OPINIO JURIS
LAW & POLITICS REVIEW

Il ruolo dell'intelligence tra vecchie e nuove sfide.

La sicurezza nazionale tra bipolarismo e multipolarismo

A cura di Fabio Antonio Vigneri

Il bipolarismo pre-Guerra Fredda

Le trasformazioni che hanno avuto luogo nel sistema internazionale negli ultimi decenni sono così macroscopiche da rendere desuete molte regole e procedimenti su cui si basa tradizionalmente la politica e la politica estera in particolare[1].
Quella attuale è una politica post-internazionale, dove attori nazional-statali si dividono lo scenario globale e il potere con organizzazioni internazionali, gruppi industriali internazionali e movimenti sociali e

[1] U. GORI, *Intelligence e terrorismo nel sistema internazionale post-bipolare*, in *Osservatorio dell'Istituto di Studi Militari Marittimi*, n. 138/2006, p. 21.

ISSN 2531-6931

politici transnazionali[2]. Una politica turbolenta, con una fondamentale caratteristica: l'incertezza[3], che soppianta la prevedibilità e l'ordine internazionale del periodo bipolare. Una sorta di anarchia internazionale divenuta ancora più palese in seguito ai tragici eventi dell'11 settembre 2001.

Nell'arco di cinquant'anni, il confronto simmetrico ha garantito alla configurazione del sistema internazionale una certa stabilità, permesso un'apprezzabile prevedibilità nei comportamenti sia degli attori principali che delle pedine che si muovevano, come 'clienti', alla periferia del sistema[4] e ha prevenuto conflitti bellici tanto su scala regionale, quanto su larga scala, all'interno delle zone di influenza dei due blocchi: a est quello socialista e a ovest quello del c.d. "mondo libero" capeggiato dagli Stati Uniti.

Il possesso di apparati nucleari assicurava la reciproca deterrenza e, conseguentemente, le esigenze di stabilità e controllo interno. L'equilibrio di potenza, imposto dalle armi nucleari, c.d. 'equilibrio del terrore', non consentiva agli alleati minori di turbare la situazione di simmetria, con conflitti locali o tentativi di rivolta. Il fattore MAD (*Mutual Assured Distruction*), per il quale una guerra aperta avrebbe portato all'uso dell'arma atomica, scongiurava che si giungesse a uno sbocco bellico. Tuttavia, siffatto equilibrio non cancellava le tensioni internazionali; le spingeva, piuttosto, verso forme coperte di cui i Servizi segreti sarebbero stati gli strumenti necessari.

Il multipolarismo 'post-89'

[2] J. N. ROSENAU, *Study of world politics: volume II: globalization and governance*, London-New York, 2006.

[3] A tal riguardo, autorevolmente Gori sostiene che «l'incertezza oggi è la regola. I cc.dd. 'eventi inaspettati' diventano casi comuni. L'unico modo per dominare il mutamento e vincere la turbolenza è la capacità di apprendere e di adattarsi alle nuove situazioni. Ciò implica capacità di analisi, d'*intelligence*, di previsione e di pianificazione/programmazione. In una parola: capacità di analisi strategica». Con tali parole, U. GORI, *Intelligence e terrorismo*, cit., p. 21.

[4] P. BATACCHI, *L'evoluzione dei conflitti moderni*, Centro Militare di Studi Strategici, Ricerca 2010, p. 6.

Quello 'post-89', diversamente, si identifica come un sistema in cui le aspettative non sono prevedibili e in cui regna l'indeterminatezza e il disordine mondiale. Il carattere distintivo degli attuali scenari è che, accanto allo Stato westfaliano, detentore legittimo della forza, sono emersi un'altra serie di attori della più disparata natura e dal carattere anche transnazionale – si pensi ai cc.dd. '*non-State actors*' – che, al pari del primo, hanno la capacità di incidere sulle dinamiche politiche, ridislocando l'autorità e la legittimità politica degli Stati; fra tutti, le organizzazioni terroristiche aventi, quale fattore aggregante e mobilitante, la religione, o comunque, la sua manipolazione in chiave radical-fondamentalista.

In uno scenario siffatto, non ha quasi più senso limitarsi, come durante il bipolarismo, a parlare di difesa territoriale, pianificando in funzione di questa e organizzando di conseguenza le proprie forze armate. Ne consegue che il concetto di 'sicurezza' si è ampliato a dismisura, sia nella sua accezione *oggettiva*, sia in quella *soggettiva*; senza contare, in aggiunta, gli spazi e i profili problematici apertisi a seguito della rivoluzione informatica[5] che offrono sì nuove prospettive all'azione politica, ma anche condizionamenti e limiti che hanno spostato il conflitto su un piano differente da quello tradizionale.

L'implosione del bipolarismo, ampliando e modificando i problemi di sicurezza, di conseguenza, ha, in parte, trasformato le attività delle agenzie d'*intelligence*.

Il venir meno dell'impero sovietico con la dissoluzione del Patto di Varsavia siglato nel 1955 ha, anzitutto, privato l'Occidente della principale minaccia militare, diretta, e del principale avversario ideologico. Contestualmente, le piccole e medie Potenze hanno visto restituita parte della loro sovranità, in precedenza limitata, trovandosi

[5] Il *cyberspace*, difatti, è il nuovo campo di battaglia e di competizione geopolitica del XXI secolo. Tale nuova dimensione ha la capacità (unica) di rendere uniformi gli squilibri politici, che dominano le relazioni internazionali, ponendo sullo scacchiere soggetti della più diversa natura: singoli individui, attori non-statali, così come gli Stati. Tutti questi agiscono su un piano di gioco quasi paritario, venendo meno, così, ogni forma di asimmetria. In ogni atto di guerra, infatti, la fisicità di chi agisce per terra, per mare, in aria o nello spazio rende facilmente identificabili gli attori, così come facilmente individuabili sono anche i confini dello Stato belligerante. Lo stesso non avviene nello spazio cibernetico, dove, a causa della sua intrinseca natura digitalizzata, risulta molto complesso non solo imputare l'azione in tempi utili a uno o più determinati soggetti e/o a uno Stato, ma anche comprendere la ragione dell'attacco e i suoi obiettivi, quanto, soprattutto, evitare che chi ha realmente agito possa agevolmente sottrarsi da ogni responsabilità giuridica, politica, diplomatica, economica e militare. Si tratta, in definitiva, di un *ungoverned space* slegato da ogni normativa di riferimento. Cfr., sul punto, S. MELE, *Privacy ed equilibri strategici nel cyber-spazio*, in *Diritto, economia e tecnologie della privacy*, numero unico, 2010, p. 68.

ISSN 2531-6931

coinvolte nella ristrutturazione geopolitica mondiale e nei relativi problemi di difesa e di sicurezza, sia nell'Europa centrale e orientale, sia nei Balcani che nel Medio ed Estremo Oriente[6].
La fine del c.d. "periodo simmetrico", altresì, ha determinato effetti ancor più rilevanti e di più lungo periodo; la Comunità internazionale è stata privata di una delle parti della struttura duale, l'Unione Sovietica, la quale, oltre ad avere un ruolo di Potenza, era un fattore di stabilizzazione e d'ordine del sistema. Mancando una delle parti, dunque, sono state indebolite le capacità sistemiche di controllo e autoregolazione delle conflittualità latenti all'interno determinandosi, conseguentemente, l'aumento dei conflitti di tipo limitato, a carattere regionale o locale[7].
Inoltre, è venuto meno, in Occidente, il più solido argine entro il quale erano state contenute le spinte competitive tra le maggiori Potenze economiche. Ancora, si è relativizzato il concetto di 'frontiera', in quanto sono sparite le cortine di ferro che avevano frammentato l'Europa. È aumentato, in aggiunta, il grado di disordine interno al sistema internazionale e con l'instabilità internazionale, complici i forti dislivelli di reddito e la globalizzazione dell'informazione, si sono rafforzate le pressioni migratorie.
Tutto ciò ha profondamente modificato la natura delle minacce alla sicurezza nazionale in tutti i Paesi occidentali, accentuandone la multidimensionalità e, in particolare, la rilevanza degli aspetti economici e sociali rispetto a quelli puramente militari prevalenti nel passato[8].
La geopolitica ha cessato, in tal modo, di appiattirsi sulla geostrategia della deterrenza nucleare, che aveva dominato i decenni della Guerra Fredda. Al suo interno è cresciuto il peso della geofinanza, della geoinformazione e della geoeconomia[9].

[6] M. DE MARCHI, *Intelligence in un mondo multipolare*, reperibile all'indirizzo: https://www.academia.edu/1597909/Intelligence_in_un_mondo_multipolare, p. 122.
[7] *Ibidem*.
[8] G. DOTTORI, *Intelligence per il XXI secolo*, reperibile all'indirizzo: http://www.geocities.ws/gdottori2002/saggi/intelXXI.pdf, p. 63.

[9] C. JEAN, *Politica e informazione*, in *Rivista Militare*, n. 1/1997, pp. 32-43.

Il dopo-Guerra Fredda è soprattutto l'età della geoeconomia. Il peso crescente che i fattori economici esercitano nella determinazione dei rapporti di potenza tra gli Stati e sulla loro stessa stabilità attribuisce, difatti, un significato nuovo alla dimensione economica della sicurezza nazionale[10].

Dai classici indicatori di potenza, misurati attraverso indici militari quali il numero delle navi, gli aerei, le divisioni corazzate e di fanteria, tipici del periodo pre-Guerra Fredda, si è progressivamente passati a un confronto e a una classificazione incentrata sul numero delle testate nucleari possedute e dei relativi vettori di lancio. Negli anni '80, tuttavia, con la Presidenza Reagan, la corsa agli armamenti ha cessato di essere fine a sé stessa per divenire l'elemento accessorio di una più complessa strategia globale di guerra economica, mirante all'esaurimento finanziario e industriale dell'Unione Sovietica[11].

La rivoluzione informatica, la globalizzazione dei mercati e la dematerializzazione dell'economia, spostando il baricentro della politica internazionale sugli aspetti prettamente geoeconomici, hanno modificato i compiti dei Servizi d'informazione riorientando, pertanto, le principali attività. A questo proposito, si parla oggi di *intelligence* economica.

In un ordine del mondo a geometria variabile, definito incisivamente quale *nuovo disordine mondiale* e basato su velocità, interdipendenza e complessità, cambia il concetto di 'guerra', divenuto polisenso nonché assorbente una serie di comportamenti sconosciuti nel passato. Cambia, inoltre, l'idea stessa di 'potenza': più sfumata, ambigua e meno legata all'idea di supremazia militare.

In un contesto siffatto, tuttavia, le minacce militari non sono completamente venute meno, ma sono state affiancate da un complesso di altri fattori di rischio. La politica di sicurezza nazionale è, pertanto, divenuta più complessa, oltrepassando la sfera di competenze della politica di difesa e interessando la politica economica, quella monetaria e finanziaria, la politica del commercio estero e, per certi versi, quella delle telecomunicazioni, delle scoperte scientifiche, dei trasporti, dell'istruzione e dei lavori pubblici.

L'*intelligence* nel contesto bipolare

[10] G. DOTTORI, *Intelligence*, cit., p. 66.

[11] *Ibidem*.

ISSN 2531-6931

Quanto ai compiti dei Servizi segreti durante l'equilibrio di potenza[12], i due schieramenti erano concentrati nella defatigante opera di acquisizione dei segreti militari e industriali dell'avversario, nella conduzione di attività di influenza e di disinformazione, nell'individuazione di cellule spionistiche nemiche, nella protezione della riservatezza del *know-how* militare e delle comunicazioni strategiche, nella previsione delle intenzioni dell'avversario e nell'annullamento di ogni margine di manovra dell'avversario, così come l'azione dei Servizi segreti non escludeva l'uso e il supporto, sapientemente dosato, di forze antagoniste al sistema avversario, onde non alterare lo *status quo* e gli equilibri generali consolidati.
L'*intelligence* si impantanava, conseguentemente, in una guerra di posizione la cui trincea era rappresentata dalla c.d. "cortina di ferro". Si scatenarono, in aggiunta, da ambo le parti, frenetiche azioni di 'bonifica interna' – si pensi alle attività intrusive e capillari del KGB (Comitato per la sicurezza dello Stato dell'Unione Sovietica) e della STASI (Ministero per la Sicurezza di Stato della Repubblica Democratica tedesca) – rivolte contro chi venisse identificato quale nemico interno. In Occidente tale azione si indirizzò verso coloro che condividevano l'ideologia comunista, mentre nel blocco sovietico il bersaglio erano le istanze borghesi, portatrici di valori controrivoluzionari[13].
I Servizi d'*intelligence*, nel nuovo scenario internazionale fluido e dinamico, diventano un elemento di fondamentale comprensione e di analisi delle cangianti situazioni critiche esistenti, nonché tassello imprescindibile della tenuta degli assetti democratici, abilitati a fornire previsioni, scoprire i nuovi rischi e garantire la struttura politica nazionale dalla disgregazione politica, economica e culturale[14].
L'*intelligence* si fa carico, pertanto, di individuare l'autore di un'offesa 'coperta' – ed eventualmente di preparare una risposta altrettanto

[12] In argomento, si rimanda alle considerazioni di A.C. VILASI, *Manuale d'intelligence*, Reggio Calabria, 2011, p. 75 ss.

[13] P. SALVATORI, *Spie? L'intelligence nel sistema di sicurezza internazionale*, Roma, pp. 131-132.

[14] Diversamente, durante la Guerra Fredda, i Servizi segreti dei vari Paesi e gli strumenti a loro disposizione erano 'tarati' in funzione di un nemico certo e le cui mosse erano costantemente sotto monitoraggio con strumenti adatti, fra i quali l'*intelligence* elettronica (ELINT) e quella fotografica (IMINT).

coperta – anche al di là della percezione pubblica, di informare l'Autorità politica del reale stato dei fatti e di valutare ipotesi di c.d. "guerra catalitica" sapientemente eccitata da un terzo attore nascosto[15].
In un mondo in cui gli strumenti classici dell'azione estera di uno Stato – diplomazia e guerra – risultano sempre più di complesso utilizzo, ecco che si innesta l'*intelligence* che – rileva il Direttore dell'AISE Manenti – «al contrario, nasce proprio per navigare con successo questo sistema: la non convenzionalità della sua natura è data dalla capacità e responsabilità di parlare 'di tutto' e 'con tutti'»[16].

Funzione attuale delle agenzie d'*intelligence*

«Il prezzo della libertà è l'eterna vigilanza»: così avvertiva l'epistemologo Popper ne *La società aperta e i suoi nemici*[17] (1945), opera destinata, nell'attuale contesto di emergenza sanitaria, di conflittualità diffusa e di imprevedibilità nelle relazioni internazionali a una necessaria rilettura.
Innanzi alle sfide attuali, concretantesi in nuovi fattori di rischio per la sicurezza nazionale, la vigilanza di popperiana memoria è sempre più complessa e impegnativa in quanto le democrazie occidentali e la comunità *intelligence* si trovano ad affrontare – secondo chi scrive – dinamiche plurime particolarmente insidiose e incombenti, di cui si delineano sommariamente i caratteri fondamentali[18].

1. I rischi derivanti dalla **competizione economica globale**, che impongono ai Servizi d'informazione di mitigare il rischio di azioni di tipo predatorio/speculativo nei confronti di *asset* pregiati nonché le iniziative condotte da attori ostili contro la politica economica, monetaria e finanziaria nazionale, specie nel contesto pandemico inteso quale amplificatore di vulnerabilità e rischi; garantire l'afflusso in sicurezza di capitali nel tessuto economico-finanziario

[15] A. GIANNULI, *Come i servizi segreti stanno cambiando il mondo*, Milano, p. 42.
[16] «L'*intelligence* contribuisce alla risoluzione di problemi complessi anche attraverso l'interazione con il dispositivo bellico nazionale. La necessità di saper operare in maniera non invasiva richiede un'attenta integrazione delle capacità, tale da consentire interventi 'chirurgici' che non lascino impronte negative sul terreno». In questo senso, A. Manenti (Direttore AISE) in P. SALVATORI, *Spie?*, cit., *Postfazione*, p. 277.
[17] K.R. POPPER, D. ANTISERI (a cura di), *La società aperta e i suoi nemici. Platone totalitario - vol. I*, Roma, 2014, p. 632.
[18] L'elenco riportato non è da intendersi come esaustivo.

interno; acquisire le linee guida della politica economica e finanziaria dei potenziali *competitor* del proprio Stato; supportare l'internazionalizzazione delle imprese e delle filiere industriali, specie quelle di rilevanza strategica, ma anche proteggendo le imprese dallo spionaggio di *know-how* pregiato, alta tecnologia e scoperte scientifiche, in un'ottica rivolta alla tutela degli interessi nazionali: da qui l'importanza assunta dalla *economic intelligence*[19];

2. La **minaccia terroristica** di matrice jihadista, incarnata da DAESH, che comporta articolate manovre informative, il monitoraggio delle evoluzioni del fenomeno, delle dinamiche interne alle principali formazioni e dei canali di approvvigionamento finanziario, l'analisi della propaganda e dei processi di radicalizzazione innescati o alimentati soprattutto nello spazio cibernetico e l'osservazione precisa dell'articolazione strutturale, delle dottrine operative e delle motivazioni dei gruppi dediti alla lotta armata[20];
3. Il **fenomeno migratorio clandestino**, con specifica attenzione riservata alle evoluzioni del teatro libico e di quello siriano in cui i perduranti conflitti contribuiscono ad alimentare le partenze verso le coste italiane, ma anche ai Balcani occidentali, e la connaturata gestione criminale delle tratte terrestri e marittime da parte delle locali filiere che lucrano sul traffico di esseri umani;

[19] Secondo la definizione più accreditata, formulata da C. Jean e P. Savona, l'*intelligence* economica è la disciplina che, studiando il ciclo dell'informazione necessario alle imprese e agli Stati per effettuare scelte corrette di sviluppo, si prefigge di affinare le abilità cognitive e decisionali applicate alle complessità del contesto competitivo globale. Per una nitida disamina sulla disciplina *de qua*, si rimanda a C. JEAN, P. SAVONA, *Intelligence economica. Il ciclo dell'informazione nell'era della globalizzazione*, Soveria Mannelli, 2011. L'*intelligence* economica, si occupa, pertanto, dello sviluppo di tecniche di raccolta dei dati, di loro analisi, di decisione operativa e di verifica dei risultati, configurandosi come materia di comune interesse per le imprese e gli Stati. Tutto ciò a difesa degli attori economici dello Stato – siano essi imprese pubbliche o private – da minacce esterne.

[20] L'organizzazione mantiene postura e orizzonti dell'attore globale, confermandosi riferimento ideologico per simpatizzanti e sostenitori su scala mondiale; Le azioni di stampo jihadista realizzate in Europa nel 2019 sono valse a ribadire l'insidiosità di una minaccia che resta prevalentemente endogena e che ha visto, in linea di continuità con gli ultimi anni, l'attivazione di *lone wolf* e il ricorso a mezzi offensivi facilmente reperibili. Ciò mentre si è confermato centrale il ruolo del *jihad* digitale, in grado di offrire agli aderenti una sorta di 'cittadinanza' di un Califfato ancora in vita nella sua dimensione virtuale. Un'indagine accurata dello stato attuale della minaccia jihadista la si rinviene in PRESIDENZA DEL CONSIGLIO DEI MINISTRI, SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA, *Relazione sulla Politica dell'Informazione per la Sicurezza*, 2019 e 2020, p. 79.

4. La **minaccia cibernetica**[21] agevolata dalla persistenza e pervasività delle *cyberweapons*[22] a disposizione di Stati e organizzazioni criminali. Le armi cibernetiche si configurano come strumenti privilegiati per la conduzione di manovre ostili in danno di *target* di rilevanza strategica per gli Stati e afferenti a settori nevralgici, specie nell'attuale contesto pandemico (settore della sanità e della ricerca, Dicasteri e Pubbliche Amministrazioni dello Stato). Al riguardo, a livello globale si sta giocando una partita strategica nella quale sicurezza cibernetica, benessere della popolazione e sicurezza nazionale sono indissolubilmente legate. La minaccia cibernetica è suddivisa, a seconda del grado di offensività dell'attacco informatico, in diverse tipologie quali *hacktivism*, *cybercrime*, *cyberespionage*, *cyberterrorism* e *cyberwar*. Nell'ordinamento italiano, la L. n. 133/2019[23] ha positivizzato l'iniziativa promossa dal Comparto *intelligence* italiano al fine di consentire al sistema-Paese di fronteggiare adeguatamente le sfide poste dall'evolversi della minaccia cibernetica nelle sue molteplici forme, a partire da quelle di matrice statuale.
5. Le **economie parallele illegali** e la permanente criminalità organizzata transnazionale, basata su sodalizi in grado di infiltrare il tessuto socio-economico interno e di ingerirsi indebitamente nei processi decisionali pubblici, di movimentare e reimpiegare

[21] La minaccia cibernetica, definita dal *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico* come «l'insieme delle condotte controindicate che possono essere realizzate nel o attraverso il cyberspace, o in danno di quest'ultimo e dei suoi elementi costitutivi», […] che si «sostanzia in particolare nelle azioni di singoli individui o organizzazioni, statali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi», ha assunto, in ragione delle sue intrinseche caratteristiche e degli effetti prodotti, crescente rilievo nel novero delle minacce non convenzionali. Testualmente, PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico,* dicembre 2013, p. 11.

[22] Secondo la definizione legale formulata in dottrina da S. Mele, 'arma cibernetica' è «un'apparecchiatura, un dispositivo ovvero un qualsiasi insieme di istruzioni informatiche utilizzato all'interno di un conflitto tra attori, statali e non, al fine di procurare anche indirettamente un danno fisico a cose o persone, ovvero di danneggiare in maniera diretta i sistemi informativi di un obiettivo critico nazionale del soggetto attaccato». Così, S. MELE, *Cyber-weapons: legal and strategic aspects (version 2.0)*, 2013, reperibile all'indirizzo: http://dx.doi.org/10.2139/ssrn.2518212, p. 10.

[23] Recante «Conversione in legge, con modificazioni, del Decreto-Legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica». Tale normativa vuole contribuire a innalzare la sicurezza del sistema-Paese verso le minacce *cyber*, individuando, da un lato, alcuni obblighi in capo a coloro che gestiscono infrastrutture essenziali per il Paese e, dall'altro, definendo un'architettura in grado di valutare *ex ante* l'adeguatezza dei diversi componenti informatici che andranno a essere utilizzati da tali gestori.

ISSN 2531-6931

finemente denaro di provenienza delittuosa, eludendo i presidi antiriciclaggio e antievasione e in grado di 'aggiornarsi' guardando con particolare interesse agli strumenti della c.d. 'tecnofinanza' quali le criptovalute;

6. L'**eversione interna e gli estremismi**, con particolare riferimento all'anarco-insurrezionalismo, alla destra radicale e al neonazismo globalizzato, anche nella dimensione virtuale, nel cui ambito, in relazione alla pandemia, sono proliferate campagne di disinformazione e teorie cospirative, accompagnatesi a retoriche ultranazionaliste, xenofobe e razziste, nonché a interventi propagandistici dagli accesi toni antisistema[24].
7. La **proliferazione di armi di distruzione di massa** – (*Weapon of Mass Distruction*, WMD[25]) – rappresenta un'oggettiva minaccia per la pace e la sicurezza internazionale in quanto tali armi possiedono un potenziale distruttivo enorme e una forza d'impatto largamente indiscriminata. Gli investimenti globali in forze nucleari aumentano, sono stati avviati processi di modernizzazioni degli arsenali e la deterrenza resta ancora centrale nella dottrina strategica degli Stati. Particolare attenzione è riservata, da parte dei Servizi di *intelligence*, ai rapidi avanzamenti dell'aggressivo programma missilistico e nucleare della Corea del Nord che, con il suo *leader* Kim Jong-un, ha fatto registrare finora 91 test atomici, costituendo una minaccia per la stabilità dell'Asia orientale e per la comunità internazionale[26].

[24] Sul versante italiano, l'emergenza pandemica ha inciso pure sul versante dell'eversione interna: da un lato, limitando le potenzialità mobilitative dell'estremismo politico, dall'altro, facendo da volano, in concomitanza con il ruolo aggregante e amplificatore della Rete, a una montante effervescenza propagandistica, trasversalmente orientata a strumentalizzare la crisi sanitaria per rilanciare progettualità conflittuali e istanze antisistema. In argomento, v. PRESIDENZA DEL CONSIGLIO DEI MINISTRI, SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA, *Relazione sulla Politica dell'Informazione per la Sicurezza*, 2020, p. 85 ss.

[25] Si tratta di una espressione che non ha origine nella scienza e nella tecnica militare. La sua origine – per così dire civile – risale al 1937 in un'omelia dell'arcivescovo di Canterbury W. Cosmo, in riferimento ai bombardamenti tedeschi e giapponesi a Guernica e in Cina. Oltre che in riferimento al nucleare, il concetto di WMD, all'indomani del secondo conflitto mondiale, fu applicato anche alle armi biologiche e chimiche e, in generale, a tutte quelle definite 'non convenzionali'.

[26] Nel 2017, quando il regime ha mostrato al mondo i vettori intercontinentali Hwasong-14 e Hwasong-15, si è registrata una *escalation* delle tensioni sulla penisola coreana, alimentata dagli scambi di intimidazioni tra Kim Jong-un e il presidente Trump, che ha risposto alle sollecitazioni militari e al programma nucleare messo a punto dalla Corea del Nord adottando una linea di 'massima pressione', minacciando a più riprese un intervento militare preventivo per distruggere le

8. La **minaccia ibrida**[27], per definizione veicolata su diversi domini (quello diplomatico, militare, economico/finanziario, *intelligence*, etc.) da attori ostili propensi all'uso combinato di più strumenti a fini manipolatori, in concomitanza con il dispiegarsi della crisi sanitaria, è stata caratterizzata da costanti tentativi di intossicazione del dibattito pubblico attraverso campagne di disinformazione e/o di influenza. Nell'attuale crisi pandemica, è stata registrata una elevatissima produzione di *fake news* e narrazioni allarmistiche, sfociate in un surplus informativo, c.d. 'infodemia, di difficile discernimento per la collettività.

installazioni militari del regime. Per un approfondimento dell'ISPI sulla minaccia nucleare di Pyongyang si rinvia a A. BERKOFSKY, F. FRASSINETTI (a cura di), *La sfida nordcoreana agli equilibri internazionali. La minaccia non convenzionale di Pyongyang*, n. 137 – febbraio 2018.

[27] Nell'ambito dell'Unione Europea, il concetto intende esprimere la combinazione di attività coercitive e sovversive, di metodi convenzionali e non convenzionali (cioè diplomatici, militari, economici e tecnologici), che possono essere usati in modo coordinato da entità statali o non statali per raggiungere determinati obiettivi, rimanendo però sempre al di sotto della soglia di una guerra ufficialmente dichiarata. L'accento è generalmente messo sullo sfruttamento dei punti deboli del bersaglio, e sulla creazione di ambiguità per ostacolare il processo decisionale. Le campagne massicce di disinformazione, che usano i *social media* per controllare il discorso politico o per radicalizzare, reclutare e dirigere mandatari, possono essere vettori di minacce ibride. Rientrano in questa macro categoria operazioni di tipo militari, *cyber* attacchi a infrastrutture critiche, campagne di *fake news*, di manipolazione dei *social media*, ingerenze nei settori economico-finanziari di un Paese, disinformazione mediatica in occasione di consultazioni elettorali, ma anche attacchi di tipo chimico, biologico, radiologico e nucleare. Sul punto, v. COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Comunicazione congiunta al Parlamento Europeo e al Consiglio. Quadro congiunto per contrastare le minacce ibride. La risposta dell'Unione Europea*, Bruxelles, 2016, p. 2.