L'attacco cibernetico nell'era della guerra ibrida

di Andrea Spaziani

Abstract: *Cyber-attack in the hybrid warfare* - Hybrid warfare poses a new threat to international security. Armed forces and conventional tactics are no longer sufficient in a conflict. Today, thanks to technological development, states have new tools – disinformation, propaganda and critical infrastructure attacks – and new domains – cyberspace – at their disposal to exploit adversary's vulnerabilities. In academic circles, attempts have been made to capture the complexity of these new conflicts through the concept of "hybrid warfare". However, there is still no universally accepted definition of hybrid warfare, making complicated the possible response of policy makers and international organizations.

Keywords: Hybrid warfare; Hybrid threats; Cyberspace; Disinformation; Hybrid response.

1. Premessa

Nel corso degli ultimi decenni, i conflitti armati, pur conoscendo una riduzione sul piano della loro frequenza, hanno conosciuto importanti mutamenti a causa dell'emersione di nuovi avversari (attori statali e non statali), di nuovi strumenti di attacco e, finanche, di nuovi domini (*cyberspace*). In particolare, lo sviluppo tecnologico ha incrementato la precisione delle armi convenzionali, con l'introduzione di droni, robotica militare, sistemi di difesa missilistica e armi cibernetiche.

Ad oggi, tali strumenti consentono agli apparati militari di condurre non solo operazioni più precise e mirate, riducendo al minimo i danni collaterali e aumentando la loro efficacia sul campo di battaglia, ma anche di diversificare lo spettro di azione. Questo può avvenire mediante il ricorso, in particolare, ad attacchi cibernetici al fine di destabilizzare l'avversario, influenzare i processi democratici e compromettere le infrastrutture critiche nazionali e sovranazionali.

In questo nuovo scenario, il concetto di "guerra ibrida" è sempre più utilizzato «per cercare di catturare la complessità della guerra del XXI secolo, che coinvolge una molteplicità di attori e sfuma le tradizionali distinzioni tra i diversi tipi di conflitto armato e persino tra guerra e pace»[1]. Difatti, questa tipologia di conflitto, come tra poco si vedrà, si caratterizza per l'utilizzo di una combinazione di mezzi convenzionali, non convenzionali, *cyber*, informazioni e propaganda allo scopo di raggiungere obiettivi politici e militari, che finiscono per complicare di molto la risposta sul piano

[1] J.K. Wither, *Making Sense of Hybrid Warfare*, in *Connections*, 15, 2, 2016, 74.

DPCE online
ISSN: 2037-6677

giuridico, dato che le azioni degli attori ibridi – per lo più, appunto, non cinetiche – non superano le soglie di intensità che legittimerebbero il ricorso all'uso della forza.

Il presente lavoro cercherà di analizzare il ruolo e i caratteri dell'attacco cibernetico nell'ambito della "guerra ibrida", al fine di aprire una riflessione orientata ad offrire nuove categorie di analisi che consentano di comprendere come tale tipologia di conflitto possa destabilizzare – forse molto più del tradizionale conflitto militare – la tenuta e la stabilità degli ordinamenti democratici.

2. La "guerra ibrida": una ricostruzione in chiave diacronica

Dal punto di vista storico, la "guerra ibrida", pur avendo acquisito inusitata vitalità a seguito dell'avvento dell'era digitale, non rappresenta una nuova categoria di conflitto, in quanto «le sue radici possono essere fatte risalire a tempi immemorabili»[2]. Anzi, nella fase attuale, la "guerra ibrida" può considerarsi «un'interpretazione moderna dell'antica combinazione di approcci convenzionali e non convenzionali»[3]. Dello stesso avviso è anche il Segretario generale della NATO, Jens Stoltenberg, il quale ha sostenuto che «la prima guerra ibrida che conosciamo potrebbe essere il cavallo di Troia»[4].

Murray e Mansoor, nella loro interessante opera "*Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*"[5], collocano addirittura nel V secolo a.C. – durante la Guerra del Peloponneso tra Sparta e Atene – la prima apparizione di una tipologia di conflitto di tipo "ibrido"[6]. In tempi più vicini, le azioni militari britanniche contro la Turchia ottomana, durante la Prima Guerra Mondiale, contenevano elementi "ibridi", visto che tale campagna ottenne il successo sperato grazie alla rivolta delle forze irregolari arabe, guidate dallo sceriffo al-Husayb ibn Ali e dal capitano inglese Thomas Edward Lawrence, anche conosciuto con lo pseudonimo "Lawrence d'Arabia"[7].

Durante la Seconda Guerra Mondiale, invece, l'esercito tedesco, sul fronte orientale, subì varie interruzioni alle proprie linee di comunicazione a

[2] J. Víšek, C.D. Chisereu, *The Law Enforcement Agencies' Relevance in Countering Hybrid Armed Conflicts*, in *Lex Humana*, 15, 4, 2023, 310.
[3] B. Giegerich, *Hybrid Warfare and the Changing Character of Conflict*, in *Connections*, 15, 2, 2016, 67.
[4] Il segretario generale della NATO Jens Stoltenberg, *Zero-sum? Russia, Power Politics, and the Post-Cold War Era*, Bruxelles Forum, 20-03-2015, http://www.nato.int/cps/en/natohq/opinions_118347.htm.
[5] W. Murray, P.R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge, 2012.
[6] In tale conflitto, Atene utilizzò alcuni stratagemmi – come la costruzione di una base di spedizione a Pilo o le successive incursioni dei Messeni in Laconia che spinsero gli Iloti a disertare verso Pilo, creando un'emergenza nazionale a Sparta – introducendo la dimensione non convenzionale all'interno dello scontro con Sparta (in W. Murray, P.R. Mansoor, *op. cit.*, 3-4).
[7] Le azioni delle tribù arabe si rivelarono particolarmente preziose per i britannici grazie ai diversi attacchi contro le forze turche, alla rivelazione di informazioni circa le posizioni ottomane e all'interruzione dei rifornimenti turchi. Tali attività non convenzionali contribuirono alla vittoria britannica a Megiddo nel settembre del 1918 (in W. Murray, P.R. Mansoor, *op. cit.*, 6-7).

causa delle continue attività dei partigiani sovietici e di altri attori irregolari. La *Wehrmacht* si trovò così all'interno di una morsa lacerante, che non le consentiva di utilizzare le unità, già impegnate sul fronte principale, per affrontare la minaccia sovietica che proveniva dalle retrovie[8]. Esempi di "guerra ibrida" si riscontrano anche in Asia, in particolare nel secondo conflitto sino-giapponese (dal 1937 al 1945), che vide opposte la Repubblica cinese e l'impero giapponese. Mao Zedong e i suoi generali si distinsero per le proprie abilità strategiche, combinando forze regolari e irregolari e riuscendo, alla fine, a liberare la Repubblica cinese dal controllo nipponico. Dopo la resa del Giappone, le forze comuniste utilizzarono le stesse tecniche anche contro gli avversari nazionalisti, successivamente espulsi e costretti a rifugiarsi a Taiwan[9].

A metà degli anni Novanta, il lemma "guerra ibrida" compare in un contributo di J. Mockaitis, in relazione ad alcuni conflitti coloniali britannici[10]. Successivamente, viene ripreso da altri autori (Walker[11], Nemeth[12], Dupont[13], Carayannis[14] e Simpson[15]) per definire guerre "atipiche", ovvero non aderenti ai classici paradigmi della guerra tradizionale, non riuscendo tuttavia a offrirne una definizione giuridicamente esauriente.

La prima formulazione ufficiale del concetto di "guerra ibrida" viene fatta risalire all'opera del teorico militare statunitense Frank Hoffman. Già nel 2005, lo stesso Hoffman – unitamente al generale James Mattis – avevano pubblicato un articolo dal titolo "*Future Warfare: The Rise of Hybrid Wars*", nel quale si sottolineava l'emersione di nuove e irrituali modalità di confronto militare che avrebbero potuto rappresentare una seria minaccia per gli Stati Uniti[16].

[8] W. Murray, P.R. Mansoor, *op. cit.*, 4.
[9] *Ivi*, 5.
[10] J.R. Mockaitis, *British Counterinsurgency in the Post-Imperial Era*, Manchester, 1995.
[11] R.G. Walker, *SPEC FI: The United States Marine Corps and Special Operations*, Monterey, California, Naval Postgraduate School, 1998, https://apps.dtic.mil/sti/pdfs/ADA359694.pdf.
[12] W.J. Nemeth, *Future war and Chechnya: a case for hybrid warfare*, Monterey, California, Naval Postgraduate School, 2002, https://core.ac.uk/download/pdf/36699567.pdf.
[13] A. Dupont, *Transformation or Stagnation? Rethinking Australia's Defence*, Strategic and Defense Studies Centre, Australian National University, Canberra, 2003, https://sdsc.bellschool.anu.edu.au/sites/default/files/publications/attachments/2016-03/WP-SDSC-374_0.pdf.
[14] T. Carayannis, *The Complex Wars of the Congo: Towards a New Analytic Approach*, in *Journal of Asian and African Studies*, 38 (2-3): 232–255.
[15] E.M. Simpson, *Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims*, Paper presented to the Annual Meeting of the Midwest Political Science Association, Chicago, 7-11-04-2005.
[16] «La nostra superiorità convenzionale crea una logica irresistibile per gli Stati e gli attori non statali che vogliono uscire dalla modalità di guerra tradizionale e cercare una capacità di nicchia o una combinazione inaspettata di tecnologie e tattiche per ottenere un vantaggio [...] Ci aspettiamo che i futuri nemici guardino ai quattro approcci come a una sorta di menù e scelgano una combinazione di tecniche e tattiche a loro gradita. Non ci troviamo di fronte a una serie di quattro sfidanti separati, quanto piuttosto alla combinazione di nuovi approcci – una fusione di diversi modi e mezzi di guerra. Questa sintesi senza precedenti è ciò che chiamiamo guerra ibrida» (traduzione dell'A.). J.N. Mattis, F.G. Hoffman, *Future Warfare: The Rise of Hybrid Wars*, U.S. Naval Institute,

DPCE online
ISSN: 2037-6677

Due anni dopo, nel 2007, Hoffman ha affinato ulteriormente il concetto nell'opera "*Conflict in the 21st Century: The Rise of Hybrid Wars*"[17], sostenendo

131/11/1, 233, 2005, https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.

[17] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington (Virginia), Potomac Institute for Policy Studies, 2007. Il presente contributo è stato influenzato dalle idee di altre teorie che hanno tentato di cogliere i caratteri dei conflitti nel contesto contemporaneo e che sono state sintetizzate mediante il ricorso a talune accezioni, quali, la "guerra senza limiti", la "guerra di quarta generazione" e la "guerra composta" – e dal documento *The National Defense Strategy of the United States of America* del 2005. La "guerra senza limiti" è stata teorizzata da due colonnelli cinesi, Qiao Ling e Wang Xiangsui, i quali nel febbraio del 1999 pubblicano il libro "Unrestricted Warfare". Tra i passi più importanti dell'opera, che hanno ispirato Hoffman, c'è sicuramente quello relativo alla combinazione di diverse operazioni, metodi ed elementi in battaglia: «Indipendentemente dal momento storico, tremila anni fa come alla fine del ventesimo secolo, sembra che tutte le vittorie rivelino un fenomeno comune: il vincitore è colui che ha saputo ottenere la giusta combinazione» in Q. Liang, W. Xiangsui (a cura di F. Mini), *Guerra senza limiti*, Gorizia, LEG Edizioni, 2019, 123. La "guerra di quarta generazione" viene introdotta per la prima volta, nel 1989, dallo stratega militare William Lind nell'articolo "*The Changing Face of War: Into the Fourth Generation*" (in W.S. Lind, K. Nightengale, J.F. Schmitt, J.W. Sutton, G.I. Wilson, *The Changing Face of War: Into the Fourth Generation*, in *Marine Corps Gazette*, 1989, 22-26). In breve, la guerra di quarta generazione è quella in cui gli avversari, solitamente i più deboli, fanno ricorso ad un'ampia gamma di azioni offensive e difensive, le quali includono tutte le reti disponibili – politiche, militari, economiche, sociali e psicologiche – al fine di distruggere la volontà politica del nemico di combattere. La "guerra composta", poi, è un concetto ideato alla fine degli anni Novanta dallo storico militare Thomas Huber. Secondo quest'ultimo, la guerra composta prevede «l'uso simultaneo di una forza regolare o principale e di una forza irregolare o di guerriglia contro un nemico» (in T.M. Huber, *Compound Warfare: That Fatal Knot*, in *U.S. Army Command and General Staff College Press*, Combat Studies Institute, Fort Leavenworth (Kansas), 2002, 1). Le operazioni della forza regolare e di quella irregolare, poi, prevedono diversi vantaggi reciproci. Quella irregolare aiuta quella regolare poiché «potenzia lo sforzo della forza regolare offrendo informazioni, beni e truppe, mentre li nega al nemico» (*Ivi*, 2). Viceversa, la forza regolare interviene in soccorso della guerriglia fornendo «un sollievo dalla presenza del nemico nella località, addestramento e rifornimenti, informazioni strategiche e influenza politica locale» (*Ibid*). In sintesi, dunque, la guerra composta, attraverso queste interazioni tra forza regolare e irregolare, diventa particolarmente efficace, dato che «il tutto è superiore alla somma delle parti» (*Ibid*). Un altro documento importante per la concettualizzazione di Hoffman è stato il *The National Defense Strategy of the United States of America* del 2005, pubblicato dall'allora segretario della difesa, Donald Rumsfeld. Analizzando le sfide alla sicurezza che attendono gli Stati Uniti nel XXI secolo, il contributo le riunisce in quattro gruppi principali: sfide tradizionali, irregolari, catastrofiche e distruttive. Le prime si riferiscono alle classiche forme della competizione militare; le seconde sono quelle portate avanti da avversari che utilizzano metodi irregolari per tentare di danneggiare l'influenza e la volontà politica americana; le terze sono rappresentate da attori in grado di utilizzare armi di distruzione di massa; infine, le quarte possono essere condotte da avversari che dispongono di tecnologie rivoluzionarie e capacità militari in grado di rovesciare lo stile tradizionale di guerra. Un altro suggerimento presente nel documento in parola – e raccolto da Hoffman nella sua concettualizzazione della guerra ibrida – riguarda il fatto che le sfide del XXI secolo non saranno distinte e separate, ma potrebbero conoscere un complesso e drammatico gioco di sovrapposizione, con conseguente aumento dell'intensità dello scontro.

che lo stesso incorpora «una serie di diverse modalità di guerra, tra cui capacità convenzionali, tattiche e formazioni irregolari, atti terroristici che includono violenza indiscriminata, coercizione e disordini criminali»[18]. Un altro elemento chiave dell'opera del teorico militare statunitense riguarda la formulazione del termine "minaccia ibrida". Secondo Hoffman, quest'ultima è rappresentata da «qualsiasi avversario che impiega simultaneamente e in modo adattivo una combinazione di armi convenzionali, tattiche irregolari, terrorismo e comportamenti criminali nello spazio di battaglia per ottenere i propri obiettivi politici»[19]. Ciononostante, i due termini sono talvolta utilizzati in modo intercambiabile e questo ha finito per alimentare ulteriore confusione. Come sottolineato da Monaghan, la "guerra ibrida" «descrive la sfida rappresentata dalla crescente complessità dei conflitti armati, in cui gli avversari possono combinare tipi di guerra e mezzi non militari per neutralizzare il potere militare convenzionale»[20]; viceversa, le minacce ibride «combinano un'ampia gamma di mezzi non violenti per colpire le vulnerabilità dell'intera società o minare il funzionamento, l'unità o la volontà dei loro obiettivi, degradando e sovvertendo lo status quo [...] ma senza scatenare risposte decisive, comprese quelle armate»[21]. In altre parole, la "guerra ibrida" si focalizza principalmente sul cambiamento nel carattere della guerra e sulla combinazione di mezzi e metodi convenzionali e non convenzionali, mentre le "minacce ibride" concentrano la propria attenzione sui soggetti attivi (attori statali e non statali) che tentano di ottenere vantaggi sfruttando il confine, sempre più sfumato, tra guerra e pace.

Come notato da Fridman, il concetto hoffmaniano di "guerra ibrida" «descrive meglio il carattere evolutivo del conflitto rispetto alla "contro-insurrezione; sfida l'attuale pensiero e i contenitori intellettuali binari che inquadrano il dibattito; sottolinea la reale ampiezza dello spettro dei conflitti umani; aumenta la consapevolezza dei rischi potenziali e dei costi di opportunità presentati dalle varie opzioni nel dibattito in corso sulla minaccia/posizione di forza»[22]. Inoltre, il grande merito del contributo della teoria di Hoffman, sempre secondo Fridman, è la sua praticità, soprattutto per i decisori militari a livello operativo[23].

Hoffman sottolinea anche un aspetto molto importante della "guerra ibrida", ossia la possibilità che la stessa possa essere condotta sia da attori

[18] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, Potomac Institute for Policy Studies, 2007, 14.
[19] F.G. Hoffman, *"Hybrid Threats": Neither Omnipotent Nor Unbeatable*, in *Orbis*, 54, 3, 2010, 443.
[20] S. Monaghan, *Countering Hybrid Warfare: So What for the Future Joint Force?*, in *Prism*, 8, 2, 2019, 87.
[21] *Ibid.*
[22] O. Fridman, *Russian Hybrid Warfare. Resurgence and Politicisation*, Oxford, Oxford University Press, 2022, 34.
[23] Secondo Fridman, «Le analisi di Hoffman sono ristrette al livello operativo, rendendo la guerra ibrida comprensiva abbastanza per incorporare le idee della guerra senza limiti, ma abbastanza semplice per essere usata dagli operatori. A differenza dei suoi predecessori, Hoffman non cerca di delineare e definire la natura della sua teoria, egli cerca anche di "spiegarne la rilevanza per l'attuale dibattito sulla postura delle forze", offrendo non solo un nuovo concetto basato sull'analisi di casi storici, ma anche una ricetta dettagliata per i necessari adattamenti alle nuove realtà» (O. Fridman, *op. cit.*, 34).

DPCE online
ISSN: 2037-6677

statali che non statali. Questi, infatti, potrebbero «spostare le loro unità convenzionali verso formazioni irregolari e adottare nuove tattiche, come hanno fatto i Fedayeen iracheni nel 2003»[24]. Hoffman, infine, identifica anche il prototipo di "guerra ibrida" che meglio aderisce alla sua concettualizzazione: la Seconda Guerra del Libano combattuta tra Israele e Hezbollah, quest'ultimo definito come il «rappresentante della crescente minaccia ibrida»[25].

Poco dopo, la teoria di Hoffman ha conosciuto notevole diffusione, specialmente nei circoli militari statunitensi, nei quali diversi autori hanno ripreso la sua concettualizzazione, arricchendola di nuove riflessioni[26], soprattutto in ragione dell'emersione di strumenti tecnologicamente sempre più avanzati»[27].

3. La "guerra ibrida" e la sua diffusione globale

A partire dal 2014, l'annessione della Crimea e le operazioni aggressive nell'Ucraina orientale da parte della Russia, hanno riacceso e "rinfiammato" il dibattito attorno al concetto di "guerra ibrida", tanto che una ricerca su *Google Scholar* dei termini "guerra ibrida" e "minacce ibride" ha prodotto circa 9.900 risultati, con la maggior parte delle pubblicazioni – circa 6.970 – prodotte dal 2014[28]. Nel Vertice NATO del Galles nel settembre 2014, la "guerra ibrida" viene associata con le azioni russe in Ucraina e, di conseguenza, il concetto in questione diventa «sinonimo di Russia piuttosto che di attori non statali»[29], tanto da essere inteso come «la minaccia più immediata per la sicurezza dell'Occidente»[30]. Questo ha portato studiosi ed analisti ad allontanarsi dal concetto originale di Hoffman, fondato sulla combinazione di forze ed elementi regolari e irregolari all'interno di un conflitto. Le azioni di Mosca, infatti, come sottolineato da Solmaz, includono anche elementi non cinetici[31].

[24] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, Potomac Institute for Policy Studies, 2007, 28.
[25] *Ivi*, 36.
[26] Si veda, a tal proposito, T. McCulloh, R. Johnson, *Hybrid Warfare*, in *JSOU Report* 13, 4, 2013.
[27] A. Deep, *Hybrid War: Old Concept, New Techniques*, in *Small Wars Journal*, 02-03-2015, (https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques).
[28] R. Babbage, *Stealing a March: Chinese Hybrid Warfare in the Indo-Pacific: Issues and Options for Allied Defense Planners*, vol. II, in *Center for Strategic and Budgetary Assessment*, 2019, 1.
[29] I. Käihkö, *The Evolution of Hybrid War: Implications for Strategy and the Military Profession*, in *Parameters* 51, 3, 2021, 116.
[30] *Ibid.*
[31] Secondo alcuni, «la Russia ha raggiunto i suoi obiettivi politici in Ucraina utilizzando un mix di strumenti non cinetici, tra cui attacchi informatici, propaganda, disinformazione, coercizione economica e pressione diplomatica, e metodi militari, come la conduzione di operazioni segrete e il potenziamento di guerrieri per procura. Inoltre, la Russia ha sistematicamente negato il proprio coinvolgimento in Ucraina. Pertanto, la cosiddetta "guerra ibrida" della Russia in Ucraina non consisteva solo in una combinazione di elementi regolari e irregolari o nella combinazione di strumenti militari e non militari, ma anche in azioni segrete e inganni. Le principali caratteristiche

Sulle risposte alle minacce ibride da parte della NATO e dell'Unione Europea ci si soffermerà più avanti[32], ciò che adesso è importante sottolineare è come le azioni russe in Crimea e in Ucraina abbiano di fatto riacceso l'interesse della NATO verso la "guerra ibrida", come evidenziato nella Dichiarazione del Vertice NATO in Galles del 2014[33].

Nonostante la presa di posizione in occasione del Vertice del Galles, la NATO, come sostenuto da Fridman, si era già occupata nel 2010 di ridefinire i concetti di "guerra ibrida" e "minaccia ibrida", elevando i due termini a livello di strategia. La NATO, infatti, sostenne che «Le minacce ibride sono quelle poste da avversari con la capacità di impiegare simultaneamente mezzi convenzionali e non convenzionali in modo adattivo nel perseguimento dei loro obiettivi [...] Le minacce ibride comprendono e operano contemporaneamente attraverso più sistemi/sottosistemi (tra cui quello economico/finanziario, legale, politico, sociale e militare/sicurezza) e pertanto risulteranno problematiche per la risposta della NATO, che inizialmente si concentrerà su una linea operativa militare/sicurezza. Le minacce ibride possono espandere e contrarre rapidamente queste linee operative per raggiungere i loro obiettivi»[34].

La nuova concettualizzazione della NATO, dunque, superava la dimensione militare-operativa del pensiero di Hoffman, diventando una sorta di apripista per le successive revisioni del concetto, le quali, come si vedrà, hanno poi ricompreso «l'intero spettro delle possibili minacce militari e non militari che mettono a repentaglio la sicurezza dello Stato e la stabilità interna ed esterna»[35]. Alla *NATO Allied Command Transformation* (ACT)[36], in collaborazione con lo *US Joint Forces Command Joint Irregular Warfare Centre* (USJFCJIWC) e con la *National Defense University* (NDU) degli Stati Uniti, venne affidato il compito di sviluppare un nuovo approccio nozionistico riguardante il pericolo ibrido. Il lavoro congiunto dei tre istituti

della campagna sovversiva della Russia in Ucraina sono state quindi la creazione di ambiguità e la possibilità di una negazione plausibile». (in T. Solmaz, *Hybrid Warfare: One Term, Many Meanings*, in *Small Wars Journal*, 2022, https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings).

[32] Cfr., *infra*, § 7.

[33] «Garantiremo che la NATO sia in grado di affrontare efficacemente le sfide specifiche poste dalle minacce di guerra ibrida, in cui viene impiegata un'ampia gamma di misure militari, paramilitari e civili, palesi e occulte, in un disegno altamente integrato. È essenziale che l'Alleanza possieda gli strumenti e le procedure necessarie per scoraggiare e rispondere efficacemente alle minacce di guerra ibrida e le capacità di rafforzare le forze nazionali. Ciò comprende anche il miglioramento delle comunicazioni strategiche, lo sviluppo di scenari di esercitazione alla luce delle minacce ibride e il rafforzamento del coordinamento tra la NATO e le altre organizzazioni, in linea con le decisioni prese in materia, al fine di migliorare la condivisione delle informazioni, le consultazioni politiche e il coordinamento tra il personale». (NATO, *Wales Summit Declaration*, https://www.nato.int/cps/en/natohq/official_texts_112964.htm).

[34] NATO, *Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threat*, 2010, 2-4.

[35] O. Fridman, *Russian Hybrid Warfare. Resurgence and Politicisation*, 105.

[36] La missione principale dell'*Allied Command Transformation* è quella di contribuire a preservare la pace, la sicurezza e l'integrità territoriale degli Stati membri dell'Alleanza guidando lo sviluppo bellico di strutture, forze, capacità e dottrine militari. Per ulteriori informazioni si faccia riferimento a: https://www.act.nato.int/who-we-are.

DPCE online
ISSN: 2037-6677

ha dato nuovo impulso alla minaccia ibrida, la quale si configurava come "termine ombrello" comprendente molteplici circostanze e azioni avverse come «terrorismo, migrazione, pirateria, corruzione, conflitto etnico»[37]. Tuttavia, la vera novità è la possibilità che la NATO si trovi a dover affrontare «l'uso adattivo e sistematico di tali mezzi, singolarmente e in combinazione, da parte di avversari che perseguono obiettivi politici a lungo termine, in contrapposizione al loro verificarsi più casuale, guidato da fattori casuali»[38].

Il termine ombrello "minaccia ibrida" ha ampliato ulteriormente la sua portata grazie alla definizione fornita dallo *US Joint Forces Command Joint Irregular Warfare Centre* (USJFCOM JIWC). Secondo quest'ultimo, infatti, alla base dell'origine delle minacce ibride ci sarebbero avversari multidimensionali che impiegano una «complessa miscela di mezzi che comprende l'orchestrazione della diplomazia, l'interazione politica, gli aiuti umanitari, le pressioni sociali, lo sviluppo economico, l'uso sapiente dei media e la forza militare»[39]. Un'ulteriore estensione concettuale del termine è avvenuta grazie al contributo di Bachmann e Gunneriusson, secondo cui, «le minacce ibride sono minacce multimodali, a bassa intensità, cinetiche e non cinetiche alla pace e alla sicurezza internazionale»[40]. I due autori, inoltre, illustrano anche gli esempi di minacce ibride, tra cui «gli scenari di conflitto asimmetrico, il terrorismo globale, la pirateria, la criminalità organizzata transnazionale, le sfide demografiche, la sicurezza delle risorse, la riduzione della globalizzazione, la proliferazione delle armi di distruzione di massa e la guerra cyber»[41].

Tuttavia, nonostante la forte intensità del dibattito, la NATO nel 2012 ha deciso di interrompere gli impegni strategici sulla "guerra ibrida", a causa «dell'assenza di volontà politica da parte dei membri della NATO di investire risorse nello sviluppo delle capacità necessarie per far fronte alle minacce ibride»[42].

La situazione muta drasticamente con l'annessione della Crimea e con le operazioni in Ucraina Orientale da parte della Federazione Russa. Tale stato di fatto avvalora ulteriormente la tesi già sostenuta circa la connessione tra le azioni russe e la "guerra ibrida". Anzi, l'aggettivo russo è finito per diventare un elemento permanente del concetto di "guerra ibrida", tanto che dal 2014 in poi la maggior parte della produzione scientifica occidentale ha fatto propria la locuzione di "guerra ibrida russa" o "*Russian Hybrid*

[37] M. Aaronson, S. Diessen, Y. De Kermabon, M.B. Long, M. Miklaucic, *NATO Countering the Hybrid Threat*, in *Prism*, 2, 4, 2011, 115, in O. Fridman, *Russian Hybrid Warfare. Resurgence and Politicisation*, 104-105.
[38] *Ibid.*
[39] Joint Irregular Warfare Center, *Irregular Adversaries and Hybrid Threats, an Assessment*, 2011, 24, in O. Fridman, *Russian Hybrid Warfare. Resurgence and Politicisation*, 105.
[40] S.D. Bachmann, H. Gunneriusson, *Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere*, 16 in *Geo. J. Int'l Aff.*, 2015, 198, in O. Fridman, *op. cit.*, 105.
[41] *Ibid.*
[42] O. Fridman, *The Danger of Russian Hybrid Warfare*, in *Cicero Foundation Great Debate Paper*, 17/05, 2017, 6.

Warfare"[43]. Tale cambio di paradigma si giustifica, come già accennato, in ragione della nuova concettualizzazione introdotta dalla NATO già a partire dal 2010. A questo si sommano gli eventi intervenuti tra l'inizio del 2014 e la fine del 2016 in Ucraina Orientale e in Crimea, che hanno colto di sorpresa il blocco occidentale e la NATO, i quali, data la complessa combinazione di azioni portata avanti dalla Federazione Russa – forze speciali negazioniste, milizie locali per procura, pressioni economiche, disinformazione e sfruttamento delle divisioni sociali per presentare il fatto compiuto all'Ucraina e all'Occidente – hanno descritto una simile strategia «etichettandola come guerra ibrida»[44]. I primi ad esplicitare questo collegamento – "guerra ibrida" e azioni russe in Ucraina – sono stati Anders Fogh Rasmussen[45] (ex segretario generale della NATO), Frank van Kappen[46] (ex consigliere della NATO per la sicurezza) e Heidi Reisinger[47] del *NATO Defense College*.

Tuttavia, nonostante la forte circolazione del lemma "guerra ibrida russa", il 2016 è stato l'anno in cui diversi autori hanno avanzato dubbi circa la pertinenza della nuova concettualizzazione al caso russo, proponendo una sua rivalutazione, che si sarebbe dovuta concentrare sia sulle motivazioni russe, sia sugli strumenti militari e non-militari. Secondo Renz e Smith, il concetto di "guerra ibrida", «non riflette adeguatamente il contenuto e la direzione della modernizzazione militare russa e sottovaluta le ambizioni russe e allo stesso tempo sovrastima le capacità russe; semplifica eccessivamente la politica internazionale/estera russa, che è più complessa di quanto l'etichetta lasci intendere; non ci dice nulla sugli obiettivi o sulle intenzioni della Russia e implica erroneamente che la politica estera russa sia guidata da una "grande strategia globale"»[48].

Per Adamsky, invece, è opportuno prestare la giusta attenzione alla corretta terminologia perché pretendere di «applicare il quadro concettuale occidentale di "*Hybrid Warfare*" per spiegare la strategia operativa russa,

[43] O. Fridman, *Russian Hybrid Warfare. Resurgence and Politicisation*, 101.
[44] S. Monaghan, *op. cit.*, 84.
[45] Nel corso di un'intervista, Rasmussen ha descritto le tattiche portate avanti dal Cremlino come guerra ibrida, definita come «una combinazione di azioni militari, operazioni segrete e un programma aggressivo di disinformazione». Per saperne di più, si faccia riferimento a M. Landler, M.R. Gordon, *NATO Chief Warns of Duplicity by Putin on Ukraine*, in *The New York Times*, 08-07-2014, https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html.
[46] Il 26 aprile 2014 Frank van Kappen ha affermato che «le azioni russe in Ucraina sono un esempio di guerra ibrida». Sulla stessa linea, cfr. O. Fridman, *Russian Hybrid Warfare. Resurgence and Politicisation*, 108.
[47] Secondo l'autore, «Il comportamento e le azioni recenti della Russia sono spesso definite "guerra ibrida". Si è trattato di un mix efficace e talvolta sorprendente di componenti militari e non militari, convenzionali e irregolari, e può includere tutti i tipi di strumenti come le operazioni informatiche e cibernetiche». Ulteriori dettagli in H. Reisinger, A. Golts, *Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*, in *Research Paper - Research Division - NATO Defense College*, Roma, 15, 2014.
[48] B. Renz, H. Smith, *After 'Hybrid Warfare', What Next? – Understanding and Responding to Contemporary Russia*, in *Publications of the Government´s analysis, assessment and research* activities 44/2016, Helsinki, 2016, 8-9.

DPCE online
ISSN: 2037-6677

senza esaminare i riferimenti russi a questo termine, isolandolo dal contesto ideativo russo e senza contrastarlo con ciò che i russi pensano di sé stessi e degli altri, può portare a percezioni errate»[49]. Anche secondo Kofman, il collegamento tra le azioni russe in Crimea e in Ucraina e il concetto di "guerra ibrida" è paragonabile ad una sorta di "moda intellettuale", in base alla quale, «la conversazione odierna sull'uso della "guerra ibrida" è diventata un discorso su qualcosa di più arcano, simile alla magia nera». Anzi, secondo tale autore, «le generalizzazioni sulla "*Russian hybrid warfare*" non solo non sono utili, ma stanno diventando un *cliché*»[50].

Con la nuova concettualizzazione politica della "guerra ibrida" in riferimento agli eventi in Crimea e nell'Ucraina Orientale, la dottrina si è effettivamente interrogata sull'utilità del termine nella comprensione delle azioni russe. Il lavoro più esaustivo è quello compiuto da Fridman, il quale ne ridefinisce il perimetro teorico mediante quattro interessanti considerazioni. In primo luogo, l'autore mette a confronto il concetto originale di "guerra ibrida" (quello coniato da Frank Hoffman) con quello di "guerra ibrida russa", sottolineando il carattere ambiguo di questo collegamento. Secondo Fridman esisterebbero due diverse declinazioni di "guerra ibrida": quella originale – che implica una combinazione di metodi militari e mezzi convenzionali e irregolari – e la cosiddetta "guerra ibrida russa" che include ogni possibile combinazione di attività ostili (militari e non). Il carattere inclusivo della "guerra ibrida russa" conduce al secondo punto messo in evidenza da Fridman, ossia che, quest'ultima ha conosciuto una forte circolazione poiché permette di «riunire qualsiasi azione ostile sotto lo stesso ombrello concettuale, creando la continuità di un messaggio politico certificato e permettendo ai diversi attori politici interni di serrare i ranghi contro una minaccia esterna»[51]. La terza considerazione dell'autore si basa sulla sottolineatura del «pericoloso uso improprio della parola guerra quando si descrive qualcosa che non comporta scontri armati»[52]. Infine, per Fridman, è pericoloso «estendere il fenomeno della guerra a qualsiasi possibile combinazione di confronto politico»[53], soprattutto per quel che concerne l'apparato militare. Quest'ultimo, infatti, potrebbe essere indotto a non ben delineare i propri interventi, dato che le azioni e le contro-azioni richieste da una simile minaccia non rientrano nel novero delle responsabilità militari. Dunque, conclude Fridman, «sebbene le azioni russe siano effettivamente ibride (nel senso più ampio e ambiguo del termine), difficilmente rientrano nella definizione di "guerra" e qualsiasi tentativo di definirle tali è una politicizzazione molto pericolosa e irresponsabile di un fenomeno serio e altamente indesiderabile»[54].

Alla luce della ri-concettualizzazione della "guerra" ibrida ad opera della NATO, Giannopoulos, Smith e Theocaridou hanno messo a punto una tassonomia esaustiva delle possibili minacce ibride, basandosi su quattro

[49] O. Fridman, *The Danger of 'Russian Hybrid Warfare'*, 9.
[50] M. Kofman, *Russian Hybrid Warfare and Other Dark Arts*, in *War on the Rocks*, 11-03-2016, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.
[51] O. Fridman, *op. cit.*, 14.
[52] O. Fridman, The Danger of 'Russian Hybrid Warfare', 14.
[53] *Ibid.*
[54] O. Fridman, *op. cit.*, 14-15.

pilastri principali: gli attori e i loro obiettivi strategici, gli strumenti utilizzati, i domini presi di mira e le fasi[55]. Tra gli strumenti è possibile citare l'attacco alle infrastrutture critiche, lo spionaggio industriale e *cyber*, compromissione dell'economia nazionale, operazioni *cyber* o elettroniche spaziali, violazione dello spazio aereo e del territorio, esercitazioni militari, finanziamento di gruppi culturali o *think tank*, promozione di disordini sociali e di corruzione, sfruttamento di punti ciechi, ambiguità o lacune legali, infiltrazioni, boicottaggi, controllo dei media e interferenze, campagne di disinformazione e propaganda, coercizione dei politici o del governo. È chiaro che tali attività perseguono l'obiettivo di scardinare e scalfire i principi e i valori fondamentali di uno Stato bersaglio. Una simile situazione, oltre a rendere sempre più sfumati i tradizionali confini tra guerra e pace, complica sia l'attribuzione giuridica, sia la risposta fattiva delle "vittime".

A tal proposito, di seguito si vedrà in dettaglio come la tecnologia digitale influisca sullo sviluppo e sulla condotta della "guerra ibrida".

4. L'attacco cibernetico nella "guerra ibrida"

Gli attacchi cibernetici sono uno degli strumenti più utilizzati dagli attori ibridi per sfruttare le vulnerabilità avversarie e raggiungere gli obiettivi prefissati. Si tratta di azioni compiute all'interno di un nuovo dominio: il cyberspazio, che rappresenta, a tutti gli effetti, «la quinta dimensione della conflittualità»[56] al pari di terra, mare, aria e spazio.

Come già analizzato in precedenza, attacchi condotti in questa area fanno parte di quel variegato set di minacce che gli Stati e le organizzazioni internazionali devono affrontare. Un conflitto con armi cibernetiche – più propriamente denominato *cyberwarfare* o guerra cibernetica – indica l'utilizzo delle *Information Technologies* (IT) per «condurre operazioni militari, cioè la proliferazione delle tecniche belliche nello spazio cibernetico»[57].

Gli attori ibridi ricorrono agli attacchi in parola per colpire le vulnerabilità avversarie. Tra gli obiettivi principali ci sono le infrastrutture critiche dello Stato bersaglio, quali, ad esempio, le infrastrutture vitali, le risorse idriche, il sistema di trasporti, i servizi sanitari, gli apparati istituzionali e finanziari e così via. Distruggere, rendere malfunzionanti o temporaneamente non disponibili le infrastrutture critiche di uno Stato può generare gravi ripercussioni non soltanto a livello economico, ma anche a livello politico e sociale, dato che il loro corretto funzionamento è di vitale importanza per la stabilità dello Stato e per l'accesso ai servizi essenziali da parte della popolazione. Oltre alla *cyberwarfare*, sono presenti altre cinque minacce cibernetiche: *cyber crime*, *hacktivism*, *cyber espionage*, *cyber terrorism* e *insider threat*[58].

---

[55] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A conceptual model*, European Commission, Ispra, 2020.

[56] L. Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Il Mulino*, 2018, 62.

[57] G. Giacomello, G. Badialetti, *Manuale di studi strategici. Da Sun Tzu alle "guerre ibride"*, Milano, 2016, 185.

[58] Il *cyber crime* implica tutte quelle azioni malevoli compiute sfruttando gli strumenti informatici (furto di dati e informazioni riservate, frodi, vendita di materiale illegale) e

DPCE online
ISSN: 2037-6677

Una menzione a parte merita la c.d. *lawfare*, che indica «la strategia che prevede l'uso – o l'abuso – del diritto come sostituto dei tradizionali mezzi militari per raggiungere un obiettivo operativo»[59]. La *lawfare* si inserisce nella sfera delle operazioni di influenza, mirando a stravolgere e/o modificare i paradigmi legislativi dello *jus ad bellum*, *jus in bello* e diritto internazionale, «reinterpretando le norme giuridiche in modo fuorviante»[60] o diffondendo disinformazione. Nonostante una tradizionale connotazione negativa, Munoz Mosquera e Dov Bachmann ne sottolineano anche una valenza positiva, rappresentata dalla capacità di uno Stato bersaglio di usare il diritto per difendere e tutelare i propri interessi e raffigurata dall'eterna lotta tra il bene e il male, come quella tra Zeus e Ade. Per i due autori, quindi, l'uso del diritto come arma non cinetica ha una doppia sfaccettatura: se utilizzata per distorcere i principi guida e i fondamenti dello stato di diritto si qualificherebbe come "hadesiana", viceversa, sarebbe "zeusiana" se usata per riaffermare e rafforzare i principi della legge[61].

Definite le minacce, è necessario sottolineare le *cyber weapons* che possono essere utilizzate dagli attori malevoli nel cyberspazio. Tra le più diffuse troviamo i *malware* – qualunque tipo di *software* «creato per disturbare il normale funzionamento di un dispositivo IT o altresì infettare, rubare o distruggere le informazioni in esso contenute»[62] – i *worm* – tipi di *malware* che infettano svariati dispositivi – il *ransomware* – tipo di *malware* in grado di bloccare l'accesso ai contenuti dei dispositivi digitali, richiedendo successivamente un riscatto per rilasciarli – e l'attacco DDoS (*Distributed Denial of Service*) – una sorta di «bombardamento molto intenso e concentrato»[63] di traffico dati verso un obiettivo fino a quando lo stesso non risulterà inaccessibile agli utenti.

Con lo sviluppo tecnologico e la conseguente emersione del cyberspazio, anche la disinformazione ha visto crescere il suo enorme

indirizzate, per lo più, verso utenti e aziende. L'hacktivismo consiste nell'utilizzare i sistemi digitali per lanciare campagne online in linea con le cause – sociali, politiche, religiose ed economiche – sostenute dal gruppo di appartenenza degli *hacktivisti*. Lo spionaggio cibernetico è il tentativo di acquisizione indebita di materiali, informazioni e dati senza l'autorizzazione del proprietario degli stessi. Il terrorismo cibernetico, invece, comprende tutte quelle attività terroristiche compiute nel cyberspazio con l'intento di destabilizzare uno Stato bersaglio e i cittadini, incutendo paura e panico. Infine, la minaccia interna si riferisce a un attacco subìto da un'organizzazione che proviene dal suo interno (in R. Marchetti, R. Mulas, *Cyber Security. Hacker, terroristi, spie e le nuove minacce del web*, Roma, 2017, 55).

[59] C. Dunlap, *Lawfare Today: A Perspective*, in *Yale Journal of International Affairs*, 2008, 146.

[60] D. Moeckli, S. Shah, S. Sivakumaran, *International Human Rights Law*, Oxford University Press, 2022; J. Cardona, S. Sanz-Caballero, A. Arrufat, *La protección internacional de la persona*, Tirant, 2022 in S. Sanz-Caballero, *The concepts and laws applicable to hybrid threats, with a special focus on Europe*, in *Humanit Soc Sci Commun*, 10, 360, 2023, 4.

[61] A.B. Munoz Mosquera, S. Dov Bachmann, *Lawfare in Hybrid Wars: The 21st Century Warfare*, in *Journal of International Humanitarian Legal Studies*, 7, 2016, 73.

[62] *Ivi*, 76.

[63] A. Giannulli, A. Curioni, *Cyber War. La Guerra Prossima Ventura*, Milano, 2019, 54.

potenziale all'interno dei nuovi conflitti, rientrando a pieno titolo tra gli strumenti più utilizzati dagli attori malevoli nell'ipotesi di attacco ibrido[64].

L'incremento del potenziale della disinformazione è in parte spiegato dall'ascesa di *Internet* e dei *Social Media*, inizialmente accolti con lauto entusiasmo, in quanto si pensava che avrebbero «democratizzato le voci degli individui e avrebbero rafforzato le nostre culture democratiche»[65], influenzando positivamente anche contesti nazionali non-democratici. Tuttavia, il quadro che è emerso ha poi mostrato una realtà diversa dalle aspettative iniziali. I *Social Media* e i motori di ricerca *online*, potenziati da algoritmi e tracce virtuali lasciate dagli utenti all'interno delle cronologie (le c.d. *digital footprints*), hanno minato il dibattito pubblico e la libertà di pensiero degli individui. Questi ultimi, travolti da *filter bubbles*, camere d'eco e contenuti selezionati – in base alle preferenze espresse – abitano un mondo virtuale informativo chiuso, in cui risulta difficile avere accesso a fonti di informazioni alternative, cioè quelle che contrastano le loro convinzioni e opinioni. Tale scenario rappresenta il terreno ideale per l'attecchimento di campagne di disinformazione *online*[66].

Sono molteplici gli obiettivi che spingono gli opponenti ibridi a lanciare campagne di disinformazione. Uno di questi è la volontà di minare la credibilità delle istituzioni governative di un Paese bersaglio mediante attività di influenza che sfruttano le vulnerabilità interne. Gli attori ostili possono, dunque, servirsi della facile accessibilità delle piattaforme digitali per lanciare attacchi virtuali informativi che abbiano come fine quello di sovvertire l'ordine democratico, sfruttando argomenti controversi agli occhi dell'opinione pubblica come l'immigrazione, i diritti delle minoranze, la sicurezza, la difesa, la corruzione, le politiche sociali ed estere. Seminando confusione e odio, gli attori ibridi mirano anche a spingere alcuni strati della società a porre in essere azioni in grado di sovvertire l'assetto istituzionale. Influenzare la società civile in questo modo potrebbe generare due tipi di

[64] Per Josep Borrell, Alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza, «le campagne di disinformazione intenzionali e coordinate dovrebbero essere trattate come una minaccia ibrida alla sicurezza europea e globale» in J. Borrell, *Disinformation around the coronavirus pandemic: Opening statement by the HR/VP Josep Borrell at the European Parliament*, 30-04-2020, https://www.eeas.europa.eu/eeas/disinformation-around-coronavirus-pandemic-opening-statement-hrvp-josep-borrell-european-parliament_en.

[65] S. Giusti, E. Piras, *Democracy and Fake News. Information Manipulation and Post-Truth Politics*, New York, 2021, 68.

[66] La Commissione europea, nella comunicazione "Contrastare la disinformazione *online*: un approccio europeo", definisce la disinformazione come «un'informazione falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico». Quest'ultimo include «minacce ai processi politici democratici e di elaborazione delle politiche e a beni pubblici quali la tutela della salute dei cittadini, dell'ambiente e della sicurezza dell'UE». La disinformazione, si legge nella comunicazione, non include «gli errori di segnalazione, la satira e la parodia, o notizie e commenti chiaramente identificabili come di parte» in Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Contrastare la disinformazione online: un approccio europeo*, 26-04-2018, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0236&from=IT, 4.

DPCE online
ISSN: 2037-6677

cambiamenti: contestuale e comportamentale[67]. Il cambiamento contestuale prevede un rovesciamento del governo in carica, che potrebbe portare alla stipulazione di nuove alleanze internazionali o alla revisione di accordi, trattati e leggi. Il cambiamento comportamentale, invece, non ha come conseguenza il rovesciamento del governo, ma il suo cambio di rotta dal punto di vista politico interno e internazionale.

5. "Guerra ibrida" e strumenti di contrasto: le risposte di NATO e Unione Europea

La crisi in Ucraina del 2014, oltre ad aver aumentato la popolarità del lemma "guerra ibrida" all'interno del dibattito politico-istituzionale, ha accelerato il processo di risposta della NATO. In occasione del Vertice del Galles, al di là della forte presa di posizione nei confronti delle azioni russe sul suolo ucraino[68], gli Alleati hanno deciso di istituire il *Readiness Action Plan*, il quale prevedeva un pacchetto completo di misure necessarie per rispondere ai cambiamenti nell'ambiente della sicurezza internazionale e un rafforzamento della capacità di gestione delle crisi e della difesa collettiva della NATO.

Un anno più tardi, la NATO si è dotata di una strategia per contrastare le minacce ibride: la *Strategy on NATO's Role in Countering Hybrid Warfare*, la quale include le risposte della NATO al pericolo ibrido, raggruppate in tre categorie: preparazione, dissuasione e difesa[69].

Nella fase di preparazione, la NATO raccoglie, condivide e valuta continuamente informazioni per individuare e attribuire qualsiasi attività ibrida in corso. A tal proposito, la *Joint Intelligence and Security Division*, creata nel 2016, migliora la comprensione e l'analisi delle minacce ibride da parte dell'Alleanza. Inoltre, in questa fase, la NATO funge anche da centro di competenza, fornendo supporto agli Alleati in settori come la protezione delle infrastrutture critiche, le comunicazioni strategiche, la protezione dei civili e la difesa informatica. Risultano fondamentali, in questa fase, anche l'addestramento, le esercitazioni e la formazione. Nella fase di dissuasione, lo sforzo della NATO e dei suoi Alleati si concentra sul lato diplomatico, ovvero far comprendere agli avversari il *mismatch* tra le conseguenze (probabilmente sotto forma di sanzioni) delle loro azioni e i potenziali vantaggi.

Nella fase di difesa, infine, l'obiettivo della NATO è quello di contenere e limitare la libertà d'azione dell'avversario e sconfiggere la minaccia, da sola o come parte di una risposta internazionale. La NATO assisterà anche i

[67] T.E. Niessen, *Social media's role in 'Hybrid Strategies'*, in *NATO Strategic Communications Centre of Excellence*, Riga, 2016, 1.

[68] I capi di Stato e di Governo dei paesi membri dell'Alleanza si espressero così riguardo le azioni russe in Ucraina: «Condanniamo fermamente l'*escalation* e l'intervento militare illegale della Russia in Ucraina e chiediamo che la Russia fermi e ritiri le sue forze dall'Ucraina e lungo il confine ucraino». Per ulteriori dettagli si faccia riferimento al seguente *link*: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[69] NATO, *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=NATO's%20strategy%3A%20prepare%2C%20deter%2C,whatever%20form%20they%20may%20take.

singoli alleati e contribuirà a mitigare gli effetti di un attacco alle popolazioni civili o alle infrastrutture critiche.

Nel Vertice di Varsavia del 2016, poi, la NATO e i suoi alleati hanno istituito una nuova *Joint Intelligence and Security Division* (JISD), la quale comprende un'unità che si occupa del monitoraggio e dell'analisi delle minacce ibride[70]. Rappresenta, inoltre, un ponte tra gli Stati e la NATO dato che i primi condividono i propri sviluppi e le minacce interne rilevate.

Sempre in occasione del Vertice di Varsavia, un passaggio chiave riguarda la risposta degli Alleati in caso di attacchi ibridi, che potrebbe portare il Consiglio a invocare l'applicazione dell'articolo 5 del Trattato di Washington: «[...] La più grande responsabilità dell'Alleanza è proteggere e difendere il nostro territorio e le nostre popolazioni dagli attacchi, come stabilito dall'articolo 5 del Trattato di Washington»[71]. Queste affermazioni rappresentano il punto di partenza per analizzare la problematica inerente al contrasto, dal punto di vista normativo, delle minacce ibride. Le dichiarazioni al Vertice di Varsavia, circa il possibile ricorso da parte della NATO all'articolo 5, mostra evidenti difficoltà e contraddizioni. In primo luogo, occorre evidenziare come l'attivazione di tale articolo sia subordinata al verificarsi di un attacco armato. La medesima condizione inoperante coinvolge anche l'articolo 42, par. 7, del Trattato UE, contenente una clausola di assistenza reciproca nel caso in cui uno Stato membro subisca un'aggressione armata all'interno del suo territorio. Considerando che la caratteristica principale di una campagna ibrida è quella di aggirare i confini legali, non oltrepassando determinate soglie che possano far scattare una risposta basata sull'uso della forza, va da sé che un attacco ibrido non può essere paragonato, per intensità ed efficacia, ad un attacco armato. Il rischio è che anche se uno Stato ritenga che siano soddisfatte le precondizioni dell'autodifesa, «prima o poi dovrà giustificare la sua decisione di esercitare l'autodifesa davanti alla comunità internazionale»[72]. Qualora non riuscisse nel suo intento, lo Stato si troverebbe dinnanzi ad un'accusa molto pesante: quella di aver commesso un atto di aggressione. Di conseguenza, la NATO si troverebbe costretta a fare riferimento all'articolo 4 del Trattato Nord Atlantico, il quale prevede una reazione non militare della parte che considera minacciata la propria integrità territoriale, l'indipendenza politica o la sicurezza. Allo stato attuale, però, la «struttura della NATO e la sua ragion d'essere sono fondamentalmente orientate a garantire la difesa collettiva nei conflitti interstatali, non a contrastare le minacce ibride attraverso l'articolo 4»[73]. Il fatto che gli avversari ibridi evitino l'uso palese della forza e conducano operazioni all'interno della zona grigia, sfruttando il vuoto legislativo, complica anche l'appello allo *jus ad bellum* e allo *jus in bello*. Fermo restando l'abolizione dell'uso della forza, come stabilito dall'art. 2, par. 4 della Carta delle Nazioni Unite, lo *jus ad bellum* disciplina l'entrata in

[70] M. Rühle, C. Roberts, *Enlarging NATO's toolbox to counter hybrid threats*, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.
[71] NATO, *Warsaw Summit Communiqué*. Per ulteriori dettagli si faccia riferimento al seguente link: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[72] R. Värk, *Legal Complexities in the Service of Hybrid Warfare*, in *Kyiv-Mohyla Law and Politics Journal*, 6, 2020, 36.
[73] S. Sanz-Caballero, *op. cit.*, 5.

DPCE online
ISSN: 2037-6677

guerra dei belligeranti, che può avvenire solo in presenza di due criteri eccezionali: il diritto all'autodifesa e l'autorizzazione del Consiglio di Sicurezza delle Nazioni Unite. Tuttavia, come già accennato, se gli attacchi ibridi non vengono considerati al pari di un attacco armato per via dell'opacità di simili situazioni si corre il serio rischio di vedere inapplicabili lo *jus ad bellum* e lo *jus in bello*. Dunque, a meno che i mezzi e i metodi della "guerra ibrida" non siano combinati con i mezzi e i metodi della guerra cinetica, è improbabile che la sola "guerra ibrida" non cinetica possa essere considerata al pari di un conflitto armato[74]. Oltre all'utilizzo di operazioni segrete e condotte principalmente nella zona grigia, gli avversari ibridi conoscono approfonditamente le soglie d'intensità che potrebbero far scattare una reazione armata e, quindi, potrebbero raggiungere i loro obiettivi strategici senza l'uso della forza. A quanto già detto va a sommarsi un'altra prerogativa delle "ostilità ibride moderne": la questione dell'attribuzione della responsabilità di un'azione malevola. Molto spesso gli Stati belligeranti o non agiscono in prima persona, servendosi di ribelli, insorti, mercenari o *proxy* (basti pensare agli "omini verdi" e alle loro azioni in Crimea con addosso una divisa militare sprovvista di simboli riconducibili alla Federazione Russa), oppure scelgono di negare strenuamente un loro coinvolgimento con tali attività, rendendo ancora più problematica una risposta in punto di diritto. Nonostante lo scenario appena delineato, il diritto in generale resta ancora un'opzione valida da tenere in considerazione. nonostante le minacce ibride non siano configurabili come azioni militari, gli Stati possono sempre avvalersi della «propria legislazione nazionale, di solito applicando il Codice penale nazionale, sebbene a volte si ricorra anche alla legislazione civile»[75]. Rientrano in questa sfera, ad esempio, le operazioni cibernetiche che possono comportare lo spionaggio o un attacco alle infrastrutture critiche del Paese bersaglio.

Tuttavia, urge sottolineare un aspetto dominante nelle caratteristiche delle minacce ibride. La "guerra ibrida", infatti, sempre più spesso si svolge al di sotto della soglia della guerra o della violenza diretta e questo, oltre ad offuscare i confini tra guerra e pace, complica e non poco i piani di risposta della NATO e dei suoi Alleati, costretti a propendere per risposte alternative quali le sanzioni o l'espulsione dei diplomatici[76].

Se la NATO ha alzato l'attenzione nei confronti delle minacce ibride in seguito alle azioni russe in Crimea e nell'Ucraina Orientale, l'Unione Europea ha reso prioritaria la lotta al contrasto ibrido nel 2016, con l'istituzione della *Hybrid Fusion Cell* all'interno dell'*Intelligence and Situation Center* del Servizio europeo di azione esterna. L'obiettivo dell'unità è quello di migliorare la consapevolezza della situazione, facilitando lo scambio di informazioni tra gli Stati membri e diventando l'unico punto di riferimento per l'analisi degli aspetti esterni delle minacce ibride.

[74] R. Värk, *op. cit.*, 39.
[75] *Ibid.*
[76] A. Hagelstam, *Cooperating to counter hybrid threats*, https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html.

6. "Guerra ibrida", attacco cibernetico e disinformazione

Come già sottolineato, le campagne di disinformazione sono uno degli strumenti a disposizione degli attori ibridi per sfruttare le vulnerabilità dello Stato bersaglio e minare le sue istituzioni governative. La NATO, su questo fronte, ha deciso di intervenire con varie iniziative. Oltre ad avere un rapporto costante e diretto con i media – ai quali chiede di correggere eventuali notizie non vere – l'organismo internazionale, all'interno del proprio sito web, ha una sezione "*Setting the record straight*"[77], nella quale si occupa di smascherare le campagne di disinformazione lanciate dalla Russia e i falsi miti che si sono accumulati negli anni e che hanno avuto come protagonista proprio la NATO. Dal canto suo, invece, l'Unione Europea ha iniziato a fronteggiare la disinformazione nel 2014, a seguito delle azioni aggressive russe in Crimea e in Ucraina Orientale. In quella circostanza, il Consiglio europeo sottolineò l'esigenza di «contrastare le campagne di disinformazione in corso da parte della Russia»[78] e questo è coinciso con l'istituzione della task force *East StratCom*, impegnata nella realizzazione di una comunicazione mirata alla promozione delle attività dell'Unione Europea sul fronte orientale e non solo. L'*East StratCom*, inoltre, ha sviluppato una piattaforma multilingue, la *EUvsDisinfo*, al fine di arginare, mediante una pubblica smentita, le campagne disinformative lanciate dal Cremlino contro l'Unione Europea e i suoi Stati membri. Oltre al recente Digital Services Act, che verrà approfondito subito dopo, si evidenzia il terzo pacchetto di sanzioni indirizzate alla Federazione Russa dopo la nuova invasione dell'Ucraina. In virtù del Regolamento (UE) 2022/350 del Consiglio, del 1° marzo 2022, che modifica il regolamento (UE) 833/2014 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, il Consiglio europeo ha bloccato la diffusione, sul suolo europeo, dell'agenzia di informazione *Sputnik* e del canale televisivo *Russia Today (RT English*, *RT UK*, *RT Germany*, *RT France* e *RT Spanish)*. I due organi di informazione sono stati accusati di promuovere e sostenere le azioni del Cremlino in Ucraina e di alimentare la destabilizzazione nei confronti dell'Unione Europea e degli Stati membri, come sostenuto da Joseph Borrell, «La manipolazione delle informazioni e la disinformazione sistematiche sono utilizzate dal Cremlino come strumento operativo nella sua aggressione contro l'Ucraina. Rappresentano inoltre una minaccia consistente e diretta all'ordine pubblico e alla sicurezza dell'Unione. Oggi stiamo compiendo un passo importante contro le operazioni di manipolazione di Putin, chiudendo i rubinetti ai media russi controllati dallo Stato nell'UE. Abbiamo già imposto sanzioni alla dirigenza di RT, compreso il caporedattore Simonyan, ed è logico prendere di mira anche le attività che tali organizzazioni svolgono all'interno della nostra Unione»[79]. A questa misura è seguita quella del 4 giugno 2022, in cui si è

[77] La sezione "*Setting the record straight*" è consultabile al seguente link: https://www.nato.int/cps/en/natohq/115204.htm?#myths.

[78] Conclusioni del Consiglio europeo, 19/20-03-2015, 6, https://www.consilium.europa.eu/media/21876/st00011it15.pdf

[79] Consiglio dell'UE, *L'UE impone sanzioni agli organi di informazione pubblici RT/Russia Today e Sputnik che svolgono attività di radiodiffusione nell'UE*, (https://www.consilium.europa.eu/it/press/press-releases/2022/03/02/eu-imposes-

DPCE online
ISSN: 2037-6677

stabilita la sospensione delle emittenti *Rossiya RTR*, *RTR Planeta*, *Rossiya 24*, *Russia 24* e *TV Centre International*. Dunque, se almeno inizialmente l'UE ha tentato di colpire la Russia con sanzioni di tipo economico-finanziarie, adesso il tiro è rivolto alle sue capacità manipolatorie dei media e di distorsione dei fatti[80]. La reazione del Cremlino, tuttavia, non si è fatta attendere. Mosca, dopo aver ricevuto il terzo pacchetto di sanzioni, ha chiuso la sede russa dell'emittente tedesca *Deutsche Welle* e ha annunciato due nuove leggi che mirano a restringere ulteriormente la libertà di stampa[81].

Nel tentativo di arginare il fenomeno della disinformazione, le difficoltà maggiori si incontrano nel garantire la libertà di espressione, di informazione e l'attendibilità delle notizie e dei contenuti presenti *online*. In poche parole, la disinformazione e le *fake news* risultano essere concetti sfumati, non perfettamente codificati a livello legislativo e inseriti nella zona grigia tra libertà di espressione e manifestazione del pensiero. Il bilanciamento tra lotta alla disinformazione e rispetto dei diritti fondamentali coinvolge il già menzionato *Digital Services Act* (DSA), che entrerà in vigore il 17 febbraio 2024. Dopo il *laissez-faire* che ha contraddistinto la direttiva *e-Commerce*, l'Unione Europea ha orientato la sua attenzione dalla autoregolamentazione alla co-regolamentazione delle piattaforme online, investite di responsabilità maggiori nella moderazione dei contenuti pubblicati dai propri utenti. Gli iniziali interventi del legislatore europeo, fondati sulla c.d. *soft law*, hanno portato all'adozione del primo *Code of Conduct on countering illegal hate speech online*[82]. La regolamentazione delle piattaforme attraverso strumenti di soft law ha assunto nuovi contorni e sfaccettature due anni più tardi, nel 2018, quando i più importanti intermediari di servizi digitali hanno sottoscritto l'*EU Code of Practice on Disinformation*[83]. Tuttavia, nel frattempo, l'esigenza di limitare e circoscrivere il perimetro di azione e di potere delle *big tech companies* si è fatta sempre più intensa ed insistente ed è sfociata nell'adozione di due regolamenti, giuridicamente vincolanti, appartenenti alla strategia di regolamentazione digitale dell'UE, "*Shaping Europe's Digital Future*": il *Digital Markets Act* (DMA) e il già citato *Digital Services Act* (DSA). Alla base

sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/).

[80] S. Lattanzi, *La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino*, in *MediaLaws*, 3, 2022, 160.

[81] *Ivi*, 177.

[82] Il primo *Code of Conduct on countering illegal hate speech online* è stato adottato il 30 maggio 2016 dalla Commissione europea e ad esso hanno aderito le più importanti *IT companies* come *Facebook*, *Microsoft*, *Twitter*, *YouTube* e, successivamente, *Google*. All'origine del Codice c'era la volontà di dotare i *social media* del potere di rimuovere i discorsi d'odio diffusi online dai propri utenti. Per una consultazione più approfondita, si veda: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

[83] Con l'*EU Code of Practice on Disinformation*, l'Unione Europea ha incaricato i principali intermediari digitali di fronteggiare la disinformazione mediante l'eliminazione di contenuti e informazioni ingannevoli e/o fuorvianti. Il Codice, inoltre, introduceva per la prima volta la figura dei *fact-checkers*, il cui compito è quello di verificare le informazioni e i contenuti condivisi sui *social media*. Per consultare il Codice, si veda: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

dei due provvedimenti c'è la volontà, da parte delle istituzioni europee, di creare uno ecosistema digitale più sicuro – in cui siano tutelati i diritti fondamentali degli utenti online – e di creare condizioni di parità per promuovere l'innovazione, la crescita e la competitività, sia nel mercato unico europeo che a livello globale. Il DSA, per raggiungere gli obiettivi prefissati, assegna un grado di responsabilità più stringente per le piattaforme e i motori di ricerca e di creare una netta correlazione tra ciò che è vietato offline e ciò che è vietato online in modo da evitare che «la Rete rappresenti un "porto franco" per la circolazione di qualsivoglia contenuto illegale»[84]. Il cambio di paradigma, alimentato da un approccio più duro rispetto ai precedenti interventi da parte del legislatore europeo, mira a ridimensionare il crescente potere delle piattaforme tecnologiche, come sintetizzato dalle parole di Thierry Breton, commissario europeo per il mercato interno e i servizi: «Con il DSA, il tempo in cui le grandi piattaforme online si comportavano come se fossero "troppo grandi per preoccuparsi" sta per finire»[85]. Tutti gli intermediari di servizi digitali saranno sottoposti a regole più severe al fine di controllare e/o rimuovere eventuali contenuti illegali circolanti al loro interno e a disinnescare le campagne di disinformazione, che destabilizzano il dibattito civico, l'opinione pubblica e i processi elettorali. Il Digital Services Act, che entrerà ufficialmente in vigore il 17 febbraio 2024, introduce una serie di nuove regole – che riguardano il modo in cui gli intermediari digitali partecipano alla distribuzione dei contenuti – in sezioni particolari, tra cui: termini e condizioni, maggiore trasparenza, moderazione dei contenuti con annesse motivazioni in caso di rimozione, gestione dei reclami e risoluzione extragiudiziale delle controversie. Come già accennato, nel DSA sono presenti obblighi ulteriori nei confronti delle piattaforme (*Meta*, *Amazon*, *TikTok*, *X*, *Apple*, *YouTube*, *Zalando*, ecc.) e dei motori di ricerca *online* di grandi dimensioni (*Google*, *Bing*) – cioè quelli che hanno un numero medio mensile di utenti pari o superiore a 45 milioni[86]. In particolare, i seguenti intermediari sono chiamati a valutare gli eventuali rischi sistemici connessi ai propri servizi e sistemi[87] come ad esempio: (i) la diffusione di contenuti illegali, (ii) gli eventuali effetti negativi per l'esercizio dei diritti fondamentali, (iii) gli eventuali effetti negativi sul dibattito civico e sui processi elettorali (nonché sulla sicurezza pubblica), (iv) qualsiasi effetto negativo in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona. La mitigazione dei rischi sistemici[88] può avvenire mediante l'adozione di misure specifiche, tra cui: l'adeguamento della progettazione e del funzionamento dei propri servizi, delle condizioni generali, delle procedure di moderazione dei contenuti e dei sistemi algoritmici.

[84] G. Morgese, *Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE*, in *Federalismi.it*, 1, 2022, 82.
[85] Commissione Europea, *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment*, (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545).
[86] DSA, art. 33, par. 1.
[87] DSA, art. 34, par. 1, comma a-d.
[88] DSA, art. 35.

DPCE online
ISSN: 2037-6677

Un altro aspetto sul quale le "*Very Large Online Platform*" sono obbligate ad intervenire riguarda, ai sensi dell'art. 36, il meccanismo di risposta alle crisi (minaccia per la sicurezza o la salute pubblica, calamità naturali o terrorismo). Qualora dovesse verificarsi una delle situazioni citate, la Commissione – come si legge nel considerando 91 del DSA – «dovrebbe poter chiedere ai prestatori di piattaforme online di dimensioni molto grandi e ai prestatori di motori di ricerca online di dimensioni molto grandi, su raccomandazione del comitato europeo per i servizi digitali, di avviare con urgenza una risposta alle crisi». Le misure applicabili possono includere – continua il considerando 91 – «l'adeguamento dei processi di moderazione dei contenuti e l'aumento delle risorse destinate alla moderazione dei contenuti, l'adeguamento delle condizioni generali, i sistemi algoritmici e i sistemi pubblicitari pertinenti, l'ulteriore intensificazione della cooperazione con i segnalatori attendibili, l'adozione di misure di sensibilizzazione, la promozione di informazioni affidabili e l'adeguamento della progettazione delle loro interfacce online». Da quanto espresso dall'articolo 36, tuttavia, emergono una serie di interrogativi: eventuali nuove emergenze potrebbero coincidere con la limitazione della libertà di informazione? Inoltre, tra le misure che le piattaforme sono obbligate ad attuare si fa riferimento alla promozione di informazioni affidabili: cosa si intende per informazioni affidabili? E chi stabilisce quale tipo di contenuto rientra nella sfera delle informazioni affidabili?

Nonostante rappresenti un valido tentativo di arginare la disinformazione e di garantire un ambiente digitale più sicuro, il *Digital Services Act* non sembrerebbe aver trovato un consenso unanime. La moderazione dei contenuti, presente all'art. 15, suscita più di una perplessità circa la sua capacità di contrastare la disinformazione, di ridurre il potere delle *big tech companies* e di assicurare il rispetto della libertà di espressione e del diritto di informazione. Secondo Morgese, allo stato attuale delle cose, le piattaforme digitali conserverebbero il «potere assoluto sul decidere, in base alle loro condizioni di servizio, cosa è disinformazione e cosa non lo è. Ne deriva [...] la possibilità che, all'esito di attività di moderazione non regolamentate, vengano rimossi contenuti non disinformativi (e cancellati specifici account) oppure, al contrario, che non si proceda alla rimozione di quelli chiaramente ingannevoli, spesso in base all'applicazione di algoritmi automatizzati senza successiva verifica umana [...]»[89]. Una posizione condivisa anche dal Garante per la *privacy* italiano: «il Regolamento sembrerebbe intenzionato a riconoscere – come, peraltro ormai avviene diffusamente – ai gestori delle piattaforme il diritto-dovere di decidere in autonomia e sulla base semplicemente delle proprie condizioni generali quale contenuto lasciare online e quale rimuovere e quale utente lasciar libero di pubblicare e quali condannare all'ostracismo digitale»[90].

Il *Digital Services Act* rappresenta il punto di approdo nel processo di regolamentazione delle piattaforme digitali, inaugurato – come già accennato – sotto forma di autoregolamentazione fino ad arrivare all'attuale

[89] G. Morgese, *op. cit.*, 112.
[90] G. Sforza, *Digital services act, Scorza: "Le luci e le poche ma gravi ombre delle nuove regole Ue"*, in *Garante per la protezione dei dati personali*, 28-04-2022, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9765212.

configurazione co-regolamentativa. Ad oggi, si tratta di un atto che aggiorna la Direttiva *e-Commerce* (approvata circa 20 anni fa) e i cui effetti sono ancora da verificare sul piano fattuale. Solo allora si potrà valutare se il DSA sarà stato in grado di offrire uno strumento atto a bilanciare la moderazione e/o rimozione dei contenuti illegali e la salvaguardia della libertà di espressione, rifuggendo dalla trappola censoria.

6.1 "Guerra ibrida" e salvaguardia del Cyberspazio

Per quanto concerne il dominio del cyberspazio, la difesa della NATO si fonda su quattro obiettivi principali: proteggere le proprie reti, operare nel *cyberspace* (anche attraverso le operazioni e le missioni dell'Alleanza), aiutare gli alleati a migliorare la loro capacità di contrasto a livello nazionale e fornire una piattaforma per la consultazione politica e l'azione collettiva. Nel 2008, un anno dopo gli attacchi informatici subìti dall'Estonia, la NATO decide di dotarsi di una *Cyber Defence Policy*, successivamente rivista (in occasione del Vertice NATO di Bruxelles del 2021) e rinominata *Comprehensive Cyber Defence Policy* a causa dell'intensificarsi degli attacchi informatici – soprattutto della tipologia r*ansomware* – che hanno colpito le infrastrutture critiche e democratiche. La nuova *Policy* mira a portare avanti i tre principi cardine della NATO: scoraggiare, difendere e contrastare l'intero spettro delle minacce *cyber* in ogni momento – in tempi di pace, crisi o conflitto – e a livello politico, militare e tecnico[91]. Un passo significativo nella lotta ai pericoli cibernetici è stato compiuto durante il Vertice NATO a Varsavia nel 2016. In quell'occasione, gli Alleati hanno sottoscritto il *Cyber Defence Pledge* il quale, oltre a potenziare le difese *cyber* delle reti e delle infrastrutture nazionali, si articola in altri sei punti salienti[92]: assegnare risorse adeguate a livello nazionale per rafforzare le capacità di difesa; rafforzare l'interazione tra i rispettivi attori nazionali della difesa *cyber* per approfondire la cooperazione e lo scambio di *best practices*; migliorare la comprensione delle minacce attraverso la condivisione di informazioni e valutazioni; aumentare la consapevolezza e le competenze tra tutti gli attori coinvolti; promuovere l'istruzione, l'addestramento e le esercitazioni *cyber*; accelerare l'attuazione degli impegni in materia *cyber defence* concordati, anche per i sistemi nazionali da cui dipende la NATO.

Tuttavia, nell'ottica del contrasto alle minacce provenienti dal cyberspazio, la NATO, nel corso degli anni e durante il recente Summit di Vilnius, ha sottolineato come un attacco informatico nei confronti di uno Stato alleato potrebbe, in determinate circostanze, essere considerato alla stregua di un attacco armato aggressivo, tanto da far scattare il ricorso al già citato Articolo 5 del Trattato Nord Atlantico.

Restando sempre sul tema delle minacce *cyber*, anche l'Unione Europea si è attivata per arginare il fenomeno. Il primo tassello di questa sfida è stato realizzato nel 2004, con la nascita dell'*ENISA* (l'Agenzia europea di sicurezza delle reti e dell'informazione), il cui compito è quello di sostenere

[91] NATO, *Cyber defence*, https://www.nato.int/cps/en/natohq/topics_78170.htm
[92] NATO, *Cyber Defence Pledge*, https://www.nato.int/cps/su/natohq/official_texts_133177.htm

DPCE online
ISSN: 2037-6677

gli Stati membri, le istituzioni dell'UE e tutti i soggetti coinvolti nella gestione degli attacchi informatici. A livello normativo, invece, il primo insieme di regole sulla sicurezza europea è arrivato dalla *Direttiva NIS* (Ne*twork and Information Security*), entrata in vigore nell'agosto 2016. La Direttiva, rivista e modificata nel 2020, obbliga, tra le altre cose, gli Stati membri a dotarsi di una strategia nazionale in ambito *cyber* e a identificare le proprie infrastrutture critiche, ovvero quelle che erogano servizi essenziali. Insieme alla *Direttiva NIS*, la lotta al contrasto *cyber* si è arricchita con il *Cyber Security Act* e il *Cyber Competence Europe*. Il primo rafforza la sicurezza dei prodotti *ICT* e dei servizi digitali, oltre ad estendere i poteri dell'*ENISA* attraverso maggiori poteri e risorse e con un mandato permanente. Il secondo, invece, sulla scia dei modelli dei Centri di Eccellenza, è stato istituito nel 2021 – con sede a Bucarest – con l'obiettivo di rafforzare le capacità europee di *cybersecurity* e di promuovere l'eccellenza della ricerca. Infine, nel dicembre 2020, l'Unione Europea ha approvato una nuova strategia per la *cybersecurity*. La nuova strategia contiene progetti e missioni inquadrabili in tre aree specifiche: resilienza, sovranità tecnologica e *leadership*; sviluppo delle capacità operative di prevenzione, deterrenza e risposta; promozione di un cyberspazio globale e aperto attraverso una maggiore collaborazione.

Al di là delle singole risposte, è importante sottolineare la collaborazione tra NATO e Unione Europea. Se da un lato la "guerra ibrida" si avvale della sinergia di diversi attori e strumenti, allo stesso modo i due organismi internazionali hanno deciso di unire le forze nella lotta al pericolo ibrido. Da questa cooperazione è scaturita l'idea di dare vita allo *European Centre of Excellence for Countering Hybrid Threats*[93] (o più comunemente detto *Hybrid CoE*), al quale hanno già aderito 33 Stati. Il Centro di Eccellenza, nato a Helsinki nel 2017, rappresenta un ulteriore strumento in grado di fornire supporto dinanzi alle minacce ibride. Ciò avviene attraverso la condivisione delle *best practices*, la formulazione di raccomandazioni e la sperimentazione di nuove idee e approcci. Il Centro costruisce anche le capacità operative degli Stati partecipanti attraverso la formazione di professionisti e l'organizzazione di esercitazioni pratiche.

L'*Hybrid CoE* è composto da tre reti di *Community of Interest*: *Hybrid Influence*, *Vulnerabilities and Influence*, *Strategy and Defence*. L'*Hybrid Influence* esamina il modo in cui gli attori statali e non statali conducono attività di influenza mirate agli Stati partecipanti e alle istituzioni nell'ambito di una campagna ibrida. Inoltre, si occupa di analizzare il modo in cui gli attori statali ostili utilizzano gli strumenti di influenza nel tentativo di rovesciare la democrazia, seminare instabilità o limitare la sovranità di altre nazioni e l'indipendenza delle istituzioni. Le aree di interesse dell'*Hybrid Influence* sono la dissuasione dalle minacce ibride, la salvaguardia dei processi democratici e il ruolo degli attori non statali, con particolare attenzione al modo in cui essi conducono operazioni di influenza come *proxy* di Stati ostili. L'area *Vulnerabilities and Influence* è responsabile dell'individuazione e della comprensione delle vulnerabilità degli Stati e delle organizzazioni partecipanti e del miglioramento della loro resilienza. L'attenzione è quindi

[93] Per ulteriori dettagli, si faccia riferimento al sito dell'*Hybrid CoE*: https://www.hybridcoe.fi/

rivolta alle minacce ibride presenti nell'economia, nella sicurezza marittima, nella migrazione e nelle infrastrutture critiche. La *Strategy and Defence*, infine, si occupa della "guerra ibrida", delle strategie correlate e delle conseguenti implicazioni per la politica di sicurezza. Ha il compito di individuare l'essenza e la natura delle guerre ibride, nonché la logica e il modello delle strategie ibride per sviluppare una migliore comprensione delle minacce ibride e delle relative sfide. Il suo obiettivo principale è quello di fornire competenze agli Stati partecipanti, all'UE e alla NATO al fine di promuovere una comprensione comune e completa quando si tratta di contrastare e rispondere a minacce e crisi ibride. L'*Hybrid CoE*, tuttavia, non è l'unico organismo in seno alla NATO che si occupa di contrastare le minacce ibride. Tra gli altri ci sono lo *Strategic Communications*[94] (o anche *StratCom COE*) a Riga e il *Cooperative Cyber Defence* a Tallinn. Diventato operativo nel gennaio 2014, lo *StratCom COE* contribuisce a migliorare la comunicazione strategica della NATO e dei suoi alleati e partner. Il *Cooperative Cyber Defence*, invece, è stato istituito nel 2008 dopo i diversi cyber attacchi che colpirono l'Estonia un anno prima. Il 27 aprile 2007, infatti, i siti governativi, le banche, i ministeri e i media estoni furono colpiti da ripetuti e prolungati attacchi *DDoS*, causando disagi e disservizi a livello amministrativo e finanziario. Secondo molti analisti, dietro l'attacco si celerebbe la Russia, infastidita dalla decisione del governo estone di rimuovere la statua di bronzo di un soldato dell'Armata Rossa della Seconda Guerra Mondiale[95]. A seguito di questo evento, la NATO decise di costituire il *Cooperative Cyber Defence*, il quale si occupa di promuovere la cooperazione, le capacità e la condivisione di informazioni sulla sicurezza informatica tra i Paesi della NATO, utilizzando, ad esempio, esercitazioni, *workshop* di diritto e politica, corsi tecnici e conferenze per preparare la NATO e le Nazioni partner a rilevare e combattere gli attacchi informatici. Conduce inoltre attività di ricerca e formazione in diverse aree della guerra informatica[96].

La NATO, infine, sostiene i paesi alleati in caso di attacco ibrido mediante i *Counter Hybrid Support Team* (CHST), squadre di consulenza che assistono gli Stati partner sia in caso di crisi e sia come supporto nella costruzione di capacità nazionali di contrasto all'ibrido. Nel novembre 2019, il primo *Counter Hybrid Support Team* è stato inviato in Montenegro per cercare di sventare le minacce ibride ad un anno dalle elezioni presidenziali[97].

7. Considerazioni conclusive

Il progresso tecnologico, alimentato dallo sviluppo di Internet come rete pubblica e dalla pervasività delle tecnologie delle *ICTs* ha creato nuove

[94] Per ulteriori dettagli, si faccia riferimento al sito dello *StratCom COE*: https://stratcomcoe.org/
[95] I. Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, in *The Guardian*, 17-05-2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia
[96] Per ulteriori dettagli, si faccia riferimento al sito del *Cooperative Cyber Defence*: https://www.ccdcoe.org/
[97] S. Lekic, *First NATO counter-hybrid warfare team to deploy to Montenegro*, in *Stars and Stripes*, 08-11-2019, https://www.stripes.com/theaters/europe/first-nato-counter-hybrid-warfare-team-to-deploy-to-montenegro-1.606562

DPCE online
ISSN: 2037-6677

opportunità, ma ha anche generato nuovi pericoli. L'interconnessione globale tra reti, comunicazioni, *server*, *software*, dati, informazioni e utenti ha creato le condizioni per la nascita di un nuovo ambiente nel quale collegare queste attività: il cyberspazio. Ed è in questa nuova dimensione, riconosciuta come quinta dimensione della conflittualità, che si celano nuove minacce per Stati, organizzazioni, infrastrutture e popolazione. Tra questi è possibile citare gli attacchi alle infrastrutture critiche, la manipolazione delle reti e la disinformazione. Si tratta, a tutti gli effetti, di nuove *cyber weapons* a disposizione di attori maligni per raggiungere i propri obiettivi strategici. Quindi, la tecnologia e il cyberspazio aprono due nuovi fronti all'interno della guerra: uno digitale e uno comunicativo.

Negli ambienti militari, accademici e strategici si è cercato di catturare la complessità dei conflitti del XXI secolo attraverso il concetto di "guerra ibrida". Tuttavia, il termine risulta ancora nebuloso e confuso, tanto che non esiste una sua definizione universalmente accettata. Dalla semplice combinazione di elementi convenzionali e non convenzionali nello stesso campo di battaglia si è giunti all'inserimento di strumenti non cinetici (disinformazione, propaganda e operazioni *cyber*, giusto per citarne alcuni) nella definizione di "guerra ibrida". E questo ha finito per creare confusione all'interno del dibattito. Una condizione non proprio ideale per i decisori politici chiamati a contrastare lo spettro ibrido. Il presente contributo, ripercorrendo la genesi del concetto e analizzando le sue similitudini e i suoi elementi innovativi, ha cercato di rispondere a queste sollecitazioni. Un primo passo da compiere dovrebbe essere indirizzato verso una definizione completa ed esaustiva della "guerra ibrida", delle sue caratteristiche e dei suoi elementi caratterizzanti. Uno scenario che migliorerebbe la preparazione, la risposta e la difesa globale e nazionale.

Per quanto concerne la risposta fornita nella lotta al contrasto ibrido si è sottolineato come le azioni degli attori malevoli avvengano nella c.d. "zona grigia" e senza superare la soglia dell'intensità, riducendo la certezza del diritto internazionale e l'attivazione di clausole di assistenza reciproca come quelle stabilite dall'articolo 5 del Trattato Nord Atlantico, dall'articolo 42 del Trattato UE o l'articolo 51 della Carta delle Nazioni Unite. Nonostante l'inapplicabilità dei suddetti provvedimenti, la risposta collettiva globale ed europea non può trascendere dall'applicazione e dal rispetto della legge. Il diritto riveste ancora un ruolo importante nel decidere cosa è legale e cosa non lo è. Nonostante le problematiche evidenziate, gli Stati e le istituzioni occidentali dovrebbero difendere l'integrità del sistema giuridico internazionale e utilizzare il diritto internazionale contro i propri avversari «in modo da salvaguardare i suoi valori fondamentali e preservare la sottile distinzione tra uso e abuso della legge»[98]. A tal proposito, secondo Aurel Sari, l'Occidente dovrebbe agire con misure volte a rafforzare le tre seguenti aree[99]: preparazione giuridica, resilienza e deterrenza giuridica e capacità di difesa giuridica. Tuttavia, gli Stati non dovrebbero limitarsi a cercare risposte anti-ibride solo nel diritto internazionale. È necessaria una legislazione nazionale chiara che vada a disciplinare tutte le vulnerabilità che

[98] A. Sari, *Blurred Lines: Hybrid Threats and the Politics of International Law*, in *Hybrid CoE Strategic Analysis*, 4, 2018, 6.
[99] *Ibid.*

possono essere colpite dagli attori ibridi: cyberspazio, infrastrutture chiave, migrazione e così via. Per Sanz-Caballero è fondamentale che gli Stati emanino una legislazione interna «sulla difesa nazionale e sulle leggi sulla sicurezza informatica il più presto possibile. Inoltre, dovrebbero legiferare sui propri servizi diplomatici per aggiornare le loro funzioni e la capacità di affrontare queste minacce nel lavoro quotidiano. Pertanto, il diritto internazionale non può e non deve sostituire il diritto statale in questo senso»[100].

Oltre ad una collaborazione internazionale tra Stati, Unione Europea e NATO, la "guerra ibrida" richiede anche delle azioni di contrasto e di difesa a livello nazionale, mediante lo sviluppo di una strategia interna[101] che, data l'ampia gamma di strumenti a disposizione degli attori malevoli, non si regga più sull'architettura della sicurezza classica, ma abbia come perno fondante la resilienza. La resilienza, nel contesto della sicurezza nazionale, è la

[100] S. Sanz-Caballero, *op. cit.*, 7.

[101] In ambito cibernetico, gli Stati Uniti, dopo l'attacco dell'11 settembre 2001, sono stati il primo Paese ad interessarsi alla messa in sicurezza del dominio mediante l'adozione di una strategia nazionale: la *National Strategy to Secure Cyberspace* (2003). A questo documento fece seguito la *National Cyber Strategy* (2016) per volontà dell'ex Presidente Trump. Lo scorso marzo, poi, il governo Biden ha aggiornato la strategia della precedente amministrazione, istituendo la *National Cybersecurity Strategy*, che si basa su cinque pilastri fondamentali: la difesa delle infrastrutture critiche, l'interruzione e lo smantellamento degli attori malevoli, il modellamento delle forze di mercato per promuovere la sicurezza e la resilienza, l'investimento in un futuro resiliente e la creazione di partenariati internazionali per perseguire obiettivi comuni (in United States of America, *National Cybersecurity Strategy*, marzo 2023). Per quanto riguarda l'Italia, invece, è possibile notare come la prima iniziativa in tal senso sia stata sviluppata con il Decreto Monti del 24 febbraio 2013, che si è occupato di definire l'architettura *cyber* nazionale, successivamente modificata dal Decreto Gentiloni del 17 febbraio 2017. Tra le misure più recenti occorre sottolineare l'istituzione del Perimetro di Sicurezza nazionale cibernetico (PSNC) e dell'Agenzia per la cybersicurezza nazionale (ACN). Il PSNC è stato istituito con il d.l. 105/2019 con lo scopo di mettere in sicurezza gli attori, pubblici e privati, che svolgono una funzione o forniscono un servizio essenziale per gli interessi dello Stato in settori critici (difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti provvidenziali / sanitari) e dal cui malfunzionamento o interruzione può derivare un pregiudizio per la sicurezza nazionale. Istituita con il d.l. n. 82 del 14 giugno 2021, seguendo l'esempio di altri Stati (la Francia con l'*Agence nationale de la sécurité des systèmes d'information*, il Regno Unito con il *National Cyber Security Centre* e la Germania con il *Bundesamt für Sicherheit in der Informationstechnik*), l'Agenzia nasce con il preciso compito di rideterminare l'architettura nazionale di *cybersecurity*, con l'obiettivo di mitigare il maggior numero di attacchi cibernetici e di perseguire il raggiungimento dell'autonomia strategica nazionale ed europea. Oltre a stimolare lo sviluppo di percorsi formativi, a diffondere la cultura della cybersicurezza, a supportare i soggetti privati e pubblici – che erogano servizi essenziali – nella prevenzione degli incidenti, l'ACN è impegnata nell'implementazione della Strategia Nazionale di Cybersicurezza. Quest'ultima mira ad affrontare le seguenti sfide: autonomia strategica nazionale ed europea nel settore del digitale, gestione di crisi cibernetiche, anticipare l'evoluzione della minaccia *cyber*, contrastare la disinformazione *online* nel più ampio contesto della minaccia ibrida, assicurare una transizione digitale *cyber* resiliente della Pubblica Amministrazione e del tessuto produttivo. Nel piano di implementazione della Strategia, poi, vengono delineate diverse misure (di protezione, di risposta, di sviluppo) e fattori abilitanti per raggiungere gli obiettivi appena menzionati.

DPCE online
ISSN: 2037-6677

capacità delle società di «gestire le minacce e i rischi, di adattarsi ad essi e di riprendersi in caso di attacco o evento senza perdere la capacità di fornire funzioni e servizi di base ai membri di quella società»[102]. Cruciale nella strategia di resilienza è l'identificazione preliminare delle vulnerabilità presenti all'interno di ogni Stato, siano esse legate alla protezione delle infrastrutture critiche o all'individuazione di quei gruppi sociali emarginati, che potrebbero diventare uno dei bersagli ideologici di campagne di disinformazione. Ogni Stato, dunque, deve essere a conoscenza del tipo di minacce ibride che potrebbero attaccarlo, sfruttando le sue vulnerabilità interne. Queste ultime, se attaccate, rischiano di provocare reazioni a cascata a livello sovranazionale. Si pensi, ad esempio, ai sistemi di trasporto o alle reti elettriche interconnesse; un attacco rivolto ad uno Stato vulnerabile genererebbe ripercussioni anche in uno Stato non vulnerabile. La promozione della resilienza a livello statale nella "guerra ibrida" richiede, quindi, una visione olistica e un approccio integrato che coinvolga gli aspetti politici, economici, sociali e di sicurezza. Gli sforzi per aumentare la resilienza dovrebbero essere guidati da una combinazione di politiche nazionali, cooperazione internazionale e investimenti a lungo termine nella capacità di adattamento e risposta.

In conclusione, risulta complicato delineare il prossimo futuro della "guerra ibrida" e delle sfide cui la sicurezza internazionale e nazionale andrà incontro. Ciò che è certo è che il pericolo ibrido richiede la massima attenzione da parte di Stati, organizzazioni internazionali, imprese e cittadini. Nessuno, da solo, è in grado di arginare e contrastare efficacemente il problema. Soltanto una cooperazione costante e concreta fra tutte le parti coinvolte può rappresentare un ottimo strumento di difesa e contrasto contro le minacce ibride nella consapevolezza che le risposte che si riusciranno a fornire, determineranno le sfide globali e regionali del prossimo decennio.

Andrea Spaziani
Università degli Studi di Teramo
aspaziani@unite.it

[102] B. Giegerich, *Hybrid Warfare and the Changing Character of Conflict*, in *Connections*, 15, 2, 2016, 69.