto internazionale umanitario, dei diritti umani e del diritto penale internazionale, seppure non esista alcuno strumento giuridico internazionale che regoli o proibisca specificamente i sistemi di armi letali autonome. Altre preoccupazioni sollevate riguardano l'impatto ambientale dei sistemi di armi letali autonome, in particolare i costi energetici e l'impronta di carbonio associata allo sviluppo e al funzionamento di tali sistemi. Gli Stati hanno osservato che la scelta di armi, mezzi e metodi di guerra, compresi i sistemi di armi letali autonome, deve essere conforme al diritto internazionale, in particolare al diritto internazionale umanitario. Gli Stati hanno sottolineato l'importanza dei principi di distinzione, proporzionalità, necessità militare e precauzioni in caso di attacco, nonché l'obbligo di evitare lesioni superflue o sofferenze inutili. Diversi Stati hanno sottolineato che qualsiasi arma, compresi i sistemi di armi letali autonome, che non sia conforme al diritto internazionale umanitario è di fatto già proibita e non deve essere utilizzata. D'altronde, diversi Stati hanno chiesto di specificare ulteriormente le regole e i principi del diritto internazionale umanitario da applicare ai sistemi di armi letali autonome.

Ecco che il principio del controllo umano potrebbe essere un concetto rilevante nell'attuazione di vari obblighi di diritto internazionale umanitario.[19] Al fine di garantire il rispetto del diritto internazionale umanitario, gli Stati dovrebbero regolamentare i sistemi di arma autonomi in modo da:

- valutare la presenza di civili;
- limitare la durata, la portata geografica e la scala di funzionamento delle armi autonome;
- limitare i tipi di obiettivi con cui un sistema potrebbe interagire;
- definire le regole di ingaggio;
- ·mettere in atto misure di sicurezza tecniche, come l'autodistruzione e l'autodisattivazione.

Gli Stati sottolineano l'importanza di garantire, in conformità con il diritto internazionale, che gli esseri umani mantengano la responsabilità e il resoconto per gli effetti delle armi nelle operazioni militari, compresi i sistemi di armi letali autonome, e che tale responsabilità non possa essere trasferita alle macchine, per cui i sistemi di armi letali autonome non devono essere progettati in modo tale da impedirne la responsabilità o il resoconto.

4. Considerazioni dell'uso di sistemi di armi letali autonome sulla sicurezza internazionale

Diversi Stati hanno osservato che l'uso di sistemi di armi letali autonome potrebbe essere un fattore destabilizzante, anche abbassando la soglia per l'uso della forza, il che potrebbe peggiorare la frequenza e l'intensità dei conflitti e il precipitare in crisi umanitarie. È stata espressa preoccupazione anche per il potenziale effetto destabilizzante della proliferazione di sistemi di armi letali autonome. Diversi Stati hanno fatto riferimento ai rischi di escalation causati dall'imprevedibilità dei sistemi di armi letali autonome, tra cui il potenziale di interazione macchina-macchina, l'aumento della velocità della guerra, il rischio ridotto di vittime militari per lo Stato utilizzatore e la guerra asimmetrica. Gli Stati hanno espresso preoccupazione per il fatto che i sistemi di armi letali autonome potrebbero diventare oggetto di una corsa agli armamenti. È stato espresso il punto di vista secondo cui i sistemi di armi letali autonome non dovrebbero essere utilizzati per cercare la superiorità militare assoluta e l'egemonia. Gli Stati hanno espresso preoccupazione per le

---

[19] Gli Stati hanno presentato diverse caratteristiche dei sistemi di armi letali autonome che non potrebbero essere utilizzati in conformità al diritto internazionale umanitario e che renderebbero tali sistemi:

·Intrinsecamente indiscriminato.

·Impossibile distinguere tra combattenti e civili.

·Progettato per applicare la forza contro civili o oggetti civili.

·Non è possibile determinare se un attacco potrebbe causare danni incidentali agli oggetti civili che sarebbero eccessivi rispetto al vantaggio militare previsto.

·Di natura tale da causare danni superflui o sofferenze non necessarie.

·Avere effetti che non potevano essere previsti, anticipati, compresi o spiegati in modo affidabile.

·Avere effetti che non potevano essere limitati e controllati.

conseguenze della proliferazione di sistemi di armi letali autonome per attori non statali, come gruppi terroristici e criminali, ma anche da parte di funzionari delle forze dell'ordine nazionali, il che potrebbe sollevare preoccupazioni in materia di diritti umani.

Vi sono delle considerazioni tecnologiche riguardanti l'uso dei sistemi di armi letali autonome dove diversi Stati hanno espresso preoccupazione, identificando una serie di rischi tecnologici insiti a tali sistemi, tra cui:

- attività informatica dannosa;
- anomalie e malfunzionamenti hardware e software;
- decisioni basate su informazioni errate o interpretate in modo errato;
- imprevedibilità dell'applicazione dell'intelligenza artificiale alle funzioni critiche dei sistemi di armi letali autonome.

In riferimento ad alcune considerazioni etiche,[20] diversi Stati hanno espresso preoccupazione per i processi delle macchine che sostituiscono il giudizio umano, poiché ritengono che le considerazioni etiche e morali siano fondamentali per i sistemi di armi letali autonome. Tali sistemi sono stati considerati privi di empatia, compassione e capacità di ragionamento morale. Infatti, le responsabilità etiche in relazione alle decisioni di applicare la forza richiedono il giudizio degli esseri umani basato sul valore e sul contesto specifico. Diversi Stati ritengono che prendere di mira gli esseri umani e, in particolare, delegare la decisione di togliere una vita umana alle macchine sia immorale. Inoltre, diversi Stati hanno espresso preoccupazione per il fatto che l'uso di sistemi di armi letali autonome potrebbe portare alla perdita di dignità e alla disumanizzazione, nonché causare violenza ingiustificata e vittime civili.

D'altronde, è stato anche osservato che i sistemi di armi autonome possono offrire legittimi benefici militari, tra cui:

- migliorare la sicurezza e l'efficienza;
- migliorare il rispetto del diritto internazionale umanitario, migliorare la protezione dei civili e ridurre il rischio di danni collaterali, anche migliorando la precisione;
- ridurre il rischio per il personale della difesa;
- evitare errori causati dallo stato mentale o fisico dell'operatore umano, nonché dalla sua predisposizione morale, religiosa ed etica;
- rendere più efficiente l'uso del lavoro.

---

[20] Cfr. P. Asaro, "Autonomous Weapons and the Ethics of Artificial Intelligence", in S. M. Liao (Ed.), Ethics of Artificial Intelligence, Oxford, Oxford University Press, 2020.

5. Sviluppi futuri Lo sviluppo del quadro normativo sui sistemi di armi letali autonome.

Diversi Stati hanno chiesto un ulteriore sviluppo del quadro normativo e operativo che disciplini i sistemi di armi letali autonome. Mentre diversi Stati hanno chiesto di rafforzare il quadro giuridico internazionale e di specificarlo ulteriormente in relazione ai sistemi di armi letali autonome, altri hanno espresso l'opinione che il quadro giuridico esistente fosse sufficiente per affrontare le nuove capacità militari, compresi i sistemi di armi letali autonome. Diversi Stati hanno chiesto negoziati su uno strumento giuridicamente vincolante sui sistemi di armi letali autonome al fine di:

- Continuare la codificazione e lo sviluppo progressivo delle norme di diritto internazionale applicabili nei conflitti armati.
- Chiarire l'applicazione del diritto internazionale umanitario ai sistemi di armi letali autonome e facilitarne l'attuazione.
- Colmare le lacune del diritto internazionale, in particolare del diritto internazionale umanitario.

Diversi Stati hanno fatto riferimento all'appello del Segretario generale affinché sia definito, entro il 2026, uno strumento giuridicamente vincolante per vietare i sistemi di armi letali autonome che funzionano senza controllo o supervisione umana e che non possono essere utilizzati in conformità con il diritto internazionale umanitario, e di regolamentare tutti gli altri tipi di sistemi di armi autonome.

6. I sistemi di armi autonome e gli sviluppi dell'Intelligenza Artificiale

È notizia recente che OpenAI, la società di intelligenza artificiale più importante al mondo, quella che sta dietro ChatGPT, si sia resa disponibile a collaborare con Anduril Industries, una startup americana di tecnologia di difesa specializzata in sistemi autonomi, per aggiungere per l'appunto la sua tecnologia di IA ai sistemi che l'esercito statunitense utilizza per contrastare gli attacchi dei droni. Tale partnership, per la prima volta, rappresenta il coinvolgimento di OpenAI con il Dipartimento della Difesa degli Stati Uniti nonché il suo primo rapporto con un produttore commerciale di armi.[21]

Del resto, l'IA è entrata nel settore delle guerre su quattro livelli[22]: il primo è quello della guerra cibernetica, dove dei tecnici conducono degli attacchi informatici a infrastrutture dell'avversario; il secondo livello è quello di supporto ai sistemi di armamento tradizionali; il terzo livello è quello di una rete digitale che un Paese realizza per difendersi da attacchi esterni; il quarto livello è quello dell'intelligence, dove l'IA supporta

---

2[1] H. Somerville, D. Seetharaman, OpenAI Enters Silicon Valley's Hot New Business: War, The Wall Steet Journal, 4 December 2024, <https://www.wsj.com/tech/ai/openai-enters-silicon-valleys-hot-new-business-war-7beccf6e>.

[22] Cfr. M. Zanzucchi, "IA tra guerra e pace", in Città Nuova, febbraio 2024, p. 17.

l'attività dei servizi segreti. Poi, l'IA è entrata anche nel settore degli armamenti con lo sviluppo di sistemi d'arma autonomi letali, che, però, dovrebbero avere sempre una supervisione umana adeguata, significativa e coerente dei sistemi d'arma; poiché questi, come evidenziato anche da Papa Francesco,[23] «non potranno mai essere soggetti moralmente responsabili: l'esclusiva capacità umana di giudizio morale e di decisione etica è più di un complesso insieme di algoritmi, e tale capacità non può essere ridotta alla programmazione di una macchina che, per quanto "intelligente", rimane pur sempre una macchina».[24] Inoltre, bisogna considerare anche il pericolo che tali armi vengano utilizzate da Stati canaglia o terroristi, per interventi volti a destabilizzare istituzioni di governo legittime. È opportuno menzionare il processo di Hiroshima sull'IA è, nell'ambito del G7, e il Codice di condotta per le organizzazioni che sviluppano sistemi di intelligenza artificiale avanzati. Nello specifico, le organizzazioni non dovrebbero sviluppare o implementare sistemi di intelligenza artificiale in modo da compromettere i valori democratici, che siano particolarmente dannosi per gli individui o le comunità, facilitino il terrorismo, promuovano il crimine o comportino rischi sostanziali per la sicurezza e i diritti umani e siano quindi inaccettabili. Gli Stati devono rispettare i propri obblighi ai sensi del diritto internazionale per garantire che i diritti umani siano pienamente rispettati e protetti, mentre le attività del settore privato dovrebbero essere in linea con i quadri internazionali come i Principi guida delle Nazioni Unite su imprese e diritti umani e le Linee guida dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) per le imprese multinazionali. [25]

---

[23] La prima opposizione della Santa Sede all'uso di armi letali autonome risale al 2018, nella considerazione che la tecnologia deve essere compatibile con la giusta concezione etica e giuridica dell'essere umano. Cfr. M. Raviart, "Onu: la Santa Sede condanna l'uso di robot automatici in guerra", Vatican News, 10 aprile 2018, <https://www.vaticannews.va/it/vaticano/news/2018-04/santa-sede-onu-armi-jurkovic0.html>

[24] Francesco, Messaggio per la LVII Giornata Mondiale della Pace, 8 dicembre 2023, p. 6.

[25] Il processo di Hiroshima sull'IA è stato istituito in occasione del vertice G7, guidato dal Giappone, del 19 maggio 2023 per promuovere misure protettive a livello mondiale per i sistemi avanzati di IA. Gli undici principi guida adottati dai leader dei sette Paesi più l'Ue, che insieme costituiscono il G7, offrono orientamenti alle organizzazioni che sviluppano, diffondono e utilizzano sistemi avanzati di IA, come i modelli di base e gli strumenti di IA generativa, per promuovere la sicurezza e l'affidabilità della tecnologia. Questi principi comprendono impegni per mitigare i rischi e gli abusi, individuare le vulnerabilità e promuovere una condivisione responsabile delle informazioni, la segnalazione degli incidenti e gli investimenti nella cibersicurezza, nonché un sistema di etichettatura che consenta agli utenti di individuare i contenuti generati dall'IA. Questi principi, che si basano sui risultati di un'indagine, sono stati sviluppati congiuntamente dall'Ue e dagli altri membri del G7 nel quadro, per l'appunto, del processo di Hiroshima sull'IA. A loro volta i principi guida sono serviti come base per l'elaborazione di un codice di condotta che fornisce orientamenti dettagliati e pratici alle organizzazioni che sviluppano l'IA. Il codice di condotta internazionale per le organizzazioni che sviluppano sistemi di IA avanzati mira a promuovere un'IA sicura e affidabile in tutto il mondo e fornirà orientamenti volontari per le azioni delle organizzazioni che sviluppano i sistemi di IA più avanzati, compresi i modelli di base e i sistemi di IA generativa più avanzati. Entrambi i documenti saranno riesaminati e aggiornati, se necessario, anche tramite consultazioni partecipative e inclusive, per fare in modo che rimangano adatti allo scopo che perseguono e tengano il passo con questa tecnologia in rapida evoluzione. I leader del G7 hanno invitato le organizzazioni che sviluppano sistemi avanzati di IA ad assumere l'impegno di applicare il codice di condotta internazionale. I primi firmatari saranno annunciati nel prossimo futuro. Cfr.

Conclusioni

L'utilizzo dei sistemi d'arma autonomi letali è una questione complessa, che riguarda dimensioni etiche, giuridiche, filosofiche, politiche e militari. Il dibattito accademico, seppure sviluppatosi da tempo, ha visto gli Stati interessarsi alla questione di una possibile regolamentazione dell'uso dei sistemi d'arma autonomi letali solo di recente, nel consesso delle Nazioni Unite. Richiamando, per l'appunto, le conclusioni del Segretario Generale delle Nazioni Unite nel suo report sul tema, nella Comunità internazionale c'è una preoccupazione diffusa che i sistemi di armi autonome letali abbiano il potenziale per cambiare significativamente la guerra e possano mettere a dura prova o persino erodere i quadri giuridici esistenti. È ampiamente riconosciuto dagli Stati che il controllo umano è essenziale per garantire responsabilità e rendicontazione, in conformità al diritto internazionale e secondo un processo decisionale etico. Da qui la necessità di agire con urgenza per preservare il controllo umano sull'uso della forza, in considerazione del fatto che le macchine che hanno il potere e la discrezione di togliere vite umane siano politicamente inaccettabili e moralmente ripugnanti e dovrebbero essere vietate dal diritto internazionale. Oltre le iniziative delle Nazioni Unite, è indubbio che anche il G7 può giocare un ruolo chiave nel regolamentare l'uso delle armi letali autonome.[26] Il consenso che sarebbe stato raccolto nella comunità internazionale non può che far pensare ad una prossima regolamentazione dell'uso delle armi letali autonome, che ne rifletta il rispetto del Diritto Internazionale Umanitario e, in definitiva, ristabilisca il controllo democratico sull'uso della forza.

Hiroshima Process International Code of Conduct for Advanced AI Systems, <https://digital-strategy.ec.europa.eu/it/library/hiroshima-process-international-code-conduct-advanced-ai-systems>.

[1] Cfr. E. Greco, F. Marconi and F. Maremonti, The Transformative Potential of AI and the Role of G7, IAI, 2024.

FONTI PRINCIPALI

- D. Amoroso, Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains, Edizioni Scientifiche Italiane – Nomos Verlag, Napoli, 2021.

- P. Asaro, "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making", International Review of the Red Cross, 94(886), 2012.

- P. Asaro, "Autonomous Weapons and the Ethics of Artificial Intelligence", in S. M. Liao (ed.), Ethics of Artificial Intelligence, Oxford University Press, Oxford, 2020.

- M. Artoni (a cura di), L'impiego dell'intelligenza artificiale – Una trasformazione inevitabile. Evoluzione e stato dell'arte, Centro Alti Studi per la Difesa (CASD) – Istituto di Ricerca e Analisi della Difesa (IRAD), 2022.

- P. L. Bergen, D. Rothenberg, Drone Wars: Transforming Conflict, Law, and Policy, Cambridge University Press, New York, 2014.

- V. Boulanin, N. Davison, N. Goussac, M. P. Carlsson, Limits on Autonomy in Weapon Systems. Identifying Practical Elements of Human Control, SIPRI – Stockholm International Peace Research Institute, Stockholm, 2020.

- V. Boulanin, L. Bruun, N. Goussac, Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human-Machine Interaction, SIPRI – Stockholm International Peace Research Institute, Stockholm, 2017.

- G. Chamayou, Teoria del drone. Principi filosofici del diritto di uccidere, DeriveApprodi, Roma, 2014.

- C. Catalano (a cura di), Evoluzione e stato dell'arte dello "SWARMING" e la sua relazione con le Multi-Domain Operations (MDOs): progressi tecnologici, ambiti di applicazione, punti di forza, vulnerabilità, opportunità, minacce, Centro Alti Studi per la Difesa (CASD) – Istituto di Ricerca e Analisi della Difesa (IRAD), 2022.

- P. Ceola, "Macchine guerriere autonome", Filosofia, LXV, Mimesis Edizioni, Milano-Udine, 2020.

- P. Ceola, C. R. Gaza, Non-human Warfare. Robot e cyborg tra postmoderno e postumano, Collana SISM, 4, Società Italiana di Storia Militare, Torino, 2013.

- G. Contissa, F. Lagioia, G. Sartor, "La Manopola Etica: I veicoli autonomi eticamente personalizzabili e il diritto", Sistemi intelligenti, 29(3), 2017.

- F. Farruggia (a cura di), Dai droni alle armi autonome. Lasciare l'Apocalisse alle macchine?, Franco Angeli, Milano, 2023.

- Francesco, Messaggio per la LVII Giornata Mondiale della Pace, 8 dicembre 2023.

- M. Galeotti, The Weaponization of Everything. A Field Guide to the New Way of War, Yale University Press, New Haven, 2023.

- M. Galeotti, "Il modello Osint in ambito militare: dinamiche di open/closed access nel trattamento dell'informazione a fini strategici", Rivista di Digital Politics, 3(2), 2023.

- E. Greco, F. Marconi, F. Maremonti, The Transformative Potential of AI and the Role of G7, Istituto Affari Internazionali (IAI), Roma, 2024.

- International Committee of the Red Cross (ICRC), Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects. CCW Expert Meeting, Geneva, 2014, https://www.icrc.org/en/document/report-icrcmeeting-autonomous-weapon-systems-26-28-march-2014.

- International Committee of the Red Cross (ICRC), Views of the International Committee of the Red Cross on Autonomous Weapon Systems, Paper submitted to the Informal Meeting of Experts on Lethal Autonomous Weapons Systems of the Convention on Certain Conventional Weapons (CCW), Geneva, 11 April 2016.

- International Committee of the Red Cross (ICRC), Position on Autonomous Weapons Systems, Geneva, 12 May 2021.

- IRIAD – Istituto di Ricerche Internazionali Archivio Disarmo, LAWS: Lethal Autonomous Weapon Systems: La questione delle armi letali autonome e le possibili azioni italiane ed europee per un accordo internazionale, IRIAD Review – Studi sulla pace e sui conflitti, 7–8, 2020.

- A. Iaria, “Da autonomi a completamente autonomi: l’applicazione dell’Intelligenza Artificiale nei sistemi d’arma autonomi (LAWS)”, Rassegna della Giustizia Militare. Rivista della Giustizia e della Procedura Penale Militare, 6, 2018.

- A. Krishnan, Killer Robots. Legality and Ethicality of Autonomous Weapons, Ashgate Publishing Limited, Farnham, 2009.

- M. Leonard, L’era della non-pace. Perché la connettività porta al conflitto, Bocconi University Press, Milano, 2023.

- Lethal Autonomous Weapons Systems, General Assembly Resolution 78/241, 13 October 2023.

- Lethal Autonomous Weapons Systems, Report of the Secretary-General of the United Nations, 1 July 2024.

- M. M. Maas, “How Viable is International Arms Control for Military Artificial Intelligence? Three Lessons from Nuclear Weapons”, Contemporary Security Policy, 40(3), 2019.

- F. Sabry, Armi autonome. In che modo l’intelligenza artificiale prenderà il sopravvento sulla corsa agli armamenti, 1BK One Billion Knowledgeable, Abu Dhabi, 2021.

- M. Sacchi, La guerra delle macchine. Hacker, droni e androidi: perché i conflitti ad alta tecnologia potrebbero essere ingannevoli e terribilmente fatali, Algama Editore, Milano, 2020.

- G. Sartor, L’intelligenza artificiale e il diritto, Giappichelli, Torino, 2022.

- H. Somerville, D. Seetharaman, “OpenAI Enters Silicon Valley’s Hot New Business: War”, The Wall Street Journal, 4 dicembre 2024, https://www.wsj.com/tech/ai/openai-enters-silicon-valleys-hot-new-business-war-7beccf6e.

- S. Pietropaoli, “Un altro modo di fare la guerra. La cyberwar come problema giuridico”, Ars interpretandi. Rivista di ermeneutica giuridica, 1/2023.

- M. Raviart, “Onu: la Santa Sede condanna l’uso di robot automatici in guerra”, Vatican News, 10 aprile 2018, https://www.vaticannews.va/it/vaticano/news/2018-04/santa-sede-onu-armi-jurkovic0.html.

- Risoluzione del Parlamento europeo sull'utilizzo di droni armati, 27 febbraio 2014 (2014/2567(RSP)).
- F. Ruschi, "Il volo del drone. Verso una guerra post-umana?", Jura Gentium, 1, 2016.
- M. Zanzucchi, "IA tra guerra e pace", Città Nuova, febbraio 2024.
- Hiroshima Process International Code of Conduct for Advanced AI Systems, Commissione Europea, Bruxelles, 2023, https://digital-strategy.ec.europa.eu/it/library/hiroshima-process-international-code-conduct-advanced-ai-systems

Atti di convegno

Il campo di battaglia "fantasma" del nuovo Leviatano digitale: guerra cibernetica, ambiguità giuridiche e ascesa della sovranità tecnologica dello Stato nel diritto internazionale

Matteo Fulgenzi
Docente - Dipartimento di Scienze Giuridiche - Università degli Studi di Verona

"The "Phantom" Battlefield of the New Digital Leviathan: Cyber Warfare, Legal Ambiguities, and the Rise of State Technological Sovereignty in International Law"

Abstract

In the 21st century, digital technologies have profoundly reshaped state power and the dynamics of interstate conflict. The rise of cyber warfare presents significant challenges to the established framework of international law, driven by rapid advancements in the field of Information and Communications Technology (ICT) and the evolution of hybrid warfare. Cyber operations, cyber-kinetic attacks, and online disinformation campaigns have become essential instruments for both state and non-state actors, enabling them to project influence and affect both the military and civilian dimensions of sovereignty. This study explores the complex legal implications posed by cyberspace as an "invisible" battleground amidst intensifying global competition. Through an analysis of international norms and jurisprudence, it highlights the inadequacies of current legal paradigms in addressing the digital transformation of warfare. The research advocates for the development and consolidation of innovative legal frameworks and interpretative standards to regulate the growing "militarization" of the digital domain, emphasizing the importance of territoriality in understanding the ontological assumptions of cyberspace—particularly in light of the evolving role of Artificial Intelligence (AI).

Keywords: Cyber Warfare - Hybrid Warfare - International Law; - State Responsibility - Due Diligence - Ius Publicum Cyberneticum (IPC)

Introduzione: la nuova frontiera informatica dei conflitti internazionali

L'alba del XXI secolo sta assistendo a un radicale mutamento della natura della guerra. Lo scontro tra gli Stati – dalle battaglie fisiche combattute su terra, mare e aria – sta prontamente accedendo al dominio digitale, dove le operazioni informatiche si dimostrano in grado di fungere sia da strategie offensive che da azioni difensive attuate dagli Stati (o da entità comunque connesse alla dimensione statuale) così come da attori non-statali. Il ricorso alle moderne tecnologie digitali – come le reti informatiche o il più ampio catalogo degli strumenti della c.d. Information and Communications Technology (ICT) oggi disponibili – per interrompere, disabilitare o distruggere le risorse rientranti nella giurisdizione di un altro Stato (tanto più se di rilevanza critica) sta producendo la trasposizione dei conflitti dal classico campo di battaglia materiale a una nuova dimensione (percettivamente) collocata nella sfera dell'intangibile: il c.d. cyberspazio. Così, mentre si assiste alla migrazione della guerra nel regno del digitale – un dominio in cui i confini di sovranità, potere e legge appaiono come confusi in una nebbia indistinta – l'idea stessa del potere dello Stato e della potenza militare posta a presidio delle sue fondamenta di effettività e indipendenza sembra scivolare in una zona d'ombra che si rivela irta di ambiguità giuridiche e carente di chiarezza definitoria[1].

La progressiva "militarizzazione" della sfera delle informazioni, nei tratti di nuova arena della conflittualità, agisce tuttavia secondo modalità che in apparenza aggirano i tradizionali vincoli fisici, rendendo il cyberspazio un terreno conteso, sferzato da iniziative palesi così come da sortite condotte nella totale segretezza[2]. Di conseguenza, la proiezione esterna del potere dello Stato emerge sempre più non solo nei termini dei tradizionali mezzi militari (soldati, armamenti, logistica etc.) ma anche in base alla crescente disponibilità di apparati e capacità cibernetiche che consentano di condurre efficacemente operazioni di spionaggio o di controllo sul flusso delle informazioni che viaggiano sulle reti di comunicazione digitale, come anche azioni di sabotaggio o distruzione mirata indirizzate alle infrastrutture nemiche (se non persino di realizzare l'eliminazione fisica degli avversari, come nel caso della nuova frontiera degli attacchi cyber-cinetici cc.dd. "ibridi"). A differenza dell'idea "convenzionale" della guerra, la c.d. cyber warfare non comporta un utilizzo finale della violenza armata da parte dello Stato o di altri attori, ma persegue l'inabilitazione o l'abbattimento delle risorse materiali del nemico – come reti o strutture adibite all'espletamento di funzioni governative (incluse quelle operanti in ambito civile o c.d. dual-use) oppure installazioni di valore militare strategico –

---

[1] Cfr.: N. Melzer, Cyberwarfare and International Law, UNIDIR, Ginevra, 2011, 3 ss.; M. Mirti, La disciplina giuridica del cyberspace: una panoramica sulle problematiche attuali e le principali linee evolutive, in Opinio Juris, 3, 2016, 1 ss.; D. Moore, Offensive Cyber Operations: Understanding Intangible Warfare, Londra, 2022.

[2] Cfr.: W. J. Lynn III, Defending a new domain: The Pentagon's cyber strategy, in 89 Foreign Affairs 97, 98-101 (2010); L. Martino, La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale, in Politica & Società, 1, 2018, 61-76; H. Kissinger, Ordine mondiale (trad. it.), Milano, 2023.

attraverso la violazione e la manipolazione dei sistemi digitali fondati sul flusso di dati[3].

Alla luce di una simile rivoluzione nella definizione degli equilibri di potenza sullo scacchiere geopolitico, l'atavico concetto di Leviatano – simbolo ultimo dell'autorità sovrana e dell'indiscussa supremazia del potere costituito[4] – non può dunque che acquisire rinnovata rilevanza nel dominio del cyberspazio, dove gli Stati concentrano sempre più i propri sforzi politici, economici e tecnologici allo scopo di rivendicare e mantenere il controllo sugli scambi di dati e sui "nodi sinaptici" in cui si struttura il funzionamento planetario di quel "sistema nervoso" artificiale oggi costituito dalle reti mondiali di comunicazione digitale. Muovendo da tali presupposti, il cyberspazio si manifesta nelle vesti di una dimensione (apparentemente) "eterica" dell'esistenza, idonea a fungere da estensione astratta del reale in cui combattere "guerre invisibili" e dove i classici strumenti di preparazione e conduzione dello scontro bellico sono sostituiti da loro simulacri sottili, tradotti in sequenze di dati e informazioni atte a sostanziare il conflitto di nomoi concorrenti. Ogni potenza, nel proprio afflato di influenza sul cyberspazio, cerca infatti di modellare il mondo digitale secondo la propria immagine ideologica, i propri principi giuridici e l'impostazione dei propri interessi (a partire dalle inerenti valutazioni circa la stessa opportunità di formalizzare o meno la presenza sovrana dello Stato nello spazio informatico).

L'ascesa del "Leviatano digitale" rappresenta dunque una nuova concezione della sovranità statuale, che sembra estendersi oltre gli elementi fisici del territorio e assimilare la proiezione digitale del potere dello Stato e delle entità ad esso sottoposte fino a fagocitare tutti gli spazi virtuali dove si svolge la moderna vita sociale ed economica delle diverse nazioni del globo. In un'epoca in cui le piattaforme digitali (i cc.dd. social) plasmano le dinamiche del discorso politico, delle interazioni sociali e delle transazioni economiche, l'affermazione del controllo sul cyberspazio è divenuta una caratteristica distintiva della nuova sovranità digitale, rivolta a sublimare l'accezione geografica del potere nel senso dell'ascesa dell'autorità informatica dello Stato e della configurazione di un cyber-Grossraum quale sfera di influenza cibernetica "allargata" in cui gli Stati agiscono producendo effetti anche al di là dei confini della loro potestà territoriale[5]. Nel regno senza peso degli algoritmi, la "volontà di potenza"[6] dello Stato non si percepisce circoscritta da limitazioni fisiche. Nel microcosmo dell'ICT, esso pretende di trovare un campo d'azione astratto dove dare forma al proprio afflato

---

[3] Sul tema, cfr.: L. Tabansky, Basic Concepts in Cyber Warfare, in 3 Military and Strategic Affairs 75 (2011); P. A. L. Ducheine, P. B. M. J. Pijpers, The Notion of Cyberspace, in N. Tsagourias, R. Buchan (Eds), Research Handbook on International Law and Cyberspace, Cheltenham, II ed., 2021, 272-296; C. Ashraf, Defining cyberwar, in 37 Def. Secur. Analysis 274 (2021).

[4] T. Hobbes, Leviathan, or the Matter, Forme, and Power of a Commonwealth Ecclesiasticall and Civil, 1651.

[5] Sul tema, cfr. C. Schmitt, Der Nomos der Erde im Völkerrecht des Jus Publicum Europaeum, 1950, dove il concetto di Diritto Pubblico Europeo definisce un sistema giuridico condiviso per la stabilizzazione, in chiave "westfaliana", delle relazioni interstatali in Europa, riconoscendo gli equilibri di potere e creando regole per i conflitti in funzione della pace.

[6] Cfr.: F. W. Nietzsche, Also sprach Zarathustra, 1883-1885; Jenseits von Gut und Böse, 1886; Der Wille zur Macht, 1901.

di egemonia assoluta, manifestandone tacitamente il frutto fatale, senza attrito né opposizione apparente. Attraverso le operazioni informatiche, gli Stati non hanno bisogno di occupare materialmente un territorio per esercitarvi il controllo; piuttosto, vi proiettano in maniera indiretta la propria influenza, raggiungendo obiettivi di primario valore strategico tramite l'alterazione di sistemi, l'interruzione di infrastrutture, la silenziosa supervisione dei flussi di informazioni e la manipolazione della pubblica opinione per mezzo delle campagne di c.d. "disinformazione". In questi termini, a differenza delle tradizionali dimostrazioni di potenza militare, il potere informatico opera come un esercizio di forza "invisibile" e, dietro lo scorrere impercettibile dei dati, il comando non parla: si compie.

Nel panorama volatile e in evoluzione della cyber warfare, lo scontro tra spazialità rivali si eleva nella contesa del predominio su un nuovo piano di concezione del potere, dove la tangibilità del dato fisico trasmuta nell'effigie digitale di sequenze alfanumeriche e sfugge a definizioni statiche, sfidando non solo il diritto internazionale e le cc.dd. leggi di guerra ma anche la stessa concezione della potestà dello Stato[7]. In tale prospettiva, il cyberspazio si pone allora come il non-luogo di una diversa "trama demiurgica", di una "matrice ordinatoria di significato" (Gestell)[8] rivelatrice della paradossale declinazione del mondo secondo i canoni (valoriali, estetici, etc.) sottesi allo spirito prometeico della moderna tecnologia ICT e alla promessa di una dimensione "altra" delle interazioni, del sapere e della stessa esistenza, perseguita presentando dati, identità e relazioni umane come mere risorse quantificabili, ridotte in un ordine calcolabile, prevedibile e riproducibile di informazioni plasmato "a immagine e somiglianza" dei software predisposti ad animare la capacità di elaborazione delle infrastrutture fisiche in cui la "contrazione digitale" della realtà materiale conferisce forma al doppione cibernetico di quest'ultima, creando un nuovo "vuoto" atto ad accogliere inusitati orizzonti di arbitrio[9]. La tecnologia diventa quindi uno strumento tanto di espansione quanto di deterrenza, che consente a chi ne detiene le redini di influenzare la politica globale e di indebolire i propri avversari senza sostenere i rischi di un conflitto aperto. La capacità di direzionare, controllare e alterare i flussi di informazioni sulla rete globale può d'altronde conferire agli Stati un formidabile vantaggio nella definizione degli equilibri mondiali della forza, imponendosi quale strumento complementare – se non ancora propriamente sostitutivo – rispetto ai consueti apparati militari.

---

[7] Sul tema, cfr.: M. Ferruglio, Cyber operation e responsabilità internazionale degli Stati: uno sguardo d'insieme, in P. Ivaldi, S. Carrea (Eds), Spazio cibernetico: rapporti giuridici pubblici e privati nella dimensione nazionale e trans-frontaliera, Genova, 2018, 91 ss.; N. Tsagourias, The legal status of cyberspace, in N. Tsagourias, R. Buchan, op. cit., 13-29; C. Antonopoulos, State Responsibility in Cyberspace, ivi, 113-129. Inoltre: C. C. Joyner, C. Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, in 12 EJIL 825, 842-845 (2001); R. Buchan, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions, in 17 J.C.& S.L 211, 211-227 (2012).

[8] M. Heiddeger, Die Frage nach der Technik (1954), in Vorträge und Aufsätze, Pfullingen, 1957.

[9] Suggestione ispirata ai costrutti ("concentrazione", "vuoto" e, come si vedrà nel prosieguo, "frammentazione") elaborati dalla Cabala luriana (XVI sec.). Cfr. G. Israel, La Kabbalah, Bologna, 2005.

L'essenza evasiva e la virtualità dello strumento informatico mutano infatti profondamente la percezione del limes territoriale quale limite dell'esercizio della sovranità degli Stati, riproponendo problematicità nella demarcazione dei confini quali delimitazione dello spazio di effettività del potere pubblico che si supponevano definitivamente superate con la consacrazione westfaliana dello Stato-nazione[10]. La guerra cibernetica si impone allora come un'idea in contrasto con qualsiasi definizione semplicistica e assurge a frutto ferale della moderna "magia" dell'ICT che permette a soggetti statali e non-statali di condurre operazioni elusive ma, allo stesso tempo, capaci di compromettere i sistemi di governance o addirittura la tenuta del tessuto sociale di un altro Stato, avvalendosi dello schermo evanescente della rete. Questa nuova forma di conflitto, dove silenti stringhe di codice subentrano al fragore scomposto di bombe e cannoni, non può dunque che segnare un sostanziale allontanamento dalla guerra tradizionale. Le capacità informatiche degli Stati, del resto, rappresentano oggi risorse cruciali più o meno allo stesso livello delle classiche dotazioni militari, inserendosi nel quadro di una strategia di dissimulazione in cui lo Stato può agevolmente nascondere il perseguimento di obiettivi militari sotto le vesti di operazioni civili. La "negazione plausibile" di ogni responsabilità ai sensi del diritto internazionale vigente diviene pertanto un segno distintivo della cyber warfare come nuova dimensione del caos dominata dalla forza tecnologica sottratta a qualunque regola[11].

Il carattere sfuggente e anonimo dell'incantesimo tecnologico della sfera ICT non può quindi che acquisire sempre maggiore centralità nella proiezione dello Stato a livello regionale e globale. Ad ogni modo, ciò che può essere percepito come puramente "etereo" e frutto dell'intervento di forze "invisibili" è, in verità, anche un dominio in cui opera materialmente la tecnica, nelle forme della localizzabile fisicità tanto delle macchine più sofisticate quanto dei più banali grovigli di cavi, prese e interruttori. Il cyberspazio si pone di conseguenza come uno spazio liminale tra pensiero e materia, nel quale il moderno Principe[12] individua una zona crepuscolare tra pace e conflitto dove, ancora una volta, poter "continuare la politica con altri mezzi"[13]. Alla pretesa virtualità degli strumenti "penta-dimensionali" che imperversano nello spazio informatico,

---

[10] Cfr. CPA, Island of Palmas case (Netherlands v U.S.A.), Award, 4 Aprile 1928, in RIAA, II, 1949, 829-871, 838. Sul tema, cfr. I. N. Nigro, Problemi applicativi alla luce del diritto internazionale nel contesto delle cyber operations, in Ann. Dip. Giur. Univ. Molise, 24, 2023, 433-447, 435 ss. Si veda: I. Forgione, Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna, in R. Ursi (Ed.), La sicurezza nel Cyberspazio, collana «Scritti di Diritto Pubblico», Milano, 2023. Cfr. L. Kello, Cyber Security: Gridlock and Innovation, in D. Held, T. Hale (Eds), Beyond Gridlock, Cambridge, 2017, 205-228. Sulla base di tali premesse, dunque, la dimensione cyberspaziale si porrebbe oggi anche come ulteriore orizzonte della c.d. "de-territorializzazione" della sovranità dallo Stato, corroborando il percorso tracciato dalle architetture neoliberali per cui il potere decisionale è trasferito a meccanismi transnazionali di governance reticolare, controllati da attori (in questo caso, digitali) globali. Cfr.: A.-M. Slaughter, A New World Order, Princeton, 2004; W. Davies, The Limits of Neoliberalism: Authority, Sovereignty and the Logic of Competition, Londra, 2014.

[11] Cfr. J. Brown, T. Fazal, Why states neither confirm nor deny responsibility for cyber operations, in 6 EJIS 401 (2021).

[12] N. Machiavelli, Il Principe, 1513 (pubblicato nel 1532).

[13] C. von Clausewitz, Vom Kriege, 1832.

tuttavia possono corrispondere effetti reali, brutali e devastanti, al pari di quelli prodotti dai mezzi della classica guerra cinetica capaci di sferzare la terra, il mare, l'aria e persino lo spazio extra-atmosferico. In questo campo di battaglia dalla materialità sottile – né pienamente tangibile, né interamente astratto – in cui i confini sono porosi, le intenzioni velate e i concetti fondati sulla concretezza geografica del territorio faticano a contenere le mosse ostili (tanto più se impercettibili nell'immediatezza e, soltanto a posteriori, palesi in tutte le loro implicazioni), l'attuale quadro giuridico internazionale è trascinato in un certame senza precedenti.

La guerra informatica sfida infatti principi fondamentali del diritto internazionale come la sovranità, il diritto di autodifesa e il divieto di uso unilaterale della forza (armata), poiché gli attacchi informatici possono essere lanciati da qualsiasi luogo fisico e dirigersi verso l'infrastruttura bersaglio attraverso le più disparate distanze[14]. Sebbene le posizioni della più affermata dottrina tendano, oggi, a classificare come internazionalmente illeciti gli attacchi perpetrati attraverso il cyberspazio che si dimostrino nei fatti comparabili, per entità e conseguenze, alle azioni di guerra cinetica lanciate contro l'integrità e l'indipendenza di uno Stato sovrano o in qualsivoglia modo incompatibili con lo Statuto delle Nazioni Unite[15], gli stessi studiosi riconoscono le difficoltà intrinseche al tentativo di inscrivere il regime giuridico delle operazioni informatiche – quand'anche, per definizione, provochino lesioni o la morte di persone, oppure danni o la distruzione di beni materiali[16] – nel quadro internazionalistico pre-digitale, attingendo ai principi consolidati e alle norme convenzionali del diritto internazionale. La crisi russo-ucraina e la rivalità tecnologica tra Cina e Stati Uniti forniscono vividi esempi di come il cyberspazio sia diventato il nuovo terreno di scontro della geopolitica globale. Fin dagli esordi della guerra nel Donbass nel 2014 – così come nel contesto della crisi russo-georgiana del 2008, con l'intervento militare del Cremlino nel territorio dell'Ossezia del Sud[17] – sono stati imputati alla Russia numerosi attacchi informatici indirizzati a minare il funzionamento di infrastrutture di rilevanza vitale (soprattutto per il ramo energetico)

---

[14] Al riguardo, cfr. C. Focarelli, Self-Defense in Cyberspace, in N. Tsagourias, R. Buchan, op. cit., 317-344.

[15] Cfr. M. Roscini, Cyber operations as a Use of Force, ivi, 297-316; M. N. Schmitt, L. Vihul (Eds), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, NATO CCDCOE, Tallinn, 2017, Rule 5, Rules 68-70, Rule 80.

[16] Cfr. ivi, Rules 71-72, Rules 91-94, Rule 99, Rules 104-121 (in riferimento all'applicazione del c.d. diritto di guerra). Giova già qui richiamare che, ai sensi degli artt. 2-3 comuni alle Convenzioni di Ginevra del 1949, le previsioni del diritto umanitario trovano applicazione nel contesto dello svolgimento di situazioni identificabili alla stregua di conflitti armati, di carattere internazionale o non-internazionale.

[17] Analoga matrice "russa" è stata attribuita agli attacchi subiti dall'Estonia nel 2007, che hanno disabilitato infrastrutture governative e finanziarie critiche ma non hanno prodotto danni fisici né causato vittime dirette. Sull'argomento, cfr. C. Czosseck, R. Ottis, A.-M. Talihärm, Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security, in 1 IJCWT 24 (2011).

dell'Ucraina[18] nonché a manipolare i flussi delle informazioni in rete a vantaggio di Mosca allo scopo di influenzare la narrazione che circonda le dinamiche del conflitto, animando così l'ulteriore accusa – poi mossa nei confronti della Federazione Russa in concomitanza con gli esiti delle elezioni americane del 2016[19] – di ostacolare il libero svolgimento dei processi elettorali di altri Stati[20]. Analogamente, l'ascesa del potere cibernetico di Pechino, caratterizzata dai grandi progressi segnati nel campo dello spionaggio informatico e nello sviluppo di sistemi avanzati di intelligenza artificiale (IA), contende apertamente il predominio degli USA[21], trascinando nell'agone della competizione globale anche altri importanti attori internazionali, come l'Unione europea (UE), con quest'ultima strenuamente impegnata nello sforzo di inscrivere la condotta degli attori cyberspaziali nel prisma del diritto internazionale[22], nonché di una concezione della cyber-sicurezza fortemente incentrata sulla tutela dei dati personali[23] e sull'acceso

---

[18] Tra questi, l'attacco NotPetya del 2017 (ransomware) aveva inizialmente come obiettivo l'infrastruttura ucraina ma si è rapidamente diffuso in tutto il mondo, colpendo multinazionali e agenzie governative, a dimostrazione della difficoltà di controllare le conseguenze di un'operazione informatica. Si considerino anche le operazioni cibernetiche condotte da gruppi filo-russi come Sandworm e Killnet, dirette contro infrastrutture critiche ucraine sullo sfondo della deflagrazione del conflitto russo-ucraino a partire dal 2022. Cfr.: M. Baezner, Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict, CSS, Zurigo, 2018; S. Duguin, P. Pavlova, The role of cyber in the Russian war against Ukraine, PE 702.594 (2023); M. C. Vitucci, Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo-ucraino, in La Comunità Internazionale, 1 (2023), 7-32. È opportuno sottolineare come la definizione di "guerra ibrida" tenda sempre più a designare l'estrema flessibilità di una strategia militare capace di integrare tattiche convenzionali e non-convenzionali con operazioni cibernetiche di attacco, sabotaggio o interferenza su più livelli. Cfr.: C. Sbailò, Guerre ibride: quali risposte possibili?, in DPCE online, 63, SP-1 (2024), 437-446; A. Spaziani, L'attacco cibernetico nell'era della guerra ibrida, ivi, 511-536.

[19] Cfr. A. Bonfanti, Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale, in Riv. Dir. Int., 102, 2019, 694-728.

[20] Cfr.: art. 21 UDHR; art. 25 ICCPR; art. 3, Prot. n. 1 CEDU. Inoltre, cfr.: art. 10 TUE; art. 23 CADH; art. 13 CADHP.

[21] Sul tema, cfr. S. Mele, Le attività di spionaggio elettronico e di cyber warfare della Cina, in U. Gori, L. Martino (Eds), Intelligence e interesse nazionale, Roma, 2015, 223-236.

[22] Cfr. Commissione, Comunicazione congiunta al Parlamento europeo e al Consiglio, La politica di ciberdifesa dell'UE, JOIN(2022) 49 final, 10 novembre 2022; Consiglio dell'UE, Declaration on a Common Understanding of International Law in Cyberspace (15833/24), 18 novembre 2024, 3.

[23] In merito, cfr.: art. 2 TUE; art. 16 TFUE; art. 8 EUCFR. Nel diritto derivato, cfr. Direttiva 2002/58/EC; Regolamento (EU) 2016/679 (GDPR); Direttiva (EU) 2016/680; Regolamento (EU) 2018/1725. In riferimento al contributo della Corte di Lussemburgo, si vedano: CGUE, Sentenza della Corte (Grande Sezione) del 13 maggio 2014, C-131/12, Google Spain SL e Google Inc. c. AEPD (EU:C:2014:317); CGUE, Sentenza della Corte (Grande Sezione) del 6 ottobre 2015, C-362/14, Maximillian Schrems c. Data Protection Commissioner (c.d. Schrems I – EU:C:2015:650); CGUE, Sentenza della Corte (Grande Sezione) del 16 luglio 2020, C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd. e Maximillian Schrems (c.d. Schrems II – EU:C:2020:559). Inoltre: CGUE, Sentenza della Corte (Prima Sezione) del 12 gennaio 2023, C-154/21 (EU:C:2023:3); CGUE, Sentenza della Corte (Terza Sezione) 14 dicembre 2023, C-340/21 (EU:C:2023:986). Nel quadro del Consiglio d'Europa, si veda in analoga prospettiva la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (ETS n. 108, 1981, in vigore dal 1985), così come sarà emendata ("Convenzione 108+") – al momento della sua entrata

contrasto al cybercrime e ad ogni utilizzo illecito della rete (in specie a danno delle cc.dd. infrastrutture critiche)[24]. Riflettendo sulla prassi degli Stati, sulla giurisprudenza internazionale e sul contributo offerto dall'accademia, questo studio indagherà le riforme necessarie per un'efficace regolamentazione della cyber warfare nel diritto internazionale ed evidenzierà alcuni elementi utili a sollevare il "velo di Maya"[25] che sembra opporsi alla piena comprensione del sostrato materiale sotteso all'esistenza dello spazio cibernetico, sancendone la pretesa vocazione al caos in quanto dominio di per sé insuscettibile di regolazione. In primo luogo, apparirà chiaro come lo stesso concetto di sovranità debba evolversi per includere la complessa realtà dell'infrastruttura digitale. Grandi potenze, come la Cina e la Russia, hanno già affermato la propria sovranità sulla sfera del digitale, implementando rigidi controlli sulle strutture della rete Internet e sui flussi di dati all'interno dei loro confini[26]. Questo, mentre gli Stati occidentali si soffermano sull'importanza di un Internet libero e aperto, da tenere tuttavia al riparo da fenomeni di manipolazione delle informazioni (le cc.dd. fake news)[27].

---

in vigore – dal Protocollo di Strasburgo (CETS n. 223, 2018), che affronta i problemi posti al rispetto della vita privata dall'uso delle nuove tecnologie ICT e rafforza il meccanismo di contrasto ad abusi e illeciti nel trattamento automatizzato dei dati personali, includendo – salvo giustificate deroghe previste per via legislativa (ex art. 11 del testo consolidato) – i settori della sicurezza nazionale e della difesa delle Parti aderenti (e ciò a differenza dell'EU-GDPR, come esplicitato dal considerando 16 del Reg. UE 2016/679). Suggestivo, in tale contesto, può rivelarsi il richiamo al concetto di "capitalismo della sorveglianza", secondo cui il potere si esercita ben oltre i confini statali e la stessa "sovranità" è ridefinita attraverso il controllo dei dati personali. Cfr. S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York, 2019.

[24] Cfr.: Direttiva 2008/114/CE del Consiglio dell'UE, 8 dicembre 2008; Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, 14 dicembre 2022. Si vedano: N. De Scalzi, L. Gudas, L. Martino, Guerra dal cyberspazio. La difesa delle reti infrastrutturali critiche dalla minaccia cibernetica, in U. Gori, L. Martino, op. cit., 181-222. Si veda, altresì: Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, 12 agosto 2013. Cfr.: K. Ambos, International Criminal Responsibility in Cyberspace, in N. Tsagourias, R. Buchan, op. cit., 152-181; Inoltre: R. A. Wessel, European Law and Cyberspace, in N. Tsagourias, R. Buchan, op. cit., 491-508. È interessante ricordare che il primo storico caso di utilizzo criminale della rete delle telecomunicazioni avvenne nel 1834, quando una coppia di ladri violò il sistema telegrafico francese per sottrarre denaro. Cfr. L. M. Cherry, P. P. Pascucci, International Law in Cyberspace, in American. Bar Ass'n J. (2023).

[25] Cfr. A. Schopenhauer, Die Welt als Wille und Vorstellung, 1859.

[26] Il Great Firewall cinese è un esempio di come lo Stato eserciti il controllo sui flussi di informazioni, regolando l'accesso alle reti globali e l'uso domestico di Internet (significativa, al riguardo, la disputa Google-China del 2010). Il progetto di Internet sovrano della Russia ha invece mirato a strutturare una rete Internet nazionale che possa essere isolata dal web globale, agevolando la gestione dei conflitti informatici e favorendo un approccio resiliente dinanzi all'imposizione di sanzioni internazionali. Cfr.: S. Sayapin, Russian Approaches to International Law and Cyberspace, in N. Tsagourias, R. Buchan, op. cit., 525-546; Z. Huang, Y. Ying, Chinese Approaches to Cyberspace Governance and International Law in Cyberspace, ivi, 547-562.

[27] Cfr.: Commissione europea, 2022 Strengthened Code of Practice on Disinformation, 16 giugno 2022; Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, 19 ottobre 2022 (Digital Services Act – DSA), tramite cui si configurano obblighi di trasparenza per le piattaforme online, con l'obiettivo di prevenire attività illegali o dannose (come le cc.dd. manipolazioni algoritmiche) e, in particolare, si mira a combattere le pratiche di disinformazione (avvalendosi dei cc.dd. fact-checkers). Il 13 febbraio 2025, la Commissione e il Comitato europeo per i servizi digitali hanno approvato l'integrazione ufficiale

Tenendo anche conto di come i giganti privati della tecnologia controllino enormi porzioni dei flussi globali di informazioni nonché partizioni significative del cyberspazio – spesso stabilendo "zone di influenza" in coordinamento o per conto dei propri governi – emergerà chiaramente come il cyberspazio manifesti la tendenza a seguire il destino a suo tempo affrontato dall'orbe terracqueo, ossia quello di "frammentarsi" in zone di controllo nazionalizzate in base alle capacità degli Stati di far valere le proprie istanze di sicurezza informatica e di imporre conseguenti restrizioni sui flussi di dati che interessino la loro giurisdizione. Nella cornice di un approccio interdisciplinare, la ricerca mirerà a fornire una comprensione completa di come l'orizzonte della cyber warfare richieda un nuovo modo di pensare il potere dello Stato – così come la responsabilità internazionale di quest'ultimo – in un mondo digitale sempre più interconnesso. Intrecciando teoria giuridica, visioni della geopolitica e intuizioni filosofiche, l'analisi cercherà di decifrare il cammino, ancora irto di ostacoli, attraverso cui la comunità internazionale potrà affrontare le minacce poste dalla dimensione informatica del conflitto, articolando gli scenari di complessità necessari a reimmaginare i principi giuridici utili per governare questo sfuggente teatro della fervida contesa per la supremazia mondiale. Sul piano metodologico, si provvederà pertanto a sistematizzare i risultati dell'analisi dottrinale in rapporto alla disamina comparativa di strumenti chiave del quadro giuridico internazionale, corroborando i risultati ottenuti con i riscontri empirici mutuati da rilevanti casi di studio nonché da un'esplorazione delle profonde implicazioni legate all'avvento del cyberspazio come nuovo orizzonte di sublimazione dello scontro tra spazialità terrestri concorrenti.

1. Il quadro giuridico internazionale alla prova della dimensione cibernetica del conflitto

Le Nazioni Unite, attraverso iniziative come il lavoro del Gruppo di esperti governativi sulla sicurezza informatica[28], cercano da tempo di individuare regole di indirizzo idonee a promuovere una condotta responsabile da parte degli attori del cyberspazio. L'Assemblea Generale dell'ONU, del resto, si è dimostrata particolarmente attiva nel perorare la causa della sicurezza globale correlata alla sfera dell'ICT, insistendo nella progettualità condivisa di: «continuare, in via prioritaria, a sviluppare ulteriormente le regole, le norme e i principi di comportamento responsabile degli Stati e le modalità per la loro attuazione e, se necessario, apportare modifiche o elaborare ulteriori regole di condotta; prendere in considerazione le iniziative statali volte a garantire la sicurezza nell'uso delle tecnologie dell'informazione e della comunicazione; stabilire, sotto

---

del Codice di buone pratiche volontario come Code of Conduct nel quadro del DSA, con effetto a decorrere dal 1° luglio 2025 (su richiesta degli stessi VLOPs e VLOSEs firmatari). Sul tema: M. Hellman, C. Wagnsson, How can European states respond to Russian information warfare? An analytical framework, in 26 European Security 1 (2017); A. Strongwater, Combating Disinformation through International Law, in 55 Int'l Law and Politics 33 (2023).

[1] United Nations Group of Governmental Expert on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), ReportA/70/174, 22 luglio 2015. Si vedano: UNGA, A/RES/58/32; A/RES/68/243; A/RES/73/266; A/RES/75/240. Inoltre: Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 luglio 2021.

gli auspici delle Nazioni Unite, un dialogo istituzionale regolare con un'ampia partecipazione degli Stati; continuare a studiare, al fine di promuovere intese comuni, le minacce esistenti e potenziali nel campo della sicurezza informatica – tra cui la sicurezza dei dati e le possibili misure di cooperazione atte a prevenire e contrastare tali minacce – e il modo in cui il diritto internazionale si applica all'uso delle tecnologie dell'informazione e della comunicazione da parte degli Stati, nonché le [possibili] misure di rafforzamento della fiducia [tra gli Stati] e di miglioramento delle capacità [di gestione del dominio informatico]»[29]. Tutti questi sforzi enfatizzano i valori unitari della trasparenza e della cooperazione internazionale in funzione della prevenzione dei conflitti, conservando le fattezze di disegni ambiziosi ancorché privi di forza esecutiva[30]. L'attivo coinvolgimento di organi delle Nazioni Unite non manca di riflettere il crescente riconoscimento del ruolo essenziale della sicurezza del cyberspazio nel mantenimento della stabilità internazionale, sebbene rimangano ancora considerevoli le difficoltà che si frappongono alla stesura di accordi vincolanti in un dominio a "controllo diffuso" come quello cibernetico[31]. Le organizzazioni internazionali come l'ONU, con le sue agenzie specializzate – tra cui l'Unione internazionale delle telecomunicazioni (ITU), deputata alla supervisione degli standard globali delle telecomunicazioni – svolgono un ruolo cruciale nel dare forma ad una regolamentazione planetaria del cyberspazio e i loro tentativi, per quanto finora frammentari, non potranno che dimostrarsi utili nella prospettiva del consolidamento di un approccio unificato al tema della governance informatica mondiale, aiutando a mitigare i rischi correlati ai conflitti cibernetici e, in prospettiva, a creare vere e proprie norme internazionali obbligatorie per la comunità degli Stati. Nel novero degli esempi di coordinamento attuati in funzione della futuribile disciplina unitaria dello spazio informatico rientra anche l'operato dell'Internet Corporation for Assigned Names and Numbers (ICANN) che presiede il sistema di attribuzione e gestione dei nomi di dominio attivati sulla rete Internet globale. Questi organismi, pur nella varietà delle loro attribuzioni costitutive, fungono da forze di contenimento del caos cibernetico, tentando di stabilire un ordine condiviso per mezzo degli strumenti della cooperazione internazionale e contribuendo, in tal modo, a prevenire l'insorgere e l'aggravarsi delle divergenze tra "potenze del digitale" che possano altrimenti sfociare in attacchi informatici contro beni pubblici e infrastrutture critiche[32].

---

[29] UN Open-ended Working Group on the Security and Use of Information and Communications Technologies (OEWG), Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (A/77/275, 8 agosto 2022), 6, § 3. Cfr. UNGA, A/RES/75/240, 31 dicembre 2020.

[30] Si vedano, in ampia prospettiva, anche le risoluzioni dell'Assemblea Generale dell'ONU: A/RES/55/63; A/RES/56/121; A/RES/57/239; A/RES/58/199; A/RES/64/211; A/RES/66/24; A/RES/70/237. Inoltre, cfr. A/RES/79/1, 12, § 33.

[31] Sul tema, cfr. I. Chiarugi, N. De Scalzi, L. Martino, M. Mayer, La politica internazionale nell'era digitale. Dispersione o concentrazione del potere?, in U. Gori, L. Martino, op. cit., 63-132. Si veda anche: The Pact for the Future (UNGA, A/RES/79/1, 22 settembre 2024), 11, International Peace and Security.

[32] Cfr.: O. Gross, Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents, in 48 Cornell Int'l L. J. 481, 506 (2015); A. Klimburg, The Darkening Web: The War for Cyberspace, Londra, 2017.

1.1 La Carta dell'ONU e le norme sui conflitti armati nell'era della guerra digitale

La Carta delle Nazioni Unite è la pietra angolare del diritto internazionale che disciplina l'uso della forza ma – al netto di affermazioni di principio – la sua applicazione alla guerra informatica presenta ancora tratti fortemente controversi. I fondamenti giuridici che stabiliscono il divieto dell'uso della forza nel diritto internazionale affondano infatti le loro radici in un mondo permeato dall'accezione "convenzionale" e cinetica del conflitto tra Stati. L'art. 2.4 della Carta del 1945 proibisce agli Stati il ricorso all'uso unilaterale della forza contro l'integrità e l'indipendenza di qualsiasi altro Stato mentre il successivo art. 51 della Carta riconosce a ciascuno Stato il diritto di ricorrere all'autodifesa laddove subisca un attacco armato. L'Assemblea Generale dell'ONU, nel 1974, è altresì intervenuta a tipizzare le diverse fattispecie in cui può sostanziarsi l'uso della forza armata da parte di uno Stato in violazione della Carta, individuando tali condotte come evidenze prima facie di un'aggressione internazionale intesa come crimine internazionale contro la pace[33]. Dalla collocazione temporale di tali pietre miliari dell'architettura internazionalistica – ben anteriore all'avvento dell'era dell'ICT – sovviene tuttavia la problematicità della loro formale applicabilità al contesto della cyber warfare e ciò a partire dalla cruciale azionabilità delle previsioni di cui al Capitolo VII della Carta in risposta alle minacce alla pace e agli atti di aggressione, con l'inerente coinvolgimento del Consiglio di Sicurezza nel ruolo di supremo garante per il mantenimento e il ripristino della pace e della sicurezza internazionale in virtù del combinato disposto degli artt. 24, 25 e 39 ss. della Carta.

Partendo dalla necessaria constatazione di come, nell'ambito del diritto internazionale, resti ancora animatamente dibattuta la definizione di cosa integri o meno la nozione di "uso della forza" nelle relazioni interstatali in violazione della Carta dell'ONU[34], nel contesto della cyber warfare ci si può interrogare su

---

[33] UNGA, Risoluzione 3314 (XXIX), Definition of Aggression, 14 dicembre 1974, artt. 2 e 5. Si tenga presente, a titolo esemplificativo, come la NATO abbia chiarito che un grave attacco informatico, o il significativo impatto cumulativo di più attività informatiche dannose, potrebbe causare l'invocazione – ad opera di uno Stato membro dell'Alleanza – della clausola di difesa collettiva di cui all'art. 5 del Trattato del Nord Atlantico (1949), come confermato in: North Atlantic Council, Brussels Summit Communiqué, Bruxelles, 14 giugno 2021, §§ 31-32. In ottica analoga, nell'ambito dell'UE, si legga il quadro tracciato dall'art. 42.7 TUE (clausola di assistenza reciproca) e dall'art. 222 TFUE (clausola di solidarietà). Cfr. A. Bendiek, The EU as a Force for Peace in International Cyber Diplomacy, in SWP Comment, 19, 2018, 2.

[34] Si pensi, in merito, alla prospettiva della configurazione di un divieto dell'uso della forza economica, sulla base della strenua condanna – portata avanti dalle molteplici realtà del c.d. Global South (oggi maggioranza in seno all'UNGA) e riaffermata nel contesto della crescente influenza di piattaforme emergenti come i BRICS – delle pratiche di coercizione economica unilaterale, al contrario ampiamente recepite nella prassi dei paesi occidentali. Si veda, sul punto, il copioso filone di risoluzioni con cui l'Assemblea Generale dell'ONU si è ripetutamente pronunciata contro l'utilizzo unilaterale di strumenti di coercizione politica ed economica atti a interferire nello spazio di sovranità di Stati indipendenti. Inoltre, cfr. The Declaration on the Prohibition of Military, Political or Economic Coercion in the Conclusion of Treaties, allegata alla Convenzione di Vienna sul diritto dei trattati del 1969, quale strumento non-vincolante collegato al suo art. 52.

come, ad esempio, un'operazione informatica che disabiliti irreversibilmente il funzionamento di una determinata infrastruttura adibita alla produzione e distribuzione di elettricità – producendo, oltretutto, pesanti effetti collaterali a cascata su tutte le utenze (basi militari ma anche scuole e ospedali) servite dall'infrastruttura colpita – possa essere differenziata, tanto a livello logico quanto pratico, da un attacco mirato condotto utilizzando missili o moderni droni[35]. Se da una parte può essere concepita l'assimilazione di tale evento (e dei suoi effetti sul piano fisico) ad un attacco militare tradizionale perpetrato per mezzo di armi dal massimo effetto distruttivo – valutandone, quali parametri di riferimento: la gravità, l'immediatezza, la precisione, l'invasività, la misurabilità degli effetti, il carattere militare, il coinvolgimento di Stati stranieri e, in generale, la presunzione della loro legittimità internazionale – diventa d'altro canto lecito chiedersi se questa constatazione risulti di per sé sufficiente al fine di determinare la sussunzione di tale condotta nella disciplina dell'uso della forza ai sensi del diritto internazionale. In particolare, diviene dirimente determinare se a un'azione di matrice cibernetica – idonea a distruggere asset di valore strategico in modo analogo a un attacco armato "convenzionale" – possa legittimamente giustificare (seppure in via di extrema ratio) una risposta militare da parte dello Stato vittima dell'operazione informatica, a titolo di autodifesa[36].

Nel contesto della guerra cibernetica, il diritto internazionale si ritrova quindi impegnato in un ampio processo di ripensamento, incentrato sul complesso tentativo di conciliare le nuove realtà del conflitto con le norme giuridiche vigenti[37]. La Carta dell'ONU e le Convenzioni di Ginevra[38], poste rispettivamente alla base della disciplina dell'uso della forza (ius ad bellum) e del diritto dei conflitti armati (ius in bello), sono state concepite in riferimento ad azioni militari di natura cinetica – come assalti con mezzi corazzati,

---

[35] Al riguardo, cfr. R. A. Clarke, R. K. Knake, Cyber War: The Next threat to National Security and What to Do About It, New York, 2012. Inoltre, si veda: N. Ronzitti, Diritto internazionale dei conflitti armati, Torino, 2022, 23 ss.

[36] Cfr.: M. N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, in 37 CJTL 885, 914-915 (1999); A. Papanastasiou, Application of International Law in Cyber Warfare Operations, 2010, 14; H. Kuru, Prohibition of Use of Force and Cyber Operations as 'Force', in 2 JOLTIDA 46 (2017); H. Samuli, Cyber Attacks and International Law on the Use of Force, Abingdon, 2018, cap. 4.

[37] Cfr.: H. Lahmann, On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace, in 32 DJCIL 61 (2021), che traccia una definizione di cyber sovereignty partendo dalla contrapposizione tra il cyber imperialism anglosassone e la cyber-Westphalia rappresentata da Russia e Cina (con altri membri BRICS). Inoltre, cfr.: M. Foulon, G. Meibauer, How cyberspace affects international relations: The promise of structural modifiers, in 45 Contemp. Secur. Policy 426 (2024).

[38] Le quattro Convenzioni di Ginevra, del 12 agosto 1949, per la protezione delle vittime di guerra (insieme ai Protocolli aggiuntivi I e II del 1977, e a quello del 2005), i cui riferimenti sono ampiamente assurti al rango di diritto consuetudinario. Si consideri, inoltre, il c.d. Corpus dell'Aia, formato dalle Convenzioni dell'Aia del 1899 e 1907, focalizzate su metodi e strumenti di conduzione delle ostilità con l'obiettivo di evitare sofferenze inutili e sproporzionate ai partecipanti al conflitto. Si veda la Sezione II: Delle ostilità del Regolamento annesso alla IV Convenzione dell'Aia concernente le leggi e gli usi della guerra per terra e, in particolare, il contenuto degli artt. 22-23, confluito nella consuetudine internazionale e nel testo degli artt. 35 e 51 del già menzionato Protocollo I del 1977.

bombardamenti d'artiglieria e dispiegamenti di truppe – in cui l'identità dell'aggressore e l'impatto degli atti di guerra sono chiari ed evidenti. Nel cyberspazio, al contrario, gli attacchi informatici possono essere lanciati in modo anonimo, con effetti distruttivi spesso ritardati, dispersi o indiretti. Ai sensi dell'art. 51 della Carta, agli Stati è inoltre riconosciuto the inherent right of individual or collective self-defence nel caso subiscano un attacco armato. Ne consegue che, ai fini della presente disamina, la questione giuridica centrale sia appurare se (e quando) gli attacchi informatici possano essere a tutti gli effetti classificati come attacchi armati, innescando così il meccanismo della legittima difesa. Tradizionalmente, un attacco armato è inteso come uso della forza militare volto a causare all'avversario danni significativi, come morte, lesioni e distruzione di proprietà. Allo scopo di colmare il divario che, in termini quasi metafisici, continua a separare guerra militare e guerra digitale al netto della comune attitudine a causare effetti distruttivi nel mondo materiale, in dottrina si sostiene che le azioni condotte nel dominio cibernetico possano, in determinate circostanze, raggiungere il livello di un attacco armato, in particolare quando causino una significativa distruzione fisica o la perdita di vite umane[39]. Pur persistendo la difficile adattabilità, al regno digitale, di norme progettate per il tradizionale campo di battaglia fisico, tale assimilazione concettuale parrebbe altresì imporsi in considerazione dell'ulteriore carattere "ibrido" di recente assunto da alcune tipologie di operazioni cyber-cinetiche, coordinate per produrre simultaneamente effetti nei due diversi spazi fisico e cibernetico nel deliberato intento di causare vittime umane[40]. L'assenza di una definizione universalmente accettata di guerra informatica complica del resto gli sforzi per regolamentare questo fenomeno nell'ambito del regime giuridico esistente. L'incertezza dei confini tra il mondo materiale e la sfera digitale, pertanto, solleva interrogativi circa l'applicabilità del diritto internazionale umanitario nel contesto della cyber warfare e ciò sebbene, in ossequio a un approccio effect-oriented, il riferimento ai principi consolidati del diritto di guerra resti fondamentale nell'ottica di mitigare concretamente gli effetti di qualsiasi forma di conflitto, specialmente sulla sfera civile, a prescindere dalla legittimità internazionale posta a monte delle azioni in cui il conflitto prenda forma (come nel caso dell'autodifesa) e dalla natura degli agenti che lo abbiano innescato (includendo anche gli attori [41]

---

[39] Cfr.: M. C. Waxman, Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions, in 89 Int. Law Stud. 109, 111 ss. (2013); F. Rugge, Le ragioni per una rafforzata cooperazione tra NATO e UE per la protezione dello spazio cibernetico, in U. Gori, L. Martino, op. cit., 339-354; S. Hill, NATO and the International Law of Cyber Defence, in N. Tsagourias, R. Buchan, op. cit., 509-524.

[40] Basti pensare ancora al recente attacco di Israele a cercapersone, walkie-talkie, smartphones e pannelli solari in Libano, dove questi dispositivi, a uso perlopiù civile, sarebbero stati fatti esplodere a distanza. Al riguardo, cfr.: B. Saul, Exploding pagers and radios: A terrifying violation of international law, in UN Press – OHCHR, 19 settembre 2024; M. Milanovic, Were the Israeli Pager and Walkie-Talkie Attacks on Hezbollah Indiscriminate?, in EJIL:Talk!, 20 settembre 2024.

[41] In relazione ai conflitti privi di carattere internazionale, rilevano altresì l'art. 3 comune alle quattro convenzioni di Ginevra del 1949, il II Protocollo addizionale del 1977 (cfr. Preambolo e art. 1.1) e l'art. 19 dell'Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention, UNESCO, n. 3511, 1954. Cfr. D. E. Graham, Cyber Threats and the Law of War, in 4 JNSLP 87, 91 ss. (2010). Inoltre, cfr. ICTY, Prosecutor v. Tadic, Case n. IT-94-1-A, Decision on the defence motion for interlocutory appeal on jurisdiction, 2 ottobre 1995, §§ 66-70, 72, 94-99.

non-statali). Nel cyberspazio, tuttavia, i confini tra guerra e pace, tra combattenti e civili, rimangono perlopiù offuscati. Non tutti i tipi di cyber operations superano peraltro la soglia di gravità dell'aggressione militare. Lo spionaggio informatico e le azioni di intelligence, ad esempio, comportano esclusivamente la raccolta segreta di informazioni a discapito di entità o strutture di uno Stato straniero e – pur contravvenendo a leggi nazionali e norme internazionali, costituendo una forma di ingerenza straniera e di violazione dello spazio di sovranità di altri Stati – non necessariamente presentano un animus aggressionis e infrangono le regole internazionali sull'uso della forza[42]. Allo stesso modo, gli attacchi informatici che interrompano le reti o manipolino dati senza però causare sensibili danni diretti a cose o persone non possono essere classificati come forme di aggressione[43]. Ad ogni modo, l'attuale cornice del diritto internazionale umanitario è chiamata a svolgere un essenziale ruolo di indirizzo nella regolamentazione delle operazioni cyber-cinetiche che implichino effetti fisici, in particolare sulla sfera civile. Secondo gli artt. 48-51 del Protocollo I alle Convenzioni di Ginevra[44] – il cui contenuto è peraltro ormai acquisito a livello consuetudinario – le operazioni militari devono distinguere tra obiettivi civili e militari, garantendo la proporzionalità degli attacchi in osservanza dello stesso canone di necessità in cui restano comunque inscritte le previsioni dell'art. 51 della Carta delle Nazioni Unite. La diretta applicazione di questi principi agli attacchi informatici rimane in ogni caso assai complessa, specialmente in ragione dei continui progressi della tecnica, la cui eccezionale rapidità sembra vanificare i già affannosi sforzi regolatori. Questi ultimi, come visto, assumono comunque massima urgenza dinanzi all'impiego offensivo di dispositivi di uso prettamente civile come smartphones, cercapersone, attrezzatura di domotica e addirittura pannelli solari, i quali possono essere presi di mira non soltanto nel corso di attacchi orientati a violarne il contenuto o a pregiudicarne il normale funzionamento, ma addirittura nel contesto di attacchi cyber-cinetici di stampo "ibrido" volti a causarne l'incendio o la detonazione a distanza al pari di vere e proprie armi di sterminio. Quanto appena descritto rappresenta senza alcun dubbio un'evoluzione pericolosa nel panorama delle capacità informatiche, che espande la portata di

---

[42] Sul tema, cfr.: T. Rid, Cyber War Will Not Take Place, Londra, 2013; E. Greco, Cyber war e cyber security: Diritto internazionale dei conflitti informatici, contesto strategico e strumenti di prevenzione e contrasto, in SIS, 11, 2014, 3-88. Inoltre: R. Mastrolembo, Imminence and States' Right to Anticipatory SelfDefence: Responding to Contemporary Security Threats, in 16 Canberra Law Rev. 143, 155 ss. (2019); R. Buchan, I. Navarrete, Cyber espionage and International Law, in N. Tsagourias, R. Buchan, op. cit., 231-252.

[43] Cfr.: M. Roscini, World Wide Warfare: Jus ad bellum and the use of cyber force, in A. von Bogdandy, R. Wolfrum, C. E. Philipp (Eds), UNYB, Leiden, 2010, 85-130; H. Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge, 2012; C. Henderson, The Use of Cyber Force: Is the Jus ad Bellum Ready?, in 27 QIL, Zoom-in 3, 7-9 (2016); H.-J. Heintze, P. Thielbörger, Progressive Development of International Law: From Cold War to Cyber War: an Introduction, in Iid. (Eds), From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the last 25 Years, Berlino, 2016.

[44] Protocollo aggiuntivo alle Convenzioni di Ginevra del 12 agosto 1949, relativo alla protezione delle vittime dei conflitti armati internazionali (Protocollo I), adottato l'8 giugno 1977, che integra, rafforza, aggiorna ed estende, in particolare, le previsioni della la IV Convenzione di Ginevra per la protezione delle persone civili in tempo di guerra, 12 agosto 1949.

futuri conflitti digitali potenzialmente ben oltre gli obiettivi militari e le infrastrutture dual-use, per colpire direttamente la popolazione dello Stato target in totale spregio dei principi consolidati di umanità, proporzionalità, necessità militare, distinzione e precauzione[45] in base ai quali il vantaggio militare ottenuto da un attacco specifico non deve cagionare sofferenze superflue e non deve infliggere danni inutili ed evitabili ai civili, i quali devono comunque restare nettamente distinti dal personale e dai mezzi militari[46].

La disciplina della legittima difesa, inoltre, consente agli Stati di rispondere a simili attacchi non solo con mezzi simmetrici di carattere informatico, ma anche tramite l'uso della forza militare, purché la risposta aderisca a sua volta agli appena elencati principi del diritto di guerra. Le difficoltà giuridiche, di conseguenza, si estendono anche alla valutazione di questi fondamentali elementi che, nell'ambito di una rappresaglia asimmetrica, restano di problematica valutazione, in considerazione dei molteplici effetti indiretti o ritardati che possono interferire con l'esatta quantificazione dell'entità di un attacco cibernetico. Alla luce di tali constatazioni, gli Stati (e le organizzazioni internazionali) parrebbero incentivati ad adottare un approccio di marca preventiva alle questioni della cyber-security – come l'introduzione di misure di matrice diplomatica o il ricorso alla coercizione economica contro le possibili fonti (soggetti statali e non-statali) che possano rappresentare un pericolo per la sicurezza informatica[47] – piuttosto che ricorrere ad azioni "ritorsive" di

---

[45] Si guardi parimenti agli artt. 57-58 del Protocollo I, cit., 1977.

[46] Cfr.: E. Mavropoulou, Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks, in 4 JLCW 23 (2015); J. Kulesza, R. Balleste, Cybersecurity and Human Rights in the Age of Cyberveillance, Lanham, 2015; G. D. Solis, The Law of Armed Conflict: International Humanitarian Law in War, II ed., Cambridge, 2018; K. Bannelier, Is the Principle of Distinction still Relevant in Cyberwarfare? From Doctrinal Discourse to States' Practise, in N. Tsagourias, R. Buchan, op. cit., 427-456.

[47] Al riguardo, cfr. Consiglio dell'UE, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption, 9916/17, 7 giugno 2017. Inoltre: Decisione (PESC) 2019/797 del Consiglio dell'UE, 17 maggio 2019, considerando 4 e 8; Regolamento (UE) 2019/796 del Consiglio dell'UE, 17 maggio 2019, considerando 7. Sul tema, cfr.: M. Fulgenzi, Il Global Human Rights Sanctions Regime dell'UE (EU-GHRSR): uno strumento-chiave per la politica estera dell'Unione europea, in Ann. Dip. Giur. Univ. Molise, 22, 2021, 243-275, 269. Si vedano ancora: T. Lațici, EU cyber sanctions: Moving beyond words, PE 652.092, EPRS (2020); S. Poli, E. Sommario, The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions, in 24 German Law Journal 522 (2023). L'UE è emersa come avanguardia nello sviluppo di un framework giuridico utile ad affrontare la crescente minaccia degli attacchi informatici (e ciò sebbene, ai sensi dell'art. 4.2 TUE, la sicurezza nazionale resti di esclusiva competenza di ciascuno Stato membro dell'UE). Questi sforzi normativi riflettono la volontà di un'ampia affermazione di sovranità nel cyberspazio, rivolta a instaurare una forma di giurisdizione digitale (anche di raggio extraterritoriale) dell'UE per mezzo di regole che estendono la propria portata oltre i confini degli Stati membri, in riconoscimento del cyberspazio come dominio transnazionale. È qui che le strutture giuridiche – per il fine superiore di garantire sicurezza e attribuzione di responsabilità – sono chiamate a trascendere le demarcazioni geografiche se non già a sublimare i termini del rapporto dualistico tra territorialità "materiale" e "virtuale", sancendone l'inesione concettuale in recepimento dell'assunto per cui "i limiti del linguaggio significano i limiti del mondo" (cfr. L. Wittgenstein, Tractatus logico-philosophicus, 1921). Si vedano altresì: Direttiva (UE) 2016/1148 del

stampo retributivo, tanto meno se manu militari. Ad ogni modo, non potrà essere ignorata la persistenza di incertezze sull'attribuzione della responsabilità per le attività di volta in volta oggetto di contestazione, così come non potrà essere eluso l'obbligo internazionalmente previsto di assicurare la proporzionalità, la temporaneità e la reversibilità delle contromisure (in quanto tali "non implicanti l'uso della forza"[48]) che si intendano adottare[49].

Parlamento europeo e del Consiglio, 6 luglio 2016 (NIS Directive); Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, 17 aprile 2019 (Cybersecurity Act – CSA) nel cui quadro, in particolare, rilevano il rafforzamento del ruolo dell'Agenzia dell'UE per la sicurezza delle reti e dell'informazione (ENISA) e l'introduzione di un sistema europeo per la certificazione della sicurezza informatica dei dispositivi connessi a Internet e di altri prodotti o servizi digitali; Commissione europea e Alto Rappresentante dell'Unione per la PESC, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 dicembre 2020; Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, 14 dicembre 2022 (NIS 2 Directive), che all'art. 16 istituisce il Cyber Crisis Liaison Organisation Network (EU-CyCLONe); Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (Cyber Resilience Act – CRA); Regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, 19 dicembre 2024, che modifica il Regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti. Da ultimo, cfr.: Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il Regolamento (UE) 2021/694 (Cyber Solidarity Act), tramite cui, all'art. 3, è istituito il Sistema europeo di allerta per la cibersicurezza quale rete paneuropea di infrastrutture costituita da poli informatici nazionali e transfrontalieri (Security Operations Centres – SOCs) preposto ad azioni di CTI (Cyber Threat Intelligence) anche attraverso strumenti di AI e tecnologie di data analytics, mentre, all'art. 10, si introduce il Meccanismo per le emergenze di cibersicurezza che si avvale della costituzione di una EU Cybersecurity Reserve. L'art. 21 del medesimo provvedimento definisce invece il Meccanismo europeo di riesame degli incidenti di cibersicurezza, in base al quale, su richiesta della Commissione o delle autorità nazionali (EU-CyCLONe o la rete di Computer Security Incident Response Team – CSIRTs), l'ENISA sarà responsabile della revisione di specifici incidenti di sicurezza informatica, significativi o su larga scala. Il tutto, sostenuto da finanziamenti per l'Obiettivo strategico Cybersecurity del programma UE Digital Europe (DIGITAL). Per uno sguardo programmatico sulle azioni di contrasto, da parte dell'UE, nei confronti delle cc.dd. minacce ibride, tra le quali figurano i rischi e i pericoli connessi all'avvento dell'era del cyberspazio, cfr.: Commissione europea, Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats: A European Union response, JOIN(2016)18 final, 6 aprile 2016. Nel più ampio respiro di tale strategia evolutiva rientra altresì il Regolamento (UE) 2023/2675 del Parlamento europeo e del Consiglio, 22 novembre 2023, sulla protezione dell'UE e dei suoi Stati membri dalla coercizione economica da parte di paesi terzi (Anti-Coercion Instrument – ACI). Nel contesto della sussidiarietà multistrato che permea costitutivamente la struttura dell'UE, si consideri infine la valorizzazione del ruolo delle autorità locali e regionali (LRAs) quali "prima linea" di risposta alla cangiante realtà degli attacchi ibridi, nella prospettiva dell'ulteriore integrazione delle autorità subnazionali nelle strategie di resilienza a livello dell'UE, tramite finanziamenti dedicati, partnership per la sicurezza informatica e reti di allerta precoce transfrontaliere. Sul tema, cfr. M. Fulgenzi, Subnational Authorities as Key Global Actors: Glocal Diplomacy in Pursuit of World Peace and Security in the Prism of the Vision and Goals of the UN 2030 Agenda, in Athena – Critical Inquiries in Law, Philosophy and Globalization, 4.2/24, 2024, 92-168.

[48] Si veda l'elenco (in sé non esaustivo) delle azioni contemplate nel testo dell'art. 41 Carta delle Nazioni Unite.

[49] Sul tema, cfr.: O. A. Hathaway et al., The Law of Cyber-Attack, in 100 Calif. Law Rev 817, 879 (2012); F. Delerue, Cyber operations and international law, Cambridge, 2020, cap. 10, 423-490. Si veda, in particolare: Italian Position Paper on

Nondimeno, rilevanti posizioni accademiche concordano nell'inscrivere la guerra informatica nel combinato disposto tracciato dagli attuali ius ad bellum (i.e., la legge internazionale che regola il diritto di usare la forza) e ius in bello (i.e., le norme che regolano la condotta durante lo svolgimento del conflitto), sottolineando come il divieto imperativo di uso della forza, le regole di autodifesa e il diritto umanitario inscritto nelle leggi di guerra possano applicarsi anche alle operazioni cibernetiche pur in coscienza delle criticità sopra menzionate[50]. Data l'estensione ormai planetaria del cyberspazio, l'affermazione delle sovranità nazionali sullo spazio digitale solleva oltretutto ineludibili interrogativi sulla giurisdizione, sui diritti di accesso e, in generale, sul rispetto dei diritti umani[51]. L'evoluzione del quadro giuridico della cyber warfare richiede perciò meccanismi più solidi per definire i parametri di attribuzione e i presupposti della responsabilità statale, insieme a una maggiore cooperazione a livello internazionale in vista di un più efficace tracciamento delle operazioni informatiche attraverso la condivisione di dati di intelligence. Sempre alla luce delle prevalenti conclusioni della dottrina, gli Stati devono pertanto astenersi dal condurre operazioni informatiche che violino l'integrità territoriale o l'indipendenza politica di altri Stati[52] e ciò – come particolarmente rilevante nel contesto odierno – anche in tempo di pace[53], dato che simili azioni, anche quando non assimilabili a un attacco armato, possono comunque integrare una violazione del principio di non-intervento quale assunto consolidato del diritto internazionale consuetudinario[54].

'International Law and Cyberspace', cit., 7. Inoltre, cfr. M. N. Schmitt, Tallinn Manual 2.0, cit., Rules 20-25.

[3] Cfr.: M. Roscini, Cyber Operations and the Use of Force in International Law, Oxford, 2014; I. Kilovaty, Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare, in 5 Am. U. Nat'l Sec. L. Brief 91 (2014), 95 ss.

[51] Cfr.: M. Mirti, Il Cyberspace. Caratteri e riflessi sulla Comunità Internazionale, Napoli, 2021, 10 ss.; D. P. Fidler, Cyberspace and Human Rights, in N. Tsagourias, R. Buchan, op. cit., 130-151.

[52] Cfr. M. N. Schmitt, Tallinn Manual 2.0, cit., Rules 1-3.

[53] Cfr. ivi, Rule 32.

[54] Cfr.: P. B. Stephan, Big Data and the Future Law of Armed Conflict in Cyberspace, in M. C. Waxman, T. W. Oakley (Eds), The Future Law of Armed Conflict, collana «The Lieber Studies», New York-Oxford, 2022, cap. 4; M. N. Schmitt, The Law of Cyber Conflict: Quo Vadis 2.0?, ivi, cap 6, 103-121.

1.2 Il contributo della giurisprudenza della CIG dinanzi alle sfide della cyber warfare

Sebbene, da parte della Corte internazionale di giustizia (CIG), non siano ancora intervenute sentenze direttamente afferenti alla materia della moderna guerra cibernetica, l'acquis giurisprudenziale della Corte dell'Aia può in ogni caso fornire precedenti di rilievo emblematico, utili allo sviluppo della tematica della responsabilità internazionale dello Stato nel contesto del cyberspazio. Le pronunce della CIG, infatti, rappresentano una preziosa guida interpretativa ampiamente recepita nella cornice dell'operato degli Stati e delle varie organizzazioni internazionali così come nel contesto accademico e – oltre a certificare gli assetti normativi in vigore – possono sensibilmente contribuire a plasmare la disciplina del conflitto informatico e il consolidamento di un cyber-nomos coerente ed effettivo. Nel 1996, il Parere della CIG sulla legittimità del ricorso agli armamenti nucleari[55] ha avanzato importanti considerazioni circa l'universale applicabilità delle norme internazionali sull'uso della forza[56] e dei principi fondamentali del diritto internazionale umanitario[57], indipendentemente dalla fattura delle armi utilizzate nonché al netto di qualsiasi avanzamento tecnologico intervenuto nei modi di condurre la guerra[58]. Muovendo dall'asserzione dell'illiceità degli attacchi che causino sofferenze inutili agli esseri umani o effetti indiscriminati tra obiettivi militari e civili[59], la Corte ha infatti enfatizzato la validità paradigmatica dei criteri di necessità, proporzionalità e distinzione i quali, di conseguenza, si prestano a conservare il proprio valore anche in riferimento alle molteplici possibili declinazioni della guerra informatica. Ribadendo che l'idea di "uso della forza", nel quadro del diritto internazionale, deve essere interpretata in modo sufficientemente ampio e indipendente dai mezzi di fatto utilizzati per perseguire scopi militari, la CIG giunge a contemplare – quanto meno in astratto – scenari che potrebbero essere oggi interpretati come non direttamente cinetici, tanto più se in concreto idonei a diffondere grave distruzione o a ledere in maniera sostanziale le infrastrutture di uno Stato. Sebbene la Corte noti che non si possa escludere a priori la legittimità, ai sensi del diritto internazionale, del possesso così come dell'impiego di un particolare sistema d'arma in assenza di una norma di origine consuetudinaria o convenzionale che ne proibisca espressamente il dispiegamento o l'utilizzo[60], la validità dei principi individuati dai giudici dell'Aia in relazione agli armamenti nucleari potrebbe essere estesa alla sfera dei moderni attacchi informatici che siano capaci di causare danni estesi, fino a ricomprendere le operazioni cyber-cinetiche che possono abbattersi su infrastrutture civili come reti elettriche, ospedali e sistemi di telecomunicazione o di gestione del sistema finanziario. Il Parere della Corte ribadisce d'altronde

[55] CIG, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, in I.C.J. Reports 1996 226.

[56] Ivi, §§ 37 ss. e 41-42.

[57] Ivi, § 74 ss.

[58] Ivi, §§ 78 (dove si richiama la c.d. Martens Clause) e 86-87.

[59] Ivi, §§ 77-79. Cfr.: artt. 22-23 Convenzione (IV) dell'Aia, 1907; Dichiarazione di San Pietroburgo, 1868, cons. 4.

[60] CIG, Legality of the Threat or Use of Nuclear Weapons, cit., §§ 21 e 52. Cfr. CPGI, The case of the S.S. Lotus, Judgment n. 9, 7 settembre 1927, in P.C.I.J. Publication, series A, n. 10, 2-33, 3.

l'importanza di limitare i danni ai civili e di garantire che anche gli obiettivi militari siano perseguiti cercando di evitare o minimizzare danni collaterali, non mancando di sottolineare in più punti la centralità dei principi consolidati che, nel diritto internazionale, sorreggono il profilo umanitario della c.d. legge di guerra e la disciplina dell'autodifesa.

Già nel 1949, in occasione della sentenza sul caso Corfu Channel[61], la CIG evidenziò come tali principi basilari emergano, in tempo di pace, in guisa di «general and well recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war»[62], ai quali viene ad aggiungersi «every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States»[63]. Su ciascuno Stato grava pertanto l'obbligo di non consentire consapevolmente che il proprio territorio venga utilizzato per azioni di altri attori, statali o meno, che violino la sovranità di Stati terzi. Emerge così l'importanza del prisma interpretativo avallato in tale sede dai giudici dell'Aia in funzione del mantenimento della pace e della sicurezza internazionale, oggi nondimeno estendibile al regno digitale. Le conclusioni della Corte potrebbero infatti essere estrapolate dal contesto dell'immediato Secondo Dopoguerra ed essere adattate alla moderna guerra informatica, sostenendo come gli Stati abbiano parimenti il dovere di prevenire i cyber-attacchi contro altri Stati che possano trovare origine nel loro territorio, anche laddove tali operazioni siano intraprese da soggetti non-statali. Qualora uno Stato risulti a conoscenza di cyber operations attuate all'interno della sua giurisdizione e non intraprenda misure (ragionevoli) atte a fermarle o a contenerne gli effetti, potrà essere ritenuto internazionalmente responsabile delle sue omissioni. Un'impostazione, quella qui espressa dai giudici dell'Aia, che riecheggia coerentemente nella successiva sentenza del 1980 sul caso Tehran Hostages[64], dove la Corte conclude che approvando, supportando o mantenendo gli effetti degli atti compiuti ad opera di agenti non-statali sul suo territorio, lo Stato recepisca gli stessi atti come propri, esponendosi ai relativi addebiti ai sensi del diritto internazionale[65].

Con la celebre sentenza Nicaragua del 1986[66], la CIG ha peraltro ulteriormente chiarito che gli Stati possono essere ritenuti responsabili per atti compiuti da attori non-statali sul territorio di altri Stati nel caso in

---

[61] CIG, Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment, 9 aprile 1949, in I.C.J. Reports 1949 4.

[62] Ivi, 22. La Corte sottolinea come, in tempo di guerra, operi il riferimento alla Convenzione (VIII) dell'Aia, 1907,

[63] CIG, Corfu Channel case, cit., 22.

[64] CIG, Case concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment, 24 maggio 1980, in I.C.J. Reports 1980 3.

[65] Ivi, §§ 67-68 e 74.

[66] CIG, Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, Merits, 27 giugno 1986, in I.C.J. Reports 1986 14.

cui non solo forniscano loro coordinamento e sostegno in modo significativo[67], ma altresì esercitino un "controllo effettivo" su tali soggetti[68]. La Corte, in questo frangente, ha dunque fornito indicazioni circa la responsabilità indiretta dello Stato scaturente da un'inosservanza minoris generis[69] del divieto dell'uso della forza, concretatasi nella fornitura di supporto materiale, direttivo e organizzativo all'operato di attori di rango non-statale impegnati in azioni ostili nei confronti di un altro Stato, specificando inoltre come anche forme di sostegno di minore intensità (esclusivamente politico o economico) possano comunque integrare l'ipotesi di ingerenza negli affari di uno Stato straniero in violazione della sua indipendenza sovrana riconosciuta a livello internazionale e del principio consuetudinario di non-intervento[70]. Tali assunti, ancora una volta, possono trovare ampia applicazione nel contesto degli odierni cyber-attacchi, in particolare laddove gli Stati si avvalgano dello schermo di un proxy informatico allo scopo di rifugiarsi dietro una "negazioneplausibile" del proprio coinvolgimento diretto. Se uno Stato fornisce supporto, risorse oppure assistenza logistica a gruppi hacker o a mercenari informatici che lancino attacchi contro un altro Stato, potrebbero dunque sussistere i presupposti della sua responsabilità ai sensi del diritto internazionale. Ciò fermo restando che, per giustificare l'autodifesa ai sensi dell'art. 51 della Carta dell'ONU, il cyber-attacco deve aver prodotto un impatto talmente significativo da essere di fatto assimilabile a un attacco armato[71].

Di particolare interesse, infine, sono gli elementi mutuabili dal Parere consultivo con cui, nel 2019, la CIG si è espressa sulla questione delle Isole Chagos[72]. La Corte ha infatti riaffermato il valore nodale della sovranità, indipendenza e integrità territoriale dello Stato nel diritto internazionale, dove questi principi

---

[67] Si consideri, in proposito, il più flessibile criterio del "controllo generale" adottato in: ICTY, Prosecutor v. Tadic, Case n. IT-94-1-A, Judgment, 15 luglio 1999, §§ 98-137 (c.d. overall control test). Si veda, altresì: M. Langobardo, Rapporti fra strumenti di codificazione: il progetto di articoli sulla responsabilità degli Stati e le convenzioni di diritto internazionale umanitario, in Riv. Dir. Int., 101, 2018, 1136-1163.

[68] CIG, Case concerning military and paramilitary activities in and against Nicaragua, cit., §§ 115-116 (c.d. effective control test). Cfr.: CIG, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 26 febbraio 2007, in I.C.J. Reports 2007 43, § 393. Cfr.: A. Zorzi Giustiniani, Il Position Paper dell'Italia sull'applicabilità del diritto internazionale nel cyberspazio, la sentenza del Tribunale UE nel caso Google Shopping e l'Oxford Statement sulla regolamentazione internazionale degli attacchi ransomware, in Nomos – Cronache dal Cyberspazio, 3, 2021, 2 ss.; R. Bartels et al. (Eds), Military Operations and the Notion of Control Under International Law, Liber Amicorum Terry D. Gill, Berlino, 2021; B. Conforti, M. Iovane, Diritto Internazionale, XII ed., Napoli, 2023, 402 ss.

[69] Cfr. CIG, Case concerning military and paramilitary activities in and against Nicaragua, cit., § 205.

[70] Ivi, §§ 202, 205, 228 e 251. Cfr.: UNGA, Risoluzione 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, 21 dicembre 1965; Risoluzione 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 24 ottobre 1970, Annex.

[71] Cfr. CIG, Case concerning military and paramilitary activities in and against Nicaragua, cit., §§ 194-201 e 230 ss.

[72] CIG, Legal Consequences of the Separation of the Chagos Archipelago from Mauritius in 1965, Advisory Opinion, in I.C.J. Reports 2019 95.

emergono nella veste rafforzata di sostanziali corollari – al pari del paradigma della non-ingerenza – del principio imperativo del diritto di autodeterminazione dei popoli[73], oggi inscritto nel novero dello jus cogens internazionale. Tali concetti, tradizionalmente applicati al territorio geografico, non possono d'altronde che acquisire rinnovato rilievo per la disciplina del cyberspazio, nel momento in cui un numero crescente di Stati inizia a rivendicare la sovranità sui propri domini digitali, incluso il diritto di controllare e regolamentare i flussi di dati, i sistemi Internet e le operazioni informatiche effettuate all'interno dei loro "confini virtuali". Tutto questo, nell'intento di presidiare e proteggere la propria infrastruttura digitale e i propri asset critici dalle conseguenze di attacchi cibernetici che comportino l'interruzione di servizi di importanza vitale o la sottrazione di dati sensibili, nonché allo scopo di tenere la propria popolazione al riparo dalla diffusione di campagne disinformative e manipolatorie (le cc.dd. fake news)[74], non diversamente da come gli stessi Stati difenderebbero il proprio territorio fisico da incursioni di truppe straniere. Il rafforzamento del principio di sovranità – come caposaldo giuridico applicabile sia al mondo materiale sia a quello cibernetico – rappresenta oltretutto un valido strumento per osteggiare il recente fenomeno del c.d. colonialismo digitale, che vede le grandi multinazionali dell'hi-tech e gli Stati tecnologicamente più avanzati esercitare un controllo sproporzionato sulle infrastrutture digitali e sui flussi di dati dei paesi meno avanzati, perpetuando in nuova forma gli schemi secondo cui le potenze coloniali europee sfruttavano un tempo le risorse naturali dei territori delle colonie d'oltremare.

2. L'orizzonte della due diligence come argine al caos della guerra informatica

Coerentemente alle indicazioni della giurisprudenza internazionale, le più recenti soluzioni elaborate dalla dottrina tendono a enfatizzare il concetto di due diligence dello Stato rispetto alla gestione della sfera informatica nelle sue implicazioni per il campo delle relazioni internazionali, richiedendo agli Stati di adottare – secondo un criterio di ragionevolezza, ovvero sulla scorta delle conoscenze, delle risorse, nonché delle capacità al momento disponibili nel quadro di un'amministrazione responsabile (i.e., la c.d. stewardship[75])

---

[73] Ivi, § 156. Cfr. art. 1.2 della Carta dell'ONU. Si veda anche la coerente accezione del principio di non-intervento quale «corollario del diritto di ogni Stato alla sovranità, all'integrità territoriale e all'indipendenza politica» L. Oppenheim, International Law:A Treatise, Volume 1: Peace, New Jersey, 1996, 428.

[74] Al riguardo, cfr. W. J. Schünemann, A threat to democracies?, in M. Dunn Cavelty, A. Wenger (Eds), Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation, Londra, 2022, 32-46.

[75] Su quest'ultimo aspetto, spesso reso in contrapposizione rispetto al contenuto del concetto di sovranità, cfr. D. B. Hollis, Stewardship versus Sovereignty? International Law and the Apportionment of Cyberspace, Temple University Legal Studies Research Paper n. 25 (2012). La nozione di stewardship opera peraltro in diretta connessione con l'interpretazione che propende a inscrivere il cyberspazio nel novero dei cc.dd. Global commons (o Res communes omnium, ossia risorse di proprietà collettiva dell'umanità), per quanto le intersezioni della sfera informatica con questioni legate alla sovranità e all'interesse dei singoli Stati, o connesse alla proprietà perlopiù privata delle infrastrutture digitali fisiche (server, nodi di rete, cavi in fibra etc.) e alle inerenti criticità in tema di equità e accessibilità, impediscano un'appropriata sussunzione della dimensione cibernetica in suddetta categoria, almeno in base alle attuali norme internazionali. Ad ogni modo, restano di rilievo alcuni connotati della rete informatica, come la sua natura di bene (apparentemente immateriale) di interesse comune per tutti i popoli del globo e la portata planetaria

.

delle risorse – misure utili a impedire che il territorio, sia fisico sia digitale, posto sotto la loro giurisdizione (comprensivo di tutte le infrastrutture tecnologiche in esso presenti) funga da postazione per operazioni cibernetiche che colpiscano altri Stati, pena la prospettiva di incorrere in attribuzioni di responsabilità internazionale per tali violazioni e i danni risultanti[76]. Una posizione, quella appena descritta, manifestamente mutuata nel moderno dominio del cyberspazio attingendo alla c.d. legge di neutralità nei conflitti armati[77], in base alla quale è parimenti richiesto agli Stati di rispettare il territorio degli altri Stati e di impedire che il loro territorio sia utilizzato per attività ostili nei confronti di altri Stati, sostanziando così i termini del non-coinvolgimento dello Stato che si professi neutrale nel contesto degli scontri cibernetici tra Stati terzi "belligeranti". In modo analogo, inoltre, è possibile tracciare importanti parallelismi tra l'attuale diritto internazionale dell'ambiente e i futuribili assetti della disciplina internazionale delle operazioni informatiche. Il principio del c.d. danno da inquinamento transfrontaliero costituisce infatti un principio fondamentale del diritto internazionale ambientale dal quale scaturisce l'obbligo, in capo a ciascuno Stato, di non consentire che attività svolte sul proprio territorio, o comunque sotto la propria giurisdizione, causino danni significativi all'ambiente di altri Stati o di aree internazionalmente situate al di fuori di ogni singola giurisdizione nazionale (come nei casi dell'alto mare o dell'Antartide)[78]. Questo focale principio

---

delle dinamiche di interconnessione consentite attraverso di essa. Strettamente correlato a tale visione è il parallelo istituito – da una parte – tra la condanna della pirateria marittima come crimen iuris gentium, ossia come crimine di carattere transnazionale contro l'umanità (cfr. artt. 100 e 101 UNCLOS, 1982) per cui si configura, nella consuetudine e nel diritto convenzionale (cfr. art. 14 Convenzione internazionale concernente l'alto mare, Ginevra, 1958), l'esercizio di giurisdizione universale da parte di tutti gli Stati in ragione della sua repressione, e – dall'altro lato – il percorso verso l'universale stigmatizzazione delle operazioni cibernetiche ostili perpetrate ad opera di nuovi hostes humani generis. Cfr. J. Kalpokiene, I. Kalpokas, Hostes Humani Generis: Cyberspace, the Sea, and Sovereign Control, in 5 BJLP 132 (2012),

[76] Cfr.: M. N. Schmitt, Tallinn Manual 2.0, cit., Rules 6-7; Italian Position Paper on 'International Law and Cyberspace', MAECI (2021), 6. Si veda: A. Stiano, Attacchi informatici e responsabilità internazionale dello Stato, Napoli, 2023.

[77] Le Convenzioni dell'Aia del 1907 rappresentano il principale strumento di codificazione della "legge di neutralità", già presente nella consuetudine, e dello status legittimo di "neutralità". Cfr.: Convenzione V (diritti e doveri delle Potenze neutrali e delle persone in caso di guerra terrestre); Convenzione XIII (diritti e i doveri delle Potenze neutrali in caso di guerra marittima). Cfr. CIG, Legality of the Threat or Use of Nuclear Weapons, cit. §§ 88-90; Inoltre: M. N. Schmitt, Tallinn Manual 2.0, cit., Rules 151-152; D. Turns, Cyber War and the Law of Neutrality, in N. Tsagourias, R. Buchan, op. cit., 471-489.

[78] Il principio è ampiamente attestato come una norma consuetudinaria. Cfr.: Dichiarazione di Stoccolma (1972), Principio 21; Dichiarazione di Rio sull'ambiente e lo sviluppo (1992), Principio 2. Si veda: Trail Smelter Case (United States, Canada), Award, 16 aprile 1938 e 11 marzo 1941, in RIAA, III, 2006, 1905-1982. Inoltre: CIG, Legality of the threat or use of nuclear weapons, cit., § 29; CIG, Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), Judgment, 25 settembre 1997, in I.C.J. Reports 1997 7, § 53 ss.; CIG, Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 20 aprile 2010, in I.C.J. Reports 2010 14, §§ 101, 204-205; CIG, 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), Judgment, 16 dicembre 2015, in I.C.J. Reports 2015 665, §§ 101 e 104-107 (in riferimento ai concetti di prevention e due diligence, nonché all'obbligo to notify and consult). Si veda: Trattato sull'Antartide, firmato a Washington il 1° dicembre 1959.

internazionalistico – di matrice concettuale lato sensu aquiliana – affonda le proprie radici nella responsabilità per fatto illecito (i.e., l'omessa dovuta diligenza nella vigilanza/disciplina, da parte dello Stato, delle attività potenzialmente lesive) ed è strettamente legato al paradigma della responsabilità internazionale dello Stato, come delineato dalla Commissione di diritto internazionale (CDI) nel suo Progetto di articoli del 2001[79], oltre che al peso generalmente attribuito alla cooperazione interstatale finalizzata a prevenire, mitigare e risolvere le controversie ambientali, traducendosi nell'articolazione di obblighi di prevenzione (i.e., l'adozione di misure atte a prevenire danni ambientali transfrontalieri); di obblighi di cooperazione (i.e., il coordinamento operativo in chiave preventiva o reattiva, la condivisione di informazioni e la notifica dei potenziali rischi ambientali); nonché dei connessi obblighi di risarcimento (poiché lo Stato responsabile deve risarcire il danno ad esso imputabile)[80]. Qualora il danno ambientale transfrontaliero sia causato da attività – sia lecite sia, a maggior ragione, illecite – che si accertino provenire dal territorio di uno Stato, il diritto internazionale prevede quindi la responsabilità dello Stato che non abbia adottato tutte le misure ragionevolmente attuabili per prevenire o almeno temperare un danno all'ambiente oltre confine[81].

---

[79] CDI, Draft articles on Responsibility of States for Internationally Wrongful Acts (DARSIWA), A/56/10, 2001, artt. 1-3 (General Principles).

[80] Si tratta del resto di un principio ormai consolidato nel quadro giuridico internazionale, che impone agli Stati un obbligo di condotta coerente con il parametro della due diligence in materia ambientale. Il mancato esercizio, da parte dello Stato, di un controllo adeguato secondo canoni di ragionevolezza, può ingenerare responsabilità internazionale per omissione. In tal senso, cfr. Direttiva (UE) 2024/1760 del Parlamento europeo e del Consiglio, 13 giugno 2024, nota come Corporate Sustainability Due Diligence Directive (CS3D), tramite cui l'UE, in ottemperanza ai propri principi costitutivi, agli obiettivi dell'EuropeanGreen Deal (2019) e agli obblighi assunti in ambito internazionale, ha inteso a sua volta rafforzare la responsabilizzazione delle imprese sul piano della sostenibilità, imponendo agli Stati membri di configurare specifici regimi di due diligence (di estensione, nei fatti, extraterritoriale) al fine di identificare, prevenire, mitigare e rimediare agli impatti negativi sui diritti umani, sull'ambiente e sul clima derivanti dall'intera filiera di attività delle società che operano nel mercato interno dell'Unione. In chiave complementare, si veda la Direttiva (UE) 2022/2464, del Parlamento europeo e del Consiglio, 14 dicembre 2022, detta anche Corporate Sustainability Reporting Directive (CSRD). Tali atti comprovano l'impegno dell'UE nel perseguimento degli obiettivi di sviluppo sostenibile. Si avvalora, pertanto, l'ipotesi dell'estensione analogica del paradigma internazionale della due diligence ambientale alla governance del cyberspazio, consolidando una due diligence cibernetica multilivello in capo agli Stati e – in via mediata – agli attori privati.

[81] Si pensi dunque, sempre in chiave analogica, alla declinazione "informatica" del principio del diritto internazionale dell'ambiente secondo cui "chi inquina paga", al fine di regolamentare la "responsabilità digitale" di soggetti che pongano in essere (o contribuiscano a) fenomeni di "inquinamento cibernetico", quali malware, attacchi informatici, diffusione di disinformazione online e violazioni della sicurezza di infrastrutture critiche. Ciò, nella consapevolezza della mancanza di un corpus normativo internazionale consolidato in materia e, comunque, fatti salvi i profili di diritto interno eventualmente rilevanti ai sensi del medesimo principio, dal quale discende per lo Stato l'obbligo di apprestare gli strumenti utili affinché la responsabilità del soggetto "inquinatore" possa essere fatta valere sul piano del proprio ordinamento nazionale. Cfr. Dichiarazione di Rio (1992), cit., Principio 16. Inoltre, cfr. Convention on Civil Liability for Damage Resulting from Activities Dangerous to the Environment, Lugano, 21 giugno 1993, ETS n. 150, Chapter II – Liability. Si vedano, ancora, gli artt. 191.2, e 192.5, TFUE, nonché la Direttiva 2004/35/CE del Parlamento Europeo e del Consiglio, del 21 aprile 2004, sulla responsabilità ambientale in materia di prevenzione e riparazione del danno ambientale, considerando (2)-(18) e art. 1.

Al netto del possibile consolidamento consuetudinario o di atti di trasposizione pattizia degli apporti giuridici fin qui richiamati sul piano logico-analogico, la trasformazione della guerra in chiave cibernetica continua dunque a porre difficoltà senza precedenti per quanto concerne la compiutezza e l'adeguatezza del diritto internazionale e dei concetti di sovranità e responsabilità statale in esso contemplati, così come insiste a manifestare elementi di "rigetto" avverso la coerente applicazione di principi del diritto umanitario progettati, in origine, per calmierare le efferatezze della "normale" guerra cinetica. L'aggiornamento dei quadri giuridici appena menzionati, come già argomentato, fatica oltretutto a seguire l'evoluzione stessa degli attacchi informatici, in particolare di quelli che ricadono al di sotto della soglia degli effetti di uno scontro armato tradizionale[82]. In base al Progetto di articoli della CDI (2001), resta in ogni caso acquisito che gli Stati sono ritenuti responsabili per gli atti illeciti compiuti in ambito internazionale, inclusa pertanto qualsiasi forma di attacco digitale, laddove tali azioni possano essere direttamente o indirettamente ad essi attribuite[83].

Sebbene la suddetta due diligence descriva paradigmaticamente un obbligo di condotta – non un obbligo di risultato – lo Stato può dunque essere considerato negligente e, di conseguenza, essere ritenuto responsabile per aver esercitato un controllo nei fatti insufficiente (e.g., attraverso sue agenzie specializzate, specifiche discipline di settore o, più in generale, tramite il proprio ordinamento penale) così come per la mancata adozione di adeguate misure preventive o di contenimento, anche laddove l'autore diretto del danno (tanto più se prodotto da attività illecita) sia un attore non-statale (come un'azienda privata) soggetto alla sua giurisdizione[84]. A dispetto della vicinanza concettuale, tuttavia, l'estensione del principio del danno transfrontaliero – come anche degli estremi giuridici della legge di neutralità e dei più generali termini della due diligence appena esposti – al dominio del cyberspazio non può avvenire in via automatica. In ragione della natura dell'ordinamento internazionale e dei connotati sovrani distintivi dei soggetti in esso operanti, si renderà d'altronde comunque necessario registrare (anche per mezzo dell'operato giurisprudenziale delle corti internazionali) lo sviluppo di un'inerente prassi internazionale (diuturnitas) basata su riscontri concreti (come le varie "posizioni" tematiche) e sull'effettivo consenso tra gli Stati (opinio iuris ac necessitatis), oppure anticipare il processo di consolidamento consuetudinario attraverso la promozione di convenzioni internazionali che provvedano a codificare i summenzionati obblighi di diligenza nel contesto cibernetico[85].

---

[82] Cfr. S. J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, in 27 Berkeley J. Int. Law 191, 195 (2009).

[83] Cfr. artt. 1, 2, 3, 4, 8 e 12 DARSIWA.

[84] Cfr. H. Krieger, A. Peters, L. Kreuzer (Eds), Due Diligence in the International Legal Order, Oxford, 2020; J. J., Piernas López, The international law principle of due diligence and its application to the cyber context, in Anales de Derecho, 41, 2024, 66-95. Si veda: M. N. Schmitt, Tallinn Manual 2.0, cit., Rule 17 e Rule 33. Inoltre: A. Kastelic, Due diligence in cyberspace: Normative expectations of reciprocal protection of international legal rights, UNIDIR, Ginevra, 2021.

[85] Per quanto declinati nella specifica prospettiva del contrasto internazionale alla problematica del cybercrime, cfr.: Draft United Nations convention against cybercrime: Strengthening international cooperation for combating certain crimes committed

Tuttavia, se pratiche di carattere più "estremo" – come il ricorso all'esplosione a distanza di dispositivi comunemente in uso presso la popolazione civile – si affermassero come tattiche più diffuse, si renderebbe oltremodo necessario un ancor più radicale riesame del diritto internazionale umanitario, nel tentativo di affrontare le problematiche correlate alla natura a duplice-uso (militare e civile) della moderna tecnologia. I civili, infatti, spesso utilizzano correntemente gli stessi dispositivi di comunicazione in uso presso il personale militare, rendendo difficile distinguere i legittimi obiettivi militari da quelli civili. Questa confusione tra uso civile e militare della tecnologia crea pertanto ulteriori zone grigie che potrebbero essere sfruttate dagli attori del cyberspazio per negare le proprie responsabilità. L'alterazione e la distruzione a distanza di dispositivi della c.d. elettronica di consumo, oltretutto, dimostrano come il campo di battaglia della cyber warfare si stia espandendo fino a toccare la tecnologia "di tutti i giorni". Nel prossimo futuro, dunque, potremmo assistere con maggiore frequenza ad attacchi informatici mirati contro dispositivi della c.d. Internet of things (IoT), come tecnologie indossabili, veicoli autonomi e persino "case intelligenti". Queste tecnologie, che sono sempre più integrate nella vita quotidiana, forniscono del resto una superficie di attacco di estrema vulnerabilità[86]. Dinanzi alla gravità di una simile minaccia, gli Stati dovrebbero quindi adoperarsi in via pattizia affinché la sfera della tecnologia civile possa essere formalmente esclusa dal novero degli obiettivi di attacchi informatici o, perlomeno, sostenere il rapido consolidamento consuetudinario di un'interpretazione "estensiva" del principio di distinzione già operante nel diritto internazionale umanitario, adeguata alle minacce del cyberspazio[87]. Nondimeno, viene in risalto per ogni Stato l'opportunità di concentrarsi sulla resilienza informatica, assicurando che tanto i propri sistemi critici quanto la propria rete ad uso civile possano resistere ad attacchi cibernetici stranieri e continuare a funzionare anche di fronte ai tentativi di

---

by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes (UNGA, A/AC.291/L.15, 7 agosto 2024); Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its reconvened concluding session (UNGA, A/78/986-A/AC.291/28, 19 agosto 2024). Inoltre, cfr. The Pact for the Future (UNGA, A/RES/79/1, 22 settembre 2024), 17, Action 24. Si veda, altresì: Consiglio d'Europa, Convention on Cybercrime (Budapest Convention, ETS n. 185), 23 novembre 2001, entrata in vigore nel 2004, con i suoi due Protocolli addizionali, rispettivamente: ETS n. 189 (2003) rivolto alla criminalizzazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici (in vigore dal 2006); CETS n. 224 (2022) sulla cooperazione rafforzata e la divulgazione delle prove elettroniche (non ancora in vigore). Inoltre, sempre nell'ambito del CoE, si vedano (oltre alla già richiamata "Convenzione 108+"): Convenzione sulla prevenzione del terrorismo (CETS n. 196, 2005, in vigore dal 2007), contenente disposizioni che trasformano in reato il reclutamento e l'addestramento di terroristi tramite la rete Internet; Convenzione di Lanzarote (CETS n. 201, 2007, in vigore dal 2010) sulla protezione dei minori contro lo sfruttamento e gli abusi sessuali, anche online. Sulle tematiche qui riprese, cfr.: C. Henderson, The United Nations and the Regulation of Cyber-security, in N. Tsagourias, R. Buchan, op. cit., 582-614; H. Lahmann, State Behaviour in Cyberspace: Normative Development and Points of Contention, in 16 ZfAS 31, 32 ss. (2023).

[86] Sulla questione, cfr. F. Meneghello, M. Calore, D. Zucchetto, M. Polese, IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices, in 99 IEEE Internet of Things Journal 1 (2019).

[87] Cfr. P. P. Pascucci, Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution, in 26 Minn. J. Int'l L. 419, 451 ss. (2017).

sabotaggio digitale. Tutto ciò, tramite l'utilizzo della crittografia avanzata e di sistemi di backup e data redundancy, insieme al regolare svolgimento di test e auditing di sicurezza utili a prevenire, identificare e mitigare le possibili falle presenti nelle proprie reti informatiche.

3. Le principali criticità nella disciplina giuridica della guerra informatica

Nell'era digitale, le capacità cibernetiche consentono agli Stati di proiettare il proprio potere a livello globale, senza mai oltrepassare un confine fisico. La capacità di infiltrarsi nei sistemi critici di un altro Stato rivela come le competenze e gli strumenti tecnologici possano ridefinire l'idea stessa di supremazia. La tecnologia ha sempre rappresentato una pietra angolare del predominio militare, ma nel cyberspazio il suo ruolo acquisisce un valore ancor più dirimente. Nella guerra tradizionale, la forza è misurata sul campo in termini di beni tangibili (truppe, carri armati etc.) e, in particolare, di territorio fisico conquistato. Oggi, invece, la proiezione esterna del potere dello Stato è sempre più supportata dalla sua abilità nel dominare il regno dell'informatica, in cui le informazioni sono al contempo un'arma e un bersaglio. In questa nuova dimensione, le distinzioni classiche tra aggressione e difesa o attacco e risposta si dissolvono in un "etere" sfuggente e la nuova essenza del potere non si traduce semplicemente nell'acquisizione del controllo sulle risorse materiali di un territorio, ma soprattutto nella capacità di dissimulare l'imposizione della volontà dello Stato al di fuori del suo spazio fisico di sovranità. Il malware, pur nella sua incorporeità digitale, è ad esempio capace di garantire a uno Stato il raggiungimento degli stessi obiettivi strategici di un attacco aereo, disabilitando infrastrutture chiave collocate oltre confine senza tuttavia lasciare traccia di distruzione fisica (peraltro con ingenti risparmi sul piano economico e senza rischiare l'incolumità personale dei propri piloti o soldati). La militarizzazione del cyberspazio e l'impiego crescente della forza cibernetica da parte degli Stati non possono dunque che destare seria preoccupazione[88]. La guerra informatica, in questo contesto, non è semplicemente uno scambio di "colpi digitali", ma un terreno di dissimulazione nel quale l'arbitrio incontrollato e l'illimitato accumulo di potere da parte degli attori più forti comporta inevitabilmente il sorgere di ulteriori diseguaglianze e conflitti[89]. Per quanto l'Assemblea Generale dell'ONU abbia da tempo recepito le conclusioni del GGE secondo cui «il diritto internazionale, e in particolare la Carta delle Nazioni Unite, è applicabile ed è essenziale per mantenere la pace e la stabilità e promuovere un ambiente ICT aperto, sicuro, pacifico e

---

[88] Cfr.: A. Bufalini, Uso della forza, legittima difesa e problemi di attribuzione in situazioni di attacco informatico, in A. Lanciotti, A. Tanzi (Eds), Uso della forza e legittima difesa nel diritto internazionale contemporaneo, Napoli, 2012, 405-435; D. Mandrioli, Il caso Wannacry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati, in La Comunità Internazionale, 3 (2018), 473-492. Inoltre: The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations, Oxford University: The Oxford Process on International Law Protections in Cyberspace (2021).

[89] Cfr. J.-J. Rousseau, Discours sur l'origine et les fondements de l'inégalité parmi les hommes, 1755.

accessibile»[90], emerge palesemente l'attitudine dei fautori degli attacchi informatici a rifugiarsi in zona grigie di para-legalità elusive dei canoni in cui tradizionalmente si inscrive l'agire degli Stati sul piano internazionale. Sulla scia di tali criticità, la refrattarietà finora manifestata dai protagonisti del cyberspazio verso la definizione di una disciplina internazionalistica del conflitto informatico espone innanzitutto una delle debolezze croniche del diritto internazionale: la difficoltà di far rispettare le regole oltre i confini statali[91]. In carenza di un'autorità internazionale in grado di far rispettare dettami e sentenze in espressione dell'esercizio di una giurisdizione obbligatoria, il diritto internazionale non dispone direttamente dei mezzi richiesti per contrastare i responsabili di attacchi informatici. Questa lacuna genetica dell'ordinamento giuridico internazionale parrebbe di conseguenza sostenere le ragioni di una risposta più assertiva e pragmatica alle minacce informatiche da parte delle singole giurisdizioni statali, tanto più una volta compreso come la pretesa veste "eterica" del cyberspazio si riveli perlopiù frutto di limitazioni percettive e come, al di sotto dell'apparente "invisibilità" – e, dunque, della presunta ingovernabilità – dei flussi di dati sia invece collocata una base fisica tangibile, fortemente territoriale, come tale localizzabile e in astratto regolabile. Ad ogni modo, proprio dalla constatazione della fisicità del complesso delle componenti tecnico-funzionali della rete (i.e., server, router, cavi e, più in generale, hardware, software etc.), materialmente dislocati nell'ambito della giurisdizione territoriale dei diversi Stati, sembrerebbe trarre nuova linfa anche la prospettiva che, in ottica de iure condendo, aspira a consolidare gli oneri internazionali di vigilanza riassunti secondo gli schemi di due diligence forgiati sulla scorta della giurisprudenza della CIG e dell'esperienza maturata in altre branche del diritto internazionale.

Mentre la guerra digitale continua a evolversi, permane quindi l'urgenza di un adeguamento del quadro giuridico internazionale che possa affrontare le sfide poste dalle operazioni informatiche, bilanciando le esigenze di sicurezza degli Stati con la protezione della stabilità globale e dei diritti umani, nel cammino verso l'instaurazione di un nomos cibernetico (consuetudinario o pattizio) idoneo a inquadrare il cyberspazio entro confini normativi incuranti delle apparenze virtuali, sull'esempio degli strumenti internazionali che già regolano le armi nucleari, chimiche e biologiche[92]. Tali accordi potrebbero imporre divieti su determinati tipi di operazioni informatiche, come gli attacchi mirati alle infrastrutture civili critiche o ai sistemi finanziari.

---

[90] Cfr. GGE, Report (A/68/98, 24 giugno 2013), 8, § 19,

[91] Cfr.: E. A. Posner, A. O. Sykes, Economic Foundations of International Law, 2013; T. Altwicker, Transnationalizing rights, in 29 EJIL 581 (2018); Id. Non-Universal Arguments under the ECHR, in 31 EJIL 101, 107 (2020).

[92] Sul tema, cfr. G. Valenti, La "Cyberwar". Le sue modalità e gli strumenti giuridici per contrastarla, in DPCE Online, 63, cit., 537-554. Si pensi ai trattati TNP (1968), START (1991), CTBT (1996), New START (2010) e TPNW (2017) in relazione agli armamenti nucleari, o alle convenzioni CWC (1993) e BWC (1972) in materia, rispettivamente, di armi chimiche e armi biologiche. Russia e Cina si sono espresse in favore di una simile soluzione, diversamente dall'atteggiamento "prudente" di USA e UE. In merito, cfr.: M. E. O'Connell, Cyber Security without Cyber War, in 17 J.C.& S.L 87 (2012); K. Pipyros et al., Cyber Operations and International Humanitarian Law, in 24 Information and Computer Security 38, 39 (2016).

La disciplina internazionale incentrata sui trattati esistenti e sulla consuetudine dovrebbe dunque essere aggiornata per riflettere le problematiche del conflitto informatico e regolamentare i nuovi profili della responsabilità dello Stato, vincendo altresì le ritrosie dettate dalla (forse comprensibile) tentazione, da parte di taluni Stati, di trasporre sul piano della pretesa "libertà" delle moderne correnti informatiche i fasti del loro trascorso predominio sui mari[93]. Soltanto attraverso la creazione di una cornice giuridica coerente e giusta è possibile mitigare il potenziale caotico e distruttivo della guerra cibernetica. Prescindendo da tale presupposto, il sistema internazionale rischia di sprofondare in uno stato di conflitto perpetuo, in cui i confini tra guerra e pace risulteranno sempre più sfumati nel turbinio di un'indefinita catena delle conseguenze. Sebbene nei limiti dell'efficacia di norme prive del supporto di un'autorità per se sovraordinata e, pertanto, sempre in balia dei rapporti di forza mutuati dalla sfera politica, economica e militare – come nel caso delle norme internazionali – soltanto attraverso una profonda riforma del quadro giuridico e un serio rilancio della cooperazione internazionale sarà possibile mitigare le sfide della guerra informatica che trovano risonanza nelle ambiguità della condotta degli Stati, nei problemi di attribuzione e nelle dissimulazioni causali che ostacolano una governance efficace della dimensione del cyberspazio.

3.1 I confini sfumati tra attacco e difesa nel cyberspazio

Una delle problematiche giuridiche più significative nel contesto delle azioni di guerra informatica è la persistente difficoltà nella distinzione tra atti di carattere offensivo e difensivo[94]. A differenza dei conflitti

---

[93] Si rammenti, in chiave storica (dal XVII sec.), la rivendicazione della "libertà dei mari" prima ad opera dei fautori della potenza commerciale olandese e poi da parte dei sostenitori della c.d. talassocrazia anglosassone, interessati – sempre per ragioni economiche o legate alla propria sicurezza nazionale – a "sottrarre" il dominio marino alle diverse giurisdizioni statali e a garantire la piena "libertà di navigazione" in mari da considerare libere risorse internazionali (Res communes omnium). Ciò, fino a porsi in contrasto, come nel caso della Gran Bretagna, rispetto all'iniziale emergere della disciplina dell'estensione del mare territoriale oltre il limite tradizionale delle tre miglia marittime (la c.d. regola della "gittata del cannone", XVII-XX sec.), con i primi tentativi rivolti alla sua formalizzazione in occasione della formulazione del testo della Convenzione sul mare territoriale e la zona contigua (Ginevra, 1958). Tuttavia, soltanto l'entrata in vigore, nel 1994, della Convenzione UNCLOS (Montego Bay, 1982) fisserà il nuovo limite entro la distanza massima di 12 miglia nautiche dalla linea di base della costa. Cfr. Hansard, UK House of Commons, Deb.: 22 marzo 1926, vol. 193, col. 872; 23 aprile 1958, vol. 586, col. 924. Si pensi, tuttora, alla mancata ratifica della UNCLOS da parte degli USA, che pur riconoscono molte delle sue disposizioni come prassi consuetudinaria nel diritto internazionale. Gli USA figurano tra i firmatari ma il Senato statunitense non ha mai proceduto alla ratifica, adducendo motivazioni legate alla sfera della sicurezza nazionale e scetticismo verso gli obblighi economici (giudicati come di ispirazione perlopiù "collettivista") e il funzionamento degli organismi internazionali previsti dalla Convenzione. Per quanto esposto, cfr.: H. de Groot, Mare liberum, 1609; J. Locke, Two Treatises of Government, 1689. In antitesi dialettica: J. Selden, Mare clausum seu de dominio maris, 1635. Inoltre, cfr.: D. R. Johnson, D. G. Post, Law and Borders - the Rise of Law in Cyberspace, in 48 Stan. L. Rev. 1367, 1370 ss. (1996); M. J. Flynn, Cyberspace and Naval Power, in 13 JAMS 167 (2022). Si vedano: National position of the United Kingdom on international law applicable to cyberspace (2021); Application of international law to States' conduct in cyberspace: UK statement (2021); United States International Cyberspace & Digital Policy Strategy (2024).

[94] Sulla tematica, cfr. H.S. Lin, Offensive Cyber Operations and the Use of Force, in 4 JNSLP 63 (2010).

militari tradizionali, in cui i confini geografici possono quanto meno aiutare a distinguere tra aggressore e aggredito, gli attacchi cibernetici operano in una dimensione in cui la stessa infrastruttura digitale può essere pressoché indifferentemente utilizzata per entrambi gli scopi. L'implementazione di avanzati sistemi di sicurezza informatica da parte di uno Stato potrebbe infatti essere percepita da un altro Stato come una misura offensiva. Molte tecniche utilizzate nel corso di attacchi informatici (e.g., pen testing, malware analysis etc.) sono componenti chiave delle attività difensive ma, in quanto strumenti di scansione delle vulnerabilità, possono essere usati sia per proteggere un sistema sia per identificarne i punti deboli da attaccare. Persino le azioni più semplici, come il blocco degli accessi non autorizzati alla rete, il monitoraggio del traffico di dati o l'installazione di patch possono apparire come minacce – soprattutto se non anticipate da una comunicazione chiara e trasparente – e ciò in considerazione della difficoltà di geolocalizzare, tanto più in tempo reale, le infrastrutture coinvolte e dell'estrema rapidità con cui si svolgono i processi digitali, lasciando poco tempo per analizzare e comprendere correttamente le intenzioni che si celano dietro qualsiasi azione. In diversi casi, persino un'operazione dichiaratamente difensiva come il c.d. cyber counterattack (o hacking back) può essere facilmente percepita come una forma di aggressione nel dominio cibernetico[95]. Questo può avvenire, ad esempio, nel caso in cui la disattivazione dei server che ospitano malware o veicolano il flusso di dati di un attacco colpisca le dotazioni di uno Stato-terzo non coinvolto nel conflitto informatico.

Sebbene quanto qui descritto, in fin dei conti, non si discosti sensibilmente da interpretazioni altresì applicabili all'accumulo di truppe e armamenti in zone di confine oppure al dispiegamento di tradizionali sistemi militari di difesa aerea e missilistica – i cui vettori potrebbero essere agevolmente convertiti anche in funzione offensiva – l'intrinseca natura dual-use delle tecnologie informatiche non può che esacerbare le contese tra gli Stati, rendendo arduo discernere gli intenti sottesi alle operazioni cibernetiche[96]. Quasi per antonomasia, l'attacco Stuxnet del 2010 alle strutture nucleari dell'Iran esemplifica questa congenita ambiguità[97]. Mentre alcuni analisti considerano tale azione informatica alla stregua di un intervento difensivo rivolto a contenere – in chiave preventiva – la proliferazione nucleare, altri lo ritengono una grave violazione della sovranità dello Stato iraniano e un atto di aggressione. Tale irrisolvibile dicotomia,

---

[95] Si veda, inoltre: M. N. Schmitt, Tallinn Manual 2.0, cit., Rule 4, §§ 25-26, 24-25.

[96] Al riguardo, cfr.: I. Z. Saltzman, Cyber Posturing and the Offense-Defense Balance, in 34 Contemporary Security Policy 40 (2013); M. Robinson, K. Jones, H. Janicke, Cyber warfare: Issues and challenges, in 49 Computers & Security 70 (2015); R. Slayton, What Is the Cyber Offense-Defense Balance?, in 41 International Security 72 (2017).

[97] Il lancio del worm informatico Stuxnet è stato un attacco cibernetico sponsorizzato da Stati stranieri con l'intento di rallentare il programma nucleare dell'Iran, colpendo i sistemi di controllo delle sue centrali nucleari e le centrifughe per l'arricchimento dell'uranio. In tal modo, nel 2010, Stuxnet ha rappresentando il primo caso appurato di utilizzo di un virus informatico per danneggiare le infrastrutture fisiche critiche di uno Stato. Cfr. U. Gori, S. Lisi, Information Warfare 2012, Armi cibernetiche e processo decisionale, Milano, 2013; K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York, 2015.

ovviamente, deriva in gran parte dall'accezione dei fatti sposata dalle autorità a beneficio delle proprie scelte di politica estera, così come dalla prospettiva giuridica in concreto applicata all'interpretazione delle diverse condotte. Pertanto, ciò che uno Stato può considerare una misura legittima, posta in essere per ragioni difensive, può essere percepito da un altro Stato come un atto di guerra deliberato e non provocato.

Nel dominio del cyberspazio, del resto, la distinzione tra offesa e difesa emerge spesso come una questione di mera prospettiva, nel dissolversi di logiche binarie che si infrangono inesorabilmente sugli scogli di un nuovo topos della complessità, dove nulla sembra esistere, dove tutto assume le vesti fumose dell'interpretazione e dove «se nulla è vero, allora tutto è permesso»[98]. Nel regno della guerra digitale, infatti, l'equivoco trascende l'opinione e gli strumenti di difesa e offesa possono davvero essere la stessa cosa. Uno Stato può realmente implementare sofisticate difese informatiche al fine di proteggere le proprie infrastrutture strategiche, ma quegli stessi strumenti potrebbero essere parimenti utilizzati per compiere operazioni offensive. I programmi firewall, i sistemi di rilevamento delle intrusioni e i meccanismi di crittografia possono essere riconfigurati per scopi offensivi, come la violazione delle strutture informatiche avversarie. Questa intrinseca ambiguità è ulteriormente complicata dalla segretezza che denota molte delle azioni attuate in rete, evidenziando ancor più la preoccupante inadeguatezza dei quadri giuridici tradizionali rispetto al conflitto cibernetico, dove un attacco potrebbe apparire inizialmente proporzionato al perseguimento di un obiettivo legittimo, per poi rivelare, nel lungo periodo, ulteriori effetti connessi a suoi aspetti mantenuti volutamente segreti e che potrebbero inficiare le iniziali valutazioni di proporzionalità.

3.2 Le problematiche riguardanti l'attribuzione di responsabilità nelle operazioni informatiche

L'attribuzione si erge a pietra angolare della definizione giuridica di responsabilità per atto illecito a livello internazionale. Tuttavia, proprio lo scoglio dell'attribuzione rimane tra le questioni più difficili da affrontare in riferimento alla guerra cibernetica, dato che le operazioni informatiche possono essere lanciate da ogni angolo del pianeta anche in modalità anonima, avvalendosi cioè di meccanismi di oscuramento oppure di agenti per procura (cc.dd. proxies). Queste criticità rendono spesso complicato – se non talvolta quasi impossibile – determinare quale Stato o gruppo non-statale sia effettivamente coinvolto nelle ostilità digitali, in un contesto reso ancor più indefinito dal ruolo dirompente assunto dall'IA nel plasmare le dinamiche del conflitto cibernetico[99]. Nel contesto del cyberspazio, tracciare le esatte coordinate d'origine di un attacco – a maggior ragione durante il suo svolgimento – può rivelarsi un compito particolarmente problematico,

[98] Il nucleo essenziale della dottrina Nizarita (XI sec.) consisteva della celebre massima "nulla è vero – tutto è permesso", ripresa secoli dopo da F. W. Nietzsche in Così parlò Zarathustra, cit., 1883-1885. Si veda anche: F. M. Dostoevskij, Brat'ya Karamazovy, 1879-1880 (trad. it.; I fratelli Karamazov, Milano, 1979, vol. II, 619, 623 e 680-681).

[99] Sull'argomento, cfr. T. C. Truong, Q. B. Diep, I. Zelinka, Artificial Intelligence in the Cyber Domain: Offense and Defense, in 12 Symmetry 410 (2020); M. E. Bonfanti, Artificial intelligence and the offense–defense balance in cyber security, in M. Dunn Cavelty, A. Wenger, op. cit., 64-79.

consistente nell'inseguire le "invisibili" tracce degli impulsi elettrici e delle onde elettromagnetiche in cui si sostanziano le intricate stratificazioni dei flussi di dati. A differenza degli atti di aggressione tradizionali, perpetrati per mezzo di armi fisiche, la fonte degli attacchi cibernetici è spesso nascosta da più strati di segnali reindirizzati tramite server intermediari e reti crittografate, che ne celano l'originale emanazione dietro un velo virtuale di intenzionale dissimulazione tecnica[100].

Il cyberspazio, con la sua architettura di anonimato, sfida pertanto l'assunto Corfù per cui ogni Stato ha il dovere di adoperarsi diligentemente, secondo lo "stato dell'arte", allo scopo di impedire che dal suo territorio traggano origine atti dannosi per altri Stati. Tale obbligo di diritto internazionale, quand'anche concordemente accolto dall'intera comunità degli Stati in riferimento al cyberspazio, presuppone livelli di trasparenza e cooperazione interstatale (nonché di self-restraint) da cui l'operato nel dominio di Internet degli attori statali de iure – e dei soggetti non-statali che spesso fungono loro da schermo de facto[101] – è purtroppo ancora lontano. La natura della cyber warfare è infatti simile agli artifici di un mondo in cui solo gli effetti sono visibili, mentre le cause rimangono artatamente nascoste. Senza la chiara attribuzione della "paternità" di un atto di matrice cibernetica, la capacità di reagire in modo ad esso proporzionale resta in nuce ostacolata dall'impossibilità di direzionare compiutamente i propri sforzi, facendo sì che il principio di sovranità, il divieto di intervento, le regole per l'autodifesa e gli stessi canoni di legittimità per la rappresaglia quasi perdano il proprio fondamento logico-giuridico. Sul campo di battaglia "fantasma" in cui imperversa il nuovo Leviatano digitale, la necessità primaria di identificare gli aggressori esige dunque nuovi metodi digitali di analisi forense, atti a rinvenire prove che siano capaci di vincere gli inganni di una realtà che si conferma sfuggente ed "eterea" agli occhi della percezione[102].

Se, da una parte, le risorse della dottrina affermano che sugli Stati incombe la responsabilità internazionale per qualsiasi atto illecito loro imputabile, incluse le azioni compiute nel cyberspazio[103], d'altro canto resta irrisolto il problema di dimostrare caso per caso il coinvolgimento, in via diretta o indiretta, di uno Stato in operazioni attuate nel regno digitale, dove resta comunque difficile stabilire affiliazioni aprioristiche e dove la distinzione tra amico e nemico può sfumare nelle contraddizioni di una schermaglia tra archetipi e univoche categorizzazioni. Gli attacchi informatici potrebbero del resto trarre origine da reti di hackers, da agenti

---

[100] Si veda: B. Kuerbis, B. Badiei, K. Grindal, M. Mueller, Understanding Transnational Cyber Attribution: Moving from "Whodunit" to Who Did It, in M. Dunn Cavelty, A. Wenger, op. cit., 220-237.

[101] Cfr.: art. 8 DARSIWA. Inoltre, cfr.: C. S. Allan, Attribution Issues in Cyberspace, in 13 Chi.-Kent J. Int'l & Comp. Law 55, 64 ss. (2013); A. Gianelli, Il contributo della dottrina italiana al tema della responsabilità internazionale degli Stati per fatto illecito: qualche osservazione, in Riv. dir. int., 99, 2016, 1042-1070

[102] Cfr.: G. Mezzour, K. M. Carley, L. R. Carley, Remote Assessment of Countries' Cyber Weapon Capabilities, in 8 SNAM 62 (2018).

[103] Cfr.: M. N. Schmitt, Tallinn Manual 2.0, cit., Rules 14-19 (Law of international responsibility).

sponsorizzati da uno Stato, da sistemi malware automatizzati o persino dalle decisioni autonome di macchine intelligenti, trasferendo il contenuto del concetto di sovranità dal campo di certezza positiva del controllo dei confini fisici, segnati dalla geografia, a quello ancora eticamente fluido e giuridicamente acerbo dell'affermazione del controllo su informazioni e reti digitali[104]. Nel contesto dell'agone cibernetico, la controversa "decisione sull'eccezione"[105] abbandona quindi lo status di evento intrinsecamente singolare per riguadagnare un piano di inusitata "normalità" nella vita dello Stato, giustificata non solo dalla spada di Damocle di imprevedibili atti di anonima distruzione digitale ma, soprattutto, dalla costante minaccia di sabotaggi "a bassa intensità", dallo spionaggio informatico (si pensi al caso SolarWinds[106] o agli attacchi DDos – Distributed Denial-of-Service) e dalla diffusione in rete di c.d. "disinformazione". Atti ostili, questi ultimi, che sfruttano una zona grigia tra etica e diritto in cui la linea tra una difesa giustificata e una sconsiderata escalation resta pericolosamente confusa, rendendo palesi i persistenti limiti di un approccio puramente legalistico alla tematica della sicurezza informatica internazionale, come tale pervaso dal dissidio antinomico tra garanzie di tutela e di effettività[107].

Recependo il progetto filosofico dell'impegno internazionale "per la pace perpetua"[108], lo Statuto delle Nazioni Unite del 1945 immagina un mondo in cui gli Stati risolvono le loro controversie tramite la diplomazia e l'applicazione di un diritto "cosmopolitico" incardinato sui principi giuridici necessari per garantire la pace, la giustizia e l'ordine internazionale, così come i diritti e le libertà individuali. Nel caso della guerra informatica, la mancanza di immediata chiarezza nell'attribuzione di responsabilità crea pertanto una profonda incertezza epistemica, minando la fiducia tra le nazioni e indebolendo la forza deterrente del diritto internazionale, dato che gli Stati potrebbero percepire anche le azioni cibernetiche più devastanti come espedienti – a basso rischio e con costi contenuti – per conseguire obiettivi illeciti, in maniera del tutto scevra da conseguenze. Non sorprende, allora, che gli Stati siano costretti ad assumere decisioni partendo da informazioni incomplete, ambigue o addirittura fuorvianti, aumentando così la probabilità che gravi conflitti – anche sul piano della guerra tradizionale – possano fare seguito a errori di valutazione. Venuto meno il caposaldo dell'attribuzione, la strada della self-defense (individuale o collettiva) ai sensi dell'art. 51 della Carta

---

[104] Cfr. N. C. Rowe, Distinctive Ethical Challenges of CyberWeapons, in N. Tsagourias, R. Buchan, op. cit., 388-405.

[105] Dacché «Sovrano è colui che decide sull'eccezione». C. Schmitt, Politische Theologie: Vier Kapitel zur Lehre von der Souveränität, 1922.

[106] Diversamente da Stuxnet – che aveva chiari obiettivi di rango militare – l'attacco SolarWinds del 2020 è stato incentrato sull'intelligence piuttosto che su un'azione mirata di sabotaggio. Attribuito ad attori statali russi, l'attacco SolarWinds ha compromesso le funzionalità di migliaia di reti, incluse quelle di agenzie governative statunitensi e di aziende private. Cfr. A. Coco, T. Dias, T. van Benthem, Illegal: The SolarWinds Hack under International Law, in 33 EJIL 1275 (2022). Si veda, inoltre: M. N. Schmitt, Tallinn Manual 2.0, cit., § 27, 25 (con ulteriore riferimento alla Rule 19 e alla Rule 32).

[107] In un suggestivo parallelismo, si veda C. Schmitt in Die Theorie des Partisanen (1923) e Der Begriff des Politischen (1932) e la sua critica del "diritto liberale".

[108] Cfr. I. Kant, Zum ewigen Frieden: Ein philosophischer Entwurf, 1795-1796.

dell'ONU rimane irta di dubbi e incongruenze, che vanno ad aggiungersi alle numerose perplessità che possono di volta in volta accompagnare la formale equiparazione di un attacco virtuale a un attacco armato, aprendo le porte ai pericoli insiti nelle interpretazioni politiche e "di parte" destinate a subentrare dinanzi all'arretramento del diritto[109].

L'avvento dell'IA sta per giunta segnando l'alba di un'ulteriore rivoluzione nella dimensione – già sui generis – della cyber warfare. Alla luce della sua capacità di assumere rapidamente decisioni complesse sulla base di un fulmineo riconoscimento di schemi e informazioni[110], l'IA presenta infatti sia opportunità che sfide di portata epocale per gli Stati per il modo in cui sta quasi inerzialmente trasformando la conduzione delle operazioni informatiche, in senso tanto difensivo quanto offensivo. Se, da un lato, il ricorso all'IA è sempre più diffuso – visto il suo contributo al miglioramento della sicurezza dei sistemi informatici, per via del rilevamento in tempo reale di potenziali vulnerabilità infrastrutturali o di codificazione – dall'altro versante, i sistemi di intelligenza artificiale possono avvalersi dei propri algoritmi di apprendimento automatico non solo per rilevare eventuali azioni insolite e i rischi per una rete ma anche per concepire e avviare, del tutto autonomamente, operazioni preventive volte ad anticipare possibili attacchi informatici, azzerando così il problema dei tempi di risposta. I sistemi guidati dall'IA, inoltre, possono essere utilizzati per creare programmi malware adattivi che si evolvono in base all'ambiente di sistema del loro obiettivo, rendendo estremamente arduo il loro rilevamento e la loro completa rimozione. Oltre a presentare notevoli implicazioni etiche, il superamento della supervisione umana dei processi informatici solleva pertanto profondi interrogativi sul tema del soggetto-persona-ente quale centro di imputazione della responsabilità per le decisioni assunte in via autonoma dalle macchine pensanti. I sistemi di IA aggiungono un altro livello di difficoltà alla problematica dell'attribuzione e della responsabilità internazionale per le cyber operations, considerata la completa autonomia delle macchine nel decidere azioni tanto in tempo di pace quanto nel contesto di un conflitto informatico. Nel tentativo di colmare il divario apparentemente insanabile tra il diritto internazionale del mondo materiale e l'anarchia del "pleroma" cibernetico, questo dilemma si dimostra districabile soltanto se inquadrato ancora una volta nella cornice ermeneutica della c.d. due diligence, così come avvalorata dalle posizioni dottrinarie e dalla rilevante giurisprudenza internazionale. Una volta stabilito che sullo Stato gravi l'obbligo di condotta di non consentire che attività informatiche svolte nell'ambito della sua giurisdizione causino danni significativi ad altri Stati, tale dovere di "neutralità digitale" non potrà che estendersi implicitamente alle molteplici pertinenze site all'ombra della sua autorità, ivi compresa la responsabilità per le azioni delle macchine "senzienti", alla luce dei molteplici rischi impliciti[111] al loro funzionamento al servizio di interessi statali così come di soggetti non-statali. Tutto ciò, fino a configurare

[109] Si veda, in proposito: Consiglio dell'UE, Cyber Diplomacy Toolbox, 9916/17, cit., § 4.

[110] Cfr. I. H. Sarker, AI-Driven Cybersecurity and Threat Intelligence. Cyber Automation, Intelligent Decision-Making and Explainability, Berlino, 2024.

[111] Per un approfondimento sul concetto di "regolazione del rischio" nell'orizzonte della complessità, cfr. R. De Giorgi, Il diritto nella società del rischio, in 3 Revista Opinião Jurídica 395 (2005); Id., Temi di filosofia del diritto, Lecce, 2015.

l'ipotesi di una responsabilità internazionale di tipo oggettivo (e assoluto) in capo allo Stato per gli eventi critici legati all'operatività dell'IA nel cyberspazio, sulla scorta della disciplina internazionale prevista per le attività condotte nello spazio esterno extra-terrestre[112]. Tale soluzione, del resto, potrebbe emergere in risultato di un'oculata combinazione delle diverse preoccupazioni legate alla sicurezza, alla prevenzione dei danni e alla necessità di promuovere la fiducia e la cooperazione interstatale nello sfruttamento pacifico della dimensione digitale, alla luce della valutazione dell'elevato rischio intrinseco, dell'imprevedibilità, della latenza di eventuali errori di calcolo o programmazione e delle difficoltà attributive di accadimenti dall'impatto potenzialmente devastante – nonché dell'esigenza di garantire risarcimenti rapidi e certi – in relazione alle attività cyberspaziali dei computer intelligenti.

3.3 Ambiguità causali nella guerra informatica

Nel panorama della cyber warfare, la concatenazione tra causa ed effetto rappresenta un'altra criticità con cui l'applicazione del diritto internazionale è chiamata a cimentarsi. A differenza degli attacchi effettuati con metodi convenzionali, in cui le conseguenze sono perlopiù immediate e visibili, le operazioni cibernetiche dimostrano con elevata frequenza la predisposizione "dolosa" alla produzione di effetti ritardati, in quanto tali ancor più facili da occultare e, mutuando dalla sfera penale, si può altresì notare come tali atti tendano a manifestare un'intrinseca inclinazione all'aberrazione e alla degenerazione preterintenzionale, in ragione della causazione di una pluralità di scaturigini indirette (quand'anche in principio involontarie). La disconnessione temporale tra evento e risultato – al pari della potenziale elefantiasi dell'orizzonte della comune sequenzialità causale – infrange i crismi della tradizionale logica di causalità lineare e sembra introdurre l'idea che le leggi che hanno finora retto la rilevanza giuridica del concetto di consecutio, sotteso all'ordine naturale di causa-effetto, debbano essere riviste al fine di ricomprendere la poliedricità dell'impatto materiale delle forze "invisibili" che imperversano nella virtualità del digitale.

La natura dispersa delle operazioni cibernetiche, l'asincronia dei loro impatti concreti e la loro attitudine a scatenare imprevedibili effetti-domino complicano notevolmente il tracciamento della molteplicità dei legami causali e la giustificazione di un atto di attacco o difesa digitale ai sensi del diritto internazionale dei conflitti, ostacolando in particolare la valutazione della proporzionalità e il rispetto del principio di distinzione. Un attacco informatico contro un istituto finanziario potrebbe infatti non determinare l'immediata paralisi della sua operatività, ma potrebbe gradualmente generare instabilità e turbolenze sistemiche, anche non direttamente volute, che potrebbero tuttavia provocare nel tempo il crollo del mercato finanziario e la

[112] Si vedano: Trattato sulle norme per l'esplorazione e l'utilizzazione, da parte degli Stati, dello spazio extra-atmosferico, compresi la Luna e gli altri corpi celesti (Outer Space Treaty) del 1967, artt. VI e VII; Convenzione sulla responsabilità internazionale per danni cagionati da oggetti spaziali (Liability Convention) del 1972, art. II e IV.1. Il regime previsto si applica anche agli oggetti spaziali lanciati da soggetti non-statali, con lo Stato di lancio responsabile in ultima istanza.

completa perdita di risorse da parte di piccoli ed inermi risparmiatori, nonché fallimenti a cascata nel tessuto bancario ed economico di un intero paese. Allo stesso modo, un virus informatico potrebbe essere segretamente impiantato nel sistema di gestione della rete elettrica di uno Stato anni prima della decisione sulla sua attivazione, ma le modifiche sistemiche prodotte dal suo avviamento potrebbero continuare a interferire con il funzionamento delle infrastrutture colpite anche dopo la sua rimozione e, dunque, provocare ancora blackout in scuole e ospedali a causa della gravità e della diffusione delle lesioni prodotte o anche solo dell'inquinamento delle linee di codice dei programmi adibiti al controllo della rete energetica.

Dinanzi alle capacità distruttive della guerra informatica – e in considerazione del carattere statuale (e, quindi, non meramente individuale) dei soggetti che sarebbero in ultimo chiamati, in via diretta o indiretta, a rispondere delle sue implicazioni ai sensi delle possibili evoluzioni del diritto internazionale discusse in questa sede – l'analisi della "cyber-causalità" potrebbe pertanto rielaborare il legame complementare tra i concetti di "potenzialità" e "attualità" delle conseguenze di una specifica operazione cibernetica, fino sublimarne la dicotomia (propria di una lettura ancora ispirata a una concezione "umana" della causalità) in un'endiadi giuridica tra potenza e atto dove "ciò che potrebbe accadere" possa fondersi con "ciò che è davvero accaduto" e dove il rapporto diacronico tra le idee aristoteliche di δύναμις (dynamis) ed ἐνέργεια (enèrgheia) possa tradursi in una εντελέχεια (entelecheia) unitaria e sincronica atta a vanificare gli artifici della non-simultaneità. La tradizionale nozione giuridica di proporzionalità potrebbe dunque essere ridefinita nel senso di includere anche quelle conseguenze secondarie e/o a lungo termine che eccedano gli obiettivi diretti dello Stato ma di cui quest'ultimo appaia comunque "accettare" l'eventualità nel momento in cui sguinzagli i suoi mezzi informatici contro un altro Stato, oppure qualora renda proprie le operazioni di soggetti terzi anche solo non facendo nulla di quanto ragionevolmente in suo potere per impedirle o contenerle. Coerentemente, il diritto internazionale dovrebbe adattarsi alle peculiari caratteristiche della guerra informatica, contemplandone i potenziali effetti differiti o a cascata su più settori e considerandone espressamente gli effetti imprevisti o involontari (ma di cui l'autore abbia di fatto accettato "il rischio")[113] come nel caso paradigmatico delle vittime civili "secondarie" derivanti dal protrarsi del mancato funzionamento della rete elettrica pubblica negli ospedali.

---

[113] A titolo di astratto esercizio teorico ed euristico – teso ad avvalorare la riflessione sulla responsabilità dello Stato per le possibili implicazioni multilivello delle operazioni informatiche condotte contro altri Stati (o territori) – e rifuggendo da ingenui tentativi di "antropomorfizzazione" dello Stato, così come da un'impropria connotazione "penalistica" del sistema internazionale, alla stregua di un qualsiasi ordinamento interno, si inserisca il ragionamento qui in essere nel quadro ermeneutico della preterintenzionalità e del c.d. dolo eventuale, eccezionalmente declinati in chiave collettiva e istituzionale.

Conclusioni: verso un moderno Ius Publicum Cyberneticum (IPC)?

La capacità di direzionare le forze dell'invisibile per organizzare lo spazio fisico e arginare l'imperio del caos ha da sempre costituito la più alta forma del potere nonché la prima ragione storica del suo accentramento e della sua istituzionalizzazione nella figura del sovrano detentore dell'autorità e della cerchia (in specie, clericale) dei suoi ministri[114]. Nell'era dell'interconnettività digitale, il cyberspazio non può dunque che imporsi come arena centrale per la rivalità geopolitica. In questo dominio, infatti, il potere si manifesta come un "atto di volontà", non limitato da contingenze fisiche ma esercitato con mani (all'apparenza) "invisibili" capaci di liquefare la spazialità e influenzare il funzionamento di sistemi distanti, dirigendo correnti di dati piuttosto che truppe e armamenti. La sovranità trasmuta in una forma di presenza virtuale rimessa all'ideale intenzionalità dello Stato, che può quindi scegliere di rivendicare il "doppione digitale" del suo territorio geografico, così come di sfidare la sovranità di altri Stati su un campo di battaglia "fantasma" nel quale azioni e reazioni lasciano di sé riflessi infranti che si dissolvono nell'astrazione. L'emergere del cyberspazio come nuovo terreno di conflitto rivela una profonda trasformazione dell'essenza del potere. La dottrina classica del diritto internazionale – basata su definizioni concrete di territorio, aggressione e difesa – tendono a trovarsi inadeguate di fronte a una dimensione in cui causa ed effetto non sono vincolati da linee dirette e dove persino il concetto di "pace" degrada nell'etichetta formale di fasi (anche prolungate) di ostilità a c.d. "bassa intensità", che non è tuttavia possibile caratterizzare apertamente come "guerra". Questa rivisitazione della sovranità dello Stato risuona come un'affermazione di comando sui flussi di informazioni, sulle infrastrutture digitali e sui fili intangibili di influenza che modellano gli affari globali, dove il sovrano torna a rivendicare gli spazi del suo dominio cibernetico attraverso un rinnovato "diritto di spada"[115]. Mentre il conflitto migra nel cyberspazio, il diritto internazionale affronta pertanto una prova di portata senza precedenti nel governare la guerra informatica, vedendo minati i tradizionali confini definitori della sovranità e della responsabilità internazionale dello Stato. In questo dominio dalle fattezze (a prima vista) "eteree", dove i confini sono "invisibili" e i vincoli della causalità oscurati, l'"invisibile" diventa primario e il fisico si ritira nella periferia, disegnando una nuova dimensione biopolitica[116] in cui non solo gli Stati, ma anche entità private (come le aziende dell'hi-tech) possono manipolare i flussi di informazioni e condurre una sorveglianza di massa. L'affermazione globale del Leviatano digitale riflette quindi una radicale rivisitazione nella natura del potere politico e militare, incentrata sul regno digitale come teatro di competizione globale. Questa arena apparentemente intangibile rappresenta del resto un "territorio" che non può essere conquistato in senso

[114] Suggestione tratta da: E. Lévi, Dogme et Rituel de la Haute Magie (Vol. I e Vol. II), 1854-1855. Si rammenti, oltretutto, che «l'ignoranza non è una protezione» e, in questo mondo, ogni forza che può essere usata in modo dannoso, può essere sorvegliata indagandone fino in fondo la natura. Cfr. W. W. Atkinson, The Secret of Mental Magic, Chicago, 1907.

[115] Si colgano gli echi del pensiero di J. Bodin, Six livres de la République, 1576. In particolare, Libro I, Cap. 10.

[116] Cfr. M. Foucault, Histoire de la sexualité, 1: La volonté de savoir, 1976.

convenzionale e che, di conseguenza, si pone intrinsecamente in contrasto con i canoni dialettici ed ermeneutici di un sistema che vede proprio nell'effettiva "appropriazione di territorio" l'atto costitutivo del diritto di normare da parte dello Stato. Nondimeno, quanto detto si rivela paradossale, poiché il cyberspazio è comunque sostenuto da un'infrastruttura fisica (data centres, server, cavi in fibra ottica terrestri o sottomarini, satelliti etc.) che lo ancora in luoghi i quali, collocati all'interno dei confini statali, restano pienamente soggetti alle singole giurisdizioni nazionali. Il posizionamento fisico di infrastrutture materiali del cyberspazio negli Stati Uniti o in Russia, ad esempio, sottopone tali centri di elaborazione e trasmissione dei dati alle normative statunitensi o russe e individua le autorità di Washington o Mosca come i possibili centri di imputazione di responsabilità per i risvolti nocivi dell'operato oltreconfine di tali strutture. Tutto ciò suggerisce come il cyberspazio non sia in realtà un mondo del tutto "deterritorializzato" e separato dal controllo fisico, ma piuttosto un'estensione virtuale della solidità del potere territoriale. La nozione di territorio applicata al cyberspazio sublima i confini geografici in uno spazio virtuale popolato di infrastrutture cibernetiche attraverso cui scorre "influenza", delimitato da router piuttosto che da monti e fiumi, dove l'illusione dell'"etereità" si rivela meramente percettiva ed epifenomenica. La sovranità territoriale tende pertanto ad acquisire nuove fattezze, trasformandosi nel controllo sulle infrastrutture digitali e attribuendo agli Stati la responsabilità di evitare che operazioni informatiche dannose siano avviate all'interno dei loro confini digitali[117]. Come evidente, la nozione di "ordine spaziale" continua a fornire una lente di fondamentale importanza attraverso cui esaminare la guerra informatica contemporanea. Sebbene concettualizzata come "eterea" e "invisibile", la vera architettura del cyberspazio dimostra di condividere le costrizioni legate alle frontiere della geografia. Questa intrinseca dualità tra virtuale e territoriale richiede dunque una completa re-immaginazione del nomos come principio che integri sia l'infrastruttura fisica che la sua funzionalità virtuale, ridefinendo i confini tradizionali della sovranità statale e della responsabilità internazionale su di essa imperniata. In questi termini, la potestà sul territorio assume la

[117] Risulta indubbiamente interessante istituire un raffronto con il periodo della tarda-latinità. La lettura di elementi del Codex giustinianeo (Corpus Iuris Civilis, VI sec.) attesta come, in origine, il termine "territorio" sintetizzasse l'essenza della funzione giuridico-amministrativa esclusiva del sovrano, elevata alla stregua di uno "spauracchio" o Moloch posto a presidio dell'ambito spaziale soggiacente al monopolio dell'esercizio del potere e del "terrore" (e della morte) da parte del sovrano nei confronti dei propri sudditi (esseri umani, così come animali e cose), considerati "pertinenze naturali" del suo dominio sullo spazio terrestre. Verso la metà del XIV sec., il giurista Baldo degli Ubaldi giunse del resto a definire la giurisdizione come consustanziale al territorio il quale, come spazio politicamente definito, era "contenuto" nel terreno, quale luogo naturalmente determinato, allo stesso modo in cui sopra la palude, generata «dall'attiva potenza del suolo», insiste la nebbia come sua naturale emanazione (cfr. Baldus de Ubaldis, Commentaria in digestum vetus, VI.24.1, in Iurisconsulti Omnium, 7, folio 70v). Già il suo maestro, Bartolo da Sassoferrato – anch'egli, come il suo discepolo, tra i più influenti giuristi dello Ius commune medievale – aveva ridefinito il concetto di territorium come l'entità stessa su cui si esercita il potere politico, ovvero l'aspetto della territorialità su cui funzionalmente insiste il dominio giuridico (Bartolus de Saxoferrato, Consilia, quaestiones et tractatus, redatti tra il 1330 e il 1357). Nell'alveo di tale convergenza tra sostrato materiale ed elemento giuridico, «[t]erritory is [...] not just the limit of the jurisdiction» ma assurge a «its very definition», dando alla luce un modello teoretico di giurisdizione segnatamente restrittivo nella dimensione della territorialità, votato a vietare agli Stati l'esercizio di prerogative giurisdizionali ultra vires, ossia al di fuori dei propri confini geografici. Cfr. S. Elden, The Birth of Territory, Chicago, 2013, 231-232.

forma del (ragionevole) controllo, da parte dello Stato, su tutti i cc.dd. "beni comuni digitali" sottoposti alla sua giurisdizione territoriale, ovvero sull'intero novero delle infrastrutture e dei nodi di rete nazionali che rendono possibili i flussi di dati anche oltre i confini statali. Riconcettualizzando il cyberspazio come una rete di dimensioni sia fisiche sia digitali, possiamo d'altronde intendere la rete digitale come una sfera ibrida che richiede meccanismi di controllo e regolamentazione innovativi nel diritto internazionale. Ancora una volta, questi strumenti – in riconoscimento della natura duplice dello spazio cibernetico – non possono prescindere dal porre l'enfasi sul controllo territoriale e sulle divisioni spazio-politiche come fondamento dell'ordine giuridico. Il cyberspazio, quindi, può essere visto come un moderno "strato di territorialità", in cui i dati digitali fluiscono virtualmente attraverso i confini geografici pur rimanendo radicati nell'infrastruttura fisica. Finché il cyberspazio è ancorato a strutture materiali, gli Stati possono far rispettare le proprie leggi (e gli impegni internazionali in esse tradotti) ai centri di elaborazione dati posizionati all'interno dei loro confini così come alle aziende che operano sotto loro giurisdizione nazionale.

Il consesso delle Nazioni Unite, pur non potendo direttamente predisporre un quadro giuridico obbligatorio per i conflitti cibernetici, ha consentito notevoli passi avanti verso la creazione di norme ad hoc per la guerra digitale, attraverso l'operato dell'UNGGE nel campo della sicurezza informatica. L'iniziativa dell'ONU mira a creare un consenso sulla disciplina del comportamento degli Stati nel cyberspazio, delineando una condotta statale trasparente e responsabile che consenta di prevenire la deflagrazione di conflitti. Sebbene recepite da parte dell'Assemblea Generale dell'ONU, la natura non vincolante di tali raccomandazioni limita tuttavia la loro efficacia, sottolineando la necessità di concludere trattati internazionali sul tema o, almeno, di favorire il consolidamento consuetudinario di un'adeguata regolamentazione della guerra informatica che prenda mossa dagli strumenti giuridici esistenti e dal contributo della pertinente giurisprudenza della CIG. L'ascesa di normative regionali sulla protezione dei dati – come nel caso dei regolamenti dell'UE e delle convenzioni del Consiglio d'Europa – o di più stringenti controlli nazionali sulla rete Internet, come avvenuto in Cina e Russia, riflette comunque questa tendenza. Ad ogni modo, questi approcci giuridici rappresentano ancora visioni differenti e potenzialmente confliggenti di come dovrebbe apparire il cyberspazio, di chi dovrebbe controllarlo e di come gli Stati possano agire per proteggere i propri interessi nel contesto esteso del proprio Grossraum informatico. Non diversamente da come, in passato, le potenze europee gareggiarono per imporre il loro nomos particolare sui territori coloniali, gli Stati si contendono ora il diritto di definire le norme che governeranno il cyberspazio come nuovo orizzonte esistenziale, rendendo necessaria una struttura giuridica che tenga conto dell'immane posta in gioco, anche sul piano culturale e ideologico. Questo "eterno ritorno"[118] della competizione ha infatti portato a un mondo cibernetico frammentato, in cui ogni grande potenza pretende di far rispettare le proprie regole (se non addirittura di addurre la loro pretesa assenza) dentro la propria "sfera di influenza". Senza un'efficace regolamentazione internazionale, fondata su una reale

[118] Cfr. F. W. Nietzsche, Die fröhliche Wissenschaft, IV, n. 341 (Das größte Schwergewicht).

volontà di cooperazione da parte degli Stati, la progressiva "militarizzazione" dello spazio digitale potrebbe portare a un'inevitabile corsa agli armamenti – tanto informatici quanto "tradizionali" – con esiti devastanti per la sicurezza globale.

L'attuale regime giuridico internazionale riguardante l'uso della forza e lo svolgimento dei conflitti armati – pur continuando a fornire indicazioni preziose – rimane non direttamente applicabile all'ambito cyberspaziale, al pari dell'inerente contributo delle corti internazionali e della dottrina. Il diritto internazionale, dunque, si rivela perlopiù inadeguato per affrontare compiutamente le plurime sfaccettature della guerra informatica, a partire da una chiara definizione normativa di cosa costituisca un attacco informatico e di cosa ne possa integrare l'equiparazione a un attacco armato nelle trame "eteree" del cyberspazio, consentendo di innescare le previsioni della Carta dell'ONU in materia di diritto all'autodifesa[119]. Parimenti urgente, inoltre, si dimostra far luce sulle problematiche afferenti alla responsabilità internazionale dello Stato per le vicende del cyberspazio e superare le difficoltà che – sul piano pratico quanto giuridico – si frappongono a una chiara attribuzione di tali condotte (così come delle molteplici implicazioni e degli oneri da esse scaturenti) agli Stati, avvalendosi sia dell'innovazione tecnologica che degli strumenti della cooperazione internazionale. Di incalzante priorità si dimostra altresì l'esigenza di predisporre linee guida uniformi che definiscano la responsabilità statale per le operazioni informatiche poste in essere da attori non-statali, anche a prescindere dal fatto che tali entità agiscano autonomamente o per conto dello Stato. Proprio come in passato avvenuto per i trattati internazionali che hanno regolato gli armamenti nucleari, proibito l'impiego delle mine anti-uomo[120] o delle munizioni a grappolo[121], oppure vietato il ricorso ad armi di tipo biologico o chimico, è ora necessario provvedere alla regolamentazione dell'utilizzo delle armi informatiche nel cyberspazio. Nel tentativo di individuare, in ottica de lege ferenda, una possibile regolamentazione per lo scottante tema della cyber warfare, diverse discipline già in vigore nel diritto internazionale sono state oltretutto suggerite come applicabili, in via analogica, per fronteggiare le sfide giuridiche uniche poste dalla pretesa anarchia del mondo cibernetico. Tuttavia, in carenza di una specifica disciplina consuetudinaria o pattizia preposta – quale lex specialis – alla regolazione di questo settore critico, non è certamente possibile trascurare le problematiche ingenerate da peculiarità

[119] Si pensi a come, nel maggio 2019, lo Stato di Israele – dopo aver bloccato un cyber-attacco attribuito ad Hamas, abbia reagito cineticamente attraverso la propria aviazione militare, distruggendo l'edificio che, nel territorio di Gaza, ospitava il centro direzionale della divisione tecnologica del gruppo palestinese. Sebbene l'iniziativa digitale di Hamas sia stata preceduta da un'offensiva missilistica (dunque, anche fisica) verso il territorio di Israele, il bombardamento israeliano del quartier-generale informatico di Hamas rappresenterebbe il primo caso – del quale si abbia notizia – in cui uno Stato abbia risposto militarmente e in tempo reale ad un (tentativo di) attacco cibernetico. Cfr. AnalisiDifesa.it, 8 maggio 2019.

[120] Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, aperta alla firma il 3 dicembre 1997 a Ottawa, e in vigore dal 1º marzo 1999.

[121] Convention on Cluster Munitions (CCM), aperta alla firma il 3 dicembre 2008 a Oslo, e in vigore dal 1º agosto 2010.

congenite del diritto internazionale, dove la "legge" non è dettata da un esercizio di giurisdizione obbligatoria ad opera di un'autorità sovraordinata agli Stati – in espressione, ipso facto vincolante, di un potere internazionale ad essi superiore – ma è definita, ancora una volta, dai comportamenti assunti da parte delle medesime entità sovrane superiorem non recognoscentes che saranno poi chiamate ad attenersi ad essa.

Anche qualora si decidesse di mutuare de lege lata i nuovi codici di condotta per il cyberspazio dal sistema di obblighi già previsto nel quadro di altri settori del diritto internazionale esistente (i.e., la legge di neutralità, il diritto ambientale, le norme umanitarie, i trattati in materia di armamenti), qualsiasi evoluzione giuridica dovrà quindi essere avvalorata dall'effettiva prassi interstatale[122] – così come ad esempio riassunta nelle "posizioni" ufficiali espresse sulla materia, in via documentale, a firma dei competenti organi dei vari Stati – oppure sancita dalla ratifica di specifici accordi internazionali. Non essendo possibile prescindere da un consenso diffuso tra le grandi cyber-potenze (e, di fatto, anche tra i rispettivi giganti tecnologici privati), un compito assai arduo attende pertanto i fautori della "pace digitale". Date le visioni contrastanti in materia di sovranità e le frammentate pretese di controllo sul dominio informatico avanzate dai diversi protagonisti del cyberspazio, numerosi ostacoli sembrano oggi opporsi sulla strada verso l'instaurazione di un ordine giuridico universale che preservi la pace e l'ordine tra potenze in costante competizione, rendendo impervia la via verso l'affermazione di un moderno Ius Publicum Cyberneticum (IPC) che inquadri le interazioni informatiche tra Stati in una dimensione di stabilità, istituendo regole (e tutele) per un'efficace gestione dei conflitti[123].

---

[122] Rivolgendo lo sguardo verso la dimensione umanitaria della (futuribile) disciplina internazionale della cyber warfare, si configura peraltro l'opportunità di avvalorare la concezione propria della c.d. Clausola Martens, già presente nei preamboli delle Convenzioni dell'Aia del 1899 e del 1907, e richiamata dall'art. 1.2 del I Protocollo Addizionale (1977) alle Convenzioni di Ginevra del 1949, per cui – nella formazione di una nuova norma consuetudinaria afferente al diritto internazionale dei conflitti armati, in chiave di maggiore tutela umanitaria – il requisito oggettivo della diuturnitas assume minore rilevanza rispetto all'elemento soggettivo della percezione della doverosità sociale di una determinata condotta degli Stati (opinio iuris ac necessitatis). Del resto, secondo il dato letterale della celebre Clausola, frutto del contributo del diplomatico e accademico russo Fëdor Fëdorovič Martens: «En attendant qu'un code plus complet des lois de la guerre puisse être édicté, les Hautes Parties contractantes jugent opportun de constater que, dans les cas non compris dans les dispositions règlementaires adoptées par Elles, les populations et les belligérants restent sous la sauvegarde et sous l'empire des principes du droit des gens, tels qu'ils résultent des usages établis entre nations civilisées, des lois de l'humanité et des exigences de la conscience publique». Cfr.: CIG, Legality of the Threat or Use of Nuclear Weapons, cit., §§ 78-87; ICTY, Prosecutor v. Kupreškić et al., Case n. IT-95-16-T, 14 gennaio 2000, §§ 525-527.

[123] D'altra parte, non può sorprendere che gli Stati siano impegnati in una costante lotta per la supremazia, e che la sfera giuridica si configuri come una delle principali arene di questa competizione strategica tra visioni confliggenti di ordine internazionale. La novità, tuttavia, risiede proprio nell'attuale contesto geopolitico, in cui gli Stati fanno crescente ricorso a strumenti ibridi per aggirare le linee di demarcazione giuridica tra pace e guerra, e dove l'uso – o l'abuso – del diritto per conseguire un vantaggio operativo, tattico o strategico assume a sua volta i contorni di un vero e proprio lawfare. Rifuggendo (per quanto possibile) da logiche di mera autoreferenzialità, gli Stati dovrebbero pertanto prioritariamente rafforzare la propria capacità di difendere, sul piano giuridico, gli interessi nazionali, inscrivendoli compiutamente nella cornice vigente del diritto internazionale; e, solo in un secondo momento, sostanziare la propria "resilienza giuridica" a livello nazionale e internazionale, implementando meccanismi di deterrenza (individuale o collettiva) idonei a contrastare attività e "narrative" giuridiche ostili. Per una declinazione di tale approccio integrato al contrasto delle cc.dd. minacce ibride, sotto gli auspici dell'UE e della NATO, cfr.: A. Sari, Blurred Lines:

La prassi e gli accordi di controllo sull'uso delle "armi cibernetiche" sono d'altronde gli unici strumenti internazionali in grado di aiutare a prevenire la proliferazione incontrollata di capacità informatiche di natura offensiva, stabilendo norme che impongano un approccio avveduto nei riguardi di tali strumenti, sia in tempo di pace sia in tempo di guerra, e configurino la messa al bando degli attacchi informatici ai beni e alle infrastrutture critiche civili (a partire da quelli di matrice cyber-cinetica, a maggior ragione se nella loro più recente versione "ibrida"). In ogni caso, si rivelerà essenziale perseverare in attività di sensibilizzazione presso tutte le sedi internazionali utili (in primis, le Nazioni Unite)[124] al fine di coltivare i riferimenti idonei a motivare l'uso responsabile del potere cibernetico e degli strumenti informatici da parte degli Stati, non mancando di promuovere pratiche virtuose di (auto)controllo in riferimento al lancio di operazioni informatiche in tempo di pace, nelle vesti di un Katechon[125] secolare che disincentivi approcci unilaterali e incoraggi la trasparenza, la condivisione di informazioni e lo svolgimento di esercitazioni congiunte, insieme alla conclusione di accordi di difesa e sicurezza collettiva contro le minacce comuni che continueranno a sorgere dal cyberspazio.

L'espansione della sovranità statale nel cyberspazio richiede infine che gli Stati esercitino la propria "sovranità tecnologica" secondo i canoni della ragionevole diligenza (due diligence) e della amministrazione responsabile (stewardship) delle risorse cibernetiche, assicurando che i rispettivi "territori digitali" non vengano utilizzati per violare la sovranità di altri Stati. In chiave prospettica, tale assetto giuridico non parrebbe peraltro precludere il (futuribile) consolidamento, sempre per via consuetudinaria o pattizia, di una responsabilità di

---

Hybrid Threats and the Politics of International Law, Hybrid CoE Strategic Analysis 4, gennaio 2018; Id., Hybrid threats and the law: Building legal resilience. Hybrid CoE Research Report 3, novembre 2021. In esatto riscontro, si considerino, da un lato, l'attivismo regolatorio dell'UE in relazione alla sfera digitale e, dall'altro, l'esempio dell'operato di ricerca interdisciplinare condotto dal Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), basato a Tallin. Rilevano, inoltre, le richiamate clausole di assistenza reciproca (art. 42.7 TUE) e solidarietà (art. 222 TFUE) nell'architettura dei Trattati europei, così come il framework di consultazione e coordinamento previsto dall'art. 4 del Trattato del Nord Atlantico (insieme a quanto deciso dagli organi dell'Alleanza in merito alla possibile applicazione del suo art. 5 alle evenienze della guerra cibernetica). Nondimeno, la vera deterrenza continua a implicare la forza (in primis militare, ma anche politica ed economica) e, nell'arena dell'agone internazionale, «il giusto [...] si giudica secondo l'eguaglianza della necessità; ma i potenti fanno ciò che consente loro la loro forza, e i deboli subiscono ciò che devono» (Tucidide, La Guerra del Peloponneso, V, 89).

[124] In merito, cfr. UN, Our Common Agenda Policy Brief 9: A New Agenda for Peace, luglio 2023, Action 11, 26-28, e in particolare la raccomandazione: «Establish an independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct. This mechanism could enhance compliance with agreed norms and principles of responsible State behaviour. Strengthen criminal justice capacity to investigate, prosecute and adjudicate cyberactivity by terrorist actors against such infrastructure», 27. Cfr. F. Delerue, Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations, in 106 QIL, Zoom-in 521 (2024). Inoltre: M. Lehto, The Rise of Cyber Norms, in N. Tsagourias, R. Buchan, op. cit., 32-45; B. Hogeveen, The UN Cyber Norms: How Do They Guide the Responsible Development and Use of Offensive Cyber Capabilities?, in 7 CDR 123 (2022).

[125] Cfr. C. Schmitt, Politische Theologie, cit. Inoltre: 2 Tessalonicesi 2:6-7.

tipo oggettivo (e assoluto) da cyber-operations – tanto più se condotte ad opera del gòlem algoritmico dell'IA – sulla scorta di quanto già oggi previsto nel campo del diritto internazionale dello spazio esterno (extraterrestre). Nella cruciale fase della transizione verso una disciplina universale della guerra e della pace digitale, tuttavia, sarà ancora la tradizionale sovranità territoriale a porsi alla base dell'autorità di emettere giudizi decisivi nello "stato di eccezione" dettato dalle crisi informatiche. Il "diritto internazionale informatico" deve pertanto andare oltre l'astrazione e consentire risposte rapide ed efficaci, anche in chiave anticipatoria, alle molteplici minacce digitali, assicurando l'applicazione pratica dei principi giuridici alle concrete esigenze di sicurezza degli Stati. Ne consegue, come ovvio, che le potenze cibernetiche continueranno intanto a riconoscersi pienamente il potere di difendersi nel cyberspazio senza attendere il consenso internazionale, riservandosi il diritto di attuare politiche informatiche unilaterali nonché di attivare – nei casi in cui la sicurezza nazionale sia a rischio – Internet kill switch[126] emergenziali quali risorsa di ultima istanza per proteggere le infrastrutture critiche presenti nei loro "paesaggi digitali", intesi come estensione della loro sovranità fisica.

[126] Per un approfondimento sulla tematica, cfr.: P. Vargas León, Tracking Internet Shut Down Practices: Democracies and Hybrid Regimes, in F. Musiani, D. L. Cogburn, L. DeNardis, N. S. Levinson (Eds), The Turn to Infrastructure in Internet Governance, New York, 2015.

FONTI PRINCIPALI

- K. Ambos, “International Criminal Responsibility in Cyberspace”, in N. Tsagourias, R. Buchan (eds.), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2021.

- C. Antonopoulos, “State Responsibility in Cyberspace”, in N. Tsagourias, R. Buchan (eds.), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2021.

- L. Bannelier, “Is the Principle of Distinction still Relevant in Cyberwarfare? From Doctrinal Discourse to States’ Practise”, in N. Tsagourias, R. Buchan (eds.), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2021.

- R. Bartels et al. (eds.), Military Operations and the Notion of Control Under International Law. Liber Amicorum Terry D. Gill, Berlin, 2021.

- A. Bendiek, “The EU as a Force for Peace in International Cyber Diplomacy”, SWP Comment, 19, 2018.

- A. Bonfanti, “Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale”, Rivista di diritto internazionale, 102, 2019.

- V. Boulanin, N. Davison, N. Goussac, M. P. Carlsson, Limits on Autonomy in Weapon Systems. Identifying Practical Elements of Human Control, Stockholm, SIPRI, 2020.

- R. Buchan, “Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions”, Journal of Conflict & Security Law, 17, 2012.

- R. Buchan, I. Navarrete, “Cyber Espionage and International Law”, in N. Tsagourias, R. Buchan (eds.), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2021.

- A. Bufalini, “Uso della forza, legittima difesa e problemi di attribuzione in situazioni di attacco informatico”, in A. Lanciotti, A. Tanzi (eds.), Uso della forza e legittima difesa nel diritto internazionale contemporaneo, Napoli, 2012.

- C. Czosseck, R. Ottis, A.-M. Talihärm, “Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security”, International Journal of Cyber Warfare and Terrorism, 1, 2011.
- W. Davies, The Limits of Neoliberalism: Authority, Sovereignty and the Logic of Competition, London, 2014.
- F. Delerue, Cyber Operations and International Law, Cambridge, 2020.
- S. Duguin, P. Pavlova, The Role of Cyber in the Russian War Against Ukraine, PE 702.594, 2023.
- A. Ducheine, P. Pijpers, “The Notion of Cyberspace”, in N. Tsagourias, R. Buchan (eds.), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, II ed., 2021.
- S. Elden, The Birth of Territory, Chicago, 2013.
- D. P. Fidler, “Cyberspace and Human Rights”, in N. Tsagourias, R. Buchan (eds.), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2021.
- M. Ferruglio, “Cyber operation e responsabilità internazionale degli Stati: uno sguardo d’insieme”, in P. Ivaldi, S. Carrea (eds.), Spazio cibernetico, Genova, 2018.
- M. Foulon, G. Meibauer, “How cyberspace affects international relations: The promise of structural modifiers”, Contemporary Security Policy, 45, 2024.
- E. Greco, “Cyber war e cyber security: Diritto internazionale dei conflitti informatici, contesto strategico e strumenti di prevenzione e contrasto”, SIS, 11, 2014.
- O. A. Hathaway et al., “The Law of Cyber-Attack”, California Law Review, 100, 2012.
- H. Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge, 2012.
- M. Heidegger, “Die Frage nach der Technik (1954)”, in Vorträge und Aufsätze, Pfullingen, 1957.
- S. Hellman, C. Wagnsson, “How can European states respond to Russian information warfare? An analytical framework”, European Security, 26, 2017.

- S. Hill, "NATO and the International Law of Cyber Defence", in N. Tsagourias, R. Buchan (eds.), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2021.
- T. Hobbes, Leviathan, or the Matter, Forme, and Power of a Commonwealth Ecclesiasticall and Civil, 1651.
- ICRC – International Committee of the Red Cross, Position on Autonomous Weapons Systems, Geneva, 12 May 2021.
- Italian Government (MAECI), Italian Position Paper on "International Law and Cyberspace", 2021.
- ICJ, Corfu Channel (U.K. v. Albania), Judgment, 9 aprile 1949, I.C.J. Reports 1949.
- ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. U.S.), Merits, 27 giugno 1986, I.C.J. Reports 1986.
- ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996.
- ICJ, Application of the Genocide Convention (Bosnia v. Serbia), Judgment, 26 febbraio 2007, I.C.J. Reports 2007.
- PCIJ, The Case of the S.S. Lotus, Judgment n. 9, 7 settembre 1927, Series A, n. 10.
- J. Johnson, D. G. Post, "Law and Borders – the Rise of Law in Cyberspace", Stanford Law Review, 48, 1996.
- J. Kalpokiene, I. Kalpokas, "Hostes Humani Generis: Cyberspace, the Sea, and Sovereign Control", Baltic Journal of Law & Politics, 5, 2012.
- P. Kastelic, Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights, Geneva, UNIDIR, 2021.
- L. Kello, "Cyber Security: Gridlock and Innovation", in D. Held, T. Hale (eds.), Beyond Gridlock, Cambridge, 2017.

- I. Kilovaty, “Cyber Warfare and the Jus ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual”, American University National Security Law Brief, 5, 2014.
- H. Kissinger, Ordine mondiale (trad. it.), Milano, 2023.
- H. Lahmann, “On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace”, Duke Journal of Comparative & International Law, 32, 2021.
- W. J. Lynn III, “Defending a New Domain: The Pentagon’s Cyber Strategy”, Foreign Affairs, 89, 2010.
- M. M. Maas, “How viable is international arms control for military artificial intelligence?”, Contemporary Security Policy, 40(3), 2019.
- N. Machiavelli, Il Principe, 1513 (pubblicato 1532).
- F. Meneghello, M. Calore, D. Zucchetto, M. Polese, “IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices”, IEEE Internet of Things Journal, 2019.
- N. Melzer, Cyberwarfare and International Law, Geneva, UNIDIR, 2011.
- M. Mirti, “La disciplina giuridica del cyberspace: una panoramica…”, Opinio Juris, 3, 2016.
- D. Moore, Offensive Cyber Operations: Understanding Intangible Warfare, London, 2022.
- NATO, North Atlantic Council, Brussels Summit Communiqué, Bruxelles, 14 giugno 2021, §§ 31-32.
- E. Mavropoulou, “Targeting in the Cyber Domain: Legal Challenges…”, Journal of Law & Cyber Warfare, 4, 2015.
- E. A. Posner, A. O. Sykes, Economic Foundations of International Law, 2013.
- J.-J. Rousseau, Discours sur l’origine et les fondements de l’inégalité parmi les hommes, 1755.
- M. Roscini, Cyber Operations and the Use of Force in International Law, Oxford, 2014.

- M. Roscini, “World Wide Warfare: Jus ad bellum and the Use of Cyber Force”, in A. von Bogdandy, R. Wolfrum, C. E. Philipp (eds.), UNYB, Leiden, 2010.

- N. Ronzitti, Diritto internazionale dei conflitti armati, Torino, 2022.

- S. J. Shackelford, “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law”, Berkeley Journal of International Law, 27, 2009.

- M. N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, Tallinn, NATO CCDCOE, 2017.

- M. N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, Columbia Journal of Transnational Law, 37, 1999.

- P. B. Stephan, “Big Data and the Future Law of Armed Conflict in Cyberspace”, in M. C. Waxman, T. W. Oakley (eds.), The Future Law of Armed Conflict (The Lieber Studies), New York–Oxford, 2022.

- UN – Assemblea Generale, Resolution 3314 (XXIX), Definition of Aggression, 14 dicembre 1974; GGE Report A/70/174, 22 luglio 2015; OEWG Report A/77/275, 8 agosto 2022.

- K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon, New York, 2015.

Atti di convegno

La tecnica in difesa della dimensione sottomarina

Francesca Martini
ricercatrice di diritto amministrativo presso il Centro Alti Studi Difesa (CASD) -Scuola Superiore Universitaria

"The technique to defend the underwater dimension"

Abstract

The contribution analyzes the role of the technique in the defense functions of submarine cables. A reflection is proposed on the relationship between the European regulation of critical underwater infrastructures security and the regulation relating to the laying of cables and pipelines contained in the UNCLOS convention. After an examination of the two disciplinary ambitions and an analysis of the trend of investments in the underwater infrastructure market, the terms of the new relationship between public and private sovereignty are highlighted.

Keywords: digital sovereignty - underwater dimension - national security - telecommunications

1. La dimensione sottomarina come mercato concorrenziale non regolamentato

I fondali marini sono un ambito sfuggito alla regolazione nazionale ed europea, sono trattati, solo marginalmente nell'ambito della Convenzione delle Nazioni Unite sul diritto del mare (UNCLOS) del 1982, volta a disciplinare la navigazione e gli usi comuni del mare, da sempre configurato come una res communes omnium[1]. L'approccio del diritto internazionale è stato quindi, in prima battuta, determinato dal multilateralismo e dall'interesse a preservare la libertà del mare, strategica per navigazione e commerci[2]. Conseguentemente le attività sottomarine di posa di cavi e condotte hanno goduto della massima libertà non essendo soggette ad autorizzazioni e controlli, salvo che per i tratti posati nelle acque territoriali. Gli operatori che hanno iniziato a investire in infrastrutture subacquee hanno regolato i loro rapporti in via privatistica sulla base del principio di non interferenza[3].

Poste quindi queste caratteristiche, a seguito della globalizzazione dei servizi a rete e dei mercati dell'energia si è aperto un nuovo mercato, quello delle infrastrutture subacquee, molto appetibile per il ritorno in termini di profitti, e strategico per consolidare posizioni monopolistiche. Questo nuovo ambito di investimento è di grande interesse soprattutto perché ad oggi la possibilità di costruire infrastrutture sottomarine è ancora pressoché illimitata. Per ciò che concerne la posa di cavi sottomarini un ulteriore incentivo alla cablatura dei mari si rinviene nel fatto che la rete marina costituisce l'unica alternativa rispetto alla connessione satellitare, ancora lontana dal poter sostenere l'intera connessione dati mondiale in tempo reale. In questa prospettiva gli investimenti nella dimensione underwater hanno l'ulteriore significato di contrappeso al monopolio delle comunicazioni satellitari detenute da Starlink che già, in più occasioni, ha potuto incidere in modo

---

[1] Si rinvia a S. Romano, Corso di diritto internazionale, Padova, 1939, p. 194, il quale per connotare l'alto mare si riferisce immediatamente alla libertà quale principale caratteristica, poiché "il mare, tranne in quelle parti che appartengono ai singoli Stati, è posto dal diritto internazionale in condizione di libertà, il che vuol dire che esso non è res nullius in senso stretto, e perciò appropriabile, ma res communes omnium: così in pace come in guerra gli stati possono farvi navigare le loro navi adibite a servizi pubblici o a scopi mercantili, le quali rimangono esclusivamente sottoposte alle loro leggi, possono sfruttarne con la pesca le risorse, possono stabilirvi cavi telegrafici sottomarini, costruirvi isolotti galleggianti ecc.." con lucida lungimiranza lo stesso affermava che "il principio di libertà del mare non deriva, come spesso si è affermato dall'impossibilità fisica di attribuirlo ad uno a più Stati determinati, ma da ragioni di interesse e di opportunità internazionali"; si veda C. Schmitt, Sovranità dello stato e libertà dei mari, in Rivista di Studi Politici Internazionali, 1941, p.60; T. Scavozzi, Il mare nel diritto internazionale pubblico, in Dig. Disc. Pubbl., 1994, p.312 ss.; C. Tommasi, La Libertà dei mari, Ugo Grozio e gli sviluppi della talassocrazia olandese nel primo Seicento, in Scienza Politiche, 1997, p. 35. Si rinvia inoltre alla traduzione completa dell'opera in italiano di U. Grozio, De jure belli ac pacis, a cura di C. Galli e A. Del Vecchio, Napoli 2023, che ha contribuito a rivitalizzare il dibattito giuridico caratterizzato, tutt'oggi, da un rapporto di tensione fra universalismo normativo e diritto naturale.

[2] B. Conforti, Il regime giuridico dei mari, Napoli, 1957.

[3] Per un'analisi aggiornata dell'andamento degli investimenti nella dimensione underwater si veda A. Petrucci (a cura di), Industria dei cavi sottomarini. Tendenze di mercato e geopolitica, Astrid-on line, Atti del convegno 25 ottobre 2021.

determinante sui conflitti bellici in corso[4]. La constatazione dalla quale parte la presente analisi è che la libertà di posa di cavi e condotte sui fondali ha favorito la crescita e il consolidamento di veri e propri poteri sovrani privati nel campo digitale, dell'energia e delle comunicazioni[5] ormai sfuggiti alla regolazione economica dei mercati propria dei paesi a market status[6].

2. Brevi cenni agli investimenti in reti subacquee nei settori dell'energia elettrica e gas

Uno dei prossimi sviluppi attesi della dimensione subacquea consisterà nella realizzazione dell'infrastruttura per il mercato energetico globale da fonti rinnovabili[7]. I fondali marini sono già attraversati da una vasta tipologia di condotte elettriche delle quali si attende uno sviluppo esponenziale, soprattutto per il trasporto dell'energia prodotta dalle fonti rinnovabili. La produzione da energia rinnovabile, non potendo essere stoccata, oltre limitate quantità, necessita di una rete di distribuzione quanto più ampia e capillare possibile. Il collegamento alla rete nazionale in cui i parchi eolici sono installati non è sufficiente per garantire la distribuzione efficiente dell'energia, sarà perciò necessario collegarsi con le reti di altri paesi per potenziare interscambi di energia e rendere regolare l'afflusso nel momento in cui se ne ha bisogno. Gli investimenti nel settore puntano a costituire un mercato globale che ancora non ha un'infrastruttura capillare che massimizzi la distribuzione[8]. A differenza delle reti di trasporto dati nell'ordinamento italiano la rete elettrica è ancora

---

[4] Per un'analisi complessiva del fenomeno si veda A. Prakash, Come le aziende tecnologiche stanno plasmando il conflitto in Ucraina, in Le Scienze, 2 novembre 2022; P. Haski, France Inter, L'influenza di Elon Musk sulla guerra in Ucraina, Internazionale, Francia 12 settembre 2023.

[5]La protezione delle dorsali dati subacquee al di fuori delle acque territoriali dipende, ad oggi, dalla capacità strategica del settore privato di operare secondo gli standard decisi dall'International Cable Protection Committee, fondato nel 1958 del quale fanno parte amministrazioni governative e società commerciali che possiedono o gestiscono cavi sottomarini per telecomunicazioni o energia, nonché altre società che hanno interessi nell'industria dei cavi sottomarini, https://www.iscpc.org/about-the-icpc/.

[6]Per un'analisi del concetto di sovranità digitale di rinvia a G. Finocchiaro, La sovranità digitale, in Diritto Pubblico, Fasc. 3, 2022, p.809. ss. Per un'analisi empirica che compari gli approcci strategici cinesi, occidentali e statunitensi nella corsa alla cablatura degli oceani si veda L. Martino, Sovranità digitale e competizione geopolitica nel contesto dei cavi sottomarini: analisi comparata degli approcci di Cina, Stati Uniti e Unione europea, MEDIA LAWS, 2024, n. 2, p.144. Per un'analisi dell'andamento del mercato dei cavi sottomarini e del crescente peso degli investimenti delle big tech si rinvia inoltre a F. Bassanini, A. Perrucci, Industria dei cavi sottomarini. Tendenza di mercato e geopolitca, Atti del Convegno 25 ottobre 2021, Astrid on-line.

Per un quadro dell'andamento degli investimenti si veda lo studio di TeleGeography, The State of the Network, 2023 Edition, ove si analizza la domanda di banda a livello internazionale, che quasi raddoppia ogni due anni, alla quale le aziende rispondono sia con investimenti nelle reti esistenti e in nuove infrastrutture. AA

[7]La Banca Europea degli Investimenti (BEI) nel 2022 ha finanziato con 1,9 ml il Tyrrhenian Link che verrà realizzato da Terna S.p.a. che unisce la Sicilia alla Campania e alla Sardegna, per un totale di circa 970 km di collegamento, mille Mw di potenza e 3,7 miliardi di euro di investimento.

[8]Si veda S. De Michele, I cavi sottomarini per l'elettricità, in https://orizzontemarino.wordpress.com/2023/03/05/i-cavi-sottomarini-per-lelettricita/ consultato ultima volta il 5 marzo 2024.

caratterizzata dall'unicità della stessa, separata dal servizio, e gestita in modo unico attraverso Terna s.p.a. che provvede al dispacciamento[9] È tuttavia probabile, soprattutto se la produzione da fonti rinnovabili si concentrerà nei paesi del Nord Africa, che anche la rete elettrica possa in futuro subire duplicazioni infrastrutturali e proprietarie nelle acque internazionali. Anche le infrastrutture per il trasporto e lo stoccaggio del gas, ancorché con maggior rigidità stanno evolvendo e attraendo investimenti privati. Le infrastrutture italiane, fino agli anni duemila, erano quasi esclusivamente di proprietà di ENI, ma a seguito delle ripetute crisi energetiche dovute alla difficoltà di approvvigionamento del gas dalla Russia molti investimenti privati sono stati indirizzati su nuovi impianti di stoccaggio e trasporto del gas, molti dei quali localizzati in mare[10]. Lo stesso Nord Stream, che ha subito un sabotaggio nel tratto posizionato nella ZEE di Danimarca, vede intersecarsi investimenti diversi su un'infrastruttura strategica che, comunque, l'UE intendeva riassoggettare alle regole europee volte a impedire costituzioni di concentrazioni proprietarie fra la gestione della rete e la gestione del servizio nonostante l'assetto proprietario della società investitrice.

La progettazione e costruzione del gasdotto Nord Stream 2 è stata realizzata dalla società di diritto svizzero Nord Stream 2 AG, il cui azionariato è interamente detenuto dall'holding di stato russa Gazprom. Il finanziamento dell'intera opera, pari a EUR 9,5 miliardi, era tuttavia fornito per il 50% dalle società ENGIE SA (Francia), OMV AG (Austria), Royal Dutch Shell plc (Paesi Bassi e Regno Unito), Uniper SE (Germania) e Wintershall Dea GmbH (Germania)[11]. Il Nord Stream 2 una volta entrato in funzione sarebbe stato soggetto alla disciplina europea sull'"unbundling" di cui all'articolo 9 della Direttiva 2009/73/CE, ossia l'obbligo della separazione proprietaria tra le società che detengono la proprietà delle reti ed effettuano la gestione delle attività di trasporto e le imprese esercenti attività di approvvigionamento/produzione e fornitura di gas naturale. Va tuttavia evidenziato che anche sul mercato del gas naturale sta emergendo un crescente interesse alla costruzione di nuove infrastrutture di distribuzione e stoccaggio underwater che

---

[9] V. Balocco, Cavi sottomarini, dalla Bei ultima tranche da 500 milioni per il Tyrrhenian Link, Digital 360, 8 febbraio 2024, https://www.corrierecomunicazioni.it/digital-economy/cavi-sottomarini-dalla-bei-ultima-tranche-da-500-milioni-per-il-tyrrhenian-link/.

[10]Si rinvia a V. Barletta, L'esenzione dall'accesso alle essential facilities nel mercato del gas naturale, in F. Merusi, V. Giomi (a cura di), Principio di precauzione e impianti petroliferi costieri, p. 141 ss. Si veda inoltre A. Cavaliere, Liberalizzazione e accesso alle essential facilities: regolamentazione e concorrenza nello stoccaggio di gas naturale, in Politica Economica, n. 1, 2007, p. 32 ss. Per un aggiornamento delle misure di incentivo alla costruzione di rigassificatori si rinvia a T. Salonico, La parabola dei rigassificatori di gas naturale liquefatto. Una riflessione sulla urgente necessità di investire in nuovi terminali, in Mercato Concorrenza Regole, 2023, pp. 179-202.

[11]Per una dettagliata analisi degli assetti proprietari del Nord Stream 2 si rinvia alle vicende dell'impugnativa Nord Stream2/ Parlamento e Consiglio Causa T-526/19 RENV, e C-348/20 P - Nord Stream 2/ Parlamento e Consiglio, la questione controversa atteneva all'applicabilità della direttiva 2009/73/CE ai gasdotti da o verso Paesi terzi, ovvero all'applicazione dell'obbligo di separazione della proprietà fra gestore della rete e gestore dei servizi ai fini di non alterare la libera concorrenza e pregiudicare il mercato.

costituiscono uno dei presupposti principali della sicurezza economica degli stati. A tal fine l'UE ha coniato l'istituto giuridico dell' interconnettore ossia "quell'infrastruttura che comprenda non solo ogni gasdotto di trasporto che attraversa o si estende oltre una frontiera tra Stati membri allo scopo di collegare i sistemi nazionali di trasporto di tali Stati membri, ma ormai anche ogni gasdotto di trasporto tra uno Stato membro e un paese terzo fino al territorio degli Stati membri o alle acque territoriali di tale Stato membro" per estendere la disciplina europea ad ambiti marittimi extraterritoriali[12]

3. Il regime giuridico di cavi e condotte nel diritto del mare

Il diritto del mare tratta solo in via residuale le infrastrutture subacquee, la fonte di disciplina è la Convenzione delle Nazioni Unite sul diritto del mare (UNCLOS) del 1982 che fissa un regime globale degli oceani e dei mari, soprattutto con riguardo agli usi connessi alla navigazione. Si tratta di una disciplina che ha valenza erga omnes, poiché viene considerata diritto consuetudinario applicabile anche ai paesi che non l'hanno ratificata, ma che risale a un periodo in cui la tecnica relativa allo sfruttamento dei fondali era ancora molto arretrata e, perciò, le attività di sfruttamento e passaggio dei cavi e condotte avevano un peso economico e politico marginale, così come tutte le forme di sfruttamento minerario dei fondali oggi invece possibili[13]. Nelle acque territoriali[14] ciascuno stato ha piena giurisdizione ed esercita poteri sovrani anche sui cavi e condotte. La giurisdizione dello stato costiero sussiste quindi solo sul mare territoriale anche per ciò che riguarda la posa e le operazioni di manutenzione di cavi e condotte. Sussiste un potere regolatorio pubblico che può subordinare ad un atto autorizzatorio le attività di posa dei cavi a salvaguardia di interessi ambientali, archeologici o di sicurezza tipizzati dall'art. 21 dell'UNCLOS. In osservanza del generale spirito libero che ha improntato, da sempre, questa materia, gli ambiti nei quali introdurre limitazioni da parte degli stati non hanno riguardato questioni di difesa nazionale[15].

---

[12]Per quanto riguarda i gasdotti tra uno Stato membro e un paese terzo completati prima del 23 maggio 2019, l'articolo 49 bis, paragrafo 1, della direttiva 2009/73, come inserito dall'articolo 1, punto 9, prevede tuttavia che lo Stato membro nel cui territorio è situato il primo punto di collegamento di un simile gasdotto alla rete di tale Stato membro possa decidere di derogare agli obblighi previsti dalla direttiva 2009/73 per le sezioni di detto gasdotto situate sul suo territorio e nelle sue acque territoriali (in prosieguo: l'«articolo 49 bis»). Tale deroga è concessa per motivi oggettivi quali consentire il recupero dell'investimento realizzato o per motivi legati alla sicurezza dell'approvvigionamento, a patto che la deroga non abbia ripercussioni negative sulla concorrenza, sull'efficace funzionamento del mercato interno del gas naturale o sulla sicurezza dell'approvvigionamento nell'Unione europea, si rinvia alla recente Sentenza Del Tribunale Ue (Quinta Sezione ampliata) 27 novembre 2024, T-526/19 RENV.

[13]Si rinvia a F. Caffio, JP Pierini , La protezione delle infrastrutture critiche subacquee in tempo di pace: profili giuridici, in Rivista Marittima, luglio-agosto 2023, p. 40.

[14] Secondo la convenzione di Montego Bay ogni stato è libero di stabilire l'ampiezza delle proprie acque territoriali fino a un'ampiezza massima stabilita in 12 miglia marine dalla linea di base.

[15] Un'eccezione è rappresentata dalla normativa adottata da Malta, la Legge sulla Piattaforma continentale (Atto n. XXVIII del 2014) di Malta che all'art. 4 comma 1 prevede che "d) regulating the laying, maintenance and monitoring of submarine cables and pipelines which in the opinion of the Government of Malta could result in any unjustifiable interference with navigation, fishing, or the conservation or management of the natural resources of the sea, including the seabed and subsoil, or which could interfere

L'evoluzione del progresso scientifico e tecnologico ha inoltre determinato un nuovo interesse degli stati in ordine alla proclamazione delle Zone Economiche Esclusive (ZEE) sulle quali lo stato costiero esercita diritti sovrani, nei limiti dei diritti degli altri stati, fra gli altri, in materia di installazione e utilizzazione di isole artificiali, impianti e strutture con sfruttamento esclusivo delle risorse biologiche e minerali presenti nella colonna d'acqua sul fondo del mare e sottosuolo, sia le attività connesse con l'esplorazione e lo sfruttamento economico della zona quali la produzione di energia derivanti dalle correnti dall'acqua e dai venti. Il progresso tecnologico ha quindi indotto gli stati a sfruttare le prerogative conseguenti alla proclamazione della ZEE tanto che anche l'Italia, a seguito della proclamazione della ZEE da parte dell'Algeria che si sovrappone in buona parte alle acque territoriali italiane, ha proclamato con la legge 14 giugno 2021 n. 114, la propria ZEE. Questa nuova tendenza alla territorializzazione degli spazi marini si pone in contrasto con le politiche del passato che avevano privilegiato la libertà di navigazione e gli usi pubblici del mare a condizione di reciprocità.

In ogni caso anche nelle ZEE vige il principio della libertà di posa di cavi e condotte che trova fondamento nell'art. 70 dell'UNCLOS che si riferisce alla libertà di posa sulla piattaforma continentale. Solo il percorso dei cavi e condotte posati sulla piattaforma continentale è subordinato al consenso dello stato costiero. In occasione della posa di cavi e condotte gli stati devono tenere conto delle reti già posizionate e non devono pregiudicare la possibilità di riparare quelle esistenti[16]. Lo stato arcipelago è invece tenuto a consentire la manutenzione dei cavi che lo attraversano senza toccare la costa e a rispettare i cavi già posati sulla piattaforma continentale.

L'art. 87 in rispondenza del principio per cui l'Alto mare è aperto a tutti gli Stati sancisce la libertà di posa di cavi e condotte nel rispetto degli artt. 112-115, ossia nel rispetto delle infrastrutture già esistenti, senza pregiudicare il diritto di manutenerle e ripararle. La disciplina si completa con gli artt. 113-115 i quali dispongono in materia di rottura e danneggiamento imponendo agli stati di adottare disposizioni per tipizzare i casi di rottura dei quali rispondono le navi che ricadono sotto la giurisdizione di bandiera. Attraverso la disciplina interna gli stati dovranno inoltre prevedere le conseguenze giuridiche dei danneggiamenti, nonché prevedere misure di indennizzo per le perdite subite da una nave nell'evitare il danneggiamento di cavi o condotte[17].

---

with national defence or with marine scientific or other research or with submarine cables or pipelines".

[16] C. Cinelli, Il regime giuridico di condotte e cavi sottomarini, in (a cura di) A. Caligiuri, I. Papanicolopulu, L. Schiano Di Pepe, R. Virzo, Italia e diritto del mare, Napoli 2023.

[17] In Italia il Codice delle Comunicazioni elettroniche (D.L.vo 259 del 2003 all'art. 152) ha dato attuazione a questa disposizione.

4. La promozione della ricerca nel campo delle tecnologie subacquee come strumento di difesa nazionale

Le reti sottomarine sono state oggetto di un improvviso interesse da parte degli ordinamenti giuridici dei diversi stati nel momento in cui sono emersi rischi per la sicurezza dei servizi a fronte di rotture, anche di carattere malevolo, soprattutto dopo il caso Nord Stream. Fino all'emergere di rischi da ricondurre alle vicende belliche in essere le caratteristiche tecniche delle reti sono state appannaggio dei privati che hanno in autonomia portato avanti progetti di ricerca e innovazione al fine di commercializzare servizi affidabili e sicuri. In questa prospettiva il potenziamento dell'effetto ridondanza del trasporto dati che consente il reinstradamento del traffico in tempi velocissimi, ha costituito una ulteriore spinta all'intensificazione delle attività di posa dei cavi che ha concorso a fornire garanzia di continuità del servizio grazie alla diversificazione dell'infrastruttura. La possibilità di differenziare le reti e i percorsi offerta dalla libertà di posa è stato uno dei principali fattori di sicurezza dei sistemi che ha potuto seguire la naturale vocazione di un mercato concorrenziale senza regole. La sicurezza dell'infrastruttura è stata salvaguardata sfruttando proprio le infinite possibilità di duplicazione della stessa. Le reti in fibra sono state progettate e continuano ad essere implementate attraverso la progressiva inclusione di dispositivi tecnologici sempre più performanti e innovativi che, combinati con apparecchiature e linee di comunicazione, sono in grado di mantenere la connettività in caso di guasto del percorso principale o di una parte del collegamento[18].

Anche i percorsi fisici delle reti si stanno progressivamente differenziando, in origine seguivano le principali rotte marittime, ma oggi la differenziazione dei passaggi e degli approdi costituisce ulteriore garanzia di sicurezza e mantenimento del servizio in caso di guasto o sabotaggio. Proprio nel campo delle reti subacquee l'evoluzione tecnologica diventa un fattore dirimente per garantire la continuità e universalità del servizio veicolato, e, contestualmente, la promozione della ricerca scientifica e tecnologica costituisce un fattore dirimente per la sicurezza energetica, informativa ed economica di ogni paese. Oggi che la sicurezza di queste infrastrutture incide significativamente sulla sicurezza nazionale, al fine di garantire la sicurezza dei servizi che oggi supportano le stesse funzioni sovrane degli stati, il legislatore italiano ha riconosciuto nello sviluppo di attività di ricerca dedicate alla dimensione underwater uno degli asset strategici delle politiche di sicurezza nazionale[19]. Per questo è stato modificato il Codice dell'Ordinamento Militare inserendo una nuova competenza della Marina Militare. Il comma 1-bis all'art. 111 dispone che la Marina Militare promuove le attività per la valorizzazione delle potenzialità e della competitività del settore della subacquea nazionale, per la promozione delle connesse attività di ricerca e tecnico-scientifiche, nonché per il potenziamento delle

[18] T. Davenport, Intentional Damage to Submarine Cable Systems by States, HoovermInstitution, Stanford, 2023, University https://www.lawfaremedia.org/article/intentional-damage-to-submarine-cable-systems-by-states.

[19]Evidenzia il perdurante scollamento tra il ritmo dell'innovazione tecnologica e la capacità del diritto di rispondere in modo tempestivo Ciro Sbailù, Diritto e geopolitica nello spazio curvo del potere, dalla crisi dell'ordine moderno alla riconfigurazione strategica della sovranità nell'era della guerra ibrida, Rivista di diritti comparati, numero speciale 2025, p. 123 ss.

innovazioni e della relativa proprietà intellettuale. A tale fine, con decreto del Ministro della Difesa, di concerto con i Ministri delle Imprese e del Made in Italy e dell'Università e della Ricerca, è istituito e disciplinato il Polo Nazionale della Subacquea. Si tratta di una competenza del tutto atipica per l'ordinamento militare, ma di assoluto rilievo per connotare in termini nuovi l'importanza dell'innovazione tecnologica rispetto ai tradizionali strumenti di difesa e deterrenza. Il Polo Nazionale della Subacquea è stato istituito a ottobre 2023 e svolge attività di catalizzatore e centro di aggregazione di soggetti privati e pubblici che svolgono attività di ricerca tecnologica nel campo della subacquea. Lo scopo della disciplina che ha visto anche un primo stanziamento di risorse a valere già sul bilancio 2023 si propone di costituire un ecosistema della subacquea, per svolgere ricerca tecnico-scientifico, condividere informazioni e conoscenza, armonizzare standard e regolamenti, creare e sostenere reti di collaborazione, nonché supportare le attività sperimentali[20]. Quasi contestualmente il Piano del Mare ha previsto l'istituzione dell'Agenzia Nazionale per il controllo delle attività subacquee, incardinata presso la Presidenza del Consiglio dei Ministri, che si riferirà al Comitato Interministeriale per le Politiche del Mare e coniugherà compiti di carattere amministrativo-gestionale con azioni strategiche di carattere geopolitico[21].

5. Il riconoscimento della strategicità delle infrastrutture subacquee a livello europeo e la necessità di una mappatura dei rischi

L'UE ha tardato nel riconoscere le infrastrutture subacquee come infrastrutture strategiche. Un primo approccio alla regolazione della sicurezza dell'underwater è incidentalmente emerso nella direttiva NIS II, Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni. Il considerando 97 evidenziò come il mercato interno dipenda dal funzionamento di Internet e dai servizi forniti via internet. Al fine di garantire l'erogazione senza intoppi dei servizi forniti dai soggetti essenziali e importanti, è fondamentale che tutti i fornitori di reti pubbliche di comunicazione elettronica dispongano di adeguate misure di gestione dei rischi di cibersicurezza e segnalino gli incidenti significativi connessi[22]. In particolare, venne evidenziato che gli incidenti che interessano i cavi di comunicazione sottomarini dovrebbero essere segnalati al CSIRT o, se del caso, all'autorità competente ed

[20] Il Polo della Subacquea ha già pubblicato innumerevoli bandi di ricerca, fra i quali a titolo esemplificativo, si ricordano il bando per Studio e sviluppo di tecnologie e metodi innovativi per la navigazione di precisione in ambiente subacqueo, il bando per lo sviluppo di un sistema di cavi subacquei intelligenti per il monitoraggio marino, bando per lo Studio e sviluppo di batterie innovative a elevate prestazioni per applicazioni abissali ecc.

[21] Delibera PCM 31 luglio 2023, Approvazione del piano del mare per il triennio 2023-2025.

[22]F. Pizzetti, La UE e la sua sovranità digitale: i cavi sottomarini di trasmissione delle informazioni come strutture fondamentali nella sfida UE alla competitività digitale, atti del convegno Astrid, L'industria dei cavi sottomarini, Astrid-on line 2021; M.M. Minuto, La competizione strategica per il dominio delle infrastrutture critiche underwater, controllo e tutela delle dorsali dati, in Rivista Trimestrale della società Italiana per l'organizzazione internazionale, Quaderno 26, Napoli 2023 p. 22.

evidenziava la necessità di una mappatura dei potenziali rischi di cibersicurezza e l'individuazione di misure di attenuazione per garantire il massimo livello di protezione. Queste prescrizioni sono rimaste per lo più inattuate anche perché spesso gli incidenti o le interruzioni di cavi si sono verificate in acque extraterritoriali e non sono state segnalate ad autorità statali, prevalendo l'interesse dei gruppi privati a non divulgare informazioni che possano minare la propria immagine sul mercato dei servizi.

6. L'intervento europeo per la sicurezza e resilienza delle infrastrutture sottomarine

Successivamente la Commissione è intervenuta con la Raccomandazione 779 del 2024 sulle infrastrutture di cavi sottomarini sicure e resilienti, atto che entra maggiormente nel merito della materia prospettando nuove misure a protezione delle infrastrutture sottomarine, ma non vincolante per gli stati. Si tratta di un atto di indirizzo politico atipico proprio per il livello di elevato dettaglio che ha la finalità di indirizzare verso finalità comuni le politiche per la sicurezza marittima degli stati membri. In questa prospettiva emerge la configurazione delle reti come infrastrutture critiche che presentano profili di significativa rilevanza transfrontaliera nei settori dell'energia, dei trasporti, dello spazio e delle infrastrutture digitali.

La Commissione con questo atto esplicita chiaramente che l'ecosistema internet costituisce parte fondante della sovranità digitale europea che viene garantita attraverso le infrastrutture sottomarine, molte delle quali già valutate ad alto livello di rischio dal gruppo di cooperazione NIS. La commissione individua diverse tipologie di rischio legate all'ingerenza di paesi terzi su un fornitore, sui servizi di sicurezza o con atti diretti sulle infrastrutture fisiche sottomarine che vengono identificate, non solo nel cavo sottomarino, ma anche in qualsiasi infrastruttura connessa alla sua costruzione al suo funzionamento, alla sua manutenzione e alla sua riparazione[23].

La prima azione individuata dalla Commissione è quella di colmare il deficit informativo rispetto ai soggetti privati sulle infrastrutture sottomarine e stabilire meccanismi di cooperazione informativa fra gli stati e con la Commissione. Occorre raccogliere e aggregare dati sulla consistenza delle infrastrutture subacquee, sulla resilienza e sulla gestione della sicurezza delle medesime che ad oggi sono in mano privata. A livello europeo manca una mappatura delle reti e delle infrastrutture e le attuali fonti di studio e analisi sono quelle messe a disposizione da consorzi privati. La Commissione raccomanda agli stati di richiedere informazioni alle organizzazioni rappresentative delle imprese evidenziando che le valutazioni nazionali sarebbero più rilevanti se includessero una mappatura delle infrastrutture esistenti e programmate e se tenessero conto dei criteri di rischio per la sicurezza sia tecnici che non tecnici.

[23] Definizione art. 2 Racc. 779/24.

Si richiede agli stati di procedere a regolamentare i rapporti con i fornitori in modo da imporre ex ante vincoli informativi, ad esempio, in materia di modifiche apportate alle infrastrutture sottomarine. Dai toni della Raccomandazione emerge una piena consapevolezza del deficit di sovranità pubblica rispetto a questo ambito di rischio emergente. Solo i privati detengono le informazioni necessarie a ricostruire un quadro europeo aggiornato ed è pur possibile che gli Stati non riescano a vincolarli ad un obbligo informativo così stringente. Sicuramente questo deficit conoscitivo si accentua per quanto riguarda le infrastrutture posizionate immediatamente al di là delle acque territoriali sulle quali lo stato non ha alcuna giurisdizione. Gli stati dovrebbero inoltre incoraggiare gli operatori delle infrastrutture di cavi sottomarini a eseguire prove di stress periodiche ai fini di valutare rischi, vulnerabilità e dipendenza delle infrastrutture di cavi sottomarini.

La raccomandazione prevede poi uno specifico intervento dell'UE nel sostenere progetti di infrastrutture di interesse europeo sui cavi che coinvolgano almeno due stati membri e una o più isole, ovvero i paesi ultraperiferici o d'oltremare, nonché quei progetti che migliorino la connettività fra uno o più stati membri o paesi terzi.

I progetti dovrebbero essere finanziati su fondi privati che potrebbero essere sostenuti, nei limiti della disciplina degli aiuti di stato, da programmi dell'UE o dai singoli stati. Di rilievo per gli stati potrà essere l'inciso secondo il quale gli stati membri sono incoraggiati a valutare se si possa provvedere al sostegno dei progetti mediante l'acquisto di capacità per uso pubblico. Da una prima lettura della Raccomandazione pare potersi prospettare un primo tentativo di riconquistare una rilevanza pubblica nell'ambito del dominio privato delle infrastrutture sottomarine, peraltro ancora dai profili confusi e scarsamente efficace, posto che non esiste una linea di finanziamento dedicata e adeguata alla strategicità delle infrastrutture subacquee.

La dimensione underwater rappresenta un ambito nel quale l'esercizio dei poteri sovrani degli stati deve essere ricalibrato rispetto ad una nuova e sopravvenuta situazione di fatto in essere[24] della quale occorre prioritariamente ricostruire un quadro conoscitivo affidabile.

7. Il ritorno dell'intervento pubblico in economia

È a questo punto evidente che per estendere le protezioni data dall'applicazione delle norme europee oltre i confini territoriali e nelle acque internazionali dove non esiste un generale obbligo di cooperazione degli stati per la sorveglianza delle infrastrutture critiche, occorra un intervento delle istituzioni europee nel mercato.

[1]Per una riflessione sulla sovranità intesa come parte della definizione dello Stato si rinvia a C. Galli, Sovranità, Bologna, 2019.

Attraverso l'azionariato pubblico in imprese che operano nella dimensione underwater ovvero la realizzazione di partenariati per l'innovazione si mira a esportare oltre i confini delle acque territoriali la governance europea dei servizi.

Più in generale l'UE si propone di tutelare la sicurezza nazionale che presuppone la continuità dei servizi a rete anche attraverso l'esercizio di prerogative di stampo privatistico aumentando investimenti e presenza sui mercati di settore e mantenendo direttamente o indirettamente azionariati societari.

La stessa raccomandazione prevede che gli stati dovrebbero essere incoraggiati a cooperare per la riduzione delle dipendenze e la promozione dello sviluppo di infrastrutture anche presso paesi terzi, soprattutto nei paesi in via di sviluppo. Già sono stati varati diversi investimenti, in particolare, questo approccio, oltre a radicare in capo agli stati prerogative economiche, li inserisce nella competizione aperta a seguito degli investimenti cinesi che fanno capo al progetto della Nuova Via della Seta[25].

Sempre nella stessa ottica il G7 nel 2023 ha varato un progetto di rete Artica. Lo scopo è quello di creare una connessione diretta tra Giappone, Europa e Nord America, senza attraversare la Russia. I cavi posati nell'Artico sarebbero infatti complementari rispetto ai collegamenti esistenti nell'Area di Suez, e potrebbero garantire all'UE una nuova rilevanza nella contesa internazionale per la sovranità digitale[26].

---

[25] L'Italia ha varato diversi progetti di investimento in reti sottomarine allo specifico scopo di acquisire una posizione di vantaggio nel mercato internazionale dei cavi sottomarini uno dei più importanti è la costruzione di Blue-Raman che collegherà Francia e Italia per raggiungere il mercato emergente dell'India. Il valore strategico consiste nel proporre una rotta differenziata rispetto a Suez. Ad oggi il primo tratto, Blue è già operativo e differenzia il passaggio a Sud della Sicilia tracciando un nuovo percorso nello stretto di Messina. si veda A. Biondi, Cavi dati sottomarini, conto alla rovescia per la nuova rotta digitale Europa-Asia, Il Sole24Ore 26 giugno 2024.

[26] C. Di Gabriele, Perché il G7 vuole investire in un cavo sottomarino nell'Artico, Le Formiche, 17 marzo 2024.

FONTI PRINCIPALI

- Banca Europea degli Investimenti (BEI), “Finanziamento per il Tyrrhenian Link (1,9 mld)”, 2022.
- V. Balocco, “Cavi sottomarini, dalla Bei ultima tranche da 500 milioni per il Tyrrhenian Link”, CorCom – Digital360, 8 febbraio 2024, https://www.corrierecomunicazioni.it/digital-economy/cavi-sottomarini-dalla-bei-ultima-tranche-da-500-milioni-per-il-tyrrhenian-link/.
- F. Bassanini, A. Perrucci, Industria dei cavi sottomarini. Tendenze di mercato e geopolitica, Atti del Convegno Astrid on-line, 25 ottobre 2021.
- V. Barletta, “L’esenzione dall’accesso alle essential facilities nel mercato del gas naturale”, in F. Merusi, V. Giomi (a cura di), Principio di precauzione e impianti petroliferi costieri, s.l., s.e., s.d.
- A. Biondi, “Cavi dati sottomarini, conto alla rovescia per la nuova rotta digitale Europa-Asia”, Il Sole 24 Ore, 26 giugno 2024.
- A. Cavaliere, “Liberalizzazione e accesso alle essential facilities: regolamentazione e concorrenza nello stoccaggio di gas naturale”, Politica Economica, 1, 2007, 32 ss.
- F. Caffio, J. P. Pierini, “La protezione delle infrastrutture critiche subacquee in tempo di pace: profili giuridici”, Rivista Marittima, luglio-agosto 2023, 40 ss.
- C. Cinelli, “Il regime giuridico di condotte e cavi sottomarini”, in A. Caligiuri, I. Papanicolopulu, L. Schiano Di Pepe, R. Virzo (a cura di), Italia e diritto del mare, Napoli, 2023.
- B. Conforti, Il regime giuridico dei mari, Napoli, 1957.
- Delibera Presidenza del Consiglio dei Ministri, “Approvazione del Piano del mare 2023-2025”, 31 luglio 2023.
- T. Davenport, “Intentional Damage to Submarine Cable Systems by States”, Hoover Institution, Stanford, 2023; anche su Lawfare, https://www.lawfaremedia.org/article/intentional-damage-to-submarine-cable-systems-by-states.

- C. Di Gabriele, “Perché il G7 vuole investire in un cavo sottomarino nell’Artico”, Formiche.net, 17 marzo 2024.
- Codice delle comunicazioni elettroniche, D.Lgs. 1° agosto 2003, n. 259, art. 152.
- S. De Michele, “I cavi sottomarini per l’elettricità”, Orizzonte Marino (blog), 5 marzo 2023 (ultimo accesso 5 marzo 2024), https://orizzontemarino.wordpress.com/2023/03/05/i-cavi-sottomarini-per-lelettricita/.
- G. Finocchiaro, “La sovranità digitale”, Diritto Pubblico, 3, 2022, 809 ss.
- C. Galli, Sovranità, Bologna, 2019.
- U. Grozio (H. Grotius), De jure belli ac pacis, trad. it. a cura di C. Galli e A. Del Vecchio, Napoli, 2023.
- P. Haski, “L’influenza di Elon Musk sulla guerra in Ucraina”, Internazionale (da France Inter), 12 settembre 2023.
- International Cable Protection Committee (ICPC), “About the ICPC”, 1958-ongoing, https://www.iscpc.org/about-the-icpc/.
- Legge sulla Piattaforma Continentale (Malta), Act XXVIII of 2014, art. 4(1)(d).
- L. Martino, “Sovranità digitale e competizione geopolitica nel contesto dei cavi sottomarini: analisi comparata degli approcci di Cina, Stati Uniti e Unione europea”, MediaLaws, 2, 2024, 144 ss.
- M.M. Minuto, “La competizione strategica per il dominio delle infrastrutture critiche underwater, controllo e tutela delle dorsali dati”, Rivista Trimestrale della SIOI, Quaderno 26, Napoli, 2023, 22 ss.
- T. Salonico, “La parabola dei rigassificatori di gas naturale liquefatto. Una riflessione sulla urgente necessità di investire in nuovi terminali”, Mercato Concorrenza Regole, 2023, 179-202.
- C. Schmitt, “Sovranità dello Stato e libertà dei mari”, Rivista di Studi Politici Internazionali, 1941, 60 ss.

- C. Sbailò, “Diritto e geopolitica nello spazio curvo del potere, dalla crisi dell’ordine moderno alla riconfigurazione strategica della sovranità nell’era della guerra ibrida”, Rivista di diritti comparati, numero speciale, 2025, 123 ss.

- T. Scavozzi, “Il mare nel diritto internazionale pubblico”, Digesto delle Discipline Pubblicistiche, 1994, 312 ss.

- Sentenza Tribunale UE (Quinta Sezione ampliata), 27 novembre 2024, T-526/19 RENV, Nord Stream 2 AG / Parlamento e Consiglio.

- Sentenza CGUE, C-348/20 P, Nord Stream 2 AG / Parlamento e Consiglio, s.d.

- Direttiva 2009/73/CE (mercato interno del gas naturale), come modificata; art. 49-bis, par. 1 (deroghe per gasdotti con Paesi terzi).

- F. Pizzetti, “La UE e la sua sovranità digitale: i cavi sottomarini di trasmissione delle informazioni come strutture fondamentali nella sfida UE alla competitività digitale”, in L’industria dei cavi sottomarini, Atti del Convegno Astrid on-line, 2021.

- A. Petrucci (a cura di), Industria dei cavi sottomarini. Tendenze di mercato e geopolitica, Astrid on-line, Atti del convegno 25 ottobre 2021.

- A. Prakash, “Come le aziende tecnologiche stanno plasmando il conflitto in Ucraina”, Le Scienze, 2 novembre 2022.

- S. Romano, Corso di diritto internazionale, Padova, 1939, 194 ss.

- C. Tommasi, “La libertà dei mari, Ugo Grozio e gli sviluppi della talassocrazia olandese nel primo Seicento”, Scienza Politica, 1997, 35 ss.

- TeleGeography, The State of the Network. 2023 Edition, 2023, https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2023.pdf.

- Convenzione delle Nazioni Unite sul diritto del mare (UNCLOS), Montego Bay, 1982: art. 3 (ampiezza massima del mare territoriale: 12 miglia nautiche).

Atti di convegno

La guerra cibernetica e il diritto costituzionale italiano, tra sguardi comparatistici e possibilità di aggiornamento

Andrea Ruffo
Assegnista di ricerca (di tipo B), in diritto costituzionale, per il progetto PNRR SERICS (ACK: PE00000014) - Dipartimento di Studi Internazionali Giuridici Storico-Politici dell'Università degli Studi di Milano.

"Cyber warfare and Italian constitutional law, between updating possibilities and comparative views"

Abstract

The Italian Constitution, while repudiating war as an instrument of offence or resolution of international controversies, contemplates its recourse as a last resort, for the sacred duty of homeland defence. This approach finds similar (but gradually different) parallels in Germany and Japan.

Cyber warfare, prodromal or auxiliary to armed conflicts, due to the channels and instruments employed, transcends territories, making it difficult to recognise, actors and conduct, attacks from defences; complicating legal subsumption. The very definitions of 'war' and 'homeland defence', in the cyber dimension, appear more nuanced, suggesting the possibility of a more precise framing.

Keywords: Cyberwar - Constitution - Defence - Updating doctrine - Balancing

Introduzione

L'incessante evoluzione delle tecnologie informatiche e satellitari del XXI secolo ha comportato notevoli cambiamenti anche nel mondo militare e nelle condotte belliche.

La c.d. guerra cibernetica, collegabile a più ampie modalità offensive e destabilizzanti definite "g. ibride" (che preparano e/o affiancano gli scontri guerreggiati), è la conseguenza diretta della pervasiva, poliedrica e necessaria importanza assunta dalle tecnologie cyber nella società contemporanea.

La Cyberwar, per la natura dei canali e degli strumenti impiegati, travalica i confini territoriali, rendendo poco riconoscibili, sia gli attori che le loro condotte, e gli attacchi dalle difese (essendo quest'ultime spesso atti offensivi preventivi), rendendo la sussunzione giuridica sempre più ardua e incerta. Le stesse definizioni di "guerra" e di "difesa patria", perdendo nello specifico i riferimenti sottesi dalla Costituzione, devono essere aggiornate (anche in ottica comparatistica).

Gli attacchi cibernetici, per le modalità con cui vengono condotti, sovvertono le tradizionali categorie del diritto internazionale dei conflitti armati e sollevano interrogativi in merito alla qualificazione giuridica delle azioni offensive e difensive, poiché la sovrapposizione tra attacco e difesa impedisce di delineare con certezza quando un'azione cibernetica possa considerarsi una legittima misura di protezione o un'anticipazione illecita di un'aggressione.

Il principio di attribuzione della responsabilità statale, fondamento del diritto internazionale pubblico, risulta messo a dura prova dalla difficoltà di identificare con certezza gli autori materiali degli attacchi, soprattutto laddove siano coinvolti attori non statali, gruppi organizzati o Stati che operano attraverso proxy. Inoltre, la progressiva perdita di riferimenti normativi univoci nella definizione di "guerra" e "difesa della patria" pone sfide inedite al diritto costituzionale e internazionale, rendendo necessaria una revisione concettuale e normativa che tenga conto delle specificità del cyberspazio e delle nuove forme di minaccia alla sovranità statale.

Per questo, in un'ottica futura, l'adeguamento delle disposizioni costituzionali e delle strategie di difesa non può prescindere da un approccio comparatistico che analizzi le soluzioni adottate da altri ordinamenti, al fine di individuare strumenti giuridici idonei a disciplinare la cyberwarfare nel rispetto dei principi fondamentali dello Stato di diritto, della sicurezza collettiva e nell'interesse esclusivo della Nazione.

1. La definizione guerra cibernetica

Seguendo il principio per cui non è possibile argomentare di qualcosa senza averne colto preliminarmente l'essenza e quindi la sua sussunzione tassonomica, anche per l'inquadramento della guerra cibernetica tra le categorie del diritto costituzionale è necessario tracciare prima una sua plausibile definizione giuridica. Secondo una possibile definizione la guerra cibernetica (o cyber warfare) è una tecnica militare che riguarda l'uso di attacchi informatici da parte di uno Stato, o di uno o più gruppi di hacker o altri attori non governativi, finalizzato a danneggiare, distruggere o alterare sistemi informativi, reti o infrastrutture critiche di un altro Stato o entità privata o confederata.[1]

Ci si riferisce, quindi, ad un tipo di attacco che deve essere necessariamente apportato mediante l'utilizzo di un computer o di un sistema informatico assimilabile e deve avere come bersaglio, anche se solo di tramite per il raggiungimento di un obiettivo più ampio, un equivalente oggetto o circuito[2]. La dimensione spaziale è costituita dal dominio cibernetico, ovvero il sistema di funzionamento e interconnessione dei computer e delle strumentazioni collegate, mentre gli obiettivi – considerata la pervasività delle tecnologie – spaziano dalle interferenze socio-economico-politiche alla manomissione o sottrazione o inibizione di dati e informazioni strategiche e sensibili.

La guerra cibernetica, pertanto, presenta le caratteristiche di: anonimità, asimmetria e transnazionalità.

L'anonimato, consentito o comunque ben propiziato dalle tecnologie digitali, comporta la difficile attribuzione degli attacchi, rendendo ancor più complessa l'applicazione del diritto internazionale. Allo stesso modo, considerando che gli attacchi possono essere apportati anche da piccoli gruppi, pure di privati (hacker) o da Stati minori (però altamente specializzati nelle tecnologie cyber[3]), vi è un'estrema variabilità degli attori che porta, per questo, ad un'evidente asimmetria tra gli attaccanti e i bersagli. A ciò si aggiunge che, essendo il "campo di battaglia" costituito dallo spazio virtuale cibernetico (ovviamente Internet, comprensivo di dark web), le condotte offensive possono essere lanciate da qualsiasi luogo, che può variare anche nel corso del medesimo attacco o essere "fatto rimbalzare" su un altro dispositivo geograficamente opposto, per rendere ancor più difficile l'identificazione e superare qualsiasi confine giuridico-politico.

---

[1] G. de Vergottini, Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia, Bologna, 2004 e P. CARNEVALE, La Costituzione va alla guerra?, Napoli, 2013, 3 e ss. e ancoraG. de Vergottini, Le nuove sfide del diritto costituzionale nell'era digitale, in Diritto costituzionale, Padova, CEDAM, 2020, 567-589 e C. Colapietro, La tutela dei diritti fondamentali nell'era digitale, in Rivista AIC, 2021, pp. 15-25.

[2]P. Ceruzzi, Storia dell'informatica. Dai primi computer digitali all'era di Internet, Apogeo, Milano 2006, p. 9.

[3] Può essere un esempio l'attacco del 2010 condotto, con il malware Stuxnet, da Israele contro il programma nucleare iraniano.

Per tali caratteristiche, a differenza della guerra "classica" (definita dalla dottrina), che comporta scontri armati diretti o comunque una minaccia bellica indiretta (es. "Guerra Fredda") tra attor statuali determinati, la cyber warfare può essere condotta senza un conflitto in corso o essere prodromica a questo, colpendo selettivamente ma senza limitazioni tanto gli Stati quanto i singoli individui. Non a caso, infatti, la guerra cibernetica rientra nell'ampio ventaglio delle condotte di g. ibrida[4], rappresentandone – per lo sviluppo delle tecnologie coinvolte e la loro capillarità – forse oggi la forma più efficace e temuta.

Proprio le tecnologie informatiche alla base della cyber warfare fanno sì che questa possa essere condotta secondo diverse tecniche d'attacco (a volte anche concomitanti), quali:

- Attacchi a condotta persistente (Advanced Persistent Threats; APT);
- Attacchi Denial of Service (DoS) o Distributed Denial of Service (DDoS) per paralizzare (interrompendo la trasmissione) siti web e infrastrutture online;
- Malware (software dannosi, comunemente definiti virus) e ransomware (programmi bloccano o sottraggono dati per ottenere un riscatto) infiltrano i sistemi informatici per manomettere, paralizzare funzioni cruciali o sottrarre dati;
- Manipolazione cibernetica attraverso condotte disinformanti, misinformazione indotte da deepfake o il sabotaggio di dati sensibili;
- Phishing (tentativi di inganno per ottenere informazioni sensibili);
- Spionaggio informatico per raccogliere informazioni riservate governative, economiche o personali.

Devono annoverarsi, inoltre, anche ulteriori modalità informatiche di attacco volte all'infiltrazione e al sabotaggio delle infrastrutture strategiche (energetiche, finanziarie e sanitarie). Gli obiettivi degli attacchi, pertanto, possono essere: le infrastrutture critiche[5], i sistemi informatici economico-finanziari, reti e mezzi di comunicazione (inclusi social media e piattaforme online), dati sensibili (governativi o privati). Nonostante questo ampio ventaglio di condotte, non si è ancora giunti, ad una definizione giuridica universale di guerra cibernetica, ma si possono desumere alcuni elementi fondanti dal quadro normativo esistente.

La Convenzione di Budapest, redatta nel 2001 dal Consiglio d'Europa, può essere considerata come una delle prime fonti normative europee che – affrontando l'allora emergente problema dei crimini informatici – rileva la pericolosità seppur generica di condotte osti cibernetiche.

---

[4] M.N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge, Cambridge University Press, 2017, p. 12. Secondo cui: «Cyber operations are often employed in hybrid warfare to disrupt critical infrastructure, spread disinformation, and undermine the morale of the adversary.»

[5] Come reti di trasporto, collegamenti e stoccaggi energetici, idriche, reti di comunicazione e sistemi bancari o sistemi sanitari.

La Risoluzione 2312 del Consiglio di Sicurezza delle Nazioni Unite, invece, nel 2016 ha affrontato la questione della sicurezza cibernetica a livello internazionale, più compiutamente, evidenziando la necessità di una maggiore cooperazione tra gli Stati, al fine di prevenire gli attacchi informatici.

Inoltre, sebbene nelle convenzioni dell'Aia e di Ginevra, e, più in generale nel diritto internazionale umanitario (DIU) consolidato, non ci sia una diretta menzione degli attacchi informatici, i principi generali di distinzione degli obiettivi, necessità militare e proporzionalità, previsti in diritto internazionale umanitario (DIU), dovrebbero applicarsi anche alla guerra cibernetica. Secondo tale interpretazione, infatti, per quanto arduo e realisticamente molto improbabile, anche gli attacchi cibernetici dovrebbero distinguere tra obiettivi militari e civili (secondo il principio di distinzione). Allo stesso modo, ogni azione ostile cyber dovrebbe essere "giustificata" dalla necessità di ottenere un vantaggio militare, senza essere atta a colpire la popolazione civile (ai sensi del p. di necessità militare) e proporzionata rispetto alla finalità attesa (p. di proporzionalità).

Si deve notare, comunque, che la stessa definizione di "guerra cibernetica", risulta per certi aspetti problematica, poiché in diritto internazionale la maggior parte delle convenzioni (comprese, ovviamente, quelle dell'Aia e di Ginevra) classificano un conflitto come "guerra" solo in presenza di un attacco fisico (o uso della forza armata). Tuttavia, non è peregrino ritenere che certi azioni gravi, con danni equivalenti a quelli di un attacco convenzionale (come il sabotaggio delle infrastrutture vitali di un Paese), possano essere considerate come un "attacco armato", ai sensi dell'articolo 51 della Carta delle Nazioni Unite (che legittima difesa degli Stati in caso di aggressione armata)[6]. Si potrebbe ritenere, pertanto, che pur essendo la definizione di guerra cibernetica ancora un concetto giuridico in evoluzione, non universalmente consolidato, trovi un primo fondamento normativo, da una parte, nelle convenzioni nei trattati internazionali esistenti e, dall'altra, nelle più recenti norma nazionali e comunitarie di specifici settori (crimine cibernetico, disinformazione, responsabilità piattaforme, ecc..), direttamente correlati.

2. Il quadro normativo attuale

Il quadro normativo nazionale che cerca di prevenire e ridurre le criticità causate dalla guerra cibernetica è variegato e non unitario. In primis, si deve considerare che l'Italia, in quanto membro dell'Organizzazione del Trattato del Nord Atlantico (NATO), così come dell'Organizzazione delle Nazioni Unite (ONU), partecipa attivamente a tutte le misure di regolazione e contrasto della guerra cibernetica. L'ordinamento italiano recepisce le normative quadro di settore derivate dai Trattati di adesione a tali organizzazioni internazionali e collabora attivamente alla prevenzione e difesa dagli attacchi cibernetici. A questo, si deve aggiungere

[6] Come si approfondirà in seguito nel paragrafo dedicato agli aspetti comparatistici.

l'impulso normativo dato nell'ultimo decennio dall'Unione Europea (di cui l'Italia è paese membro e fondatore) che ha intensificato i propri sforzi normativi sul mondo di Internet e delle tecnologie ad esso collegate. Proprio in merito agli interventi normativi europei per prevenire i rischi cibernetici e contrastarli una volta in atto, un punto di svolta è rappresentato della Direttiva UE 2016/1148 Network and Information Security (NIS) relativa alla sicurezza delle reti e dei sistemi informative e alla successiva produzione regolamentare sulla sicurezza informatica delle infrastrutture critiche.

Recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 2018, che prevede gli obblighi di sicurezza per gli operatori di servizi essenziali e fornisce un quadro di prevenzione ed intervento per la gestione delle crisi cibernetiche assicurando la continuità del servizio e la cooperazione tra Stati, la Direttiva NIS contribuisce a potenziare il c.d. perimetro di sicurezza azionale cibernetica[7]. A tale Direttiva, definita anche "NIS 1" (e al relativo D.Lgs. 65/2018 di recepimento) è seguita una seconda, la Directive (EU) 2022/2555, detta per questo "NIS 2", recepita in Italia con il decreto legislativo n. 138/2024, entrato in vigore dal 16 ottobre 2024[8]. La NIS 2 (Direttiva sulla sicurezza delle reti e dei sistemi informativi), rappresenta un'evoluzione della precedente normativa con l'introduzione di novità significative quali: l'ampliamento del campo di applicazione,[9] la riforma della classificazione dei soggetti[10], l'apposizione di requisiti più stringenti[11] e di sanzioni più severe[12]. La NIS 2, infatti, introduce un quadro normativo più strutturato e armonizzato per affrontare le crescenti minacce informatiche. L'obiettivo principale è la protezione delle infrastrutture critiche, sempre più esposte a attacchi informatici potenzialmente devastanti, capaci di causare gravi disservizi pubblici, danni economici e persino compromettere la sicurezza nazionale. Per questo, è imposto agli Stati membri e agli operatori di servizi essenziali l'obbligo di adottare misure di sicurezza avanzate, garantendo che settori strategici (come l'energia, i trasporti, la sanità e le telecomunicazioni) possano essere adeguatamente protetti.

---

[7] Rientra in tale definizione qualunque soggetto pubblico o privato che fornisca un «servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato».

[8] L'entrata in vigore della Direttiva UE era avvenuta già nel 2023 ma, come da prassi, era stato dato maggior tempo agli Stati membri per il recepimento, fissando il termine proprio al 16 ottobre 2024.

[8] Con l'estensione degli obblighi di cybersecurity a un numero maggiore di settori e servizi (con l'evoluzione del panorama delle minacce informatiche).

[9] Si supera la distinzione tra OSE e FSD, con l'introduzione di due nuove categorie: soggetti essenziali (aziende di dimensioni maggiori e più critiche per il funzionamento dell'economia e della società) e s. importanti (aziende di dimensioni minori, ma che forniscono servizi essenziali collegati a specifici settori o regioni).

[10] Sono indicati requisiti di sicurezza più rigorosi, come la gestione continua dei rischi, la formazione del personale, la resilienza degli sistemi informatici e la capacità di rispondere rapidamente agli incidenti.

[11] In caso di violazione degli obblighi previsti dalla NIS 2, sono previste sanzioni amministrative più elevate.

[12] In tal senso si lega anche all'intento di potenziare il mercato europeo digitale, perseguito in modo più diretto dal Regolamento UE 2022/1925 DigitalMarket Act (DMA), dal Regolamento (UE) 2022/2065 Digital Service Act (DSA) e dal Regolamento UE 2024/1689 sull'Intelligenza Artificiale.

Inoltre, la NIS 2 promuove una maggiore resistenza dei sistemi, incoraggiando l'adozione di approcci proattivi nella gestione dei rischi cibernetici, come l'implementazione di modelli di monitoraggio continuo, la formazione del personale e l'adozione di tecnologie avanzate per la prevenzione e il contrasto degli attacchi. Questo, per quanto non immediatamente intuitivo, è strettamente correlato con il fine (sotteso dalla Direttiva) dell'armonizzazione del mercato unico digitale, al fine di creare un ambiente più sicuro per la libera circolazione dei dati e dei servizi digitali, eliminando le disparità normative tra gli Stati membri e facilitando la cooperazione transfrontaliera[13]. La NIS 2, pertanto, implementa la cooperazione tra gli Stati membri dell'UE, grazie all'istituzione di meccanismi di condivisione delle informazioni e di risposta coordinata agli incidenti cibernetici, per contrastare efficacemente le minacce informatiche che spesso superano i confini nazionali. Entrambe le direttive NIS (sia 1 che 2), quindi, rappresentano uno strumento essenziale per garantire la sicurezza cibernetica nell'Unione Europea, offrendo un quadro normativo più ampio, atto a fronteggiare le innumerevoli sfide poste dalla continua crescente sofisticazione degli attacchi informatici. Sempre nel contesto europeo si deve menzionare il c.d. "Cybersecurity Act" (Regolamento UE 2019/881) che, ancor prima delle Direttive NIS, ha costituito un inizio nel rafforzamento della sicurezza cibernetica dei 27 Paesi membri.

È stato introdotto, così, il concetto di "security by design", ovvero la presa in considerazione della sicurezza informatica fin dagli stadi iniziali della progettazione dei prodotti ICT[14]. Infatti, un sistema comune di certificazione a livello europeo dovrebbe incentivare l'attenzione alla sicurezza informatica di prodotti e servizi digitali, facilitando al contempo l'accesso delle aziende produttrici ai mercati degli altri Stati europei.
A questo si affianca la promozione della cooperazione tra enti pubblici e privati, al fine di creare un ecosistema di sicurezza cibernetica integrato e collaborativo. Sul piano nazionale, l'istituzione (con il Decreto Legge n.82 del 14 giugno 2021) dell'Agenzia per la Cybersicurezza Nazionale (ACN), come ente incaricato di tutelare la sicurezza e la resilienza nello spazio cibernetico, per prevenire e mitigare gli attacchi cibernetici e favorire il raggiungimento dell'autonomia tecnologica, costituisce il completamento italiano del quadro tracciato da Bruxelles[15]. Parallelamente all'ACN le operazioni di difesa cibernetica assumono un ruolo sempre più centrale nella sicurezza nazionale, con le forze armate italiane che svolgono un compito cruciale attraverso il Comando per le operazioni in rete (COR), formato nel 2020, per coordinare tutte le attività di gestione rete (DIFENET), gli applicativi gestionali della Difesa oltre alle attività di guerra cibernetica e supervisione per la cybersicurezza dei sistemi informatici del relativo Ministero. Tuttavia, le operazioni di difesa cibernetica devono rispettare i limiti imposti dalla Costituzione italiana e dalle norme internazionali, garantendo che le azioni intraprese non violino i diritti fondamentali dei cittadini.

---

[1] Prodotti legati a Information and Communication Technologies (ICT).

[2] Si rimanda al sito istituzionale dell'Agenzia https://www.acn.gov.it/portale/chi-siamo

In particolare, il principio di proporzionalità e il rispetto della sovranità digitale sono elementi chiave per bilanciare le esigenze di sicurezza con la tutela dei diritti individuali. In questo contesto, il quadro normativo italiano e le direttive europee come la NIS 2 rappresentano strumenti complementari per affrontare le sfide della sicurezza cibernetica, promuovendo un approccio integrato che combina prevenzione, risposta e cooperazione a livello nazionale e internazionale.

Sempre in ambito europeo, con il documento programmatico "La politica di ciberdifesa dell'UE"[16] le Istituzioni di Bruxelles, cogliendo la necessità di rafforzare gli strumenti di collaborazione e cooperazione tra gli Stati nel settore della difesa, si ponevano l'obiettivo di potenziare la conoscenza situazionale collettiva e la capacità di rilevamento precoce delle minacce cibernetiche, al fine anche di dotare l'UE di una propria sovranità tecnologica, con adeguate competenze informatiche in grado di sviluppare e gestire le tecnologie digitali. Questa volontà di migliorare le conoscenze situazionali e di divulgare le scoperte di ambito, nasceva dall'importanza di assicurare che le industrie e le attività di ricerca e sviluppo e di innovazione legate agli ambiti della cibersicurezza e della ciberdifesa cooperassero in modo più sinergico per sviluppare capacità migliori. Conseguenzialmente, con la stessa comunicazione la Commissione ha avviato un processo di rafforzamento degli strumenti di collaborazione e cooperazione degli Stati membri nel settore della difesa. In tal senso, in ambito militare, fu prevista l'istituzione di un centro di coordinamento della ciberdifesa dell'UE, denominato EU Cyber Defence Coordination Centre (EUCDCC)[17], per coordinare una maggiore conoscenza situazionale all'interno della comunità della difesa, di cui facciano parte tutti gli alti comandi europei della PSDC. Detto centro per il coordinamento della difesa cibernetica dovrebbe istituire e integrare un sistema indipendente di sensori attivi, al fine di rafforzare il monitoraggio dei nodi informatici di proprietà dell'UE di supporto alle missioni militari della PSDC con la sorveglianza continua del ciberspazio. Per questo l'EUCDCC potrà essere collegato per lo scambio di informazioni con il Centro UE di situazione e di intelligence, c.d. Intelligence Analysis Centre (INTCEN)[18], e – pertanto – anche con lo Stato maggiore dell'UE. Tale scambio di informazioni, inoltre, non potrà non coinvolgere anche il nuovo centro virtuale paneuropeo per la gestione dinamica e real-time del rischio informatico[19], che verrà incardinato nel C. di situazione e di analisi informatiche in costituzione presso Bruxelles, sotto la gestione della Commissione, con

---

[16] Si veda il documento La Politica di ciberdifesa dell'UE, presentato alla XIV Commissione Politiche dell'Unione Europea della Camera dei deputati, nel corso dell'audizione di Stefano Da Empoli, del 31 maggio 2023.

[17] Si veda il Questions and Answers: The EU Policy on Cyber Defence pubblicato sul sito dell'Unione Europea, il 10 novembre 2022, come al seguente link: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6643

[18] Si rimanda al documento pubblicato da Statewatch.org, il 05/02/2015, al seguente link: https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf.

[19] A. Leonardi, Il primo centro paneuropeo di cyber analisi è ora operativo: come funziona, articolo pubblicato in cybersecurity360.it, il 03 Ott 2023, https://www.cybersecurity360.it/cybersecurity-nazionale/il-primo-centro-paneuropeo-di-cyber-analisi-e-ora-operativo-come-funziona/

il sostegno dell'ENISA[20] e del CERT-UE[21]. Quest'ultimi due organi dell'UE costituivano, già prima della Digital Era von der Leyen, le due principali strutture europee per la sicurezza delle comunicazioni informatiche per cittadini e le imprese (l'ENISA) e per prevenire attacchi e compromissioni dei relativi canali delle Istituzioni (il CERT-UE). La nuova strategia prevista da "La politica di ciberdifesa dell'UE", quindi, oltre a rafforzare le competenze e le sinergie funzionali tra gli organi preposti prevede di potenziare ulteriormente la Conferenza dei comandanti per la sicurezza informatica dell'UE, in modo che possa riunirsi – con il supporto dell'Agenzia Europea per la Difesa (AED[22]) e dello Stato maggiore UE – almeno due volte l'anno per affrontare questioni connesse alla sicurezza cibernetica. A questo si aggiunge che è prevista l'istituzione di una rete operativa per delle "Squadre militari di pronto intervento informatico", denominate tecnicamente Military Computer Emergency Response Teams (MilCERTs).[23] Suddetta rete (abbr. MICNET), grazie al sostegno dell'AED, o EDA, promuoverà un'azione di maggiore coordinamento e contrasto alle minacce informatiche orientate ai sistemi di difesa nell'UE, compresi quelli della PSDC, provvedendo contemporaneamente ad approfondire e indicare nuovi requisiti per potenziare le attività delle milCERT[24]. A questo deve aggiungersi il ruolo dell'Accademia Europea per la Sicurezza e la Difesa (AESD o ESDC [25]) che vaglierà le modalità per facilitare lo scambio di buone pratiche e ulteriori sinergie tra il settore civile e quello militare per la formazione e lo sviluppo di competenze militari specifiche per il ciberspazio[26]. Un esempio di formazione e condivisione di esperienze in materia di difesa cibernetica è rappresentato dal corso-esercitazione combinato Cyber Phalanx, avviato dall'Unione Europea per aumentare la preparazione dei pianificatori delle operazioni militari (OPP[27]) sulle minacce cibernetiche e ibride nel

---

[20] Agenzia europea per la cibersicurezza, ufficialmente denominata European Network and Information Security Agency (ENISA), con sede centrale ad Atene, istituita nel 2004 dal Regolamento 460/2004, inizialmente con il nome di "Agenzia europea per la sicurezza delle reti e dell'informazione" e successivamente modificata e rinominata nella forma attuale con il Regolamento UE 2019/881.

[21] Denominato per esteso "Servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione europea" (CERT- UE), con sede in Belgio, a Bruxelles; per completezza si rimanda al sito istituzionale https://cert.europa.eu/.

[22] Conosciuta anche come EDA, acronimo della denominazione ufficiale in inglese European Defence Agency (EDA)

[23] Si vede in proposito i comunicati dell'EDA: Cyber defence exercise brings together military CERTs del 19 febbraio 2021 al link: https://eda.europa.eu/news-and-events/news/2021/02/19/cyber-defence-exercise-brings-together-military-certs# e MilCERT Interoperability Conference talks strategy dell'8 giugno 2021, al link https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy.

[24] Si tenga presente che, in generale, i CERT (Computer Emergency Response Team) sono delle organizzazioni, amministrate e sovvenzionate generalmente da Enti Governativi o Università, al fine di monitorare le segnalazioni di incidenti informatici e le potenziali vulnerabilità nei software che usati dalla comunità degli utenti.

[25] Acronimo dall'inglese European Security and Defence College

[26] Tutte le esercitazioni militari sono previste con il coinvolgimento dei soggetti che rappresentano infrastrutture critiche, per individuare le potenziali vulnerabilità in base alle valutazioni del rischio effettuate a livello UE, (come le iniziative già avviate dalla Commissione insieme all'ENISA),propiziando una reazione immediata per ripristinare il funzionamento dei servizi essenziali.

[27] Acronimo dalla dicitura inglese Operations Planning Process.

processo di elaborazione e conduzione dei piani, sia strategici che operativi.[28] Nelle strategie dell'UE, l'interazione tra la società civile e mondo militare risulta essere uno dei punti fondamentali, infatti, oltre alla collaborazione con le università è previsto che l'AED supporti gli Stati membri nel proporre opzioni di collaborazione con la rete nazionale di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT[29]) e la squadra di pronto intervento informatico delle Istituzioni enti e organismi dell'Unione Europea (CERT-UE). Inoltre, basandosi su iniziative esistenti nel settore civile quale il quadro europeo in materia di competenze nel settore della cybersicurezza (ECSF) sviluppato dall'ENISA, l'AED è chiamata ad elaborare un quadro di certificazione delle competenze in materia di ciberdifesa. A questo si aggiunge che, oltre al Cyber Phalanx e alle esercitazioni delle milCERT, l'Agenzia Europea per Difesa (AED) svilupperà un nuovo progetto CyDef-X[30], che coinvolgerà tutti gli Stati membri e fungerà da modello per le esercitazioni dell'UE di ciberdifesa.

In questo contesto, l'UE ha introdotto ulteriori misure per rafforzare la cibersicurezza e la resilienza digitale. Il 10 ottobre 2024 è stato adottato il regolamento sulla Ciberresilienza (Cyber Resilience Act; CRA)[31], che stabilisce requisiti obbligatori in materia di sicurezza informatica per prodotti hardware e software con un elemento digitale connesso, come smart TV, elettrodomestici, baby monitor e giocattoli. Tale atto garantisce a imprese e consumatori una protezione più solida contro le minacce informatiche. Successivamente, il 2 dicembre 2024, il Consiglio ha adottato il regolamento sulla CiberSolidarietà (Cyber Solidarity Act; CSA) [32], che mira a rendere l'Europa più resiliente e reattiva di fronte alle minacce informatiche. Tra gli obiettivi principali vi sono il sostegno al rilevamento e alla conoscenza delle minacce significative, il rafforzamento della preparazione per proteggere soggetti critici e servizi essenziali come ospedali e servizi pubblici, e il potenziamento della solidarietà e della gestione concertata delle crisi a livello dell'UE. Queste iniziative si inseriscono in un quadro più ampio di investimenti in cybersicurezza. Secondo l'ultima edizione del report "NIS Investments"[33], pubblicato dall'ENISA a novembre 2022, infatti, gli investimenti effettuati dagli Operatori di Servizi Essenziali (OSE) [34] e dai Digital Service Providers (DSP) [35] europei nel 2021 hanno

---

[28] Si veda il documento dell'UE CYBER PHALANX, pubblicato sul sito dell'AED al seguente link: https://eda.europa.eu/docs/default-source/eda-factsheets/cyph-fact-sheet_v03-eda.pdf

[29] Acronimo inglese per Computer Security Incident Response Team.

[30] Menzionato nel documento dell'European External Action Service (EEAS),del novembre 2022 al seguente link: https://www.eeas.europa.eu/sites/default/files/documents/Factsheet%20-%20The%20EU%20policy%20on%20cyber%20defence.pdf

[31] Si rimanda al documento sul sito UE https://digital-strategy.ec.europa.eu/it/policies/cyber-resilience-act#:~:text=La%20legge%20sulla%20ciberresilienza%20(CRA,tempestivi%20per%20prodotti%20e%20software.

[32] Si veda il seguente sito ufficiale UE: https://digital-strategy.ec.europa.eu/it/policies/cyber-solidarity.

[33]Si rimanda al sito ufficiale https://www.enisa.europa.eu/publications/nis-investments-2022.

[34] OSE - energia; trasporti; bancario; finanziario; salute; servizi idrici; infrastrutture digitali.

[35] DSP (Fornitori di servizi digitali) - marketplace online; cloud computing provider; motori di ricerca online.

raggiunto una media di 4 milioni di euro per organizzazione, con un aumento significativo rispetto ai 2,15 milioni del 2020. Tuttavia, nonostante questa crescita in valori assoluti, la quota media del budgetdelle tecnologie di Internet (IT), destinata alla cybersicurezza è diminuita, passando dall'8,8% nel 2020 al 7,82% nel 2021. Questo dato evidenzia la necessità di un maggiore impegno nel bilanciare gli investimenti tecnologici con quelli dedicati alla sicurezza informatica, soprattutto alla luce delle crescenti minacce nel panorama digitale. Tornando alla dimensione nazionale, è necessario considerare i principi costituzionali italiani relativi alla protezione della sovranità nazionale, alla sicurezza e ai diritti fondamentali dei cittadini. La risposta giuridica e istituzionale alla guerra cibernetica in Italia si fonda, infatti, su un approccio multilivello che integra le normative europee con le specificità del sistema nazionale. L'Italia, pertanto, ha adottato una serie di misure per rafforzare la propria ciberdifesa, allineandosi alle direttive UE ma anche valorizzando le proprie peculiarità istituzionali. Tra queste, spicca il ruolo del Perimetro di Sicurezza Nazionale Cibernetica, istituito nel 2021, che definisce requisiti stringenti per la protezione delle reti e dei sistemi informatici di interesse strategico. Inoltre, il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica[36] prevede una stretta collaborazione tra istituzioni pubbliche, settore privato e mondo accademico, con l'obiettivo di sviluppare competenze avanzate e promuovere una cultura della sicurezza informatica. Questo approccio si riflette anche nella creazione di strutture operative come il Computer Emergency Response Team italiano (CERT-IT)[37], che coordina la risposta agli incidenti cibernetici a livello nazionale. Tali misure, pur inserendosi nel quadro europeo, rispettano i principi costituzionali italiani, garantendo al contempo la protezione della sovranità nazionale e dei diritti fondamentali dei cittadini, come il diritto alla tutela e alla sicurezza dei dati personali.

3. Le sfide per il Diritto Costituzionale

Considerate la pluralità e la frammentarietà delle forme normative esistenti, ancora non del tutto affinate e uniformate tra il livello europeo e quello nazionale, si può comprendere come le tecniche di guerra cibernetica, rappresentino una delle maggiori sfide contemporanee per il diritto costituzionale italiano. Si pongono, infatti, questioni inedite riguardo al bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali[38], in un contesto in cui la digitalizzazione e la vulnerabilità delle infrastrutture critiche hanno

---

[36] Si rimanda al sito UE istituzionale: https://www.agid.gov.it/sites/agid/files/2024-05/piano-nazionale-cyber_0.pdf.

[37] Si veda la pagina dedicata nel sito ufficiale dell'ACN: https://www.acn.gov.it/portale/csirt-italia.

[38]M. Nisticò, Cybersecurity e Costituzione, in Quaderni costituzionali, 2019, 123 ss. Ex multis, di autorevole Dottrina, si rimanda a A. Baratta, Diritto alla sicurezza o sicurezza dei diritti?, in S. Anastasia e M. Palma (a cura di), La bilancia e la misura. Giustizia, sicurezza e riforme, Milano, 2001, 24 e ss., M. Ruotolo, Costituzione e sicurezza tra diritto e società, A. Torre (a cura di), Costituzioni e sicurezza dello Stato, Rimini, 2014, 588 e ss., A. Pace, La sicurezza pubblica nella legalità costituzionale, in Rivista AIC, n.1, 2015, 4 e ss., L. Scaffardi, Nuove tecnologie, prevenzione del crimine e privacy: alla ricerca di un difficile bilanciamento, in A. Torre (a cura di), Costituzioni e sicurezza dello Stato, Rimini, 2013, 425 e ss. oppure anche L. Califano, V. Fiorillo,

ampliato il perimetro delle minacce alla sovranità e alla stabilità dello Stato[39].

Sebbene la Costituzione italiana, non contenga disposizioni esplicite in materia di cyber warfare, i principi fondamentali in essa sanciti offrono un quadro di riferimento essenziale per affrontare le nuove minacce digitali[40]. L'articolo 11, ad esempio, sancisce il ripudio la guerra come strumento di offesa ma consente la partecipazione a conflitti internazionali per la difesa comune, sollevando interrogativi sulla legittimità di risposte cibernetiche a attacchi informatici, soprattutto in assenza di una chiara attribuzione della responsabilità.[41] Si tratta di un problema giuridico centrale nel contesto della guerra cibernetica, dove l'anonimato e la difficoltà di tracciare l'origine degli attacchi complicano l'applicazione del diritto internazionale e nazionale. Allo stesso tempo, l'articolo 52 sancisce il dovere di difendere la Patria, tradizionalmente inteso come protezione fisica dei confini nazionali, ma che oggi deve essere ridefinito alla luce delle minacce cibernetiche, le quali possono compromettere infrastrutture critiche (energia, trasporti, sanità) senza violare fisicamente i confini nazionali, ridefinendo così il concetto stesso di sovranità[42]. La guerra cibernetica, infatti, sfida i tradizionali paradigmi della sovranità statale, poiché gli attacchi informatici spesso non sono attribuibili con certezza a uno Stato specifico, complicando la risposta giuridica e politica e sollevando questioni in merito alla legittimità di misure di autotutela nel cyberspazio, che potrebbero confliggere con il principio di non ingerenza negli affari interni di altri Stati[43]. In questo contesto, la proporzionalità della risposta e il rispetto dei principi costituzionali, come la tutela della corrispondenza (Art.15) e della libertà di manifestazione del pensiero (Art.21), diventano elementi cruciali, poiché gli attacchi cibernetici, specialmente quelli volti a manipolare l'opinione pubblica o a raccogliere dati sensibili, pongono sfide significative alla protezione dei diritti fondamentali, richiedendo un bilanciamento tra sicurezza nazionale e garanzie individuali.[44] In caso di attacchi gravi e persistenti, lo Stato potrebbe invocare misure straordinarie ai sensi dell'articolo 77, ma l'adozione di decreti legge deve rispettare i limiti costituzionali, in particolare la tutela dei diritti fondamentali, evitando che lo stato di emergenza diventi un pretesto per

---

Videosorveglianza, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), Digesto delle discipline pubblicistiche (aggiornamento), Torino, 2015, 503 e ss. e ancora: G. de Vergottini, La difficile convivenza fra libertà e sicurezza: la risposta delle democrazie al terrorismo. Gli ordinamenti nazionali, relazione a convegno annuale (2003) dell'Associazione Italiana Costituzionalisti, v. sito e M. Benvenuti, R. Bifulco, Trattato di diritto costituzionale, vol. III, I diritti e i doveri costituzionali, 2022, 34-37.

[39] S.D. Reid, Cyber Warfare and International Politics: A Study of Cyber Conflict, London, 2018, 34 ss.

[40] G. de Vergottini, Diritto costituzionale, Padova, CEDAM, 2020, 345 e ss.

[41] NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on the International Law Applicable to Cyber Warfare, 2a ed., Cambridge, 2017, 1225https://www.cambridge.org .

[42] M.L. Mariscal, International Cybersecurity: Law, Policy, and Strategy, Oxford, 2020, 123 ss.

[43] Unione Europea, Joint Framework on Countering Hybrid Threats, Bruxelles, 2016, 34 ss.

[44] O. Pollicino, Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?, Oxford, 2021, 184e ss. e anche O. Pollicino, Potere digitale, in M. Cartabia, M. Ruotolo (a cura di), Potere e Costituzione, in Enciclopedia del Diritto, V, Milano, 2023.

limitazioni eccessive delle libertà civili.[45] La crescente rilevanza della guerra cibernetica richiede, pertanto, un adattamento del diritto costituzionale italiano per affrontare le nuove minacce e tecnologie, anche attraverso una revisione delle normative esistenti, come la Legge 155/2005 sulla sicurezza delle reti di comunicazione, che potrebbe non essere più sufficiente a garantire una protezione adeguata delle infrastrutture critiche in un contesto di attacchi sempre più sofisticati.

La creazione di una cyber-difesa nazionale, inoltre, richiede una definizione chiara delle competenze e dei ruoli delle autorità competenti, possibilmente attraverso un aggiornamento costituzionale che delinei i poteri e i limiti delle istituzioni coinvolte nella gestione delle crisi cibernetiche. Tuttavia, qualsiasi aggiornamento normativo deve bilanciare la protezione della sicurezza nazionale con la tutela dei diritti fondamentali, evitando il rischio di sorveglianza eccessiva o limitazione dei diritti civili, in particolare alla luce delle garanzie offerte dagli articoli 13 e 14 della Costituzione, che proteggono la libertà personale e il domicilio, e dall'art. 21, che tutela la libertà di espressione. La guerra cibernetica solleva numerosi interrogativi giuridici, tra cui la questione della responsabilità statale[46]. In particolare, è difficile determinare chi sia responsabile per un attacco cibernetico: è lo Stato che ospita l'infrastruttura da cui proviene l'attacco, o lo Stato che lo ha effettivamente lanciato? Questo problema è aggravato dalla natura transnazionale del cyberspazio, dove gli attacchi possono essere condotti attraverso server situati in più Paesi[47], rendendo complessa l'attribuzione della responsabilità. Inoltre, la questione dell'escalation e della risposta adeguata a un attacco cibernetico rappresenta un ulteriore dilemma giuridico. È possibile rispondere con misure cibernetiche simili, o è necessaria una risposta convenzionale, come un attacco militare fisico e, soprattutto, l'attacco cibernetico può essere considerato alla stregua di un attacco armato?

Secondo il diritto internazionale, in particolare l'articolo 51 della Carta delle Nazioni Unite, un attacco armato giustifica l'esercizio del diritto alla legittima difesa. Tuttavia, la qualificazione di un attacco cibernetico come "attacco armato" dipende dalla sua gravità e dalle conseguenze che produce. Non tutti gli attacchi informatici possono essere equiparati a un attacco armato: solo quelli che causano danni fisici, perdite di vite umane o distruzioni significative di infrastrutture critiche possono rientrare in questa categoria. Un attacco cibernetico che disabilita il sistema energetico di un Paese, provocando blackout

---

[45] Ex Multis: C. Mosca, La sicurezza come diritto di libertà, Teoria generale delle politiche della sicurezza, Padova, 2012, 239, anche T. Fenucci, Quanto spazio c'è per un diritto individuale alla sicurezza nell'ordinamento costituzionale italiano? Brevi osservazioni, in federalismi.it, n. 22, 2015,1e ss., in relazione all'analisi di P. Ridola, Libertà e diritti nello sviluppo storico del costituzionalismo, in R. Nania e P. Ridola (a cura di), I diritti costituzionali, I, Torino, 2006, 138, oppure F. Famiglietti, La sicurezza "ai tempi dell'ISIS": tra "stato di emergenza", diritto penale "del nemico" e rivitalizzazione del diritto di polizia in un sistema integrato di azioni e strutture, in Diritti fondamentali, n. 2/2016.

[46] A.C. Tassoni, e A. Mezzetti, Decreto NIS2, troppe ambiguità: guida ai nuovi obblighi cyber, in Agenda Digitale, 17 marzo 2025, https://www.agendadigitale.eu/sicurezza/decreto-nis2-guida-alla-comprensione-dei-nuovi-obblighi-di-cybersecurity/

[47] T. Rid, Cyber War Will Not Take Place, Oxford, 2013, 56 ss.

prolungati e mettendo a rischio la salute pubblica, potrebbe essere considerato analogo a un attacco armato. Durante il vertice di Galles, la NATO ha affermato che un attacco cibernetico di proporzioni significative potrebbe innescare l'applicazione dell'articolo 5, aprendo la possibilità di una risposta collettiva da parte degli Stati membri. Questa posizione è stata ribadita nel Cyber Defence Pledge del 2016, in cui gli Stati membri si sono impegnati a rafforzare le proprie capacità di cyber-difesa e a considerare gli attacchi cibernetici come una minaccia alla sicurezza collettiva.[48]

Tuttavia, la NATO riconosce che l'attribuzione di un attacco cibernetico è spesso complessa e che una risposta militare potrebbe non essere sempre appropriata. Pertanto, l'Alleanza promuove una strategia di deterrenza basata sulla resilienza, sulla condivisione delle informazioni e sulla cooperazione tra Stati membri. Inoltre, la NATO ha istituito il Cybersecurity Centre of Excellence[49] in Estonia (a Tallinn) per sviluppare linee guida e best practices nel campo della cyber-difesa. Nonostante ciò, rimangono aperte questioni cruciali, come l'attribuzione degli attacchi e la proporzionalità della risposta, che richiedono un ulteriore sviluppo del diritto internazionale e delle norme condivise nel cyberspazio.

Questa incertezza rischia di destabilizzare gli equilibri internazionali, poiché una risposta sproporzionata potrebbe innescare un conflitto armato "tradizionale", mentre una risposta insufficiente potrebbe essere interpretata come un segnale di debolezza. Allo stesso tempo, il diritto alla difesa degli Stati nel cyberspazio deve essere bilanciato con il principio di sovranità degli altri Stati[50]. Gli Stati hanno il diritto di proteggere i propri sistemi informatici e infrastrutture critiche, ma tale diritto non può giustificare violazioni della sovranità digitale di altri Paesi, ad esempio attraverso operazioni di hacking o intrusioni non autorizzate.[51]

Il principio di difesa della patria, sancito dall'articolo 52 della Costituzione italiana, è uno dei pilastri fondamentali del sistema giuridico italiano. Tradizionalmente, questo principio si riferisce alla protezione fisica dei confini nazionali e alla difesa contro minacce esterne attraverso l'uso delle forze armate. Tuttavia, l'emergere delle guerre cibernetiche sta trasformando profondamente il concetto stesso di "difesa della patria", rendendo necessarie nuove interpretazioni e adattamenti giuridici. Oggi, infatti, la difesa nazionale non può limitarsi alla protezione territoriale fisica, ma deve estendersi al dominio digitale, dove le minacce possono compromettere infrastrutture critiche senza violare fisicamente i confini nazionali.

---

[48] Si rimanda al sito NATO ufficiale: https://www.nato.int/cps/em/natohq/official_texts_133177.htm.

[49] Si veda la pagina del sito istituzionale: https://ccdcoe.org/.

[50] F.G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, Potomac Institute for Policy Studies, 2007, 45 ss.

[51] M.N. Schmitt, Cyber Operations and the Jus in Bello, in International Law Studies, Vol. 87 –International Law and Changing Characters of War, 2013, 67 ss.
https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1077&context=ils

Questo ridefinisce il concetto di sovranità, che non è più limitato al controllo del territorio fisico, ma include anche la protezione dello spazio cibernetico e dei dati digitali. In questo contesto, il concetto di sovranità digitale emerge come un tema centrale, con l'idea che gli Stati abbiano il diritto di proteggere i loro spazi cibernetici, ma anche la responsabilità di proteggere i dati dei loro cittadini. Questo porta alla creazione di politiche nazionali di cyber security e all'adozione di leggi sulla privacy che bilanciano le necessità di sicurezza con il rispetto dei diritti individuali.[52] La cyber-governance implica, quindi, un nuovo modo di pensare la sicurezza internazionale e la governance globale, con la necessità di sviluppare norme internazionali che includano principi di cooperazione tra Stati nel cyberspazio, in particolare per prevenire l'escalation dei conflitti cibernetici e proteggere le infrastrutture globali.

Dal punto di vista politologico, la sicurezza nazionale non è più limitata alla protezione territoriale fisica o alla difesa dalle minacce convenzionali, ma si estende al dominio digitale. La cyber-sicurezza è considerata un aspetto fondamentale della politica di difesa e della protezione delle infrastrutture critiche. Le politiche pubbliche devono evolversi per rispondere a minacce che provengono da attori statali e non statali, e che mirano non solo a compromettere la sovranità nazionale, ma anche a destabilizzare la fiducia nelle istituzioni pubbliche e nelle economie. I politologi evidenziano l'importanza di sviluppare una strategia di deterrenza cibernetica[53], che sia in grado di prevenire gli attacchi informatici prima che diventino dannosi. Ciò include la cooperazione internazionale per la condivisione delle informazioni e la creazione di alleanze cibernetiche, come quelle che esistono già tra Paesi membri della NATO o nell'ambito del Global Forum on Cyber Expertise (GAC).

Un tema cruciale della riflessione politologica riguarda la disparità di potere tra gli Stati.[54]

In un mondo sempre più connesso, infatti, gli attori statali e non statali che dispongono di capacità cibernetiche avanzate hanno un potere significativo nella determinazione degli equilibri internazionali. Mentre gli Stati più sviluppati hanno grandi capacità di cyber-difesa e attacco, quelli più deboli rischiano di rimanere vulnerabili. Questa asimmetria di potere crea un panorama complesso, dove gli Stati con minori risorse tecnologiche potrebbero essere più facilmente bersagliati da attacchi cibernetici. Inoltre, la guerra cibernetica solleva interrogativi riguardo alla legalità internazionale e alla responsabilità statale. L'attribuzione di attacchi cibernetici è un tema centrale: è spesso difficile identificare con certezza l'origine di un attacco,

[52] F. Pizzetti, La protezione dei dati personali nell'era digitale: sfide e prospettive, in G. Scorza, A. Sica (a cura di), Cybersecurity e privacy: nuove frontiere del diritto, Roma, 2022, 89-112.

[53] W. Murray, P.R. Mansoor, Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present, www.cambridge.org, 2012, I e ss.

[54] J. Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, New York, 2011, 102 ss.

poiché potrebbe sembrare provenire da un altro Stato, ma essere invece opera di un gruppo di hacker indipendente. Questo crea incertezze politiche e può influenzare la reazione internazionale, complicando la diplomazia e le relazioni internazionali.

Un altro aspetto centrale della dottrina politologica riguarda la crescente importanza degli attori non statali, come i gruppi di hacker, le aziende private e le organizzazioni internazionali. Questi attori, che operano spesso in modo indipendente dagli Stati, sono in grado di influenzare la sicurezza cibernetica globale attraverso attacchi cibernetici, campagne di disinformazione o la fornitura di tecnologie avanzate. La crescente privatizzazione della sicurezza cibernetica è vista come un cambiamento nelle dinamiche di potere e di governance, dove gli Stati devono adattarsi alla nuova realtà di un ciberspazio sempre più dominato da attori privati. In questo contesto, la cooperazione internazionale e lo sviluppo di norme condivise nel cyberspazio saranno essenziali per garantire una risposta efficace e proporzionata alle minacce cibernetiche, nel rispetto dei valori costituzionali e dei diritti umani, anche attraverso l'adozione di strumenti giuridici internazionali che regolino la condotta degli Stati nel cyberspazio e prevedano meccanismi di attribuzione delle responsabilità e di risoluzione delle controversie.

In un contesto globale sempre più interconnesso, la cooperazione internazionale e lo sviluppo di norme condivise nel cyberspazio saranno essenziali per garantire una risposta efficace e proporzionata alle minacce cibernetiche, nel rispetto dei valori costituzionali e dei diritti umani, anche attraverso l'adozione di strumenti giuridici internazionali che regolino la condotta degli Stati nel cyberspazio e prevedano meccanismi di attribuzione delle responsabilità e di risoluzione delle controversie. La guerra cibernetica, dunque, non solo ridefinisce il concetto tradizionale di difesa della patria, ma impone una riflessione approfondita su come adattare il diritto costituzionale italiano alle sfide del mondo digitale, garantendo che l'evoluzione tecnologica non comprometta i principi cardine dello Stato di diritto, tra cui la separazione dei poteri, la tutela dei diritti fondamentali e il principio di legalità, che devono continuare a rappresentare il fondamento dell'ordinamento giuridico anche in un'epoca di trasformazioni tecnologiche senza precedenti.

4. Sguardi comparatistici

Il Diritto Costituzionale italiano può trarre spunto da esperienze internazionali per affrontare le sfide poste dalla guerra cibernetica, un fenomeno che richiede risposte giuridiche e strategiche innovative, anche alla luce delle diverse soluzioni adottate da altri Paesi[55], soprattutto al di fuori dell'Unione Europea.[56]

---

[55] F. Di Cocco, La guerra cibernetica e il diritto internazionale, in Riv. dir. int., 2020, 567 ss https://www.rivistadirittointernazionale.it.

[56] F. Pizzetti, Attenzione, il mondo sceglie un approccio diverso da quello UE, in Agenda Digitale, 2023, 1 e ss., https://www.agendadigitale.eu/sicurezza/privacy/ai-pizzetti-attenzione-il-mondo-sceglie-un-approccio-diverso-da-quello-ue

La scelta di allargare lo sguardo oltre i confini normativi dell'UE appare scontata nel momento in cui si affrontano minacce (come quelle cyber) che travalicano i confini degli Stati, prescindendo dal distinguo tra attori/bersagli pubblici e mettendosi in atto "da remoto" solo attraverso l'interconnessione della rete Internet. Si tratta, pertanto, di insidie transnazionali e sistemiche, che spesso si originano in Paesi con ordinamenti giuridici completamente differenti, se non antitetici, da quelli europei.

In un contesto di potenziale interconnessione funzionale globale, quindi, le scelte normative e politiche dei principali attori mondiali, quantunque diversissimi tra loro per economia, ordinamento giuridico e società, creano effetti di rilevanza immediata sull'ecosistema digitale di tutti gli Stati. Sottovalutare tali fattori significherebbe elaborare risposte "alla cieca", in una sorta di vuoto informativo (senza contare le asimmetrie inf. che comunque continuano a sussistere, senza considerare la realtà giuridico-operativo. Negli Stati Uniti, ad esempio, il Cybersecurity Act of 2015 ha introdotto misure significative per rafforzare la sicurezza cibernetica a livello federale, integrando il concetto di cyberwarfare nelle politiche di difesa nazionale e attribuendo al Department of Homeland Security e al Cyber Command un ruolo centrale nella gestione delle minacce informatiche. Questo approccio, che combina legislazione specifica e strutture operative dedicate, rappresenta un modello di integrazione tra politiche di difesa e protezione delle infrastrutture cibernetiche, offrendo spunti per una possibile evoluzione del quadro normativo italiano. La NATO, a sua volta, ha riconosciuto le guerre cibernetiche come una minaccia strategica, istituendo il Cooperative Cyber Defence Centre of Excellence e includendo i cyber-attacchi tra i motivi per invocare l'articolo 5 del Trattato Atlantico, che prevede la difesa collettiva in caso di aggressione.[57]

Questo approccio multilaterale sottolinea l'importanza della cooperazione internazionale nella gestione delle minacce cibernetiche, un aspetto che potrebbe essere ulteriormente sviluppato nel contesto italiano, anche attraverso una maggiore integrazione con le iniziative dell'Unione Europea in materia di cybersicurezza.[58] Nel Regno Unito, invece, la National Cyber Security Centre (NCSC) ha sviluppato linee guida per aziende e agenzie governative, con una forte enfasi sulla prevenzione degli attacchi cibernetici, mentre il sistema giuridico britannico, pur non avendo una Costituzione scritta, ha dimostrato flessibilità nell'adattare la legislazione ordinaria alle nuove sfide digitali, integrando la difesa cibernetica con le politiche di sicurezza tradizionali. Ampliando lo sguardo, secondo un'ottica di diritto comparato per cui il confronto non deve essere circoscritto solo a ordinamenti interconnessi (o legati da trattati di alleanza), ma può estendersi anche a sistemi giuridici e valoriali antitetici, rispetto a quelli fondanti dell'ordinamento di riferimento. La comparazione giuridica, infatti, non ha solo la funzione di individuare eventuali c.d. "best practices" da

[57] NATO, NATO's Response to Hybrid Threats, Bruxelles, 2015, 23 ss. https://www.nato.int.

[58] T. Rid, The Myth of Cyber War, (a cura di.), The Oxford Handbook of Cyber Security, Oxford, 2016, 123-145.

seguire, ma anche quella di evidenziare, per contrasto, i pericoli e le derive da evitare, definendo così, in negativo, i confini entro cui un'evoluzione normativa possa spingersi, al fine di prevenirne i rischi. Inoltre, il metodo comparatistico moderno, superando un approccio meramente strutturalista, valuta i sistemi giuridici in base alla loro "funzione" di risposta a problemi comuni. Il problema della sicurezza cibernetica è globale e, in larga parte, funzionalmente equivalente per tutti gli Stati, pur ricevendo risposte diametralmente opposte a seconda degli ordinamenti giuridici di base.[59]

Non tutte le esperienze internazionali offrono, infatti, modelli da seguire senza riserve: Paesi come la Russia e la Cina hanno adottato leggi molto rigide in materia di controllo e sorveglianza del cyberspazio, spesso a discapito dei diritti individuali. La Russia, ad esempio, ha istituito una "cyber-armata" e introdotto normative severe contro le "minacce informatiche", mentre la Cina ha sviluppato un sistema di monitoraggio del cyberspazio che limita fortemente la libertà di espressione e la privacy, pur senza un quadro costituzionale dedicato.

L'utilità comparatistica di questi esempi risiede proprio nella loro distanza valoriale dall'ordinamento italiano ed europeo. Analizzarli non implica una loro condivisione, ma serve a evidenziare, in controluce, la necessità –per gli ordinamenti liberali e democratici– di ancorare qualsiasi misura di sicurezza al principio di proporzionalità e al rispetto dei diritti fondamentali. Per costruire una risposta adeguata alle insidie derivanti dall'importazione, da tali Paesi, di tecnologie critiche o la penetrazione indiretta di esse attraverso dinamiche di mercato, è inoltre fondamentale comprendere le logiche giuridiche e operative che hanno consentito il loro sviluppo. Questo vale, ovviamente, ancor più per la prevenzione delle minacce ibride e cibernetiche, che provengono da tali Paesi "ostili". La comprensione del contesto giuridico d'origine è preliminare, infatti, a qualsiasi strategia di difesa efficace e consapevole. Lo studio comparatistico di sistemi concorrenti o avversi, quindi, non è un mero accostamento descrittivo, ma un'esigenza strategica e metodologica per definire l'identità stessa dell'approccio nazionale (ed europeo), che non può prescindere dalla consapevolezza dell'intero spettro di risposte possibili a livello globale. Gli approcci –per quanto diversissimi anche tra loro – di Cina e Russia sebbene efficaci, nel medio periodo e in assenza "forzamenti esterni"[60], nel contrastare le minacce cibernetiche, pongono seri interrogativi riguardo al rispetto dei diritti fondamentali, che in tali realtà sono spesso tralasciati o, comunque, subordinati rispetto al generale interesse collettivo nazionale e alla promessa di benessere economico individuale, purché compatibile con il primo.

---

[59] C. Sbailò, Diritto e geopolitica nello spazio curvo del potere: dalla crisi dell'ordine moderno alla riconfigurazione strategica della sovranità nell'era della guerra ibrida, in Rivista di Diritti Comparati, Special Issue VII, 2025, 130 e ss.

[60] Si avvantaggiano, infatti, di un controllo e blocco capillare della rete Internet; che interdice la maggior parte (escludendo il "Deep Web") dei contatti con server e software esterni e, quindi, di un ecosistema cibernetico "ristretto".

Tornando – per contrasto – all'ambito nazionale, il diritto costituzionale italiano, pur restando un baluardo di protezione dei diritti individuali, deve adattarsi alle nuove minacce digitali, ridefinendo concetti come sovranità e difesa nazionale in chiave cibernetica. L'aggiornamento normativo potrebbe includere una nuova interpretazione della difesa nazionale, che riconosca la sovranità digitale e la necessità di proteggere le infrastrutture critiche da attacchi informatici, anche attraverso la creazione di organi specializzati e il rafforzamento delle politiche di sicurezza cibernetica. Tuttavia, qualsiasi evoluzione del quadro giuridico deve mantenere un equilibrio tra sicurezza nazionale e tutela dei diritti fondamentali, evitando che le esigenze di protezione si traducano in limitazioni eccessive delle libertà civili[61]. In questo senso, il confronto con altri ordinamenti giuridici offre spunti preziosi, ma l'Italia dovrà sviluppare un approccio peculiare, che tenga conto delle specificità del suo sistema costituzionale e dei valori fondanti dello Stato di diritto. Questo approccio unitario, tuttavia, non deve essere considerato frutto di isolamento, bensì originato da un'analisi critica e consapevole del panorama giuridico globale. L'interconnessione funzionale del mondo cyber impone di comprendere tanto gli alleati quanto gli avversari sul piano geopolitico, poiché le loro scelte normative sono utili a definire il perimetro entro cui la sovranità digitale italiana deve essere esercitata e protetta e i margini di sviluppo delle proprie tecnologie critiche di ambito. La crescente minaccia cibernetica richiede, quindi, una costante vigilanza e un adattamento dinamico delle leggi, nel rispetto dei principi di democrazia, giustizia e tutela dei diritti umani, che rappresentano il cuore della Costituzione italiana e devono continuare a guidare l'evoluzione del diritto anche nell'era digitale.

5. Possibilità di aggiornamento normativo

Come si è detto, l'Italia, pur vantando un robusto sistema costituzionale fondato su principi democratici e di tutela dei diritti fondamentali, si trova oggi ad affrontare una sfida complessa e multidimensionale: quella di integrare il diritto costituzionale con le nuove realtà digitali, in particolare con le minacce emergenti derivanti dalla guerra cibernetica. Quest'ultima, pur non configurandosi come un conflitto armato tradizionale, rappresenta una minaccia concreta e pervasiva, capace di compromettere la sicurezza nazionale, la stabilità economica e il funzionamento delle istituzioni democratiche. La risposta a tali minacce non può limitarsi a misure di difesa e prevenzione di carattere tecnico-operativo, ma deve necessariamente includere un ripensamento del quadro giuridico e costituzionale, al fine di garantire un equilibrio tra la sicurezza nazionale e la protezione dei diritti fondamentali, evitando al contempo derive autoritarie o eccessive restrizioni delle libertà civili. L'aggiornamento del diritto costituzionale italiano, in questo contesto, potrebbe rendere necessaria una revisione delle normative relative alla difesa, alla protezione delle informazioni e alla sicurezza delle infrastrutture critiche, ispirandosi anche alle migliori pratiche internazionali, ma rimanendo fedele ai principi democratici e ai valori fondanti della Costituzione repubblicana.

---

[61] F. P. Levantino, F. Paolucci, Advancing the Protection of Fundamental Rights Through AI Regulation: How the EU and the Council of Europe are Shaping the Future, Rochester (NY), 2024, 5 e ss.

Uno degli aspetti più rilevanti di questa trasformazione riguarda l'organizzazione della difesa nazionale, che deve necessariamente includere la cyber-difesa come componente essenziale e integrata. L'Italia, consapevole della portata delle minacce cibernetiche, ha già intrapreso alcune iniziative significative, tra cui la Legge 155/2005 sulla sicurezza delle reti e dei sistemi informativi, che rappresenta un primo passo verso la protezione del cyberspazio nazionale, e l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica, previsto dal decreto-legge n. 105 del 2019, finalizzato a proteggere le infrastrutture critiche da attacchi informatici. Queste misure, pur rappresentando un importante punto di partenza, appaiono insufficienti di fronte alla rapidità con cui evolvono le minacce cibernetiche e alla crescente sofisticazione degli attacchi. Affinché il principio di difesa della patria, sancito dall'articolo 52 della Costituzione, possa evolversi per includere la cyber-difesa, sarà necessario sviluppare una legislazione più specifica e dettagliata, che preveda un adeguato coordinamento tra le autorità civili, militari e private, e che possa garantire una risposta efficace e tempestiva alle minacce informatiche. Ciò potrebbe implicare, tra l'altro, il rafforzamento del ruolo delle forze armate nel campo della cybersicurezza, con l'introduzione di unità cibernetiche specializzate e l'integrazione delle competenze tecnologiche nelle strategie di difesa nazionale.

La guerra cibernetica, tuttavia, non si limita a rappresentare una minaccia di carattere tecnico o operativo, ma impone una riflessione più profonda sul concetto stesso della difesa della Patria. In un'epoca in cui il cyberspazio è diventato un dominio strategico al pari dello spazio fisico, la difesa della patria non può più essere intesa esclusivamente come protezione del territorio nazionale da aggressioni esterne, ma deve necessariamente estendersi alla protezione delle informazioni, delle tecnologie e delle infrastrutture digitali, che sono ormai parte integrante della sicurezza, della stabilità e della prosperità dello Stato.[62] Questa evoluzione richiede una reinterpretazione del principio costituzionale di difesa, che deve includere non solo la protezione fisica del territorio, ma anche la salvaguardia delle risorse informatiche e digitali, considerate ormai come beni comuni essenziali per il funzionamento della società e dell'economia. In questo contesto, il dovere di difesa potrebbe estendersi a forme di resistenza o supporto nella protezione delle risorse informatiche nazionali, coinvolgendo non solo lo Stato e le forze armate, ma anche i cittadini e le aziende private, che spesso rappresentano il primo fronte di difesa contro gli attacchi informatici.

La crescente centralità del cyberspazio e delle infrastrutture critiche impone, dunque, una ridefinizione della difesa nazionale che integri il dominio cibernetico, mantenendo al contempo un equilibrio con la tutela dei diritti fondamentali.[63] Sebbene la Costituzione italiana non menzioni esplicitamente la cyber-difesa, l'evoluzione delle minacce informatiche e la loro potenziale capacità di compromettere la sicurezza nazionale rendono necessario un aggiornamento del quadro giuridico e costituzionale, al fine di garantire una risposta

[62] M.N. Schmitt, The Law of Cyber-Attacks, Cambridge, 2017, 45 ss.

[63] T. Rid, Rise of the Machines: A Cybernetic History, New York, 2021, 78 ss.

adeguata e proporzionata. In questo scenario, il principio di difesa della patria deve evolversi per includere la protezione delle risorse digitali, dei dati e delle infrastrutture critiche, senza tuttavia sacrificare le libertà fondamentali dei cittadini. Per rafforzare la resistenza della Repubblica Italiana agli attacchi cibernetici e alla guerra cibernetica, potrebbero essere necessarie una serie di riforme del diritto pubblico e, se del caso, della Costituzione italiana, finalizzate a proteggere la sicurezza nazionale in un contesto sempre più digitalizzato, dove le minacce informatiche sono destinate a diventare uno degli ambiti principali della difesa nazionale. Tra le principali aree di intervento, si evidenzia la possibilità di aggiornare l'articolo 52 della Costituzione, che attualmente stabilisce il dovere di difendere la patria in termini prevalentemente fisici e convenzionali. La crescente rilevanza delle minacce cibernetiche potrebbe rendere necessaria una riformulazione o un'espansione di questo principio, al fine di includere esplicitamente la difesa cibernetica come parte integrante della difesa nazionale. Una possibile riforma potrebbe prevedere l'aggiunta di un comma che riconosca il cyber-dominio come ambito di difesa, stabilendo il diritto e il dovere dello Stato di proteggere le infrastrutture critiche da attacchi informatici e di garantire la sicurezza informatica nazionale. Parallelamente, potrebbe essere prevista l'integrazione delle forze armate nel campo della cyber-difesa, con la creazione di unità specializzate dedicate esclusivamente alla protezione del cyberspazio, dotate delle competenze tecnologiche necessarie per fronteggiare attacchi informatici sempre più sofisticati.

Un altro aspetto cruciale riguarda la protezione delle infrastrutture critiche, che rappresentano un bersaglio privilegiato per gli attacchi cibernetici. Sebbene l'Italia disponga già di normative in materia, come la Legge 155/2005, sarebbe opportuno introdurre una legislazione più sistematica e integrata, finalizzata a definire in modo più preciso la protezione delle infrastrutture critiche da attacchi informatici. Tale legislazione dovrebbe prevedere misure specifiche per la protezione delle reti energetiche, delle telecomunicazioni, del sistema bancario e sanitario, promuovendo al contempo la cooperazione tra pubblico e privato in materia di cyber-resilience. Inoltre, sarebbe necessario adattare le politiche di difesa civile per includere non solo la difesa fisica, ma anche la protezione digitale di queste risorse fondamentali, garantendo una risposta coordinata ed efficace alle minacce cibernetiche.[64] Il rafforzamento dei servizi di intelligence e della sicurezza nazionale in ambito cibernetico rappresenta un ulteriore pilastro di questa riforma. L'Italia, come molti Paesi, dispone di un sistema di intelligence che include organi come il DIS (Dipartimento delle informazioni per la sicurezza) e l'AISI (Agenzia informazioni e sicurezza interna), ma la guerra cibernetica richiede un potenziamento delle risorse e delle competenze in campo tecnologico. Una possibile riforma potrebbe prevedere l'istituzione di un'agenzia nazionale per la cyber security, con un mandato esplicitamente definito per monitorare, prevenire e rispondere agli attacchi cibernetici a livello strategico, coordinando le attività di cyber-intelligence tra le diverse agenzie di sicurezza. Parallelamente, sarebbe necessario investire nella formazione e

[64] S. Aterno, Sicurezza informatica. Aspetti giuridici e tecnici, Pisa, 2022, 207 e ss.

nell'aggiornamento delle competenze professionali delle forze di sicurezza, al fine di garantire una risposta adeguata alle minacce informatiche. La tutela dei diritti fondamentali e della protezione dei dati personali dei cittadini (oltre che di quelli strategicamente sensibili) rappresenta, infine, una sfida cruciale nel contesto della guerra cibernetica. Le misure di difesa contro gli attacchi informatici non dovrebbero compromettere i diritti fondamentali.. Per questo motivo, sarebbe necessario introdurre normative chiare sulla portabilità dei dati e sulla sorveglianza cibernetica, stabilendo limiti precisi all'uso dei dati personali nel contesto della difesa cibernetica e prevedendo meccanismi di controllo per evitare abusi di potere. Inoltre, sarebbe opportuno istituire un organismo indipendente incaricato di vigilare sulle pratiche di sicurezza informatica, garantendo che le politiche cyber-securitarie siano soggette a un controllo democratico e rispettino i diritti dei cittadini.

In conclusione, le riforme del diritto pubblico e della Costituzione italiana per rafforzare la resistenza agli attacchi cibernetici e alla guerra cibernetica devono mirare a modernizzare le strutture di difesa nazionale, integrando la cybersecurity e la cyber-difesa nelle politiche di sicurezza. Tali riforme dovrebbero garantire una protezione adeguata delle infrastrutture critiche, mantenendo al contempo il giusto equilibrio con i diritti civili e le libertà individuali. Una visione coerente e un approccio integrato a livello giuridico, politico e strategico sono fondamentali per rispondere alle sfide della guerra cibernetica nel contesto globale attuale, garantendo al contempo la tutela dei principi democratici e dei diritti fondamentali sanciti dalla Costituzione italiana.

Conclusioni

Come si è detto, l'evoluzione delle minacce cibernetiche e la crescente centralità del cyberspazio come dominio strategico (sia militare che civile) impongono una ridefinizione del concetto di difesa della patria, che non può più limitarsi alla protezione fisica del territorio nazionale, ma deve necessariamente estendersi alla salvaguardia delle infrastrutture digitali, delle informazioni e delle tecnologie, ormai considerate beni comuni essenziali per la sicurezza e la stabilità dello Stato.

Questo passaggio, inevitabilmente, dovrà portare ad una revisione della dottrina giuridica, che avrà la necessità di adattarsi alle nuove tecniche "conflitto ibrido" in cui l'anonimato, la difficoltà di attribuzione della responsabilità e l'asimmetria tra attori statali e non statali complicano l'applicazione delle tradizionali regole del diritto internazionale e la conseguente sussunzione dei fenomeni sotto le categorie del diritto pubblico. L'affermazione del cyberspazio come un dominio terra di scontro attuale e futuro di nuove forme di guerra, richiederà un adeguamento delle norme internazionali esistenti per regolamentare l'uso della forza nel contesto digitale e garantire che i principi di proporzionalità e distinzione vengano rispettati anche nei conflitti cibernetici.

La natura stessa della guerra cibernetica, sfumata rispetto ai tradizionali conflitti armati, rende complessa l'applicazione di queste norme, in quanto gli attacchi non sempre assumono una configurazione chiara e immediata, ponendo interrogativi sull'efficacia della risposta giuridica e istituzionale.

In questo scenario, la cyber-sicurezza dovrà diventare una priorità strategica della Sicurezza nazionale, richiedendo un aggiornamento del quadro normativo e costituzionale italiano. In particolare, una riforma dell'articolo 52 della Costituzione (e forse anche dell'interpretazione dottrinaria dell'11) potrebbe includere esplicitamente la cyber-difesa come parte integrante della difesa nazionale, riconoscendo il cyberspazio come un dominio di conflitto e stabilendo il diritto e il dovere dello Stato di proteggere le infrastrutture critiche da attacchi informatici.

Parallelamente, l'integrazione della cyber-difesa nelle politiche nazionali dovrà avvenire attraverso una legislazione più sistematica e coordinata, che promuova la cooperazione tra pubblico e privato e rafforzi le competenze tecnologiche delle forze di sicurezza e dei servizi di intelligence. In questo contesto, il rafforzamento delle capacità di cyber-intelligence diventerebbe essenziale: l'Italia, come gli altri Stati europei, deve affrontare le sfide legate all'asimmetria tecnologica e alla responsabilità internazionale per gli attacchi cibernetici, elaborando strategie di protezione delle infrastrutture critiche e di prevenzione delle minacce digitali.

La creazione dell'Agenzia Nazionale per la Cybersicurezza (ACN) ha rappresentato un passo fondamentale per monitorare, prevenire e rispondere alle minacce informatiche, in maniera coordinata ed efficace, evitando frammentazioni istituzionali e garantendo un coordinamento strategico tra le diverse agenzie di sicurezza ma è solo il "primo passo" verso l'adeguamento dell'intero sistema Istituzionale. Qualsiasi riforma in materia di cyber-difesa dovrà necessariamente bilanciare le esigenze della sicurezza nazionale con la tutela dei diritti fondamentali, evitando che le misure di prevenzione e difesa attiva si traducano in una limitazione eccessiva delle libertà civili. La guerra cibernetica pone, quindi, sfide inedite non solo dal punto di vista strategico e tecnologico, ma anche in termini di rispetto dei diritti umani e delle libertà costituzionali, in particolare per quanto riguarda la tutela e la portabilità dei dati, la libertà di espressione e la protezione dei dati personali. L'efficacia della risposta italiana alle minacce cibernetiche dipenderà dalla capacità di integrare la cyber-difesa nelle strategie di sicurezza nazionale e nella cooperazione internazionale.

La dimensione globale del cyberspazio rende essenziale un approccio multilaterale alla sicurezza informatica, che includa la collaborazione con gli alleati europei e internazionali, la condivisione di informazioni e l'adozione di norme comuni per la regolamentazione delle operazioni cibernetiche.

L'Italia dovrà trovare un equilibrio tra la difesa delle proprie infrastrutture critiche e il rispetto dei principi di sovranità digitale degli altri Stati, evitando di ricorrere a strategie di cyber-difesa aggressive che potrebbero innescare escalation indesiderate.

Il riconoscimento del cyberspazio come una nuova frontiera della sicurezza nazionale non deve tradursi in una militarizzazione indiscriminata del dominio digitale, ma piuttosto in un modello di governance che concili sicurezza, diritti fondamentali e cooperazione internazionale. Solo attraverso un approccio integrato e coerente, fondato sui valori democratici e costituzionali, sarà possibile garantire una risposta efficace e proporzionata alle sfide della guerra cibernetica nel contesto globale contemporaneo. Parimenti, solo riuscendo a sviluppare un'adeguata conoscenza e sperimentazione delle nuove tecnologie offensive cibernetiche, in dei virtuali banchi di prova (sand boxes) alleggeriti rispetto alla normale regolazione UE di settore, si potrà costruire delle risposte normative e strumentali efficaci per contrastare e prevenire gli attacchi ostili.

Non si può normare qualcosa che non si sa definire giuridicamente e che, pertanto, prima non si è provato e riscontrato nella realtà.

FONTI PRINCIPALI

- S. Aterno, Sicurezza informatica. Aspetti giuridici e tecnici, Pisa, 2022.
- A. Baratta, "Diritto alla sicurezza o sicurezza dei diritti?", in S. Anastasia, M. Palma (a cura di), La bilancia e la misura. Giustizia, sicurezza e riforme, Milano, 2001, 24 ss.
- R. Bifulco, M. Benvenuti (a cura di), Trattato di diritto costituzionale, vol. III, I diritti e i doveri costituzionali, 2022, 34-37.
- J. Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, New York, 2011.
- F. Caffio, J. P. Pierini, "La protezione delle infrastrutture critiche subacquee in tempo di pace: profili giuridici", Rivista Marittima, luglio-agosto 2023, 40 ss.
- L. Califano, V. Fiorillo, "Videosorveglianza", in R. Bifulco, A. Celotto, M. Olivetti (a cura di), Digesto delle discipline pubblicistiche (aggiornamento), Torino, 2015, 503 ss.
- P. Carnevale, La Costituzione va alla guerra?, Napoli, 2013.
- P. Ceruzzi, Storia dell'informatica. Dai primi computer digitali all'era di Internet, Milano, Apogeo, 2006.
- C. Cinelli, "Il regime giuridico di condotte e cavi sottomarini", in A. Caligiuri, I. Papanicolopulu, L. Schiano Di Pepe, R. Virzo (a cura di), Italia e diritto del mare, Napoli, 2023.
- B. Conforti, Il regime giuridico dei mari, Napoli, 1957.
- G. de Vergottini, Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia, Bologna, 2004.
- G. de Vergottini, "Le nuove sfide del diritto costituzionale nell'era digitale", in Diritto costituzionale, Padova, CEDAM, 2020, 567-589.
- G. de Vergottini, Diritto costituzionale, Padova, CEDAM, 2020, 345 ss.

- F. Di Cocco, “La guerra cibernetica e il diritto internazionale”, Rivista di diritto internazionale, 2020, 567 ss., https://www.rivistadirittointernazionale.it.
- ENISA — European Union Agency for Cybersecurity, NIS Investments 2022, 2022, https://www.enisa.europa.eu/publications/nis-investments-2022.
- European Commission, “Questions and Answers: The EU Policy on Cyber Defence”, 10 novembre 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6643.
- European Defence Agency (EDA), CYBER PHALANX — Factsheet, s.d., https://eda.europa.eu/docs/default-source/eda-factsheets/cyph-fact-sheet_v03-eda.pdf.
- G. Finocchiaro, “La sovranità digitale”, Diritto Pubblico, 3, 2022, 809 ss.
- C. Galli, Sovranità, Bologna, 2019.
- U. Grozio (H. Grotius), De jure belli ac pacis, trad. it. a cura di C. Galli e A. Del Vecchio, Napoli, 2023.
- F. G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, Potomac Institute for Policy Studies, 2007.
- L. Martino, “Sovranità digitale e competizione geopolitica nel contesto dei cavi sottomarini: analisi comparata di Cina, Stati Uniti e Unione europea”, MediaLaws, 2, 2024, 144 ss.
- M. L. Mariscal, International Cybersecurity: Law, Policy, and Strategy, Oxford, 2020.
- Malta, Continental Shelf Act, Act XXVIII of 2014, art. 4(1)(d).
- M. Nisticò, “Cybersecurity e Costituzione”, Quaderni costituzionali, 2019, 123 ss.
- NATO, NATO’s Response to Hybrid Threats, Bruxelles, 2015, 23 ss., S. Aterno, Sicurezza informatica. Aspetti giuridici e tecnici, Pisa, 2022.
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), “Sito istituzionale”, https://ccdcoe.org/.

- AgID — Agenzia per l'Italia Digitale, Piano nazionale cyber (pagina istituzionale), 2024, https://www.agid.gov.it/sites/agid/files/2024-05/piano-nazionale-cyber_0.pdf.
- O. Pollicino, Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?, Oxford, 2021.
- O. Pollicino, "Potere digitale", in M. Cartabia, M. Ruotolo (a cura di), Potere e Costituzione, Enciclopedia del Diritto, V, Milano, 2023.
- F. P. Pizzetti, "La protezione dei dati personali nell'era digitale: sfide e prospettive", in G. Scorza, A. Sica (a cura di), Cybersecurity e privacy: nuove frontiere del diritto, Roma, 2022, 89-112.
- A. Prakash, "Come le aziende tecnologiche stanno plasmando il conflitto in Ucraina", Le Scienze, 2 novembre 2022.
- S. D. Reid, Cyber Warfare and International Politics: A Study of Cyber Conflict, London, 2018.
- T. Rid, Cyber War Will Not Take Place, Oxford, 2013.
- T. Rid, "The Myth of Cyber War", in The Oxford Handbook of Cyber Security, Oxford, 2016, 123-145.
- T. Rid, Rise of the Machines: A Cybernetic History, New York, 2021.
- S. Romano, Corso di diritto internazionale, Padova, 1939, 194 ss.
- M. Ruotolo, "Costituzione e sicurezza tra diritto e società", in A. Torre (a cura di), Costituzioni e sicurezza dello Stato, Rimini, 2014, 588 ss.
- M. N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge, Cambridge University Press, 2017.
- M. N. Schmitt, "Cyber Operations and the Jus in Bello", International Law Studies, vol. 87, 2013, 67 ss., https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1077&context=ils.

Atti di convegno

L'epoca delle guerre ibride e le nuove frontiere delle attività di intelligence

Mario Schirripa
Ricercatore - Università degli Studi 'Mediterranea' di Reggio Calabria

"The age of hybrid warfare and the new frontiers of intelligence activities"

Abstract

2023 Report on Information Policy for Security highlights that cyber and hybrid threats are becoming increasingly dangerous for the stability of both European and national security, requiring targeted strategies and international cooperation. The complexity of the issue calls for a new security culture that integrates technological, regulatory, and intelligence tools. Intelligence is playing an increasingly central role in defending democracies and the rule of law. Not by chance, even in Italy, legislation is assigning increasingly significant responsibilities to the intelligence sector to safeguard the salus rei publicae.

Keywords: Hybrid warfare - Disinformation - Intelligence - Cybersecurity - Cooperation

1. Le nuove guerre ibride tra disinformazione e attacchi cibernetici

Dalla lettura dell'ultima 'Relazione sulla politica dell'informazione per la sicurezza' relativa all'operato di DIS (Dipartimento delle informazioni per la sicurezza), AISI (Agenzia informazioni e sicurezza interna) e AISE (Agenzia informazioni e sicurezza esterna) nel 2023, emerge che saremo «chiamati ogni giorno di più a confrontarci con minacce cyber e ibride, comprese le campagne di disinformazione, e l'uso dannoso di tecnologie emergenti sempre più sofisticate, come l'intelligenza artificiale, per fini malevoli»[1].

La sicurezza cibernetica ha costituito oggetto di approfondimento anche da parte del COPASIR (Comitato parlamentare per la sicurezza della Repubblica) nell'ambito di diverse audizioni e all'interno delle relazioni annuali sulle attività svolte[2], ad ulteriore riprova dell'accresciuta esposizione di molteplici settori ad attacchi e minacce a livello globale. Emerge, dunque, che il campo di battaglia non è più solo quello fisico[3], fatto di carrarmati, droni, armi e militari, ma è sempre più quello virtuale, che sfrutta le tecnologie più progredite per colpire "in silenzio" il nemico, attraverso lo spionaggio, la propaganda, la disinformazione e/o l'attacco informatico, penetrando nelle sue strutture interne e strategiche[4].

Ci si trova dinanzi ad un nuovo equilibrio geopolitico, all'interno del quale il ruolo di uno Stato nella competizione globale è definito più dal livello di innovazione tecnologica che dalla potenza militare ed economica in quanto tali, poiché queste ultime due variabili dipendono ormai dalla prima[5]. In questo scenario, le guerre contemporanee assumono una forma ibrida[6], pianificata ed alimentata dalla disinformazione, dalla produzione sistematica di false notizie e da attacchi cibernetici[7].

---

[1] La Relazione è disponibile al link https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true. Il passaggio riportato si trova a p.52.
Per un commento sulla Relazione, si consiglia la lettura di M. Santarelli, Relazione Intelligence 2023: la risposta dell'Italia a minacce ibride e conflitti globali, in www.agendadigitale.eu, 7 marzo 2024.

[2] Per un approfondimento vd. Relazione del Copasir sull'attività svolta dal 6 dicembre 2022 al 31 dicembre 2023 su https://parlamento18.camera.it/228.

[3] Per una riflessione su come sia, nel tempo, evoluto il concetto di guerra vd. G. de Vergottini, Guerra e costituzione. Nuovi conflitti e sfide alla democrazia, il Mulino, 2004; A. Vedaschi, À la guerre comme à la guerre. La disciplina della guerra nel diritto costituzionale comparato, Torino, 2007.

[4] I settori più colpiti sono le filiere delle infrastrutture digitali/servizi IT, dell'energia, dei trasporti e il settore pubblico-istituzionale.

[5] Così A. Pagani, La guerra cibernetica nell'età ibrida: tecnologie, strategie e priorità, in www.agendadigitale.eu, 22 luglio 2021.

[6] Sul concetto di guerra ibrida si veda il recente contributo di C. Sbailò, Guerre ibride: quali risposte possibili?, in DPCE online, vol. 63, no. SP1, 2024.

[7] Vd., in proposito, A. Spaziani, L'attacco cibernetico nell'era della guerra ibrida, in DPCE online, vol. 63, no. SP1, 2024 e F. Nisticò, L'elemento cyber nella guerra russo-ucraina, in aspeniaonline.it, 3 marzo 2022.

L'ingerenza sempre maggiore delle nuove tecnologie nelle guerre di oggi ha portato a coniare nuovi termini quali information warfare[8], cyberwarfare[9], electronic warfare[10], psychological warfare[11], hacker warfare[12], economic information warfare[13], tutte diverse declinazioni della hybrid warfare.

Se ci si sofferma sull'impiego della disinformazione come arma, il conflitto russo-ucraino ne rappresenta un esempio perfetto sin dal suo inizio quando, il 22 febbraio 2022, il presidente Putin definì «operazione militare speciale»[14] quella che, di fatto, è stata l'invasione di uno Stato sovrano, una guerra a tutti gli effetti. Sin dal principio, quindi, il tentativo di condizionare l'opinione pubblica è stato imponente e senza precedenti. È stata scientificamente architettata una campagna di disinformazione con diffusione di fake news frutto di una strategia ben congegnata[15].

Sia chiaro, concetti come 'disinformazione' e 'guerra ibrida' non nascono certo oggi. Si possono trovare degli esempi che risalgono alla storia dei tempi: dal famoso mito del cavallo di Troia al celebre trattato di strategia militare di Sun Tzu, L'arte della guerra, in cui l'autore sosteneva che «l'inganno è il Tao della Guerra».

Quello che cambia significativamente nell'epoca attuale è il grado di penetrazione delle tecnologie in ogni ambito dell'esistenza, il loro grado di pervasività e di diffusione che mette fuori gioco gran parte delle norme[16].

---

[8] La guerra spostata sui media, che pone al centro della sua attenzione l'informazione e il cui obiettivo è quello di ottenere un vantaggio informativo sull'avversario. Può dirsi che si tratta di una tecnica di conflitto che trasforma i mezzi di informazione in armi che entrano a pieno titolo nel campo di battaglia. Sull'evoluzione dell'Information Warfare si veda M.C. Libicki, The Convergence of Information Warfare, in Strategic Studies Quarterly, Volume 11, Issue 1, 2017, pp.49-65.

[9] Ovvero l'attività e la modalità di combattimento attraverso gli strumenti informatici volta a manipolare o distruggere i sistemi informativi per scopi strategici, politici o militari.

[10] Che impiega strumenti radio, elettronici e crittografici.

[11] Che mira ad influenzare le opinioni di persone e comunità attraverso le PSYOP(psychological operations).

[12] Riguarda gli attacchi alle reti telematiche.

[13] Attiene alla sicurezza e agli interessi economici nazionali.

[14] Sul punto, si consiglia la lettura di I. Galimova, L'"operazione militare speciale" in Ucraina e la reazione del sistema politico russo, in Nomos. Le attualità del diritto, n.1, 2022 (https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2022/06/RUSSIA-1_2022formattato.pdf)

[15] Sul tema della disinformazione si veda, ex multis, M. Caligiuri, A. Pagani, M. Chioso, Disinformare: ecco l'arma. L'emergenza educativa e democratica del nostro tempo, Rubbettino, 2024; S. Sassi, Disinformazione contro Costituzionalismo, Editoriale Scientifica, Napoli, 2021;A. Alù, Perché la disinformazione minaccia le democrazie nel 2024, in agendadigitale.eu, 7 febbraio 2024; M. Caligiuri, Come i pesci nell'acqua. Immersi nella disinformazione, Rubbettino, Soveria Mannelli, 2019; G. Pitruzzella, O. Pollicino, Disinformation and Hate Speech. A European Constitutional Perspective, Egea, Milano, 2020; C. Pinelli, C. Hassan, Disinformazione e democrazia, Marsilio Editori, 2022.

[16] Cfr. H. Kissinger, Ordine Mondiale, Mondadori, 2017, p.339.

L'arma della disinformazione implica effetti sotto diversi profili: sociali, economici e culturali. Basti pensare al fenomeno della polarizzazione creato dalle cd. echo chambers (bolle informative chiuse); alla sfiducia nelle istituzioni; alle campagne mirate su cleavages identitari; agli effetti della manipolazione informativa sui mercati (vendite, brand, indici di borsa); alle campagne sul revisionismo storico; allo sfruttamento delle fratture sociali (migrazioni, minoranze, diritti); al tentativo di alterare gli esiti delle elezioni politiche, come sembrerebbe sia avvenuto in Romania nel 2024[17].

Per contrastare tali minacce, la Svezia, sin dal 2022, si è dotata della Psychological Defence Agency, un'agenzia governativa che ha il compito di «identify, analyse and provide support in countering malign information influence and other misleading information that is directed at Sweden or Swedish interests by antagonistic foreign powers. This can concern disinformation aimed at weakening Sweden's resilience and the willingness of the population to defend itself, or unduly influencing people's perceptions, behaviours and decision-making»[18], ad ulteriore riprova che la sicurezza nazionale di un Paese dipende, ormai, anche dalla sua capacità di risposta alle insidie della disinformazione e degli attacchi informatici.

Nell'ambito dello spionaggio informatico, tali attacchi sono realizzati da attori statuali denominati Advanced Persistent Threat (APT) una tipologia di attacchi mirati e persistenti con tecniche hacking avanzate[19]. Attribuire un attacco informatico ad un gruppo ATP è un'operazione complessa e di difficile realizzazione, tuttavia alcuni di essi diventano inevitabilmente di pubblico dominio in conseguenza dei loro effetti esterni. Si pensi al virus Stuxnet, il primo malware della guerra cyber, creato nel 2010 da Usa e Israele per bloccare il programma nucleare iraniano. È considerato il primo atto di cyberwar al mondo e all'epoca compromise il sistema di controllo automatico delle centrifughe in un sito iraniano di arricchimento dell'uranio, mettendo in risalto in modo clamoroso la vulnerabilità degli impianti industriali agli attacchi cibernetici. Ancora più sconcertante fu scoprire che l'episodio era stato provocato da una semplice pen drive USB infetta, estendendo così la portata della minaccia all'intero settore industriale globale.

Rispetto alle cd. guerre convenzionali, l'hybrid warfare si caratterizza per la sua ambiguità, poiché l'attribuzione degli attacchi è spesso incerta, creando difficoltà nelle risposte politiche e strategiche; per l'incertezza degli effetti, poiché gli attacchi informatici possono assumere esiti imprevedibili; per la capacità di persistenza, poiché le operazioni cibernetiche possono essere condotte senza interruzioni, a differenza dei conflitti cinetici.

---

[17] Per un approfondimento si rimanda a F. Rosa, L'annullamento delle elezioni presidenziali in Romania e la difficile difesa della democrazia, in Federalismi.it, n.15, 2025, pp. 53-75.

[18] Vd. https://mpf.se/psychological-defence-agency/about-us/our-mission.

[19] Sul punto si veda R. Baldoni, Sovranità digitale. Cos'è e quali sono le principali minacce al cyberspazio nazionale, Il Mulino, Bologna, 2025, p. 61 e ss.

Ad oggi, non esiste un solo settore impermeabile al cyber space: servizi economici e finanziari, sistemi di comando e controllo militare, sistemi di fornitura di energia elettrica o acqua, l'assistenza sanitaria, le telecomunicazioni, dispositivi fisici con cui si interagisce giornalmente, sono tutti controllati da sistemi informatici. La complessità della questione necessita di una nuova cultura della sicurezza che coinvolga strumenti tecnologici, normativi e di intelligence. Quest'ultima assume un ruolo sempre più centrale per la difesa delle democrazie e dello Stato di diritto, non a caso, anche in Italia, per legge, si stanno assegnando compiti sempre più rilevanti al comparto intelligence per affrontare le nuove sfide della sicurezza informatica[20].

2. Il ruolo guida dell'Agenzia per la Cybersicurezza Nazionale italiana

Con l'adozione del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è stata istituita l'Agenzia per la cyber sicurezza nazionale (ACN), la cui missione istituzionale è quella di potenziare la resilienza cibernetica del Paese[21], riducendone il grado di vulnerabilità e incrementandone l'autonomia e l'indipendenza tecnologica, con la finalità di assicurare una maggiore competitività nello scenario internazionale laddove le operazioni di cyber-intelligence rimangono di esclusiva e peculiare competenza del Comparto informativo[22]. Si è, così, colmata una importante lacuna[23] che l'Italia scontava da decenni, soprattutto se posta a confronto con i maggiori partner europei[24].

Va segnalato che il percorso che ha condotto alla stesura del testo normativo che ha definito le competenze dell'ACN e ridisegnato l'architettura di cybersicurezza nazionale, ha registrato il coinvolgimento del COPASIR fin dalle prime fasi. Tale coinvolgimento

---

[20]Ex plurimis, si veda C. Mosca, Democrazia e intelligence italiana. Dieci anni dopo tra cultura, diritto e nuove sfide della democrazia, Editoriale scientifica, 2018, pp. 161-197; M. Caligiuri, Cyber intelligence. Tra libertà e sicurezza, Donzelli, 2016.

[21] Sull'attività dell'ACN ed il suo obiettivo di accompagnare una trasformazione digitale in sicurezza per la prosperità e l'indipendenza dell'Italia, vd. R. Baldoni, Così l'Agenzia cyber sta lavorando e dispiega i propri effetti, in agendadigitale.eu, 18 novembre 2021 (https://www.agendadigitale.eu/sicurezza/baldoni-cosi-lagenzia-cyber-sta-lavorando-e-dispiega-i-propri-effetti/).

[22]L'istituzione dell'Agenzia per la Cybersicurezza Nazionale è ritenuta uno snodo fondamentale nell'architettura generale dell'intelligence nella "Relazione sulla politica dell'informazione per la sicurezza" relativa all'anno 2021, curata dal Comparto Intelligence, ai sensi della quale il Governo riferisce ogni anno al Parlamento con una Relazione non classificata sulla politica dell'informazione per la sicurezza (https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2021.html). Si veda anche la Relazione del Copasir sull'attività svolta dal 1° gennaio 2021 al 9 febbraio 2022, pp. 35-37 e 100-101 (https://www.senato.it/service/PDF/PDFServer/BGT/1332539.pdf).

[23] L'Italia si trova costantemente esposta ad attacchi cibernetici, in taluni casi anche con effetti di notevole ampiezza e gravità. Si pensi ad esempio al caso dell'attacco sferrato alla fine del mese di luglio del 2021 nei confronti dei sistemi informatici della Regione Lazio e le conseguenti ricadute sulle attività e i servizi erogati dalla Regione stessa, compresi quelli connessi con il Sistema sanitario regionale in un periodo particolarmente critico come quello che stiamo vivendo a causa della pandemia da SARS-CoV-2.

[24] Per un confronto tra l'Agenzia per la cybersicurezza nazionale e gli omologhi organismi europei, vd. M. Artini, Agenzia Cibernetica Nazionale italiana, confrontiamola con gli altri attori europei, in agendadigitale.eu, 17 gennaio 2022 (https://www.agendadigitale.eu/sicurezza/lagenzia-cibernetica-nazionale-italiana-il-confronto-con-gli-altri-attori-europei/).

è apparso naturale se si considera che all'agenzia sono state trasferite anche le competenze sulla resilienza in ambito cibernetico fino ad allora affidate al Dipartimento delle informazioni per la sicurezza (DIS). Il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, attribuisce al Copasir alcune specifiche competenze ricalcando sostanzialmente quanto previsto dalla legge n. 124 del 2007 nell'ambito del Sistema di informazione per la sicurezza della Repubblica. Il Presidente del Consiglio e l'ACN sono sottoposti, infatti, ad una serie di oneri informativi che hanno come destinatari il Copasir e le Commissioni parlamentari competenti. In primo luogo, il Presidente del Consiglio dei ministri informa preventivamente tali destinatari sulle nomine del direttore e del vice direttore dell'Agenzia (articolo 2, comma 3). Inoltre, l'Agenzia invia al Copasir e alle Commissioni competenti il bilancio consuntivo accompagnato dalla relazione della Corte dei conti (articolo 11, comma 3) e dà tempestiva e motivata comunicazione dei provvedimenti adottati in materia di dotazione organica (articolo 12, comma 5). Vi sono poi ulteriori oneri informativi riguardanti unicamente il Copasir che viene informato da parte del Presidente del Consiglio sulla determinazione del fabbisogno annuo dell'Agenzia (articolo 11, comma 1) e riceve, entro il 30 giugno di ogni anno, la relazione sulle attività dell'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico, relativamente ai profili di competenza del Copasir (articolo 14, comma 2). Infine, il Presidente del Consiglio informa il Comitato sulle spese per la prima operatività dell'Agenzia fino all'adozione dei regolamenti di contabilità e su appalti e forniture (articolo 17, comma 7). L'Agenzia, inoltre, costituisce l'organismo che, per l'Italia, terrà le relazioni con il Centro di competenza europeo in cybersecurity (ECCC). Tale organismo, con sede a Bucarest, collaborando con la rete dei centri nazionali di coordinamento designati dagli Stati membri, aiuterà l'Unione europea ad aggregare e collegare in rete le sue competenze nello sviluppo industriale, nella tecnologia e nella ricerca sulla cyber sicurezza e a promuovere la diffusione delle soluzioni più recenti nel campo della sicurezza informatica. Pur osservando che il citato decreto-legge 14 giugno 2021, n. 82, non interviene sulla legge 3 agosto 2007, n. 124, è evidente la stretta interconnessione determinata dal fatto che la sicurezza cibernetica è una sfera sempre più rilevante della sicurezza nazionale. Il coordinamento tra il comparto dell'intelligence e l'Agenzia per la cybersicurezza nazionale risulta, dunque, fondamentale. Può dirsi che all'ACN spettino le attività di prevenzione e mitigazione degli attacchi cibernetici, mentre gli interventi di reazione e di contrasto a questi ultimi competono agli apparati di intelligence. Tali aspetti andrebbero definiti con una revisione della legge n. 124, al fine di armonizzare le nuove disposizioni di legge relative all'ACN, delineare i perimetri di competenza ed evitare sovrapposizioni[25].

---

[25] Sul dibattito, sempre più attuale, relativo all'aggiornamento della l.124 del 2007 vd. A. Monti, Il rinnovamento dell'intelligence ha bisogno di coerenza normativa, in formiche.net, 6 dicembre 2020 (https://formiche.net/2020/12/il-rinnovamento-dellintelligence-ha-bisogno-di-coerenza-normativa/); G. Carrer, Riforma dell'intelligence? Sì, dicono Pagani (Pd), Perego (FI) e Tofalo (M5S), in formiche.net, 29 luglio 2021 (https://formiche.net/2021/07/riforma-intelligence-pagani-perego-tofalo/); U. Saccone, Quale Intelligence per il futuro?, in formiche.net, 2 agosto 2021 (https://formiche.net/2021/08/riforma-intelligence-

2.1 Le attività svolte dall'ACN e la Direttiva NIS 2

Per misurare lo stato di salute della sicurezza cibernetica in Italia risultano preziose le relazioni annuali sulle attività svolte dall'ACN, in cui vengono illustrate le minacce affrontate, le azioni intraprese e le strategie per migliorare la resilienza digitale del Paese[26]. Il 2023 è stato caratterizzato da un aumento significativo delle aggressioni cibernetiche, spesso collegate a conflitti internazionali (si pensi, in particolare, a quanto accade in Ucraina e Medio Oriente). Uno dei pilastri su cui regge l'attività dell'ACN è rappresentato dal Computer Security Incident Response Team (CSIRT), l'organo dell'Agenzia per la cybersicurezza nazionale che si occupa di monitoraggio preventivo e risposta agli incidenti informatici. Il CSIRT Italia, solamente nel 2023, ha monitorato e gestito oltre 1.400 eventi cyber - con un aumento del 30% rispetto al 2022 - di questi, 303 sono stati classificati come incidenti, per una media di circa 25 al mese, più che raddoppiati rispetto all'anno precedente. Gli attacchi DDoS[27] sono aumentati del 625%, molti dei quali legati al cyber-attivismo filo-russo e filo-palestinese. Il ransomware[28] rimane la minaccia più grave, con un incremento del 27% rispetto al 2022, che ha portatol'Italia ad essere il terzo Paese dell'Unione europea più colpito da ransomware nel 2023 ed il sesto a livello globale[29]. Come se non bastasse, sempre nel solo 2023, sono stati segnalati 584 tentativi di phishing[30]e analizzati 100 malware[31]. Sono numeri impietosi che hanno condotto, sul piano normativo, all'implementazione della Direttiva NIS 2[32] per rafforzare la sicurezza delle reti e sistemi

---

umberto-saccone-ifi/); F. Bechis, Non solo cyber, così riformiamo l'intelligence. Parla Franco Gabrielli, in formiche.net, 14 agosto 2021 (https://formiche.net/2021/08/non-solo-cyber-cosi-riformiamo-lintelligence-parla-franco-gabrielli/).

[26] Vd. Relazione annuale al Parlamento dell'ACN del 2023 e del 2022, entrambe consultabili al seguente link https://www.acn.gov.it/portale/relazione-annuale. Sull'importanza dell'attività svolta dall'ACN si legga R. Baldoni, Il ruolo guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) verso la Cyber-Resilienza Nazionale: sinergie pubblico-private, in U. Gori (a cura di), Cyber Warfare 2021-2022. Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato, Franco Angeli, 2023, pp. 21-25.

[27] Gli eventi DDoS (Distributed Denial of Service) mirano a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. L'effetto più immediato di tale tipologia di attacco è l'indisponibilità del sito o del servizio colpito.

[28] In questo tipo di minaccia l'attaccante, di regola, si introduce nei sistemi di un privato o di un'organizzazione per cifrarne i dati, al fine di ottenere il pagamento di un riscatto per rendere nuovamente disponibili i dati al legittimo proprietario e/o non diffonderli pubblicamente.

[29] Sui numeri del CSIRT Italia vd. Relazione annuale al Parlamento dell'ACN del 2023, pp. 9-20.

[30] Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (user ID, password, numeri di carte di credito, PIN) con l'invio di false e-mail generiche a un gran numero di indirizzi. Le e-mail sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. L'attaccante utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

[31] Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

[32] La Direttiva NIS 2 (Direttiva UE 2022/2555) supera e rafforza l'impianto normativo previsto dalla precedente Direttiva NIS (Direttiva (UE) 2016/1148), facendo tesoro dell'esperienza acquisita nella sua applicazione.

informativi essenziali. La nuova direttiva amplia il numero di settori e soggetti obbligati ad adottare misure di cybersicurezza, includendo settori come energia, trasporti, sanità, servizi finanziari e pubblica amministrazione e l'ACN è coinvolta nell'attuazione normativa e nel monitoraggio dell'adeguamento delle aziende e delle amministrazioni pubbliche.

Le principali novità introdotte dalla Direttiva NIS 2 consistono: nell'espansione del perimetro di applicazione (mentre la prima NIS si applicava solo agli "Operatori di Servizi Essenziali" e ai "Fornitori di Servizi Digitali", la NIS 2 include nuove categorie di soggetti, come enti pubblici e aziende di rilevanza economica); in obblighi più stringenti per la gestione del rischio (i soggetti coinvolti devono implementare misure avanzate di sicurezza, come i sistemi di gestione del rischio basati su valutazioni periodiche delle vulnerabilità, i piani di gestione degli incidenti con una chiara definizione delle responsabilità, le misure di prevenzione e risposta contro attacchi cyber); in una maggior cooperazione tra Stati membri (la NIS 2 rafforza i meccanismi di scambio di informazioni tra le autorità nazionali ed europee in caso di crisi cibernetiche); nell'introduzione di sanzioni (i soggetti che non rispettano gli obblighi di sicurezza possono essere sanzionati con multe proporzionali alla gravità della violazione).

La Direttiva NIS 2 rappresenta, dunque, un cambiamento radicale nel quadro normativo europeo sulla cybersicurezza ed una sfida per le infrastrutture critiche italiane, che devono adeguarsi a standard più elevati in termini di sicurezza cibernetica.

In questo processo, sarà compito dell'ACN quello di garantire il coordinamento nazionale, supportare il recepimento della normativa e assistere i soggetti interessati[33].

3. Uno sguardo comparato alle agenzie di cybersicurezza europee

Allargando lo sguardo al di là dei confini nazionali, una breve analisi delle esperienze di Francia, Regno Unito e Spagna può contribuire a comprendere la grande rilevanza che il tema della cyber intelligence ricopre anche all'estero. In Francia, un ruolo fondamentale è svolto dall'Agenzia nazionale della sicurezza dei sistemi di informazione (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI), che è il principale soggetto incaricato di misurare e valutare i rischi e gli effetti degli attacchi informatici, rivolti sia ai soggetti pubblici sia ai privati.

---

[33] A tal proposito il Servizio Operazioni e gestione delle crisi cyber di ACN, il 22 febbraio 2025, ha pubblicato un rapporto sulla minaccia Denial of Service (DoS) e Distributed Denial of Service (DDoS), analizzando le strategie d'attacco più diffuse e fornendo raccomandazioni specifiche per la mitigazione del rischio. Per consultare il rapporto vd. https://www.acn.gov.it/portale/w/acn-pubblica-il-rapporto-sugli-attacchi-ddos.

Il ruolo dell'ANSSI è quello di promuovere una risposta coordinata ed efficiente ai problemi di della sicurezza digitale in Francia. L'Agenzia, istituita con il Décret n. 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information», svolge in particolare le seguenti funzioni: assicura la funzione di autorità nazionale per la difesa dei sistemi di informazione e, in questa veste, propone al Primo ministro misure per rispondere alle crisi che incidono o minacciano la sicurezza dei sistemi di informazione delle autorità pubbliche; progetta, fa realizzare e attua i mezzi interministeriali sicuri di comunicazioni elettroniche necessari per il Presidente della Repubblica e il Governo; anima e coordina i lavori interministeriali sulla sicurezza dei sistemi informativi; elabora le misure di protezione dei sistemi di informazione proposti al Primo ministro; assicura l'applicazione delle misure adottate; effettua ispezioni dei sistemi informativi dei servizi statali e degli operatori pubblici o privati[34].

L'ANSSI fa riferimento al Segretario della difesa e della sicurezza nazionale (Secrétaire général de la défense et de la sécurité nationale), che assiste il Primo ministro nell'esercizio delle sue responsabilità in materia di difesa e sicurezza. La Direzione dell'ANSSI è affidata a un Direttore generale, nominato dal Primo ministro. Così come in Francia, nel Regno Unito il tema della sicurezza delle infrastrutture di interesse nazionale (critical national infrastructures – CNI) e della loro esposizione al rischio di attacchi cibernetici è stato oggetto, negli ultimi anni, di specifiche iniziative del Governo e del Parlamento.

Significative innovazioni in materia di cybersicurezza si correlano all'adozione, nel 2016, del pioneristico piano strategico nazionale quinquennale ad essa specificamente dedicato (National Cyber Security Strategy 2016-2021 - NCSS, dotata di uno stanziamento di 1,9 miliardi di sterline) ed alla più recente Government Cyber Security Strategy 2022–2030[35]. In particolare, si è provveduto ad istituire un organismo tecnico ad hoc, il National Cyber Security Centre (NCSC), preposto alla gestione degli incidenti di rilievo nazionale nel campo della cibersicurezza e all'assistenza tecnica diretta ai dipartimenti governativi, alle amministrazioni pubbliche e alle imprese attraverso attività di analisi e di individuazione delle minacce, di consulenza, di promozione dell'innovazione e delle competenze professionali in materia. Il National Cyber Security Center è divenuto, così, il braccio per la sicurezza informatica del Government Communications Headquarters (GCHQ)[36], l'agenzia di intelligence britannica nata come British Signals Intelligence nell'agosto del 1914[37], durante la Prima Guerra Mondiale, al fine di istituire un organo deputato all'intercettazione e

[34] Per un approfondimento sulla normativa relativa all'ANSSI, vd. https://cyber.gouv.fr/sinformer-sur-la-reglementation.

[35] Per la lettura della nuova strategia nazionale per la sicurezza informatica del Regno Unito si rimanda al seguente link https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

[36] Il Government Communications Headquarters ha sede a Cheltenham e l'attuale Direttore è Jeremy Fleming. Il suo sito ufficiale è https://www.gchq.gov.uk/.

[37] Per un approfondimento sulla storia del GCHQ cfr. https://www.gchq.gov.uk/section/history/our-origins-and-wwi. Alastair Denniston è stato il primo capo del GCHQ in servizio dal 1919 al 1942.

decriptazione dei messaggi radio delle forze nemiche. Il GCHQ è specializzato nell'utilizzo delle nuove tecnologie e le sue mission areas sono: Counter Terrorism, la Cyber Security, Strategic Advantage, Serious and Organised Crime, Support to Defence[38]. Il suo ruolo principale consiste nell'assicurare assistenza e consulenza ai Dipartimenti Governativi e alle Forze Armate sulla sicurezza delle loro comunicazioni e informazioni sui sistemi tecnologici.

Anche la Spagna, sin dal 2004, si è dotata di un apposito organismo di cybersicurezza per far fronte alle nuove minacce informatiche. Si tratta del Centro Criptológico Nacional (CCN) istituito con il Real Decreto 421/2004 e connesso al Centro Nacional de Inteligencia (CNI), l'agenzia di intelligence ufficiale spagnola che si occupa sia della sicurezza estera che di quella nazionale. La Ley 11/2002[39], che delinea il quadro normativo dell'intelligence spagnola, affida al Centro Nacional de Inteligencia l'esercizio delle funzioni relative alla sicurezza delle tecnologie informatiche all'articolo 4 lett. e)[40] e, allo stesso tempo, conferisce al suo Direttore la responsabilità di dirigere il Centro Criptológico Nacional all'articolo 9 comma 2 lett. f)[41]. Per questo motivo, il CCN condivide mezzi, procedure, regolamenti e risorse con il CNI. Tra i principali compiti del CCN si annoverano lo sviluppo e la diffusione di standard, istruzioni, guide e raccomandazioni per garantire la sicurezza dei sistemi ICT (Information and Communication Technologies) e il rispetto delle normative relative alla protezione delle informazioni classificate nel proprio ambito di competenza.

4. Verso una nuova cultura della sicurezza europea e nazionale

Alla luce di quanto esposto, emerge come negli ultimi anni la materia della sicurezza informatica e della cyber intelligence abbia assunto un interesse sempre più crescente sia in ambito nazionale che europeo. Ciò rappresenta l'esito di una maggiore consapevolezza che è maturata attorno al tema a causa dell'innegabile e notevole incremento – sia in termini di numeri che di complessità – degli attacchi cyber rilevati. Tale consapevolezza si è tradotta in interventi volti a costruire un'elevata protezione dello Stato sotto il versante digitale. È nata perciò la necessità di dare una nuova forma alla difesa degli interessi strategici nazionali e di investire in maniera robusta nel campo della cyber intelligence anche tramite la creazione di agenzie

[38] Cfr. https://www.gchq.gov.uk/.

[39] Per visionare il testo completo della legge si rimanda a https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628.

[40]Artículo 4. Funciones del Centro Nacional de Inteligencia. Para el cumplimiento de sus objetivos, el Centro Nacional de Inteligencia llevará a cabo las siguientes funciones: [...] e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro.

[41]Artículo 9.2. Corresponde al Secretario de Estado Director del Centro Nacional de Inteligencia impulsar la actuación del Centro y coordinar sus unidades para la consecución de los objetivos de inteligencia fijados por el Gobierno, asegurar la adecuación de las actividades del Centro a dichos objetivos y ostentar la representación de aquél. Asimismo, le corresponde: [...] f) Desempeñar las funciones de Autoridad Nacional de Inteligencia y Contrainteligencia y la dirección del Centro Criptológico Nacional.

specializzate.

Le guerre contemporanee assumono una natura sempre più economica e digitale e vengono combattute sul web a colpi di algoritmi. Le armi sono sostituite dalle attività di informazione/disinformazione e le sanzioni dei Mercati spesso spaventano più di quelle degli Stati. In un quadro di tal genere, le nuove frontiere delle attività di intelligence non possono che riguardare il campo della cybersecurity e dell'intelligence finanziaria e necessitano di una cooperazione internazionale più robusta di quella attuale, proprio per la natura sovranazionale delle minacce da affrontare. Va detto che, da anni, è in corso un lento ma costante processo di cooperazione tra Stati europei nel campo dell'intelligence, che ha portato alla creazione di organismi di coordinamento fra i maggiori servizi di sicurezza e d'informazione come, ad esempio, il Club di Berna[42]. Ad oggi, la rete transnazionale di intelligence che più si avvicina alla cooperazione strutturata europea[43] è rappresentata dall' EU Intelligence and Situation Centre (EU IntCen). Va, però, sottolineato che nel lavoro condotto dall'EU IntCen, sono sempre i singoli Stati a decidere quali informazioni sulla sicurezza condividere (la sicurezza nazionale è di esclusiva responsabilità di ciascuno Stato membro), non l'Unione europea nella sua interezza. L'EU IntCen non è, dunque, una agenzia di intelligence europea strutturata ma è certamente ciò che più si avvicina ad essa, poiché svolge un ruolo da protagonista nel coordinamento della cooperazione di intelligence[44] e ha assunto un ruolo crescente nella politica estera europea.

Appare evidente, dunque, che un sistema di cooperazione di intelligence europea esiste, seppur non strutturato e non integrato alle istituzioni europee e basato su una condivisione di informazioni volontaria.

Un eventuale passo in avanti per la creazione di una Agenzia di intelligence europea presenta una serie di ostacoli di non poco conto. La prima, evidente, complicazione risiede nel fatto che l'attività di intelligence rappresenta, da sempre, il cuore dello Stato nazione ed una roccaforte della sovranità nazionale. Vi è, poi, da parte dei servizi di sicurezza nazionali, il timore di diffondere fonti riservate e relazioni privilegiate, soprattutto se riguardanti aree di competizione tra Stati, come ad esempio l'ambito industriale o commerciale. Non è un mistero che, soprattutto nel campo del mercato economico, alcune fonti siano preziose ed assicurino vantaggi competitivi solo a patto che siano conosciute da un solo attore.

---

[42] Oltre al Club di Berna, un altro esempio di cooperazione non strutturata di servizi di intelligence è il cosiddetto gruppo Kilowatt. Questa alleanza informativa tra i servizi di circa 15 paesi, risalente al 1977, è stata tenuta a lungo segreta. Nel 1982, la sua esistenza è stata rivelata quando sono stati scoperti alcuni documenti, presso l'ambasciata americana di Teheran, in cui veniva menzionata. Alla rete Kilowatt partecipano i paesi della comunità europea, il Canada, la Norvegia, la Svezia, la Svizzera, la CIA, l'FBI, il Mossad e lo Shin Beth israeliani.

[43] Sul punto vd. S. Bilgi, Intelligence Cooperation in the European Union: An Impossible Dream?, All Azimuth, v. 5, n.1, 2016, pp. 57-67.

[44] Vd. M.K.D. Cross, A European Transgovernmental Intelligence Network and the Role of IntCen, in Perspectives on European Politics and Society, vol. 14, n.3, 2013, pp. 388-402.

Altro impedimento è rappresentato dalla paura da parte degli Stati più grandi di condividere informazioni con Stati minori, più esposti al rischio di infiltrazioni. D'altro canto, gli Stati più piccoli temono che le loro agenzie possano essere inglobate da quelle degli Stati più grandi (è una delle conseguenze delle cosiddette powers asymmetries[45]). Il sentiero da seguire potrebbe essere quello di mantenere il cuore nazionale delle agenzie di intelligence europee e, allo stesso tempo, favorire tra loro un dialogo su alcuni terreni di interesse comune, come quello dell'ambiente cibernetico che, essendo per sua natura un ambiente sovranazionale, sfugge ad un controllo meramente nazionale. I benefici che deriverebbero da un sistema di condivisione di intelligence europeo strutturato possono rinvenirsi nell'ottimizzazione dei prodotti elaborati (evitando sovrapposizioni di analisi[46]), nel godere di un sostegno economico europeo a fronte dei bilanci nazionali sempre più ridotti nel settore della Difesa e nel far fronte, con maggiore efficacia, alle minacce transnazionali per la sicurezza e alla valanga globale di dati che invade il mondo dell'informazione.

Per far questo occorre, innanzitutto, diffondere una cultura europea dell'intelligence che generi fiducia[47] tra gli Stati membri e che individui una piattaforma di interessi comuni da perseguire al fine di garantire vantaggi reciproci tra le agenzie di informazione che condividono le loro attività (ad es. la lotta al terrorismo, alla criminalità informatica, alla tratta di esseri umani, alla criminalità organizzata internazionale). C'è bisogno di tempo e di un percorso graduale che mantenga distinte, nel campo della condivisione delle informazioni di intelligence, le aree di competizione da quelle di cooperazione.

La base di partenza non può che essere quella di rafforzare il quadro di cooperazione già esistente a partire, in particolare, dal ruolo dell'EU Intelligence and Situation Centre[48]. Il futuro di cooperazione dell'intelligence europea dipenderà, inoltre, da due fattori, uno interno e l'altro esterno: lo sviluppo dell'integrazione europea in materia di sicurezza e difesa e il grado di pericolo della minaccia terroristica. Sotto il profilo dell'integrazione europea, appare utile sottolineare che il 16 dicembre 2020 la Commissione europea e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato una nuova strategia dell'UE sulla sicurezza informatica[49].

---

[45] Si veda B. Fägersten, For EU eyes only?: Intelligence and European security, in European Union Institute for Security Studies (EUISS), n.8, 2016.

[46] Su questo punto vd. A. Gruszczak, Intelligence Security in the European Union. Building a Strategic Intelligence Community, Palgrave Macmillan, Londra, 2016.

[47] Sull'importanza del tema della fiducia ai fini di creare una comunità strutturata di intelligence vd. A. Politi, Perché è necessaria un'intelligence policy europea?, in Per Aspera Ad Veritatem, n.10, 1998; J. Estevens, Building intelligence cooperation in the European Union, in Janus.net, e-journal of International Relations, Vol. 11, n. 2, 2020.

[48] In tal senso, vd. J.M. Nomikos, European Union Intelligence Analysis Centre (INTCEN): Next stop to an Agency ?, in Journal of Mediterranean and Balkan Intelligence, 22 novembre 2015.

[49] Scaricabile a questo link https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Il documento prevede un cospicuo piano di investimenti (4,5 miliardi di euro tra il 2021 e il 2027) per rafforzare la cybersicurezza e la creazione di un'unità di coordinamento - denominata Joint Cyber Unit - tra Stati membri, UE e settore privato per la risposta agli attacchi cibernetici.

La Joint Cyber Unit è una piattaforma virtuale di cooperazione che si occuperà di coordinare la cybersecurity europea, provvedendo ad un piano di risposta alle crisi e agli incidenti cibernetici dell'UE, imperniato su piani nazionali proposti nella revisione della direttiva NIS. Si impegnerà, inoltre, a promuovere l'adozione di protocolli di mutua assistenza tra i partecipanti e a definire le capacità di monitoraggio e rilevamento nazionali e transfrontaliere. Oltre che in Europa, tuttavia, è necessario che una nuova cultura della sicurezza e dell'intelligence si affermi anche dentro i confini nazionali[50]. Sotto questo profilo, e sulla base di un'analisi comparativa, non si può sorvolare rispetto al fatto che l'Italia sia l'unico Paese del G7 a non essersi ancora dotato di una Strategia di sicurezza nazionale[51]. L'adozione di un simile strumento rappresenta un obbligo di legge per l'amministrazione degli Stati Uniti d'America fin dal 1986[52]. L'ultimo Paese del G7, in ordine cronologico, ad avere adottato la propria Strategia di sicurezza nazionale è la Germania che, il 14 giugno 2023, ha presentato la sua Nationale sicherheitsstrategie[53]. Vi è, dunque, l'urgenza di superare la frammentazione delle politiche di sicurezza nazionali, adottando una Strategia di Sicurezza Nazionale unitaria e integrata, in grado di rispondere con prontezza e lungimiranza alle sfide di un mondo in continua trasformazione.

Un passo significativo in questa direzione è stato compiuto il 24 ottobre 2024, data in cui è stata depositata la proposta di legge 2117, presentata dal deputato Lorenzo Guerini (attuale Presidente del Copasir), recante "Modifiche alla legge 3 agosto 2007, n. 124, in materia di Autorità delegata per la sicurezza della Repubblica e di strategia di sicurezza nazionale". Appare utile ricordare che con la legge 124/2007 sul «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto», è stato riformato il comparto dell'intelligence italiana che, fino a quel momento, aveva operato sotto la vigenza della legge 801/1977[54]. La proposta di legge 2117 interviene sulla legge 3 agosto 2007, n. 124, con riguardo a tre questioni essenziali:

---

[50] Per una attualizzazione del concetto relativamente alle attuali modalità tecnologiche di compromissione del valore sicurezza, cfr. A. Pansa, La sicurezza nazionale. Innovazione e nuovi limiti, in Gnosis, 2019; G. de Vergottini, Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata, in Rivista AIC, n. 4, 2019, pp. 65-85.

[51] Sul tema si veda L. Guerini, Come cambia la sicurezza nazionale, in Formiche, Anno XX, 208, 2024, pp. 10-11; A. Soi, Ripensare l'ecosistema dell'Intelligence, in Formiche, Anno XX, 208, 2024, pp. 6-8; A. Strozzi, Sicurezza nazionale: il modello unificato che l'Italia attende e la nuova proposta di legge, in aspeniaonline.it, 8 gennaio 2025.

[52] La National Security Strategy (NSS) è un rapporto imposto dalla Sezione 603 del Goldwater-Nichols Department of Defense Reorganization Act del 1986, è stata trasmessa annualmente dal 1987.

[53] Vd. https://www.bmvg.de/de/nationale-sicherheitsstrategie.

[54] La legge 124/2007 ha subito, negli anni, diverse modifiche ed aggiornamenti, da ultimo attraverso il decreto-legge n. 48 del 2025 (c.d. decreto-legge sicurezza), che introduce rilevanti modifiche al regime delle garanzie funzionali per gli operatori dei servizi di informazione e sicurezza, ampliando sensibilmente il perimetro delle condotte autorizzate.

l'istituzione dell'Autorità delegata per la sicurezza della Repubblica, la definizione della strategia di sicurezza nazionale e l'istituzione di un Consiglio per la sicurezza nazionale. Riguardo quest'ultimo, il modello di riferimento sembrerebbe essere quello del Consiglio di sicurezza nazionale degli Stati Uniti, istituito nel 1947 dal National security act e rapidamente affermatosi come il principale interlocutore del presidente in materia di difesa e sicurezza.

Con riferimento alla figura dell'Autorità delegata, la sua nomina diverrebbe obbligatoria da parte del Presidente del Consiglio[55] e le sue funzioni potrebbero essere affidate esclusivamente a un Sottosegretario di Stato, così eliminandosi la facoltà di delegare le relative attribuzioni a un Ministro senza portafoglio.

È prevista, inoltre, l'introduzione nella legge n. 124 del 2007 del nuovo capo III-bis, dedicato alla strategia di sicurezza nazionale, adottata ogni tre anni dal Presidente del Consiglio dei ministri su proposta del Consiglio per la sicurezza nazionale.

La 'strategia di sicurezza' dovrà riguardare l'intero ambito dell'azione di governo determinando: gli interessi strategici per la sicurezza della Repubblica; gli obiettivi globali della politica estera; le minacce e i rischi cui sono esposte la collettività nazionale e le istituzioni democratiche nonché le correlate attività di prevenzione che i poteri pubblici sono chiamati a svolgere; gli indirizzi per la protezione delle infrastrutture critiche.

È da auspicare che tale proposta di legge prosegua il suo cammino e che, qualora veda la luce, la strategia di sicurezza nazionale non si riduca ad un mero adempimento burocratico ma funga da faro di orientamento per le politiche di sicurezza della Repubblica.

Il diritto alla sicurezza, infatti, non solo è da considerarsi un diritto fondamentale di natura costituzionale, ma rappresenta anche la premessa necessaria degli altri diritti costituzionali, imprescindibile per il godimento di tutte le libertà individuali[56].

---

[55] Allo stato attuale, la nomina dell'Autorità delegata è tecnicamente meramente potenziale da parte del Presidente del Consiglio dei Ministri, che non è obbligato a delegare i suoi poteri ma, come disposto dall'art.3 della l. 124/2007, può compiere tale scelta «ove lo ritenga opportuno».

[56] Sul punto, G. Cerrina Feroni, G.Morbidelli, La sicurezza: un valore superprimario, in Percorsi costituzionali, n.1/2008; T.E. Frosini, Il diritto costituzionale alla sicurezza, in forumcostituzionale.it, 2006; T.F. Giupponi, La sicurezza come valore fondamentale, in Rassegna di diritto pubblico europeo, n.2, pp. 233-259 e, dello stesso A., La sicurezza e le sue "dimensioni" costituzionali, in www.forumcostituzionale.it, 2008; C. Mosca, La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza, Padova, 2012; M. Valentini, Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale, Editoriale Scientifica, Napoli, 2017.

FONTI PRINCIPALI

- Agenzia per la Cybersicurezza Nazionale (ACN), "Relazione annuale al Parlamento 2022", Sito istituzionale ACN, https://www.acn.gov.it/portale/relazione-annuale.
- Agenzia per la Cybersicurezza Nazionale (ACN), "Relazione annuale al Parlamento 2023", Sito istituzionale ACN, https://www.acn.gov.it/portale/relazione-annuale.
- Agenzia per la Cybersicurezza Nazionale (ACN), "CSIRT Italia — pagina dedicata (numeri 2023)", Sito istituzionale ACN, https://www.acn.gov.it/portale/csirt-italia.
- Agenzia per la Cybersicurezza Nazionale (ACN), "Rapporto sugli attacchi DoS/DDoS", 22 febbraio 2025, Sito istituzionale ACN.
- A. Alù, "Perché la disinformazione minaccia le democrazie nel 2024", AgendaDigitale.eu, 7 febbraio 2024.
- M. Artini, "Agenzia Cibernetica Nazionale italiana, confrontiamola con gli altri attori europei", AgendaDigitale.eu, 17 gennaio 2022.
- R. Baldoni, "Così l'Agenzia cyber sta lavorando e dispiega i propri effetti", AgendaDigitale.eu, 18 novembre 2021.
- R. Baldoni, Sovranità digitale. Cos'è e quali sono le principali minacce al cyberspazio nazionale, Bologna, Il Mulino, 2025.
- R. Baldoni, "Il ruolo guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) verso la Cyber-Resilienza Nazionale: sinergie pubblico-private", in U. Gori (a cura di), Cyber Warfare 2021-2022. Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato, Milano, Franco Angeli, 2023, 21-25.
- S. Bilgi, "Intelligence Cooperation in the European Union: An Impossible Dream?", All Azimuth, 5(1), 2016, 57-67.
- F. Bechis, "Non solo cyber, così riformiamo l'intelligence. Parla Franco Gabrielli", Formiche.net, 14 agosto 2021.

- G. Carrer, “Riforma dell’intelligence? Sì, dicono Pagani (Pd), Perego (FI) e Tofalo (M5S)”, Formiche.net, 29 luglio 2021.
- M. Caligiuri, Come i pesci nell’acqua. Immersi nella disinformazione, Soveria Mannelli, Rubbettino, 2019.
- M. Caligiuri, A. Pagani, M. Chioso, Disinformare: ecco l’arma. L’emergenza educativa e democratica del nostro tempo, Soveria Mannelli, Rubbettino, 2024.
- M. Caligiuri, Cyber intelligence. Tra libertà e sicurezza, Roma, Donzelli, 2016.
- M. K. D. Cross, “A European Transgovernmental Intelligence Network and the Role of IntCen”, Perspectives on European Politics and Society, 14(3), 2013, 388-402.
- B. Fägersten, For EU Eyes Only? Intelligence and European Security, EUISS Brief, n. 8, 2016.
- I. Galimova, “L‘‘operazione militare speciale’ in Ucraina e la reazione del sistema politico russo”, Nomos. Le attualità del diritto, 1, 2022.
- GCHQ — Government Communications Headquarters, “Our Origins and WWI”, Sito ufficiale, Cheltenham, https://www.gchq.gov.uk/.
- L. Guerini, “Come cambia la sicurezza nazionale”, Formiche, Anno XX, n. 208, 2024, 10-11.
- A. Gruszczak, Intelligence Security in the European Union. Building a Strategic Intelligence Community, London, Palgrave Macmillan, 2016.
- H. Kissinger, Ordine mondiale, Milano, Mondadori, 2017, 339.
- M. C. Libicki, “The Convergence of Information Warfare”, Strategic Studies Quarterly, 11(1), 2017, 49-65.
- M. L. Mariscal, International Cybersecurity: Law, Policy, and Strategy, Oxford, 2020.
- A. Monti, “Il rinnovamento dell’intelligence ha bisogno di coerenza normativa”, Formiche.net, 6 dicembre 2020.

- F. Nisticò, “L’elemento cyber nella guerra russo-ucraina”, Aspeniaonline.it, 3 marzo 2022.
- J. M. Nomikos, “European Union Intelligence Analysis Centre (INTCEN): Next Stop to an Agency?”, Journal of Mediterranean and Balkan Intelligence, 22 novembre 2015.
- A. Pagani, “La guerra cibernetica nell’età ibrida: tecnologie, strategie e priorità”, AgendaDigitale.eu, 22 luglio 2021.
- F. Pizzetti, “La protezione dei dati personali nell’era digitale: sfide e prospettive”, in G. Scorza, A. Sica (a cura di), Cybersecurity e privacy: nuove frontiere del diritto, Roma, 2022, 89-112.
- O. Pollicino, G. Pitruzzella, Disinformation and Hate Speech. A European Constitutional Perspective, Milano, Egea, 2020.
- C. Pinelli, C. Hassan, Disinformazione e democrazia, Venezia, Marsilio, 2022.
- Presidenza del Consiglio dei Ministri — Dipartimento delle Informazioni per la Sicurezza (DIS), Relazione sulla politica dell’informazione per la sicurezza 2023, Roma.
- M. Santarelli, “Relazione Intelligence 2023: la risposta dell’Italia a minacce ibride e conflitti globali”, AgendaDigitale.eu, 7 marzo 2024.
- U. Saccone, “Quale intelligence per il futuro?”, Formiche.net, 2 agosto 2021.
- M. Sbailò, “Guerre ibride: quali risposte possibili?”, DPCE online, 63(SP1), 2024.
- A. Soi, “Ripensare l’ecosistema dell’Intelligence”, Formiche, Anno XX, n. 208, 2024, 6-8.
- A. Spaziani, “L’attacco cibernetico nell’era della guerra ibrida”, DPCE online, 63(SP1), 2024.
- M. Vedaschi, À la guerre comme à la guerre. La disciplina della guerra nel diritto costituzionale comparato, Torino, 2007.
- G. de Vergottini, Guerra e costituzione. Nuovi conflitti e sfide alla democrazia, Bologna, Il Mulino, 2004.

Atti di convegno

L'Unione europea fa i conti con Carl Schmitt: "sdoppiare" la difesa comune?

Francesco Severa
Assegnista di ricerca in diritto costituzionale, Sapienza - Università di Roma

"The European Union grapples with Carl Schmitt: should it "split" its common defence?"

Abstract

This paper examines the European Union's evolving identity in light of Carl Schmitt's concept of Großraum ("large space"). Schmitt's link between spatial order and legal order provides a key to interpreting the EU as a post-statist structure of reciprocal influence rather than hegemonic power.

The analysis connects this theoretical framework to current geopolitical developments, especially the Russo-Ukrainian war, which has tested Europe's unity and exposed the limits of its common defense policy. While instruments such as PESCO, the European Defence Fund, and the Strategic Compass have strengthened coordination, the EU still lacks a genuine supranational authority in defense and security. The Union thus acts mainly as a functional accelerator, supporting national initiatives rather than replacing them. In Schmittian terms, European integration may be understood as a dynamic "large space" of shared legal and cultural influence: an original, non-imperial path toward strategic autonomy.

1. Lo "spazio grande" come dimensione geo-giuridica.

Prendere sul serio la speculazione schmittiana nell'indagine sulla formula istituzionale dell'Unione europea importa due precise implicazioni, che sono, in verità, un po' i presupposti di ogni ragionamento che voglia attualizzare il pensiero del giurista di Plettenberg[1]. Innanzitutto, la dimensione spaziale come coessenziale a quella giuridica: il diritto come unità di ordine e localizzazione[2]. In secondo luogo, il fatto che Schmitt ritenga ormai superata la dimensione statuale, che era stata invece essenziale nel ricostruire lo ius publicum europaeum dell'età moderna[3].

Con riguardo al primo elemento, bisogna dire che la consapevolezza di questa connessione vuole essere per Schmitt una chiave di lettura universale, un concetto di decodificazione del nomos, che permette dunque di "afferrarlo" per come ogni epoca lo ha voluto intendere. In qualche modo, la ricerca del nostro Autore non è semplicemente una presa di posizione sull'elemento originario dell'istanza giuridica, cioè, a suo dire, l'appropriazione di terra. È piuttosto un tentativo di far emergere le formule essenziali del discorso giuridico, per poter meglio declinarlo nella sua dimensione contingente e concreta. Come alcuni hanno notato, il linguaggio simbolico di Schmitt è innanzitutto una formula ermeneutica, serve a leggere gli eventi storici nella loro individualità, mai a creare archetipi o forme fisse. Nella storia gli eventi non si ripetono mai identicamente: essi sono il frutto del "pensiero che si fa mondo" e, di conseguenza, vanno interpretati per arrivarne ad una comprensione effettiva, che non è progressiva né regressiva, ma politica e filosofica[4].

---

[1] Qui si prende a riferimento il titolo del testo di A. Cantaro, Il Nomos "preso sul serio", in Teoria del Diritto e dello Stato, n. 1-2/2011.

[2] Per Schmitt, la coincidenza tra ordinamento e sua localizzazione rappresenta la circostanza fondante e costitutiva di ogni diritto, di ogni nomos che è la forma immediata nella quale si rende spazialmente visibile l'ordinamento politico e sociale di un popolo. Definizione questa che si ritrova in C. Schmitt, Il Nomos della Terra, Milano 1991, 59.

[3] Schmitt matura nel tempo la propria distanza rispetto al concetto di Stato, che in verità nei suoi primi studi egli tenta di riaffermare quale medio tra diritto e sua realizzazione storico-concreta, con il corrispondente ridimensionamento del ruolo dell'individuo. Ciò, per esempio, si ritrova con chiarezza in C. Schmitt, Il valore dello Stato e il significato dell'individuo (1914), a cura di C. Galli, Bologna 2013, 82 ss. Al contrario, alla fine degli anni Venti, l'autore di Plettenberg sembra approfondire una differenziazione tra il concetto del "politico" e lo Stato come manifestazione giuridico-amministrativa, fino ad arrivare alla piena consapevolezza del fallimento della dimensione statuale nella dottrina dei "grandi spazi" che tra poco approfondiremo. Si fa riferimento a C. Schmitt, Il concetto di Politico (1927), in C. Schmitt, Le categorie del politico, a cura di G. Miglio - P. Schiera, Bologna 1972, 87 ss. Per gli autori che hanno sottolineato tale cambiamento nella teorica di Schmitt, si veda G. Duso (A cura di), La politica oltre lo Stato, Venezia 1981 e, più di recente, C. Galli, Spazi politici. L'età moderna e l'età globale, Bologna 2001, 118.

[4] Scrive G. Sessa a proposito della «intuizione schmittiana relativa all'individualità degli eventi storici» che, stando al giurista tedesco, «l'attuale [...] non può essere interpretato in termini archetipali, jüngeriani: nel percorso storico gli eventi non si ripetono identicamente. Il presente può mostrare semplicemente similitudine (in senso klagesiano) rispetto a ciò che è stato, e va interpretato, per addivenire a una sua comprensione effettiva, in una lettura sganciata tanto dalla visione progressiva quanto da quella involutiva della storia quale manifestazione del novum» (così G. Sessa, Tertium datur. Filosofie dell'originario, Roma 2025, 31). Si veda su questo anche E. Jünger - C. Schmitt, Il nodo di Gordio, Milano 2023.

Allora anche il diritto, quale nomos, nelle sue manifestazioni positive, comunque legate alla dimensione spaziale, va recuperato al più vasto "regno di senso della terra". Scrive Cantaro, «[tale regno di senso] non è il prodotto di un'ipotetica comunità internazionale e dei suoi astratti imperativi normativi. Nulla possono né l'aprioristica fede nel precetto pacta sunt servanda, né il mito dei diritti umani, né qualsiasi altro precetto figlio di un "universalismo acritico". Il "regno di senso della terra" è radicato nella "storia", nell'immagine complessiva del mondo, nel modo in cui ciascuna epoca "pensa" la sua suddivisione. [...] Nel cuore dell'opus schmittiano la nozione di nomos si complica, si sviluppa, si arricchisce. Il nomos diventa vieppiù diritto-ordinamento comune dello spazio terrestre nella sua totalità e sua suddivisione sulla base di una immagine del mondo»[5]. Se questo è vero, il nomos condensa in sé non semplicemente l'ordinamento nella sua costruzione positiva e materiale, ma la struttura fondamentale di un'epoca[6]: manifestandosi, nell'epoca antica, come respublica christiana; poi, nella costruzione dualistica "terra-mare" del nomos dell'età moderna e preglobale; infine, nella "delocalizzazione" assoluta che caratterizza il nomos dell'età globale e contemporanea.

Schmitt anticipò questa dimensione aerea della costruzione più recente del nomos e ne colse la totale contraddizione con il principio di connessione tra Ordnung e Ortung, appunto tra ordine e spazio. Non soltanto perché questi nuovi ordinamenti delocalizzati non si possano misurare in una prospettiva dimensionale territoriale: ciò è di certo vero, in quanto essi non sono "pieni", ma fondati sul vuoto infinito delle connessioni. Ancor più perché, soggiogati alla regola del divenire, questi ordinamenti perdono la loro vocazione all'edificazione culturale e si atteggiano a mero strumento di qualcos'altro, di qualche altro potere o anche solo di qualche altra volontà. Il luogo del diritto, la sua estrinsecazione territoriale, l'appropriazione di spazio, non è mero atto violento, manifestazione di potenza, ma è resa storico-concreta del pensiero. L'ordinamento è edificazione razionale che vive in un luogo e in un tempo, che si scontra con la realtà e prova a darne ordine, a stabilirne una dike, un senso di giustizia, che quindi l'ordinamento inevitabilmente precede. È questo il motivo per cui Schmitt, nel tempo più maturo del suo pensiero, comincia ad elaborare una formula che sia capace di superare le forme imperiali contemporanee, basate appunto sul soft power economico e tecnologico, preponderanti e pervasive proprio perché fondate sul dato tecnico, sull'adesione "debole" (ma inesorabile) al sistema finanziario prima e al nuovo modello di sviluppo tecnologico poi. In contrapposizione a questo fenomeno, il giurista di Plettenberg cominciò a ragionare su un nuovo paradigma, che chiamasse nuovamente il diritto alla sua natura organica, alla sua dinamica edificante e organizzatrice[7].

---

[5] Così A. Cantaro, Il Nomos "preso sul serio", già citato, 8.

[6] Vedi H. Hofmann, Legittimità contro legalità. La filosofia politica di Carl Schmitt, Napoli 1999, 277.

[7] Su questo A. Scalone, La teoria schmittiana del grande spazio: una prospettiva post-statuale?, in Scienza e Politica, n. 56/2017, 179-205.

La teoria dei "grandi spazi", che Carl Schmitt teorizzò nel suo Völkerrechtliche Großraumordnung (1941) [8], offre una specifica lettura dei rapporti internazionali, sostituendo l'entità minima dello Stato con una formula organizzativa nuova: l'idea è quella di pensare le dinamiche geopolitiche come prospettive di coesistenza tra una pluralità di centri di influenza politica, giuridica e culturale. L'entità-guida esprime influenza sulle entità periferiche, inserendole nel proprio sistema di sicurezza, integrandole nel proprio modello politico-culturale, assicurandogli dunque una forma di protezione. Scrive Carlo Galli: «si tratta di uno spazio messo in forma da un comando politico egemone, portatore del principio organizzativo dello Stato, ma più di questo capace di dar vita a un ordine politico concreto, consapevole di dovere governare nel proprio "grande spazio" una pluralità di organismi nazionali che l'Impero gerarchizza escludendone le potenze estranee. All'imperialismo indiretto dell'universalismo marittimo-tecnico-liberaldemocratico - di cui il formalismo giuridico della Società delle Nazioni è espressione - Schmitt risponde così con la ri-spazializzazione della politica internazionale, che è anche una totalizzazione diretta, e con l'aperta affermazione delle logiche dell'unità politica declinate come "totalità": la politica interna per essere "concreta" non deve più conoscere la differenza liberale fra Stato e società»[9]. Il punto è delicato, perché questa teorica, come detto, presuppone il totale superamento dell'entità statuale. Quel complesso e ingombrante monumento all'amministrazione e alla gestione del potere, formula organizzativa minima dello ius publicum europaeum, ha terminato il suo compito: non ha resistito alla spinta destrutturante del potere della tecnica, che nella sostanza ne ha delegittimato le istituzioni, le ha rese facile preda di poteri esterni e impalpabili; in qualche modo, ne ha ridotto la carica culturale, la connessione con il politico come espressione di sintesi e unità[10]. È come se, con la perdita dello Stato, anche il politico smarrisca il suo strumento principale di egemonia, costretto ad un atteggiamento remissivo e di ultimativa resistenza rispetto a potenze altre, anzi alla potenza per eccellenza, quella della techné. Lo spazio grande è invece innanzitutto il recupero dell'unità come adesione culturale e, immediatamente dopo, sociale e politica. In questo ultimo Schmitt, paradossalmente, sembrano quasi riecheggiare alcune formule della Integrationlehre: in questa idea di integrazione sostanziale giocata sullo spazio e sul dato plurale della socialità, che assicura quella connessione ctonia che ferma la massimizzazione della potenza della tecnica, perché offre a questa una dimensione di senso, un paradigma di validità che ne annulla la natura essenzialmente strumentale[11].

---

[8] Il testo precede di nove anni il Nomos der Erde (1950), e secondo alcuni ne rappresenta un'anticipazione teorica, con tinte meno coerenti e organiche. Per une versione italiana si veda C. Schmitt, L'ordinamento dei grandi spazi nel diritto internazionale con divieto di intervento per potenze straniere. Un contributo sul concetto di impero nel diritto internazionale (1941), in C. Schmitt, Stato, grande spazio, Nomos, Milano 2015.

[9] Così C. Galli, Carl Schmitt. La politica, lo spazio, la guerra, in Gnosis - Rivista italiana di Intelligence, n. 3/2021, 90 ss.

[10] Per una lettura critica del concetto di "crisi dello stato", soprattutto attraverso la lente della teorica di Santi Romano, si veda P. Grossi, Ritorno al diritto, Roma-Bari 2015, 7 ss. Si veda anche Id., Mitologie giuridiche della modernità, Milano 2007.

[11] La connessione concettuale non è così piana, ma certo, in alcuni autori, l'apparato dottrinale di Smend e i suoi studi intorno all'integrazione nel più ampio contesto del dibattitto interno alla Repubblica weimariana sono posti in continuità concettuale (quasi in forma consequenziale, pur se in maniera invertita rispetto alla realtà cronologica) con gli sviluppi ultimi del pensiero

Un pluralismo giocato sul potere, sui dati di natura culturale, sullo scontro sensibile tra autonomie sociali, che trova una sua comunanza in uno "spazio ampio di influenza", in quella che a tutti gli effetti sembra una struttura organica di contenimento e sintesi che va oltre la gerarchia e la centralizzazione, ma costruisce confini sulla base di una coiné di giustizia, sulla possibilità di dialogo tra diverse spinte, tra diverse espressioni di potenza.

E la suggestione schmittiana appare davvero profetica in un tempo, quello attuale, in cui sembra affermarsi una vera e propria idealità degli "spazi di influenza". Tralasciando infatti le sgrammaticature della comunicazione politica, in alcune affermazioni dell'amministrazione Trump su una necessaria influenza statunitense da imporre su Canada e Groenlandia, ma anche sullo stretto di Panama, c'è qualcosa di più di una semplice velleità egemonica, nemmeno poi così nuova in realtà.

Ancora, questa rinnovata tendenza sembra palesarsi in tutta la sua tragicità nella guerra russo-ucraina, che ben potrebbe leggersi come il tentativo del Cremlino di riaffermare il proprio dominio sullo spazio culturale, economico e sociale di Kiev, sempre più sbilanciata invece verso l'occidente europeo e americano. Ma si potrebbe guardare secondo questa prospettiva anche il processo di integrazione europea, come "spazio grande di influenza" basato sui diritti. Ognuno di questi tre esempi sembra in verità descrivere un approccio diverso alla medesima tendenza.

Con riguardo agli Stati Uniti d'America, la questione della loro influenza "esclusiva" sul continente ha radici antiche, che possono farsi risalire di certo al sentimento di emancipazione dalle potenze europee presente nella "dottrina" che porta il nome del presidente Monroe[12]; oggi, tale elemento è evoluto soprattutto in una prospettiva "protezionista" e, in un certo senso, "jacksoniana"[13], cioè fondata su un "destino manifesto" che è consolidamento della cultura nazionale e non strumento di espansione, politica o culturale che sia.

---

schmittiano. Si veda su questo S. Guerra, Schmitt, Kelsen e Smend nella Repubblica di Weimar. Diagnosi si una crisi democratico-costituzionale, Torino 2024.

[1] Per un approfondimento si veda, ex plurimis, M. Della Malva, Gli sviluppi della dottrina Monroe dal 1900 ad oggi. Una lunga evoluzione, con specifico riguardo agli emblematici contesti di Colombia, Panama e Venezuela, in DPCE Online, n. 2/2024 e M. Mariano, L'America nell'Occidente. Storia della Dottrina Monroe (1823-1963), Roma 2013.

[2] Sulla risonanza della cultura politica "jacksoniana" sull'amministrazione di Donald Trump si veda G. Dottori, La visione di Trump. Obiettivi e strategie della nuova America, Salerno Editrice, Roma 2019.

Con riguardo al conflitto russo-ucraino, siamo difronte ad una inaccettabile estrinsecazione violenta del concetto di influenza, che tra l'altro non sembra abbandonare una certa cifra statuale, veicolo privilegiato (se non unico) della sintesi culturale dello spazio grande russo. Infine, l'Unione europea, che ha nel tempo costruito uno spazio di integrazione non fondato sull'egemonia di uno Stato né su una formula filosofica, ma sul comune linguaggio del diritto e sulla condivisione ideale di valori, diritti e formule di affermazione di questi ultimi. Nel nostro continente, sulla memoria di una guerra terribile, i popoli europei hanno avviato da quasi settant'anni un processo di costruzione di un grande spazio autonomo di influenza reciproca. Pur partendo da un'impostazione propriamente funzionalistica, l'integrazione è avanzata fino ad un punto che possiamo definire di relativa unità valoriale e giuridica. Nel diritto (e grazie al diritto)[14], il sistema istituzionale sovranazionale ha tentato di armonizzare e razionalizzare gli apporti delle singole tradizioni costituzionali degli Stati membri, rispettando (dove più, dove meno) il nucleo duro caratterizzante l'identità storico-politica e giuridico-costituzionale di ognuno di essi, ma anche influenzandone (dove più, dove meno) i contorni.

Seguendo anche metodologicamente l'approccio schmittiano, possiamo dire che lo "spazio grande" non rappresenta un archetipo, ma un meccanismo interpretativo della nostra realtà. In questa età globale, è possibile pensare a forme di organizzazione spaziale del diritto: modelli ordinamentali basati sui complementari principi di influenza e integrazione, che però si manifestano in formati differenti, animati da paradigmi differenti, filosofico-ideologici, statuali-espansionistici, integrativo-culturali.

Su quel confine che separa la Russia dall'Ucraina si sono confrontati due di questi modelli di spazio grande, quello europeo, votato all'integrazione di natura giuridico-culturale, e quello russo, votato all'affermazione violenta e centralista dell'entità-guida (anzi meglio, dello Stato-guida). Tale scontro ha evidentemente imposto all'Europa di ripensare il proprio "paradigma di pace", elemento essenziale del processo di integrazione continentale e dunque carattere fondativo del peculiare (se non proprio originale) spazio di influenza eurounitario.

---

[14] Vedi P. Grossi, L'Europa del diritto, Roma-Bari 2016. In verità, tale genesi giuridica e non propriamente politica è stata anche la causa delle difficoltà di ricostruzione teorica dell'ordinamento sovranazionale incontrate dai giuristi. Infatti, «[la] peculiarità del processo d'integrazione [europeo risiede nel fatto che esso si è] svolto attraverso il diritto e non per mezzo della politica come, invece, è accaduto per gli Stati. Di qui l'inversione logica che, per un certo tempo, ha tratto in inganno l'osservatore: se nel diritto costituzionale degli Stati lo studio della forma politicamente stabilita precede logicamente e causa fattualmente il sistema degli atti-fonte, nel diritto costituzionale dopo lo Stato è lo studio di questi ultimi e dei loro effetti a precedere logicamente e causare in via di fatto la forma dello spazio ove tali atti operano. È quindi possibile sostenere che, con riguardo all'Unione, il dibattito sulla forma non sia che una descrizione delle conseguenze di qualcosa che è già avvenuto» (così G. Vosa, Sull'equilibrio costituzionale dell'Unione europea. La costituzione "nata dal cambiamento" e i limiti alla priorità applicativa del diritto sovranazionale, in costituzionalismo.it, n. 3/2021).

2. La guerra alle porte dello "spazio grande" europeo

Il conflitto russo-ucraino, iniziato nel febbraio 2022, ha messo a dura prova gli Stati europei, costretti a ripensare gli assetti geopolitici del continente non solo dal punto di vista militare, ma anche sotto l'aspetto dell'approvvigionamento energetico. Fin dai primi giorni di guerra, l'intero occidente (sotto la guida degli Stati Uniti d'America) ha fortemente sostenuto gli sforzi di resistenza delle autorità nazionali ucraine, attraverso tre differenti azioni: (1) la condivisione di informazioni di intelligence, che, soprattutto nei primi momenti del conflitto, hanno contribuito in maniera essenziale ad evitare la fuga da Kiev e il conseguente crollo (se non peggio!) del governo ucraino guidato da Volodymyr Zelenskyj; (2) il massiccio invio di armamenti all'esercito ucraino, nonché l'addestramento degli uomini e il sostegno informativo alle operazioni sul campo; (3) l'applicazione di pesantissime sanzioni economiche e commerciali a singoli cittadini e alle imprese della Federazione russa[15].

Questa strategia politico-militare, più che essere nata nell'alveo eurounitario, è stata concordata su altri tavoli internazionali. Innanzitutto, quello del patto euro-atlantico, che aveva vissuto una profonda crisi di funzione e di destino nei decenni successivi alla fine della guerra fredda, ma che è tornato oggi protagonista, rinforzato dalla resurrezione del nemico. Il vero problema è che a quel tavolo l'Unione non si è seduta con una sola voce, anche perché ad essa non è affidata, se non in prospettiva[16], alcuna competenza di natura militare. Questa sovrapposizione di livelli ha sottolineato diversi elementi di divisione tra gli Stati europei con riguardo alle determinazioni della guerra, da sommare a quelli che già si erano manifestati, pur se poi recuperati, a seguito della crisi pandemica. Li riassume con efficacia l'analista francese Jean Dufourcq, quando afferma: «riuniti all'inizio di giugno [2022] sotto la presidenza francese, gli europei hanno tuttavia esibito una profonda spaccatura tra coloro che puntano a un cessate il fuoco e a un compromesso territoriale che arresti la guerra e coloro che si dicono determinati a finire Putin a qualunque costo. La Francia, che vuole mantenere i contatti con Kiev e con Mosca, preferirebbe fermare lo scontro, così come la Germania, l'Italia, il Belgio e l'Austria, mentre la Polonia e gli Stati baltici vogliono una vittoria incontestabile dell'Ucraina. [...] A Bruxelles si sta

---

[15] Per una lettura organica, si veda, ex plurimis, C. Cellerino, La difesa europea dinanzi alla guerra in Ucraina tra "autonomia strategica" e vincoli strutturali: quali prospettive per la Difesa comune?, in Il Diritto dell'Unione Europea, fascicolo n.1/2023.

[16] Il riferimento è al Titolo V del TUE e in particolare agli articoli 42 ss., che riguardano "Disposizioni sulla politica di sicurezza e difesa comune". In particolare, l'art. 42.6 TUE prevede la possibilità per gli Stati che posseggono maggiori capacità militari di instaurare una cooperazione strutturata permanente nelle forme stabilite dal successivo art. 46 TUE. Per un approccio federalista sul tema, si veda M. Frau, I nodi irrisolti della difesa comune europea. Una prospettiva federalista, in federalismi.it, n. 6/2022. Interessante l'analisi critica di C. Sbailò, secondo cui il modello di difesa comune disegnato oggi dai Trattati sarebbe rimasto "vestfaliano", cioè imperniato su un dato "nazionalizzante" o perfino ancora statuale, «in a world where geopolitical dynamics are increasingly taking on a "quantum" connotation» (così C. Sbailò, Europe's Call to arms. Philosophical roots and Public Law profiles of the confrontation with the monster of the 21st century: westernization without democratization, Baden-Baden, 2023, 146).

cristallizzando una quadripartizione europea: il Nord “frugale” contro il Sud “scialacquatore” e l’Ovest “pacifista” contro l’Est “vendicativo”. Da parte loro, gli ambienti economici, le lobby e la Commissione, già mobilitati dal piano di rilancio post-Covid-19 (intorno a cui ruotano 800 miliardi di euro), sono preoccupati dai pesanti conti che dovranno pagare per l’accoglienza e gli aiuti d’emergenza a Kiev (25 miliardi), per la rapida alternativa agli idrocarburi russi (200 miliardi) e per il rifornimento delle scorte di armi (500 miliardi). Stanno anche pensando alla ricostruzione dell’Ucraina (600 miliardi)»[17].

Le nuove divisioni emerse a causa della guerra e della contemporanea crisi energetica non si sono in verità ricomposte. Le maggiori difficoltà le ha incontrate soprattutto la Germania (non certo l’ultimo degli Stati membri), che, nella lunga stagione merkeliana, aveva scommesso, non senza il disappunto di Washington, su una salda Ostpolitik, cioè su una significativa cooperazione commerciale ed energetica con Mosca. Basti pensare a quel Nord Stream 2 che avrebbe dovuto raddoppiare l’apporto di gas da San Pietroburgo a Berlino, attraverso il Baltico, e che non a caso, già pronto per il funzionamento, è stato fatto saltare da mani ignote.

Pressati dalla scomoda posizione a cui sono costretti in ragione della guerra e dalle difficoltà di approvvigionamento energetico, i tedeschi hanno agito, mettendo in atto misure di reazione autonome e non concordate a livello europeo, tanto da mettere in difficoltà alcuni partner.

Innanzitutto, hanno avviato il più grande progetto di riarmo della loro storia dalla seconda Guerra mondiale. Tre giorni dopo l’invasione russa dell’Ucraina (il 27 febbraio 2022), il Cancelliere Scholz annunciava l’intenzione di investire in nuovi armamenti ben 100 miliardi di euro dal bilancio 2022, con l’obiettivo di raggiungere in breve tempo la soglia del 2% del PIL in spesa militare (obiettivo NATO). In secondo luogo, sfruttando l’ampio spazio di manovra offerto dal suo basso debito, Berlino ha messo in campo uno scudo da 200 miliardi per calmierare i prezzi delle bollette dei suoi cittadini, irritando l’intera comunità europea, che vede nella manovra il rischio di una destabilizzazione del mercato unico comune. A questo va aggiunta una posizione ambigua dei tedeschi sull’imposizione europea di un limite al prezzo del gas, sponsorizzata soprattutto dall’Italia, che porrebbe fine alla speculazione sui prezzi dell’energia. Questa iniziale rottura rispetto ad una linea politica decennale si è rafforzata nel tempo, sino a rappresentare una solida base programmatica per la coalizione nero-rossa che sostiene il cancelliere Merz a seguito delle elezioni federali del febbraio 2025. Ciò è emerso plasticamente con la decisione, in verità molto critica e oggetto perfino di un ricorso al Tribunale costituzionale federale, di revisionare la Carta fondamentale tedesca per escludere dal divieto di indebitamento le spese militari superiori al 1%, nonché prevedendo un fondo speciale per la modernizzazione infrastrutturale del paese per 500 miliardi. Modifica costituzionale questa votata nel marzo

[17] Così J. Dufourcq, Per Parigi è l’ora dell’Europa potenza, in Limes, n. 6/2022, 136.

2025 dal Bundestag nella sua composizione antecedente alle elezioni, convocato in tutta fretta prima della convocazione della nuova assise, elettoralmente rinnovata, per evitare che la consistenza numerica dell'opposizione di AfD potesse rendere complicato il raggiungimento della maggioranza qualificata per la modifica proposta. Una forzatura politica e giuridica, che ancor più manifesta quanto sia forte la sensazione di un cambiamento fondativo nella cultura politica tedesca[18].

Tornando però alla fase iniziale della guerra, l'azione autonoma della Germania, consolidatasi come visto negli anni successivi, ha fortemente indebolito i tentativi di risposta comune alla crisi energetica europea, rallentando ogni concreta presa di posizione delle istituzioni eurounitarie e, di certo, rendendo più complicate le trattative per le misure economiche che erano state immaginate. Nel Consiglio europeo dell'ottobre 2022, in verità, alcune aperture ci furono, soprattutto con riguardo alla costituzione di una piattaforma comune di acquisto del gas (almeno per il 15% degli stoccaggi continentali) e al possibile piano di ristori europeo (sul modello del piano SURE), con qualcosa di più di una paventata adesione all'imposizione di un vincolo temporaneo al prezzo del gas e di un finanziamento delle dette misure con l'emissione di debito comune[19].

Queste difficoltà nel coordinamento della governanza europea in materia di difesa sono evidentemente la diretta conseguenza di una scarsità di strumenti di chiara natura sovranazionale in questo ambito. Dal 2017 ad oggi, sono stati varati una pluralità di programmi di cooperazione tra gli Stati membri per implementare la collaborazione sia in tema di organizzazione istituzionale e rafforzata capacità di azione coordinata, si vedano la Permanent Structured Cooperation (PESCO - una formula di cooperazione rafforzata ex art. 42.6 TUE) e la Military Planning and Conduct Capability (MPCC - un quartiere generale operativo permanente che opera a livello strategico militare senza però compiti esecutivi) lanciate entrambe nel 2017, sia in tema di finanziamento e indirizzo dei fondi comuni, si veda la Coordinated Annual Review on Defence del 2017 (un modello di coordinamento delle spese dei singoli Stati membri in tema di difesa sotto il controllo della competente Agenzia europea) e il Fondo europeo per la difesa del 2021 (con lo scopo di finanziare progetti collaborativi europei volti al rafforzamento della base industriale e tecnologica di difesa). Ciò ha evidentemente accelerato alcune dinamiche, come lo sviluppo tecnologico e la spesa militare: non a caso, è del 2024 la notizia che il Fondo europeo per gli investimenti (Eif) e il Fondo per l'innovazione della Nato (Nif) hanno firmato un memorandum d'intesa (MoU) per cooperare nel sostenere la crescita a lungo termine dei

[18] Un primo commento e una contestualizzazione della questione si trova in A. De Petris, Una Germania senza freno, ovvero: trasformare una crisi in catarsi, in DPCE Online, n. 1/2025.

[19] Così le conclusioni del Consiglio dell'Unione del 20 e 21 ottobre 2022: «di fronte all'uso dell'energia come arma da parte della Russia, l'Unione europea resterà unita per proteggere i suoi cittadini e le sue imprese e adotterà con urgenza le misure necessarie».

settori della difesa, della sicurezza e della resilienza in Europa. Ancora, nei primi mesi del 2025, nell'ambito delle forti tensioni tra la nuova amministrazione americana guidata da Donald Trump e le autorità ucraine con riguardo alle trattative di pace con la Russia, la Commissione europea ha varato un "gigantesco" piano di finanziamento del "riarmo" europeo, pari ad oltre 800 miliardi di euro, al fine di incentivare il raggiungimento di una "autonomia strategica" da parte dell'Unione e così contrastare il rischio di un disinteresse statunitense per la difesa europea[20]. Eppure, tutto questo non ha in nessun modo aiutato la nascita di un corrispondente nucleo di governo sovranazionale delle principali dinamiche di investimento nel settore, che sono rimaste legate alla volontà degli Stati. Lo stesso si può dire del governo sovranazionale della difesa comune.

La dottrina da tempo ha individuato il problema e ha proposto alcuni possibili punti di risoluzione: «perché gli ambiziosi obiettivi affermati e più volte ribaditi dall'Unione europea possano essere concretamente realizzati, sarebbe necessaria una importante riforma che investa sia l'assetto istituzionale - chiarendo i ruoli e i poteri della governance apicale - sia la regola decisionale - che, soltanto qualora venisse sostituita dal criterio della maggioranza, darebbe forza a un "interesse comune europeo" capace di prevalere sui singoli interessi nazionali»[21]. In definitiva, una struttura di dialogo eminentemente intergovernativa è «[inidonea] alla gestione delle questioni politico strategiche dell'Europa»[22].

Ma qui la soluzione forte, di natura politico-identitaria, si scontra con la natura profondamente statuale delle strategie di difesa, che implica la dimensione sovranazionale come mero spazio di sostegno funzionalistico. Tanto più che qui la dimensione continentale si sovrappone (e a volte soccombe davanti) alla dimensione atlantica (NATO), che resta ancora l'orizzonte essenziale della difesa continentale europea.

---

[20] Nella dichiarazione alla stampa del 4 marzo 2025 con cui la presidente Von Der Leyen ha annunciato il piano "Rearm Europe", la stessa ha sottolineato come il progetto sia stato creato «in order to help Member States to quickly and significantly increase expenditures in defence capabilities». Il focus è ancora sugli Stati membri e non su un modello sovranazionale di condivisione dell'azione strategica di difesa. Tanto più che lo stesso piano, poi ribattezzato "Rearm Europe/Readiness 2030", è stato approvato per il tramite della procedura di cui all'art. 122 TFUE, cioè quella prevista nei casi di deliberazione di prestiti e misure utili a far fronte a situazioni contingenti ed eccezionali, con l'intervento del solo Consiglio, su proposta della Commissione, e senza il coinvolgimento dell'assemblea parlamentare continentale. Nel caso di specie, infatti, il Parlamento europeo si è potuto esprimere sull'argomento solo per il tramite di due risoluzioni, approvate il 12 marzo 2025 e il 3 aprile 2025.

[21] Così A. GiurickovicDato, L'Unione europea di fronte alla crisi ucraina, in federalismi.it, n. 23/2023. Si veda anche F. Gasperi, Profili costituzionali della Difesa comune europea, in Costituzionalismo.it, n. 2/2023, C. Cellerino, La difesa europea dinanzi alla guerra in Ucraina tra "autonomia strategica" e vincoli strutturali: quali prospettive per la Difesa comune?, in Il diritto dell'Unione europea, n. 1/2022, M. Vellano, La guerra in Ucraina e le conseguenti decisioni dell'Unione europea in materia di sicurezza e difesa comune, in Il diritto dell'Unione europea, n. 1/2022.

[22] Così C. Sbailò, Crisi nordafricana, καταστροφή e occasione di rilancio per l'Europa, in C. Sbailò (A cura di), Difesa europea. Quali prospettive, in federalismi.it, numero speciale n. 1/2019, 103.

Delle due l'una. La difesa comune europea ha ragione di esistere se alternativa al modello di governanza sovranazionale assicurato dalla NATO, ma perde ogni significato se rispetto a quest'ultima si pone in un semplice stato di affiancamento. Ancora, se pure vi fosse la volontà europea di porsi in alternativa allo spazio di difesa a guida americana, si dovrebbe cercare una differente guida continentale, che certo sarebbe, per forza e prestigio, la Francia. Gli altri blocchi europei, quello settentrionale a guida tedesca e quello orientale a guida Polacca, sarebbero pronti ad accettarlo? In questa Germania che corre al riarmo si intravede già una risposta negativa. In buona sostanza, il modello di solidarietà condizionata, sperimentato con successo nel 2020 per governare i rapporti di fiducia/sfiducia tra gli Stati membri (i soldi del PNRR in cambio di programmi pervasivi di riforma), che ha accompagnato una nuova forma di "legittimazione politica di garanzia" per le istituzioni sovranazionali unionali (la Commissione chiamata a trattare con i singoli Stati membri l'avanzamento dei piani nazionali), rappresenta di certo un possibile riferimento per governare l'azione comune degli Stati membri davanti all'attuale crisi, ma con più difficoltà si adatta ad un terreno sensibile come quello della difesa comune. La soluzione sovranazionale rimane comunque legata alle contingenze del momento e gioca un ruolo solo se è davvero percepita come utile agli interessi economici e geopolitici in gioco.

3. La dimensione sovranazionale come acceleratore funzionale nel processo di costruzione della difesa comune europea

In questa prospettiva, l'Unione europea ha dunque avuto difficoltà ad affermare un suo specifico ruolo geopolitico e militare. Ciò è imputabile ad una pluralità di ragioni, in qualche modo già emerse nelle pagine precedenti: (1) la difficoltà di sintetizzare la politica estera dei ventisette Stati membri, (2) la struttura istituzionale dell'Unione, che per quel che riguarda la politica estera e di difesa è troppo sbilanciata sull'istanza intergovernativa; (3) il rischio di sovrapposizione e contrasto tra un'autonoma prospettiva geopolitica europea e quella americana, espressa nella NATO. I primi due punti sono direttamente collegati con il modello di integrazione presente nei trattati. In particolare, nel preambolo del TUE si può leggere che gli Stati membri hanno siglato l'intesa anche perché «decisi ad attuare una politica estera e di sicurezza comune che preveda la definizione progressiva di una politica di difesa comune, che potrebbe condurre ad una difesa comune a norma delle disposizioni dell'articolo 42, rafforzando così l'identità dell'Europa e la sua indipendenza al fine di promuovere la pace, la sicurezza e il progresso in Europa e nel mondo»[23]. Mentre nella tradizionale formula dell'integrazione economica europea, gli strumenti funzionali alla libertà dei commerci e alla contaminazione dei mercati nazionali precede e in qualche modo sviluppa il terreno fertile su cui costruire l'identità politica, nel caso della difesa comune il paradigma si ribalta. L'esistenza di un'istanza politica unitaria è il presupposto della definizione di una difesa comune, come strumento di quella volontà politica esplicita, che, dice il TUE all'art. 42.2, si manifesterà con il voto unanime del Consiglio europeo.

[23] Così nel preambolo al TUE.

Partendo da questo dato, la sovrapposizione con le strutture NATO diviene dirimente, perché la politica estera comune, portatrice cioè di una precisa autonomia strategica degli Stati europei, non dispiegherà mai pienamente tale dimensione se chiamata a giocare sul piano transatlantico, che di per sé rappresenta un modello di elaborazione strategica ultra-europeo, per cui è difficile immaginare una partecipazione che non sia particolare e ordinata su base nazionale.

Ciò che alcuni autori hanno però rilevato è come si rintracci, nel dato positivo dei trattati, un possibile sviluppo differenziato dell'integrazione in materia di difesa. Infatti, «relativamente all'interazione funzionale tra TUE e TFUE, in materia di politiche di difesa e sicurezza comune, può essere interessante notare come l'obbligo di difesa reciproca, previsto dal paragrafo 7 dell'art. 42 TUE, pur facendo salva l'eventuale neutralità di alcuni Stati membri esentandoli dall'obbligo d'intervento, in combinato disposto con la clausola di solidarietà, ex art. 222 TFUE, fa sì che (come delineato dalla decisione del Consiglio UE del 2014), tutti i Paesi dell'Unione collaborino attivamente in materia di antiterrorismo. Tale combinazione funzionale di norme può essere in qualche modo intesa come antesignana del meccanismo di integrazione rafforzata e, al tempo stesso, differenziata che [...] emerge dalla Bussola Strategica»[24]. Quest'ultimo documento, risalente al marzo 2022, rappresenta una presa di posizione forte in tema di azione strategica comune dell'Unione, condiviso in seno al Consiglio e con l'esplicita approvazione di tutti i Capi di Stato e di Governo degli Stati membri. Ciò che interessa per la nostra trattazione è la prospettiva di ricostruzione del problema della difesa comune presente nel documento. Nei quattro capitoli che lo compongono, il tema viene sviscerato innanzitutto nella prospettiva della "azione", con l'idea di prevedere la formazione di un contingente europeo di cinquemila unità con capacità di intervento rapido in scenari internazionali di crisi e, più in generale, di rafforzare tutte le missioni di PSDC, sia nell'ambito operativo militare che nel loro ruolo ausiliario per impieghi civili, con una semplificazione delle regole d'ingaggio e delle linee di comando. Sempre di prospettive operative si parla nel secondo capitolo, dedicato alla cooperazione tra Stati in tema di "sicurezza" e all'implementazione degli strumenti di sicurezza per i singoli Stati e per le istituzioni centrali dell'Unione, sia difronte a minacce convenzionali che ibride. Un terzo capitolo si concentra sugli "investimenti", da coordinare in chiave unionale con strumenti che prediligano le cooperazioni industriali tra Stati e creino linee produttive autonome sul suolo europeo, anche riducendo la dipendenza da altri paesi. Da ultimo, i "partenariati" strategici che inseriscano questi ambiti di azione europea nella dimensione internazionale e transatlantica.

---

[24] Così A. Ruffo, La difesa europea (PSDC) e la Costituzione italiana alla prova della Bussola Strategica 2022, in federalismi.it, n. 7/2024. Si veda anche sul tema F. Fabbrini, La Bussola Strategica dell'UE: luci ed ombre, in Centro Studi sul Federalismo, n. 245/2022.

Il quadro sembra chiaro: da una parte, bisogna costruire strumenti operativi che permettano di misurare sul campo la cooperazione militare tra Stati membri, rafforzando le esperienze comuni e quindi misurando in concreto attività di cooperazione rafforzata, ancor più valorizzando nei fatti le linee strategiche comuni degli Stati membri, anche quando queste sono minime o carsiche; dall'altra, affidare alla dimensione sovranazionale il compito di coordinamento finanziario e di appoggio funzionale alla volontà strategica dei singoli Stati di rafforzare il quoziente di deterrenza dei propri sistemi di difesa (Rearm Europe è alla fine questo!). In questo panorama "sconnesso", sono emerse, dunque, queste due linee di tendenza, una intesa ad approfondire in concreto la cooperazione militare europea, con una differenziazione dell'integrazione che si sviluppi in atto, cioè sui concreti teatri di sicurezza; l'altra con l'idea che l'Unione possa offrire strumenti efficaci di potenziamento dell'attività dei singoli Stati membri, quasi fosse una piattaforma di avanzamento strategico utile a massimizzare i programmi nazionali, a fornirgli supporto, senza per forza annullare i loro specifici caratteri identitari. Alcuni dati fattuali, in parte già citati, rappresentano una conferma di questa tendenza: (a) la sottoscrizione di alcuni trattati bilaterali tra Stati membri che hanno dato una certa rilevanza alla cooperazione militare e allo scambio di informazioni di intelligence (Aquisgrana 2019); (b) l'avvio di specifiche linee di finanziamento europeo per lo sviluppo del comparto difesa (memorandum di intesa tra EIF e NIF del luglio 2024); (c) il patto strategico tra Regno Unito e Unione europea in funzione anti-russa (2025); (d) Rearm Europe (2025). Questi ci dice, in buona sostanza, che la guerra in Ucraina ha risvegliato il processo di integrazione in questo ambito, tarandolo però su prospettive del tutto nuove e peculiari, non tanto basate sulla contrapposizione dialettica tra centro sovranazionale e periferie statali, quanto piuttosto totalmente centrandolo sulla dimensione nazionale, relegando il sistema istituzionale eurounitario, con la sua forza finanziaria e di coordinamento, al ruolo di acceleratore funzionale delle dinamiche di implementazione del sistema di difesa del singolo Stato membro. In qualche modo una rinuncia all'elaborazione strategica continentale, troppo difficile in assenza di un capitale politico autenticamente continentale, libero dai condizionamenti geopolitici che sono troppo forti e differenziati in un'Europa a ventisette. Quali sono le implicazioni di lungo periodo di questo nuovo approccio?

4. Qualche cenno conclusivo sull'autonomia strategica dell'Unione europea e dei suoi Stati membri

Le brevi riflessioni qui sviluppate ci hanno portato a due determinazioni. Innanzitutto, a constatare la rinnovata affermazione di una certa idealità degli "spazi di influenza" nello sviluppo dei rapporti internazionali in questo nostro tempo. Elemento che certo può trovare una formula di decodificazione nella riflessione schmittiana sull'evoluzione del rapporto tra ordine e spazio dopo la caduta del paradigma statuale. Partendo da ciò, si possono certo isolare delle forme di manifestazione di tale "spazio grande" e l'Unione europea sembra incarnarne un modello assai peculiare, proprio perché imperniato non su una forma egemonica centrale, ma su strutture e modelli di influenza reciproca tra unità periferiche, cioè tra Stati membri.

La seconda determinazione che abbiamo dedotto dai dati qui disciolti è la peculiare forma di integrazione che sembra caratterizzare il processo di costruzione di una difesa comune europea. Stando ai trattati, il passaggio fondativo di tale processo dovrà essere una formale espressione di volontà politica unanime da parte degli Stati membri (art. 42.2 TUE), dunque un'elaborazione politico-strategica unitaria nel campo dei rapporti internazionali, calibrata non sul livello statuale ma continentale. Ma la realtà sembra andare in un'altra direzione. Tale elaborazione strategica fondativa sembra sfuggire alla dimensione europea e viene costruita su tavoli diversi, su piattaforme politiche diverse (NATO). Ciò implica che le istituzioni sovranazionali europee nulla possano fare se non sviluppare strumenti di affiancamento e implementazione degli obiettivi strategici nazionali o (peggio) di quelli fatti propri da circoli ristretti di Stati membri. Tale ruolo da acceleratori funzionali delle dinamiche strategiche singolari, soprattutto per la parte economico-finanziaria, non è di per sé una diminutio per le istituzioni eurounitarie, né se ne può escludere una utilità futura rispetto ad una possibile elaborazione di linee specifiche di approfondimento strategico da finanziare nell'interesse eurounitario. Queste osservazioni ci portano però evidentemente ad escludere un'iniziativa strategica europea davvero condivisa e quindi un possibile rafforzamento dell'influenza continentale sulle più complesse dinamiche mondiali.

Alla fine, anche dal punto di vista degli obiettivi geopolitici e di difesa, l'Europa mantiene una sua frantumazione interna, magari riconducibile a blocchi di paesi, ognuno con una proiezione strategica coerente internamente, ma spesso totalmente contrapposta rispetto alle altre rintracciabili sul continente. La cifra anti-russa del blocco dei paesi del fianco orientale, guidati dalla Polonia, non è pienamente coincidente con quella del blocco mediterraneo, trainato dalla Francia, come anche diversa è la realtà dei paesi di cultura germanica e scandinava. L'armonia di queste tendenze non si sta affermando attraverso una espressione unanime di volontà politica (quella appunto prevista dall'art. 42.2 TUE), ma in modelli relazionali che sono cresciuti nel tempo e si fondano su accordi intergovernativi, anche aperti alla collaborazione di paesi extra-unionali (si veda il ruolo del Regno Unito nel gruppo dei paesi cosiddetti "volonterosi", che dovrebbero inviare dei contingenti militari in Ucraina come forza di interposizione sul confine orientale).

Lo sviluppo dialettico e funzionale di questo specifico ambito di integrazione, proprio perché nato spontaneamente e sotto l'influenza della realtà storica contingente, forse non va allora contrastato. È vero, come alcuni autori sottolineano, che l'allargamento dell'Unione europea rischia di diventare un acceleratore della destrutturazione interna, perché addizionare altri Stati alla funzione europea significa aumentare i fattori da integrare e rendere più complesso il sistema[25]. Ciò è vero, però, soltanto se si guarda alla

[25] Si veda S. Goulard, Grande da morire. Come evitare l'esplosione dell'Europa, Bologna 2025.

costruzione europea come processo teleologicamente orientato, ideologicamente predisposto e finalizzato alla costruzione di una nuova entità integrata continentale. La conseguenza di tale ragionamento è dunque la riduzione dei fattori da tenere insieme; magari addirittura "sdoppiare" il processo, per avanzare in maniera differenziata verso l'obiettivo[26].

Lo spunto schmittiano ci permette di fare un passo oltre. L'integrazione applicata allo "spazio grande" diviene un concetto dinamico e aperto, fondato su meccanismi di influenza tra le unità da integrare, in questo caso gli Stati membri. Il sistema funziona non nella misura in cui si procede progressivamente verso l'obiettivo statico della integrazione pienamente matura, ma in quanto siano individuati e applicati strumenti di influenza reciproca, che possono essere di natura valoriale, giuridica o culturale[27]. Sono questi strumenti a tenere insieme le diversità identitarie, istituzionali, costituzionali e strategiche, in un circuito di continua influenza reciproca, anche rispetto ad un'istanza centralizzata che con queste componenti si pone in dialogo. Affermare una leva finanziaria comune per le proiezioni strategiche dei singoli Stati membri, anche quando queste non sembrano pienamente coincidenti, significa assicurare l'autonomia sostanziale e operativa di quelle stesse proiezioni. Un bene preziosissimo nel mondo di oggi.

---

[26] S. Fabbrini, Sdoppiamento. Una prospettiva nuova per l'Europa, Roma-Bari 2017. Più di recente il medesimo autore segue l'impostazione descritta in S. Fabbrini, Nazionalismo 2.0. La sfida sovranista all'Europa integrata, Milano 2025.

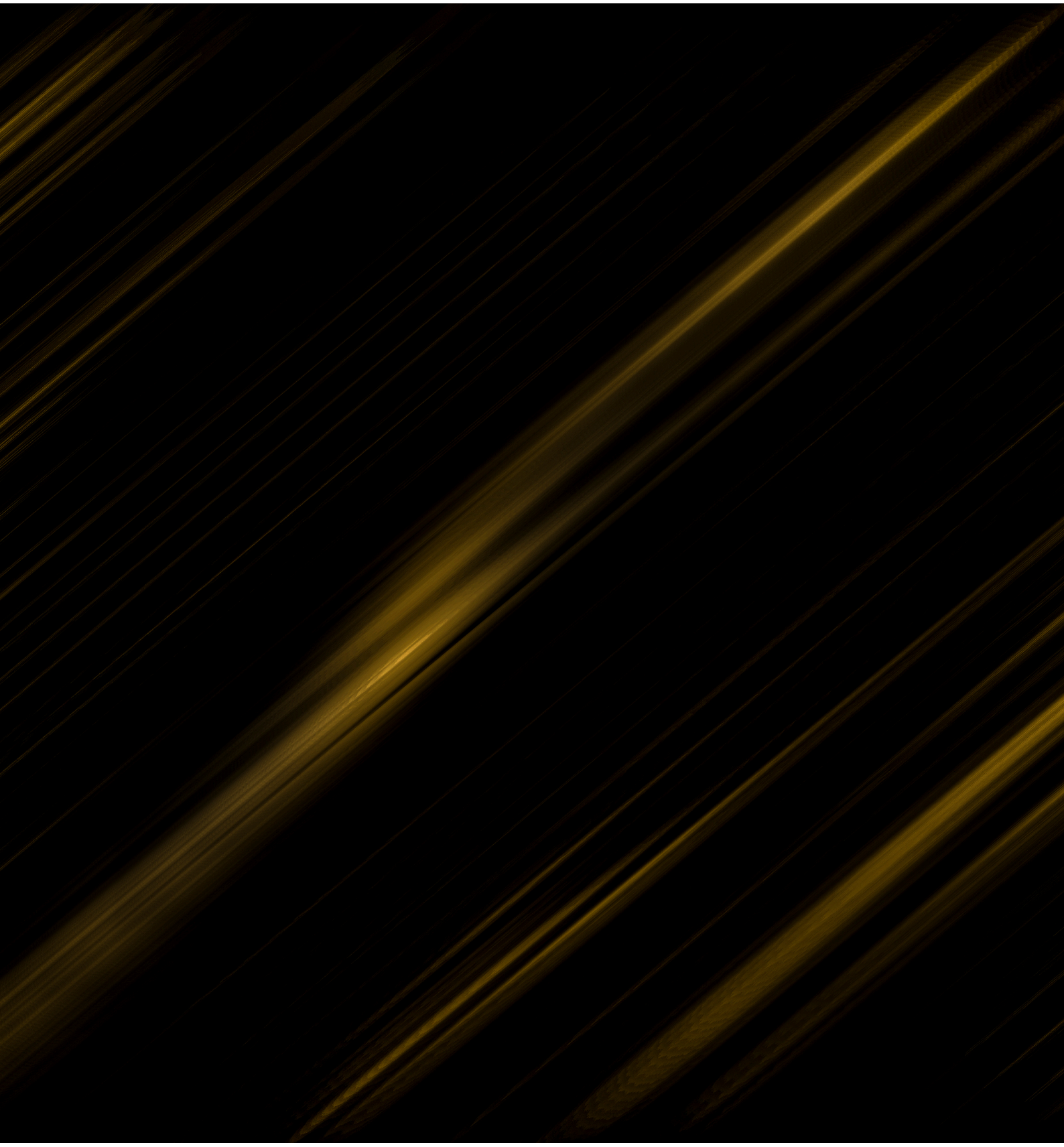
[27] Un po' la riflessione che si ritrova in A. Von Bogdandy, Il diritto europeo oltre l'"Unione sempre più stretta": ricostruzione del concetto e della metodologia comparativa della Corte di giustizia, in Il diritto dell'Unione europea, n. 1/2017.

FONTI PRINCIPALI

- A. Cantaro, "Il nomos 'preso sul serio'", in Teoria del diritto e dello Stato, n. 1-2, 2011.
- C. Cellerino, "La difesa europea dinanzi alla guerra in Ucraina tra 'autonomia strategica' e vincoli strutturali: quali prospettive per la difesa comune?", in Il diritto dell'Unione europea, n. 1, 2023.
- A. De Petris, "Una Germania senza freno, ovvero: trasformare una crisi in catarsi", in DPCE Online, n. 1, 2025.
- M. Della Malva, "Gli sviluppi della dottrina Monroe dal 1900 ad oggi. Una lunga evoluzione", in DPCE Online, n. 2, 2024.
- J. Dufourcq, "Per Parigi è l'ora dell'Europa potenza", in Limes, n. 6, 2022.
- G. Dottori, La visione di Trump. Obiettivi e strategie della nuova America, Roma, Salerno Editrice, 2019.
- G. Duso (a cura di), La politica oltre lo Stato, Venezia, 1981.
- S. Fabbrini, Sdoppiamento. Una prospettiva nuova per l'Europa, Roma-Bari, Laterza, 2017.
- S. Fabbrini, Nazionalismo 2.0. La sfida sovranista all'Europa integrata, Milano, 2025.
- F. Fabbrini, "La Bussola strategica dell'UE: luci ed ombre", Centro Studi sul Federalismo, n. 245, 2022.
- C. Galli, Spazi politici. L'età moderna e l'età globale, Bologna, Il Mulino, 2001.
- C. Galli, "Carl Schmitt. La politica, lo spazio, la guerra", in Gnosis. Rivista italiana di intelligence, n. 3, 2021, 90 ss.
- F. Gasperi, "Profili costituzionali della difesa comune europea", in Costituzionalismo.it, n. 2, 2023.
- A. Giurickovic Dato, "L'Unione europea di fronte alla crisi ucraina", in Federalismi.it, n. 23, 2023.

- S. Goulard, Grande da morire. Come evitare l'esplosione dell'Europa, Bologna, 2025.
- P. Grossi, Ritorno al diritto, Roma-Bari, Laterza, 2015.
- P. Grossi, Mitologie giuridiche della modernità, Milano, Giuffrè, 2007.
- P. Grossi, L'Europa del diritto, Roma-Bari, Laterza, 2016.
- S. Guerra, Schmitt, Kelsen e Smend nella Repubblica di Weimar. Diagnosi di una crisi democratico-costituzionale, Torino, Giappichelli, 2024.
- H. Hofmann, Legittimità contro legalità. La filosofia politica di Carl Schmitt, Napoli, Editoriale Scientifica, 1999.
- E. Jünger – C. Schmitt, Il nodo di Gordio, Milano, Adelphi, 2023.
- M. Mariano, L'America nell'Occidente. Storia della dottrina Monroe (1823-1963), Roma, Carocci, 2013.
- G. Miglio – P. Schiera (a cura di), Le categorie del politico, Bologna, Il Mulino, 1972.
- A. Monti, "Il rinnovamento dell'intelligence ha bisogno di coerenza normativa", Formiche.net, 6 dicembre 2020.
- C. Sbailò, Europe's call to arms. Philosophical roots and public law profiles of the confrontation with the monster of the 21st century: westernization without democratization, Baden-Baden, Nomos Verlag, 2023.
- C. Sbailò (a cura di), Difesa europea. Quali prospettive, in Federalismi.it, numero speciale n. 1, 2019.
- C. Sbailò, "Crisi nordafricana, καταστροφή e occasione di rilancio per l'Europa", in Federalismi.it, n. 1, 2019.
- A. Scalone, "La teoria schmittiana del grande spazio: una prospettiva post-statuale?", in Scienza e politica, n. 56, 2017, 179-205.

- G. Sessa, Tertium datur. Filosofie dell'originario, Roma, 2025.
- C. Schmitt, Il valore dello Stato e il significato dell'individuo (1914), a cura di C. Galli, Bologna, Il Mulino, 2013.
- C. Schmitt, Il concetto di politico (1927), in Le categorie del politico, a cura di G. Miglio – P. Schiera, Bologna, Il Mulino, 1972, 87 ss.
- C. Schmitt, L'ordinamento dei grandi spazi nel diritto internazionale con divieto di intervento per potenze straniere. Un contributo sul concetto di impero nel diritto internazionale (1941), in Stato, grande spazio, Nomos, Milano, Giuffrè, 2015.
- C. Schmitt, Il nomos della Terra, Milano, Adelphi, 1991.
- A. Ruffo, "La difesa europea (PSDC) e la Costituzione italiana alla prova della Bussola strategica 2022", in Federalismi.it, n. 7, 2024.
- G. Vellano, "La guerra in Ucraina e le decisioni dell'Unione europea in materia di sicurezza e difesa comune", in Il diritto dell'Unione europea, n. 1, 2022.
- G. Vosa, "Sull'equilibrio costituzionale dell'Unione europea. La costituzione 'nata dal cambiamento' e i limiti alla priorità applicativa del diritto sovranazionale", in Costituzionalismo.it, n. 3, 2021.
- A. Von Bogdandy, "Il diritto europeo oltre l'"Unione sempre più stretta': ricostruzione del concetto e della metodologia comparativa della Corte di giustizia", in Il diritto dell'Unione europea, n. 1, 2017.
- Consiglio dell'Unione Europea, Conclusioni del Consiglio del 20-21 ottobre 2022 sull'uso dell'energia come arma da parte della Russia, Bruxelles, 2022.
- U. Von der Leyen, "Dichiarazione alla stampa sul piano 'Rearm Europe/Readiness 2030'", Commissione Europea, 4 marzo 2025.



Recensioni e Schede

Una pace da temere. La lezione di Zouhir Louassini

Stefano Lovi
PhD Candidate - Università degli Studi Internazionali di Roma (UNINT)

Recensione del libro "Chi ha paura della pace?" di Zouhir Louassini

Ci sono libri che non si limitano a commentare l'attualità, ma la attraversano come con uno sguardo che scruta più in profondità, costringendo il lettore a guardare in faccia le contraddizioni del proprio tempo. Chi ha paura della pace? di Zouhir Louassini appartiene a questa categoria rara. Fin dalle prime pagine, il saggio si impone prepotentemente per chiarezza e profondità, aprendo una riflessione che travalica il caso mediorientale per toccare la sostanza politica, economica e culturale della guerra contemporanea.

Louassini sceglie di aprire con una frase di Paul Valéry: «La guerra comincia sempre lontano da chi la decide». È una citazione che racchiude l'essenza dell'intero libro. Chi decide i conflitti, siano essi generali, capi di Stato, o manager dell'industria bellica, raramente ne paga il prezzo. A morire sono altri: uomini e donne che non si conoscono, che hanno «lo stesso identico umore, ma la divisa di un altro colore», che diventano pedine nel gioco di chi si conosce fin troppo bene. È un modo secco e potente per dire che la guerra non è mai "inevitabile": è sempre una scelta politica, calcolata, razionale nel suo cinismo.

Il punto di partenza di Chi ha paura della pace? è il conflitto israelo-palestinese, ma sarebbe limitante affermare che parli solo di quello scenario, in quanto Louassini lo trasforma in una lente per leggere il mondo intero. Con una scrittura limpida, densa ma mai accademica, intreccia politica, storia e filosofia, smontando le retoriche che da decenni accompagnano le guerre del nostro tempo. Al centro della sua analisi c'è una domanda tanto semplice quanto destabilizzante: perché la pace fa paura?

La risposta sta, secondo l'autore, nella struttura stessa del potere globale. Louassini cita un discorso di Shimon Peres a Pretoria, nel 1996, in cui il leader israeliano affermava: «La guerra e la pace non si decidono sulle altezze spirituali. Si decidono nei bilanci, nei consorzi, nei calcoli». In altre parole, la pace non è un'utopia romantica che manca di realismo, ma un progetto concreto che scontra interessi economici consolidati. La guerra, invece, è un affare. E lo è sempre stata.

Come dicevamo, Louassini analizza con precisione chirurgica la parabola degli Accordi di Oslo del 1993, quel breve momento in cui israeliani e palestinesi sembravano aver trovato la forza di uscire dal ciclo dell'odio. «Non furono né l'assenza di sostegno internazionale né la carenza di immaginazione a far deragliare Oslo», scrive l'autore, «ma l'incapacità di trasformare la visione in azione». Il tempo lasciato passare aprì spazio a chi voleva bloccare il cambiamento, e alla fine vinse chi della pace aveva più paura.

La notte del 4 novembre 1995, quando Yitzhak Rabin venne assassinato da un estremista israeliano, segna per Louassini un punto di non ritorno. «Uno di quei momenti in cui la storia trattiene il fiato, e poi cambia direzione». Non è solo la morte di un uomo: è la fine di una possibilità storica. Dopo Rabin, l'idea di una pace concreta, imperfetta ma possibile, si è spenta. A prevalere sono stati gli estremismi, simmetrici e speculari, tanto nel fanatismo di Hamas quanto nella destra israeliana più radicale ed estrema. Entrambi, osserva Louassini, «consideravano la pace un pericolo mortale». Ogni attentato suicida rafforzava chi voleva chiudere con la trattativa, ogni nuova colonia in Cisgiordania dava a Hamas una nuova ragione per continuare la lotta. Un meccanismo perfetto, alimentato dalla paura e dal calcolo politico.

Il saggio di Louassini va però oltre il Medio Oriente. La sua riflessione si fa universale quando mostra come la guerra, nel mondo globalizzato, sia diventata un mestiere. Esistono carriere, economie, persino linguaggi costruiti per renderla accettabile. Le decisioni militari passano attraverso consigli di amministrazione, analisi di mercato, report di "esperti indipendenti" che spesso lavorano per think tank finanziati dall'industria degli armamenti. È un sistema autoreferenziale che trasforma il conflitto in una variabile economica. Louassini denuncia questa ipocrisia con toni sobri ma duri. L'immagine del giornalista o dell'analista televisivo che parla di "interventi chirurgici" o "danni collaterali" diventa emblematica di una narrazione che addomestica la violenza. Si parla di strategie e geopolitica, ma mai di corpi, di fame, di vite interrotte. La guerra diventa linguaggio, spettacolo, routine da rendere accettabile (e inevitabile) alle orecchie di tutti.

In questo senso, Chi ha paura della pace? è anche un libro sulla manipolazione del discorso pubblico. La pace non è solo un'assenza di guerra: è una minaccia per chi costruisce consenso sulla paura. La logica del "noi contro loro" alimenta il potere, semplifica la complessità, legittima i bilanci militari e silenzia le voci dissonanti. È un processo che ricorda ciò che Hannah Arendt chiamava "banalità del male": il male non come gesto eccezionale, ma come amministrazione efficiente della violenza.

Louassini osserva come le società contemporanee siano state addestrate a vivere in uno stato di emergenza permanente. Ogni crisi, reale o percepita che sia, giustifica nuove spese militari, nuovi muri, nuove armi "difensive". Ma in questa escalation continua, il concetto stesso di sicurezza si svuota. La sicurezza diventa paura amministrata. È un pensiero che riecheggia le riflessioni di Zygmunt Bauman: in un mondo liquido, dove l'incertezza è la regola, la paura diventa merce politica.

I numeri citati da Louassini parlano da soli. Secondo il SIPRI, nel 2024 la spesa militare globale ha toccato i 2.443 miliardi di dollari, un record storico. È come se ogni cittadino del pianeta avesse versato 306 dollari per alimentare la macchina bellica mondiale. Una cifra sufficiente, come ricorda l'ONU, a cancellare la fame nel mondo dieci volte. Eppure, la scelta collettiva continua a pendere dalla parte delle armi. «Nel mondo contemporaneo – scrive Louassini – non esistono guerre senza mercato». Ogni conflitto diventa occasione di profitto per qualcuno e di rovina per molti.

Questa logica, spiega l'autore, ha conseguenze profonde anche sul modo in cui pensiamo la pace. Se la guerra è redditizia, la pace diventa economicamente scomoda. È la riflessione che attraversa tutto il libro: la pace non è mai fallita per mancanza di idee o di buona volontà, ma perché minaccia interessi troppo radicati. È qui che la domanda del titolo acquista il suo pieno significato: chi ha paura della pace? Non i popoli, che dalla pace avrebbero solo da guadagnare, ma chi della guerra ha fatto mestiere, carriera, potere.

C'è, in Louassini, una forza morale che non si nasconde dietro il disincanto. Il suo non è un libro pacifista nel senso ingenuo del termine. È, piuttosto, un richiamo alla responsabilità. La pace, scrive, non è un sentimento, ma una costruzione politica. Richiede tempo, coraggio, immaginazione, e soprattutto la volontà di andare controcorrente. Quando Shimon Peres diceva: «Non ci ameremo subito. Ma se costruiremo insieme abbastanza cose, impareremo almeno a non distruggerle», esprimeva un realismo che oggi sembra quasi rivoluzionario.

In un mondo polarizzato, dove il conflitto è diventato linguaggio comune e l'odio si propaga in tempo reale sui social, Louassini invita a riscoprire la pace come atto di intelligenza. Non come debolezza, ma come strategia di sopravvivenza collettiva. È una visione che dialoga con quella del sociologo Johan Galtung, teorico della "pace positiva": non semplice assenza di guerra, ma presenza di giustizia, cooperazione, diritti.

Chi ha paura della pace? è, in definitiva, un libro necessario. Non tanto perché dica qualcosa di nuovo sulla guerra (la storia umana ne è piena), ma perché riesce a dire qualcosa di nuovo sulla pace. La presenta non come utopia, ma come scelta razionale, come sfida concreta alla logica della paura e del profitto. In un tempo in cui la guerra è tornata sul suolo europeo e il linguaggio della violenza sembra nuovamente "normalizzato", la voce di Louassini risuona come un richiamo alla lucidità.

La sua scrittura, chiara e incisiva, evita sia il moralismo sia l'accademismo. Parla a chi vuole capire, non a chi vuole schierarsi o è già schierato. Ed è proprio questa la forza del libro: smontare la retorica dei "buoni" e dei "cattivi", restituendo alla complessità il posto che le spetta. Perché la pace, ci ricorda Louassini, è complessa. Ma lo è anche la guerra, eppure la accettiamo ponendoci poche domande.

Alla fine della lettura, resta una sensazione duplice: amarezza e speranza. Amarezza per ciò che la storia ha perso, speranza perché l'autore mostra che la pace non è scomparsa, è solo stata messa a tacere. Tocca a noi, cittadini, lettori, ma soprattutto elettori, rimetterla al centro del discorso politico.

Recensioni e Schede

Fare bene i conti: consigli per una cittadinanza fiscalmente consapevole

Andrea De Petris
Professore aggregato di Diritto Comparato - Università degli Studi Internazionali di Roma (UNINT)

Recensione di "Facciamo bene i conti. Equità fiscale per una Italia più giusta", di Ferdinando Capuozzo

Facciamo bene i conti è un saggio molto compatto nelle dimensioni, e che tuttavia denota chiari pregi in termini di chiarezza, rigore e capacità divulgativa. Lasciando da parte i toni formali e tecnici tipici della tradizionale letteratura disponibile sulla materia, l'autore – che viene da una esperienza principalmente professionale, in veste di dottore commercialista e di consulente aziendale – presenta al lettore una riflessione ampia ed articolata, seguendo un percorso analitico equilibrato e comprensibile. Grazie ad uno stile espositivo scorrevole, a tratti persino colloquiale, e ad un linguaggio accessibile a tutti, Ferdinando Capuozzo riesce a rendere i profili in verità complessi della finanza pubblica e delle questioni fiscali ad essa collegate non solo comprensibili, ma anche coinvolgenti, guidando il lettore in un percorso di acquisizione di consapevolezza civile e finanziaria.

Il punto di partenza del testo, in apparenza semplice e tuttavia impegnato a confrontarsi con un tema di innegabile complessità, colpisce per l'impatto del suo incipit: tutti parlano di tasse, pochi ne conoscono davvero il funzionamento.

Da qui, spiega l'autore, nasce appunto l'esigenza di "fare bene i conti", ovvero di andare oltre i luoghi comuni e comprendere il significato profondo dell'imposizione fiscale come strumento operativo per raggiungere gli obiettivi espressamente sanciti dal dettato costituzionale di equità e coesione sociale. Con poche, ma efficaci motivazioni ed una dialettica diretta e colloquiale, Capuozzo svela con efficacia l'erroneità delle credenze più diffuse in materia fiscale - "paghiamo troppe tasse", "lo Stato spreca tutto", "l'evasione è inevitabile" - presentando una serie aggiornata di dati che offrono la base fattuale per sviluppare riflessioni con cui si invita il lettore a prendere visione della realtà dei fatti, e a superare i falsi miti che la comunicazione spesso spicciola e superficiale dei nostri tempi tende sistematicamente a veicolare.

Tra i temi principali trattati nel volumetto spiccano l'equità fiscale e la distribuzione delle imposte, affrontati con un taglio che accompagna alla competenza tecnica una consapevole sensibilità etica. Il libro mostra come un sistema tributario giusto non possa limitarsi a raccogliere risorse, ma debba farlo in modo proporzionato alle possibilità di ciascuno, secondo il principio costituzionale della progressività. In questo senso, l'autore sottolinea che pagare le tasse non è una punizione o un onere arbitrario imposto dall'alto, ma un pieno dovere "di solidarietà politica, economica e sociale" (come espressamente sancisce l'ultimo comma del secondo articolo della Costituzione), con cui l'individuo diviene partecipe della sfera sociale di cui, a vario titolo, fa parte.

Nel testo viene dedicato un ampio spazio anche al rapporto tra cittadini e Stato, tema rispetto al quale l'autore ammonisce di come la percezione negativa delle tasse nasca spesso da un deficit di trasparenza rispetto al modo in cui le istituzioni utilizzano le risorse finanziarie prodotte dal gettito fiscale. Attraverso esempi tratti dall'attualità e da esperienze internazionali, Capuozzo mostra come una comunicazione più chiara e una gestione più efficiente della spesa pubblica consentirebbero di rafforzare il "patto fiscale" che lega ogni cittadino alla comunità, e dal quale tuttavia molti nel sistema italiano si sentono solamente gravati, senza riuscire a cogliere le ricadute positive che esso tuttavia produce.

Un altro aspetto di grande interesse è l'analisi dell'evasione fiscale, presentata non solo come questione economica, ma soprattutto come problema culturale ed etico. L'autore evidenzia come venire meno ai propri doveri di contribuzione fiscale sottragga risorse essenziali ai servizi pubblici - sanità, istruzione, infrastrutture, ma anche sicurezza, ricerca, innovazione –, finendo in questo modo per produrre l'effetto opposto a quello che l'imposizione fiscale si prefigge di raggiungere, aumentando le disuguaglianze sociali, invece che riducendole. Le proposte di riforma per rendere il gettito fiscale più stabile ed equo non si concentrano tanto sulle azioni repressive e punitive, ma mirano prevalentemente ad incentivare la compliance e la fiducia dei cittadini contribuenti, proponendo misure atte a realizzare un sistema fiscale più trasparente, digitale e semplificato.

Un testo nel testo è la parte dedicata agli approfondimenti terminologici dei concetti fondamentali della finanza pubblica, come deficit, PIL, spesa pubblica e debito, in cui vengono spiegate in modo semplice ma preciso nozioni complesse, evitando tecnicismi e meticolosit e rendendole fruibili anche ad un pubblico ampio e privo di conoscenze pregresse.

Facciamo bene i conti va oltre la dimensione del tipico testo manualistico sui temi dell'economia e della politica fiscale, ma pone al lettore un invito a confrontarsi in modo consapevole non solo con i temi della fiscalità, ma anche con la dimensione costituzionale e sociale legata a tali argomenti. Lo scopo del saggio è ben esplicato nella parte finale del testo: comprendere il funzionamento del sistema fiscale e delle regole della finanza pubblica significa comprendere in ultimo il funzionamento dell'apparto statale, le sue finalità e gli obiettivi stessi dell'ordinamento democratico, nella convinzione che una conoscenza diffusa e una partecipazione informata di tali materie sia la condizione imprescindibile per la costruzione di un fisco più equo, sostenibile e partecipato.

In conclusione, il lavoro di Capuozzo costituisce una lettura opportuna per studenti, professionisti, amministratori e per chiunque voglia andare oltre la disinformazione che accompagna i temi fiscali, ed intenda comprendere realmente il ruolo delle imposte nella costruzione del bene comune e della democrazia. "Fare bene i conti" serve non solo per ottemperare ai doveri etici e politici costituzionalmente previsti, ma anche a dimostrarsi cittadini competenti, impegnati ed interessati alla dimensione sociale del vivere civile.