ICONOCRAZIA

RIVISTA DI SCIENZE SOCIALI E FILOSOFIA POLITICA

SAGGIO

Il concetto gramsciano di «grande potenza» ai tempi del *cyberwarfare*

ALFREDO FERRARA

Università degli Studi di Bari Aldo Moro

Abstract

Per comprendere l'evoluzione del *cyberwarfare*, il concetto gramsciano di «grande potenza» può essere un'importante risorsa critica. Partendo dalle riflessioni di Gramsci nel *Quaderno 13*, il saggio analizza il ruolo del *cyberwarfare* nei conflitti russo-ucraino e nella guerra di Gaza, evidenziando come la guerra digitale ridefinisca le gerarchie internazionali. Il *cyberwarfare* non solo integra le strategie militari tradizionali, ma amplia il ruolo degli attori non-statali, sfidando la sovranità statale. Tuttavia, le grandi potenze mantengono un vantaggio competitivo grazie al controllo delle infrastrutture digitali e alla capacità di deterrenza cibernetica. In conclusione, il saggio riflette su come la sicurezza informatica sia diventata un elemento strutturale della geopolitica contemporanea, ponendo nuove sfide alla teoria gramsciana delle relazioni internazionali.

Parole chiave: guerra, cyberwarfare, grande potenza, Antonio Gramsci, digitale.

English version

Gramsci's concept of «great power» serves as a valuable analytical tool for understanding the evolution of cyberwarfare. Drawing on his insights from Prison Notebook 13, this paper analyzes the role of cyberwarfare in the Russia-Ukraine conflict and the Gaza war, demonstrating how digital warfare is reshaping global power structures. Cyberwarfare not only complements traditional military tactics but also enhances the role of non-state actors, challenging state sovereignty. However, the paper emphasizes that great powers retain an advantage through their control of digital infrastructure and cyber deterrence strategies. Ultimately, it argues that cybersecurity has become a central element of modern geopolitics, posing new questions for Gramsci's perspective on international relations.

Kewords: war, cyberwarfare, great power, Antonio Gramsci, digital dimension.

L'importanza assunta dal digitale nel mondo contemporaneo ha imposto da ormai tre decenni una riconsiderazione di ogni ambito della vita collettiva, compreso il modo in cui vengono condotte le guerre. Alcune riflessioni contenute nel *Quaderno 13* di Antonio Gramsci, scritto in un contesto storico pre-digitale, offrono a nostro avviso una chiave interpretativa utile per comprendere l'evoluzione del cosiddetto *cyberwarfare* ed il suo legame con lo *status* di grande potenza che uno Stato può o meno assumere nel contesto delle relazioni internazionali. Come suggerisce il titolo, il contributo parte dall'analisi dei due concetti-chiave oggetto dell'analisi: il concetto di «grande potenza» negli scritti gramsciani e quello di *cyberwarfare* nel dibattito contemporaneo. Successivamente, verrà esaminata la rilevanza assunta dalle pratiche di *cyberwarfare* nel conflitto russo-ucraino e nella guerra di Gaza. In conclusione, torneremo a Gramsci, in particolare a una nota – sempre del *Quaderno 13* – in cui viene affrontata la relazione tra grande potenza e sviluppo della tecnologia militare.

Nei *Quaderni del carcere*

Il concetto di «grande potenza» compare per la prima volta negli scritti carcerari nel *Quaderno 4*, ma è soprattutto nel *Quaderno 13* che la riflessione gravitante attorno ad esso assume una dimensione più sistematica, in particolar modo nelle note 2, 15, 19 e 32. È opportuno rilevare che queste quattro note sono tutte *Testi C*, ovvero note di seconda stesura, scritte a partire dalla riproposizione e rielaborazione di note scritte da Gramsci nei *Quaderni* precedenti: questa breve notazione filologica è indicativa di quanto il concetto di «grande potenza» – sebbene non sia tra i concetti più frequentemente utilizzati da Gramsci nei *Quaderni* – sia tutt'altro che una tappa casuale ed episodica dello sviluppo del suo pensiero, ma ne rappresenti un approdo pieno e consapevole.

Nella nota 2, dedicata ai rapporti di forza, Gramsci esplicita l'interrogativo alla base del suo ragionamento, domandandosi: «i rapporti internazionali precedono o seguono (logicamente) i rapporti sociali fondamentali?»; a questo interrogativo fornisce l'immediata e netta risposta: «seguono indubbiamente» (Gramsci, 2007, p. 1562). Alieno a ogni forma di determinismo e a ogni spiegazione mono-causale,

anche in questo caso il pensiero di Gramsci non è riassumibile in un processo unilaterale che vede da un lato il dinamismo dei rapporti sociali fondamentali e dall'altro le relazioni internazionali che accolgono passivamente l'esito di tale dinamismo. Come egli scrive nella stessa nota infatti, «i rapporti internazionali reagiscono passivamente e attivamente sui rapporti politici» che avvengo nella politica interna degli Stati; tali reazioni (attive o passive) variano in virtù della condizione di dominio o di subordinazione, di egemonia o di subalternità, della «vita economica di una nazione» rispetto al contesto internazionale: maggiore è la subordinazione di un paese e maggiore sarà l'impatto di quanto avviene nelle relazioni internazionali sulla politica interna e viceversa. Scartata quindi l'ipotesi di un'interpretazione unidirezionale, il senso di quella risposta così netta su cosa preceda e cosa segua tra relazioni internazionali e rapporti sociali fondamentali risiede nel realismo trasformativo gramsciano (*cfr.* Filippini, 2024): i motori effettuali della storia e della politica sono molteplici, e tra questi vi è anche quanto avviene nella politica interna degli Stati, laddove le masse organizzate hanno agibilità politica. Un approccio realista applicato alle sole relazioni internazionali infatti, riducendo la politica interna – e in particolar modo la vita economica di uno Stato – a variabile dipendente, reciderebbe ogni possibilità di iniziativa delle masse. E invece è proprio da dove le masse possono agire attraverso il conflitto sociale e l'organizzazione politica che occorre partire per un'analisi allo stesso tempo realista e trasformativa. Ed è per questo che Gramsci scrive che «ogni innovazione organica nella struttura modifica organicamente i rapporti *assoluti* e *relativi* nel campo internazionale, attraverso le sue espressioni tecnico-militari» (Gramsci, 2007, p. 1562). Non va dimenticato che queste note sono state redatte in una fase storica in cui il più esteso paese al mondo aveva recentemente vissuto quella che la studiosa Theda Skocpol ha definito una «rivoluzione sociale» (*cfr.* Skocpol, 1981), ovvero una rivoluzione che non solo ha imposto una transizione del regime politico, ma anche una transizione del sistema di produzione, una innovazione organica della struttura economica. Negli anni Venti e negli anni Trenta del Novecento è ancora fresca la memoria di quell'evento di politica interna a uno Stato – la Rivoluzione d'Ottobre – che aveva profondamente trasformato le relazioni internazionali. Ma sono anche i decenni in cui emerge sullo scenario mondiale la potenza politica ed

economica statunitense, fattore di cui – possiamo affermare a posteriori – Gramsci coglie tutta la rilevanza con una lungimiranza imparagonabile a quella dei suoi contemporanei.

Per Gramsci quindi le dinamiche interne ad uno Stato incidono sulle sue relazioni esterne e quindi anche sulle possibilità di uno Stato di assurgere al rango di grande potenza. Un primo elemento nella definizione di una grande potenza è quella che Gramsci chiama «tranquillità interna», ovvero il grado e l'intensità della funzione egemonica del gruppo dirigente dello Stato. Nella nota 15 egli scrive: «quanto più forte è l'apparato di polizia, tanto più debole è l'esercito e quanto più debole (cioè relativamente inutile) la polizia, tanto più forte è l'esercito» (Gramsci, 2007, p. 1577). Un apparato di polizia forte e che drena risorse pubbliche (sottraendole all'esercito) è indice della necessità del gruppo dominante di far ricorso alla coercizione in quanto è incapace di produrre consenso. Laddove invece è saldo il consenso dei gruppi egemonici e la conflittualità interna è più blanda, è più facile garantire l'ordine pubblico ed è possibile destinare maggiori risorse economiche all'esercito e allo sviluppo di tecnologie militari. Gramsci non sviluppa in queste note un'argomentazione in merito allo sviluppo economico-produttivo quale fattore di tranquillità interna, ma l'attenzione rivolta allo sviluppo economico che la transizione fordista sta garantendo agli Stati Uniti è indicativa di come egli ritenga che la tranquillità interna di un paese sia garantita anche dalla solidità del suo sistema produttivo, dalla ricchezza prodotta e redistribuita.

Nell'*incipit* della nota 19 (*ivi*, pp. 1597-8) Gramsci inoltre elenca tre criteri «per calcolare la gerarchia di potenza fra gli Stati»: 1) l'estensione del territorio, 2) la forza economica e 3) quella militare. Ma quanto egli scrive subito dopo ci chiarisce che intende questi tre criteri come delle precondizioni per il calcolo della gerarchia di potenza: «il modo in cui si esprime l'essere grande potenza è dato dalla possibilità di imprimere alla attività statale una direzione autonoma» nel campo internazionale, costringendo gli altri Stati a subire il suo influsso. Alla luce di questa specificazione – che rimuove ogni residuo di potenziale determinismo contenuto nel trittico così netto elencato all'inizio della nota – è possibile riassumere il pensiero di Gramsci in merito affermando che uno Stato dalla grande estensione territoriale, una solida forza economica ed un apparato militare numeroso e

tecnicamente all'avanguardia sarà più nelle condizioni di esercitare il proprio ruolo nell'arena internazionale con autonomia, senza limitarsi a reagire alle mutevoli contingenze.

La capacità di mantenere una linea politica coerente, basata su interessi stabili e strutturali (garantiti da una tranquillità interna che non li mette in discussione e ne favorisce la tutela e la promozione), rendono uno Stato capace di non essere influenzato dalle oscillazioni contingenti del sistema internazionale, ovvero lo rendono una grande potenza. «La linea di uno Stato egemonico», scrive Gramsci, «non oscilla, perché esso stesso determina la volontà altrui e non ne è determinato» (*ivi*, p. 1629): tale autonomia di decisione è un riflesso del suo ruolo centrale nel definire il sistema e l'equilibrio delle relazioni internazionali.

Coerentemente con queste premesse, Gramsci, nella nota 32, individua nella guerra un test decisivo per stabilire lo *status* di grande potenza (*cfr. ivi*, pp. 1628-9). Essa è infatti una potenzialità strutturalmente presente nelle relazioni internazionali. Negli anni in cui scrive Gramsci è ancora viva la memoria della *Grande guerra* che aveva ridefinito profondamente la gerarchia di potenze, facendo sparire dalla cartina geografica quattro grandi imperi, vedendo quella che agli inizi della guerra era la grande potenza germanica umiliata a Versailles e l'Italia ondivaga nel sistema di alleanze ed incapace, alla fine del conflitto, di trarre dall'essersi schierata con le potenze vincitrici gli sperati avanzamenti nella gerarchia di potenze. Sembra proprio che Gramsci parli in negativo del caso italiano quando scrive che «è grande potenza quello Stato che […] al momento della pace è riuscito a conservare un tale rapporto di forze con gli alleati da essere in grado di far mantenere i patti e le promesse fatte all'inizio della campagna». La capacità di mantenere una posizione dominante in un sistema di alleanze durante e dopo la guerra è cioè un criterio distintivo delle grandi potenze. Uno Stato che invece dipende fortemente dagli alleati per risorse militari e finanziarie non può essere considerato una vera grande potenza, quanto piuttosto un «fornitore di uomini» per coalizioni guidate da potenze che dispongono dei mezzi per sostenere sé stesse e gli alleati.

Nel quadro composito delineato da Gramsci in merito al concetto di grande potenza quindi convergono una pluralità di fattori: l'estensione territoriale, la potenza economica e quella militare – ovvero i tre fattori elencati dallo stesso autore dei *Quaderni* nella nota 19 –, la tranquillità interna e l'autonomia d'azione nel campo delle relazioni internazionali, che diventa evidente soprattutto in una condizione di guerra. Tra questa molteplicità di fattori ci concentreremo sulla potenza militare, consapevoli che rappresenti solo uno dei volti delle grandi potenze. Questa scelta, infatti, non è dovuta a una valutazione relativa a cosa Gramsci reputi più rilevante nel definire una grande potenza, ma alla volontà di concentrare in questa sede l'attenzione su una questione: le implicazioni che le trasformazioni del modo di condurre le guerre e delle tecnologie impiegate da Stati e attori non-statali hanno sulle relazioni internazionali e sulle gerarchie di potenza nel nostro tempo.

L'evoluzione del cyberwarfare

A partire dagli anni Novanta sempre più studiosi di strategia militare e di guerra hanno posto attenzione alle trasformazioni sul modo di condurre le guerre impostasi attraverso l'impiego militare delle tecnologie prodotte dalla rivoluzione digitale. I due studiosi americani John Arquilla e David Ronfeldt sono stati i primi a teorizzare un concetto che ha avuto una grande eco nel dibattito e che sottolinea il cambiamento del modo di condurre le guerre: quello di *cyberwarfare*. Entrambi sono stati a lungo (Arquilla a partire dagli anni Settanta, Ronfeldt dal decennio successivo) collaboratori della *RAND Corporation*, *think tank* americano fondato nel 1948 che collabora con il governo statunitense fornendo consulenze in merito alle politiche e strategie militari. In *Cyberwar is Coming!* – un testo del 1993 dichiaratamente finalizzato a ripensare le strategie americane all'indomani della guerra fredda e agli inizi della rivoluzione digitale – Arquilla e Ronfeldt hanno affermato che «il tipo di capacità bellica che immaginiamo potrebbe consentire all'America di proteggere sé stessa e i suoi alleati in tutto il mondo,

indipendentemente dalla dimensione e dalla forza dei futuri avversari» (Arquilla e Ronfeldt, 1997, p. 24[1]).

L'approccio dei due studiosi tuttavia non è ispirato ad un determinismo tecnologico: come essi scrivono, infatti, «non è la tecnologia in sé, ma piuttosto l'organizzazione della tecnologia, in senso ampio, a essere determinante» (*ivi*, p. 25). La fase storica in corso negli anni Novanta è descritta da Arquilla e Ronfeldt come contraddistinta dalla «rivoluzione dell'informazione» (*ibidem*) e dalla costante e progressiva diffusione di nuove tecnologie. Queste innovazioni, applicate all'ambito militare, stavano già causando e avrebbero continuato a causare secondo gli studiosi «cambiamenti sia nel modo in cui le società possono entrare in conflitto, sia nel modo in cui le loro forze armate possono condurre la guerra» (*ivi*, p. 27). Per descrivere questo cambio di scenario di cui era necessario prendere atto al più presto, in *Cyberwar is Coming!* vengono proposti due nuovi paradigmi per definire e pianificare la guerra: la *netwar* e, soprattutto, la *cyberwar*. Entrambe sono correlate alle *ITC*, ma differiscono per gli obiettivi che si propongono di raggiungere e per il grado di pervasività e distruzione.

Andando con ordine, la *netwar* riguarda «conflitti ideologici a livello sociale condotti in parte attraverso modalità di comunicazione in rete», ed ha l'obiettivo «di interrompere, danneggiare o modificare ciò che una popolazione target "sa" o crede di sapere su se stessa e sul mondo che la circonda» (pp. 27-8); essa può avvenire attraverso le reti digitali con operazioni finalizzate a realizzare campagne di propaganda e di destabilizzazione psicologica delle popolazioni coinvolte, causando interferenze con il sistema mediatico locale e persino infiltrazioni in reti e *database*.

La *cyberwar* invece riguarda la conduzione e preparazione di «operazioni militari basate sui principi dell'informazione», ha l'obiettivo di «interrompere, se non distruggere, i sistemi informativi e di comunicazione su cui un avversario fa affidamento» (*ivi*, p. 30). Il terreno geografico, centrale nella maggior parte delle strategie militari, passa in secondo piano nella *cyberwar* a favore del «cyberspazio,

[1] Le traduzioni delle citazioni tratte dal testo in questione, così come da tutti gli altri testi citati di cui non è disponibile un'edizione italiana, sono opera dell'autore del presente saggio.

che può essere dominato tramite tecnologie avanzate» (*ivi*, p. 44). Questa trasformazione, auspicavano Arquilla e Ronfeldt nel 1993, potrebbe sul lungo periodo far divenire sempre più rilevante la distruzione o la paralisi delle infrastrutture critiche del nemico, producendo la conseguenza che una vittoria militare potrebbe comportare un numero sempre più ridotto di vittime civili. La *I guerra del Golfo* – conclusasi solo due anni prima della pubblicazione di *Cyberwar is Coming!* – rappresentava per i due studiosi un importante avanzamento di questa trasformazione: essi citano l'importanza dell'«attacco degli elicotteri *Apache* contro i centri di controllo della difesa aerea irachena all'inizio della guerra» quale esempio di operazione militare che, integrando «elementi significativi della cyberwar», li utilizza come «moltiplicatori di forza» (*ivi*, p. 39).

Due ulteriori aspetti del testo di Arquilla e Ronfeldt meritano di essere sottolineati in questa sede. In primo luogo i due studiosi – evidenziando come le *ICT* applicate all'ambito militare costituiscano dei moltiplicatori di forza – sostenevano che ciò comprasse per gli Stati, i loro sistemi e le loro strategie militari, quella che il futuro *Segretario di Stato americano* Colin Powell (allora *Chairman of the Joint Chiefs of Staff*, incarico che rappresenta la più alta posizione militare all'interno delle Forze Armate degli Stati Uniti) definiva una «crescente dipendenza dalla tecnologia» (ivi, p. 51). L'implementazione di sistemi e strategie di *cyberwarfare*, *cyberdeterrence* e *cybersecurity* diventano quindi sempre più un investimento ineludibile per gli Stati. Inoltre i due studiosi evidenziavano come «la rivoluzione dell'informazione, nei suoi aspetti tecnologici e non tecnologici» (*ivi*, p. 26) stesse erodendo e sovvertendo le gerarchie su cui sino ad allora si erano basate le istituzioni «spesso a beneficio di attori più piccoli e deboli» (*ibid*). Tra questi Arquilla e Ronfeldt citano «terroristi internazionali, guerriglieri, cartelli del narcotraffico, fazioni etniche, gang tribali e razziali» (*ivi*, p. 40), cogliendo un aspetto che diventerà cruciale negli anni successivi: la rilevanza degli attori non-statali nelle operazioni di guerra.

Con la successiva proliferazione di attacchi cibernetici il *cyberwarfare* è diventato sempre più un aspetto decisivo nel modo di condurre le guerre e di mettere in opera strategie di deterrenza. Nello specifico, il caso *Stuxnet* del 2010 rappresenta uno spartiacque fondamentale: un *malware* altamente sofisticato sabotò il

programma nucleare iraniano, in particolare le centrifughe di arricchimento dell'uranio situate a Natanz, a sud di Teheran. Secondo un approfondito rapporto dell'*Institute for Science and International Security (ISIS)* basato su dati di monitoraggio dell'*IAEA* (Albright, Brannan e Walrond, 2011), l'Iran ha rimosso fino a 1.000 centrifughe presso l'impianto di Natanz tra la fine del 2009 e l'inizio del 2010, un evento che gli esperti (*cfr.* Singer, 2015) collegano proprio all'attacco *Stuxnet*. Essi ritengono che fosse il risultato di un'operazione congiunta tra gli Stati Uniti e Israele, sebbene mai confermata ufficialmente. Tale evento è considerato uno spartiacque nella storia degli attacchi cibernetici perché ha mostrato per la prima volta che questi potevano danneggiare non solo dati o infrastrutture informatiche ma anche causare danni fisici, mettendo a rischio la sicurezza nazionale senza l'uso di forze convenzionali.

Nel 2021 Arquilla ha scritto un altro importante testo intitolato *Bitskrieg: The New Challenge of Cyberwarfare*. Il concetto che dà il titolo al libro indica quello che lo studioso definisce «una sotto-categoria della guerra cibernetica», una dottrina militare che offre nuove «opportunità di condurre conflitti con piccole, agili, unità interconnesse di soldati, marinai, aviatori, hacker – e i loro compagni robotici d'armi». Quella in corso sarebbe una transizione dalla guerra di manovra (*Blitzkrieg*) ad un nuovo modo di condurre le battaglie utilizzando «una vasta gamma di […] nuovi strumenti» tecnologici. La transizione, scriveva Arquilla nel 2021, è ancora in corso perché queste innovazioni «sono state semplicemente incorporate o aggiunte alle pratiche più vecchie», e le implicazioni profonde del loro impiego sono in gran parte trascurate dalle autorità militari delle grandi potenze (Arquilla, 2021).

Il dibattito sulla portata del *cyberwarfare* è aperto, e come per tutti i fenomeni nuovi c'è il rischio di sopravvalutarne la portata. È quanto ad esempio ha sostenuto Thomas Rid, docente di *Studi Strategici* presso la *Johns Hopkins University*, nel suo libro del 2013 *Cyber War Will Not Take Place* (Rid, 2013). Basandosi sulla triplice caratterizzazione di un atto di guerra proposta da Carl von Clausewitz, Rid sostiene che un'azione per essere qualificata come un atto di guerra deve essere *i)* violenta, finalizzata a imporre al nemico la propria volontà, *ii)* strumentale ad un fine che si intende imporre al nemico attraverso l'atto violento stesso, *iii)* politica,

in quanto parte di una scopo più ampio rispetto alla vittoria di una singola battaglia, attuato da un'entità politica dotata di una volontà e un'intenzione articolate che devono essere trasmesse all'avversario e che vengono attribuite a una delle parti in conflitto. Evidenziava Rid nel 2013 che «non esiste nessun attacco informatico che soddisfi tutti e tre questi criteri» e «ben pochi» sono gli «attacchi informatici nella storia che soddisfano solo uno di questi criteri» (*ivi*, p. 4). Le crescenti aggressioni informatiche, sosteneva Rid, somigliano più ad atti di crimine che ad atti di guerra, in quanto «il crimine è per lo più apolitico», mentre «la guerra è sempre politica» e se «i criminali nascondono la loro identità», i soldati in uniforme invece «la espongono apertamente». Le «offese informatiche politiche», che Rid riconosce essere crescenti, non hanno bisogno di essere «violente per essere efficaci» e «strumentali per funzionare»; inoltre, gli aggressori, anche quando agiscono politicamente «è probabile che abbiano un interesse permanente o almeno temporaneo ad evitare l'attribuzione» (*ivi*, pp. 9-10).

Cyberwarfare nel conflitto russo-ucraino e nella guerra di Gaza

L'ultimo *Global Peace Index* pubblicato dall'*Institute for Economics & Peace* descrive un mondo che vive una fase di grande intensificazione dei conflitti militari. Nel 2022 più di 200mila persone sono morte a causa delle guerre: è il numero più alto dal 1994, anno del genocidio in Ruanda; sempre nello stesso anno ci sono stati 56 conflitti che hanno coinvolto almeno uno Stato: non si registrava un numero così alto addirittura dalla Seconda guerra mondiale. Grande spazio è dedicato nel rapporto al conflitto russo-ucraino ed alla guerra di Gaza, considerati paradigmatici di conflitti «inaccettabilmente devastanti, ma anche impossibili da vincere» (IEP, 2024, p. 50).

Il conflitto russo-ucraino è scoppiato dodici anni dopo il caso *Stuxnet*, mentre la guerra di Gaza tredici anni dopo: le pratiche e le strategie di *cyberwarfare* hanno in questi anni continuato a prender piede e a ricevere una quota sempre crescente dei finanziamenti che gli Stati destinano alle spese militari. Entrambi i suddetti conflitti sono rappresentativi di quanto il *cyberwarfare* sia diventata una

componente strutturalmente presente nei conflitti del XXI secolo, in quanto tutti gli attori coinvolti vi hanno fatto ricorso.

Passiamo in rassegna – senza pretesa di esaustività – alcuni eventi di *cyberwarfare* presenti in entrambi i conflitti, a partire da quello russo-ucraiano. Il 23 febbraio 2022, il giorno prima dell'invasione russa, un *malware* distruttivo noto come *HermeticWiper* ha infettato e reso inaccessibili i siti internet di istituzioni governative e diverse banche ucraine (Tidy, 2022; Fadda, 2022). L'indomani, un'ora prima dell'inizio dell'invasione russa, un attacco informatico ha preso di mira la rete satellitare *KA-SAT* gestita da *Viasat*, bloccando l'accesso alla linea internet a decine di migliaia di utenti ucraini e provocando danni anche in numerosi paesi europei. L'*Unione europea* e gli Stati membri hanno condannato ufficialmente l'accaduto, attribuendone la responsabilità alla *Federazione Russa* (Cyber Peace Institute, 2022; Consiglio dell'Unione europea, 2022).

All'indomani dello scoppio della guerra il governo ucraino ha annunciato di aver dato vita all'*IT Army of Ukraine*, un esercito di *hacker* volontari reclutati da tutto il mondo su *Telegram* (Pearson, 2022); in un mese gli iscritti al gruppo erano diventati oltre 300mila. Gli obiettivi presi di mira da questo esercito informatico volontario sono stati i siti web della *Borsa di Mosca* e della *Sberbank* (febbraio 2022), della *Loesk*, azienda fornitrice di energia elettrica nell'*oblast* di Leningrado (la cui fornitura è stata interrotta temporaneamente nell'ottobre 2022) e della *Gazprombank* (novembre 2022) (Render-Katolik, 2023). L'Ucraina ha inoltre adottato un approccio proattivo alla difesa cibernetica, sfruttando strumenti avanzati di automazione e AI – come ad esempio le piattaforme di *Threat Intelligence* – per riconoscere e contenere attacchi in tempo reale. Grandi player globali come *Microsoft* e *Google* hanno collaborato con le autorità ucraine, fornendo supporto e sistemi di rilevamento predittivo che hanno permesso di rilevare, limitare o neutralizzare alcuni attacchi cibernetici russi (Microsoft Threat Intelligence, 2022; Huntley, 2023).

L'integrazione e il simultaneo utilizzo di mezzi tradizionali di guerra – come un'invasione di terra – e mezzi cibernetici ha portato analisti e studiosi a definire il conflitto russo-ucraino una guerra ibrida, concetto alla cui formulazione ha dato un

contributo decisivo l'analista e studioso statunitense Frank Hoffman. In un rapporto per il *U.S. Marine Corps* Hoffman scriveva:

> Le «guerre ibride» fondono la letalità dei conflitti statali con il fervore fanatico e prolungato della guerra irregolare. Il termine «ibrido» indica sia la loro organizzazione che i loro mezzi. Dal punto di vista organizzativo, possono avere una struttura politica gerarchica, unita a cellule decentralizzate o unità tattiche in rete. Anche i loro mezzi saranno ibridi nella forma e nell'applicazione. In questi conflitti, i futuri avversari (Stati, gruppi sponsorizzati dallo Stato o attori autofinanziati) sfrutteranno l'accesso alle moderne capacità militari, tra cui sistemi di comando criptati, missili aria-superficie trasportabili dall'uomo e altri moderni sistemi letali, oltre a promuovere insurrezioni prolungate che impiegano imboscate, ordigni esplosivi improvvisati (IED) e omicidi coercitivi. Ciò potrebbe includere Stati che mescolano capacità ad alta tecnologia, come le armi anti-satellite, con il terrorismo e la guerra informatica diretta contro obiettivi finanziari (Hoffman, 2007, p. 28).

Una riflessione analoga sul cambio di paradigma in corso nella guerra e nella scienza militare è avvenuta anche in Russia, e ha avuto come protagonista Valery Gherasimov, *Capo di Stato Maggiore* delle *Forze Armate* della *Federazione Russa* dal 2012 e nominato nel gennaio 2023 *Comandante del Gruppo Congiunto delle Forze Russe* in Ucraina. In un articolo pubblicato il 27 febbraio 2013 sulla rivista russa *Военно-промышленный курьер* (*VPK – Corriere dell'Industria Militare*) con il titolo *Il valore della scienza risiede nella previsione*, il Generale Gherasimov ha presentato la sua visione sul mutamento in corso nelle strategie di *warfare* (Gherasimov, 2016). Visto il ruolo di primissimo piano ricoperto nella gerarchia militare russa, queste parole di Gherasimov hanno un grande valore per comprendere non solo quanto sia cambiata la guerra, ma anche la consapevolezza con la quale la *Federazione russa* sta combattendo sul fronte ucraino. In tale articolo Gherasimov evidenzia come il confine tra guerra e pace, nei conflitti militari del XXI secolo, sia diventato sempre più sfumato: «le guerre», scriveva il Generale, «non vengono più dichiarate e, una volta iniziate, procedono secondo un modello sconosciuto». In questo nuovo quadro «il ruolo dei mezzi non militari per il raggiungimento degli obiettivi politici e strategici è cresciuto e, in molti casi, ha superato in efficacia la potenza delle armi». Ed è per questo che egli sosteneva la necessità di integrare mezzi e strategie diverse tra loro, tra i quali anche e soprattutto «le nuove tecnologie informatiche» che «hanno permesso una significativa riduzione dei divari spaziali, temporali e informativi tra le forze e gli organi di

controllo». Le «nuove idee» e gli «approcci non convenzionali» sono diventati pertanto necessari per la scienza militare del XXI secolo, ed in tal senso Gherasimov concludeva l'articolo invocando la collaborazione tra lo *Stato Maggiore* russo e l'*Accademia delle Scienze Militari*, «che concentra i più importanti studiosi militari e gli specialisti più autorevoli» (*ivi*, pp. 24-9).

Lo scoppio dell'ennesimo capitolo del conflitto israelo-palestinese è stato anch'esso contraddistinto da partiche di *cyberwarfare* da entrambe le parti coinvolte. Numerosi gruppi di *hacktivisti* si sono mobilitati contro Israele, reclutando persone in tutto il mondo e coordinandoli su *Telegram* e altre piattaforme. All'inizio dell'*escalation* a Gaza il gruppo *hacktivista* pro-palestinese *AnonGhost* ha compromesso l'applicazione *Red Alert* – utilizzata da migliaia di israeliani per ricevere avvisi sui lanci di razzi – facendo recapitare agli utenti falsi avvisi di attacchi nucleari imminenti (Petkauskas, 2023). L'8 ottobre il sito del governo israeliano e quello del quotidiano *Jerusalem Post* sono stati oggetto di attacchi rivendicati rispettivamente dal gruppo filo-russo *KillNet* e da *Anonymous Sudan*, restando inaccessibili per alcune ore (Kobialka, 2023). Il 9 ottobre 2023 sono stati violati i sistemi di controllo di alcuni pannelli pubblicitari digitali a Tel Aviv, su cui sono comparse immagini e video propagandistici pro-Palestina, tra cui la bandiera israeliana in fiamme: degli spazi pubblici e visibili da migliaia di persone sono così stati trasformati in strumenti di propaganda visiva (Domingo, 2023). Il 23 dicembre 2021 il gruppo *CyberAv3ngers* ha rivendicato attacchi ai sistemi delle aziende energetiche israeliane; sebbene non ci siano stati gravi disservizi, questo attacco ha messo in allarme le autorità israeliane (Cybermaterial, 2023).

La sera del 27 ottobre, come documentato da *Amnesty International*, Israele ha imposto il *black-out* totale delle comunicazioni all'interno della *Striscia di Gaza* (Amnesty, 2023). Israele ha inoltre intensificato l'uso sistemi di intelligenza artificiale per monitorare costantemente la *Striscia di Gaza*, raccogliendo dati in tempo reale e identificando obiettivi strategici: tra questi sistemi vi è *Lavender* che calcola la percentuale di probabilità che un potenziale obiettivo sia membro di un gruppo militare, *Where's Daddy?* che ne traccia i movimenti e *Habsora* (ovvero, *il Vangelo*) che genera suggerimenti sugli edifici in cui questi potrebbero stazionare

e operare (*cfr.* Serhan, 2024; Sylvia, 2024). *Human Rights Watch* in un rapporto intitolato *Meta's Broken Promises: Systemic Censorship of Palestine Content*, ha inoltre documentato che tra l'ottobre ed il novembre del 2023 ci sono stati oltre 1.000 casi di rimozione ingiustificata di «contenuti pacifici a sostegno della Palestina», definendo la censura da parte di *Facebook* e *Instagram* «sistemica e globale». Il rapporto dichiara che «il governo israeliano è stato aggressivo nel cercare di rimuovere contenuti dai social media», denuncia una «mancanza di trasparenza riguardo alle richieste governative» ed inserisce tra le cause di questa politica messa in atto da *Meta* una «apparente deferenza alle richieste dei governi per la rimozione di contenuti, come le richieste della *Israel's Cyber Unit* e delle unità di segnalazione internet di altri paesi» (Human Rights Watch, 2023).

L'ex capo dell'intelligence militare israeliana e direttore dell'*Institute for National Security Studies (INSS)*, Amos Yadlin, in un articolo pubblicato su *Foreign Affairs* l'8 marzo 2024, ha sostenuto che «Israele deve adottare misure più ampie per evitare un altro 7 ottobre», in particolar modo ristabilendo la deterrenza, in quanto «il massacro del 7 ottobre ha dimostrato che i nemici di Israele non temono più le sue capacità militari come un tempo». Per prevenire minacce future, secondo Yadlin, «Israele deve rafforzare i suoi confini, migliorare la sua intelligence e modernizzare le sue capacità di difesa», nonché «essere pronta ad agire con decisione contro qualsiasi minaccia emergente, ristabilire la deterrenza e rafforzare le sue capacità di intelligence» (Yadlin, 2024).

Arquilla in un dibattito con il giornalista *Premio Pulitzer* Thomas Friedman svoltosi nel marzo del 2024 ha sostenuto che la guerra di Gaza rappresenti «una sorta di spartiacque che dimostra come una rete possa ora condurre una guerra contro una nazione»: mentre «Israele sta seguendo un approccio estremamente convenzionale a quella che è sostanzialmente una guerra irregolare», Hamas opera come una «*flat distributed network*», cioè una rete decentralizzata e orizzontale, composta non da grandi schieramenti militari ma da tante piccole formazioni. In questa nuova fase Arquilla riscontra una «corsa organizzativa per costruire legami con le reti», ed a riguardo cita la Russia che coltiva relazioni e offre rifugio a «vari *cyber-groups*, che ogni giorno compiono operazioni dannose». Arquilla parla inoltre di una lezione strategica che emerge sia dalla guerra a Gaza che dal conflitto

russo-ucraino: la necessità di ripensare l'industria militare con la consapevolezza che oggi «il contenuto informativo di un'arma conta più del suo contenuto esplosivo» (Arquilla, Friedman and Kator-Mubarez, 2024).

Le grandi potenze tra *cybersecurity* e *cyberwarfare*

In conclusione torniamo al nostro punto di partenza, ovvero a Gramsci. Come abbiamo visto all'inizio, l'autore dei *Quaderni* delinea un concetto di grande potenza che sembra mal conciliarsi con una metamorfosi della guerra nella quale attori non-statali riescono ad avere un ruolo così rilevante. In un'altra nota del *Quaderno 13* Gramsci individua il «tratto più caratteristico e significativo» della tecnica militare nel primo dopoguerra nella circostanza che «la tecnica militare in alcuni suoi aspetti tende a rendersi indipendente dal complesso della tecnica generale e a diventare un'attività a parte, autonoma». Se fino a prima della guerra che dette avvio al *Secolo breve* infatti, scrive sempre Gramsci, «la tecnica militare era una semplice applicazione specializzata della tecnica generale e pertanto la potenza militare di uno Stato o di un gruppo di Stati […] poteva essere calcolata con esattezza quasi matematica sulla base della potenza economica», all'indomani del conflitto «questo calcolo non [era] più possibile, […] e ciò costitu[ì] la più formidabile incognita dell'attuale situazione politico-militare». Come casi emblematici di questo mutamento Gramsci cita «il sottomarino, l'aeroplano da bombardamento, il gas e i mezzi chimici e batteriologici applicati alla guerra». Proponendo un caso di scuola introdotto dalla formula «ponendo la questione nei suoi termini limite, per assurdo», Gramsci evidenzia come tale evoluzione della tecnica militare potrebbe portare all'ipotesi che la piccolissima «Andorra [possa] produrre mezzi bellici in gas e bacteri da sterminare l'intera Francia» (Gramsci, 2007, pp. 1222-3).

Gramsci coglieva prima dell'avvento del digitale (e dell'atomica) un elemento fondamentale nello sviluppo della tecnica militare: il suo progressivo svincolarsi dal legame con lo sviluppo economico, con l'estensione territoriale e la composizione demografica di uno Stato, fattori che aveva individuato come condizioni, sebbene non sufficienti, fondamentali affinché uno Stato potesse

assurgere al rango di grande potenza. La tecnica militare cominciava a diventare un ambito dotato di una relativa autonomia da questi aspetti, e lo sviluppo del *cyberwarfare* ne è il capitolo estremo, con il protagonismo di attori non-statali e di gruppi di *hacktivisti* capaci di mettere a rischio la sicurezza nazionale di Stati sovrani. Questo, come abbiamo visto nel caso dei due conflitti in corso, non implica la fine della sovranità statale e delle grandi potenze, ma fa parte di una fase in cui la contesa sulla sicurezza digitale vede allo stesso tempo contrapposti e alleati attori statali e attori non-statali. La *cybersecurity* e la *cyberwarfare* rappresentano un campo sul quale gli Stati sono obbligati oggi a investire risorse, strutture ed uomini, ed in questo ambito quegli Stati che rispondono ai criteri individuati da Gramsci per definire le grandi potenze detengono un vantaggio competitivo rilevante ma non auto-sufficiente per garantirgli la conservazione di tale *status*.

Acknowledgments

Questo studio è stato cofinanziato dal Fondo Sociale Europeo REACT EU – Programma Operativo Nazionale (PON) Ricerca e innovazione 2014-2020 CCI2014IT6M2OP005 (Tematica azione IV.4 "Dottorati e contratti di ricerca su tematiche dell'Innovazione"), a titolarità del Ministero dell'Università e della Ricerca; programma di ricerca: Sviluppo della Cyber Intelligence attraverso l'analisi dell'egemonia geopolitica.

Bibliografia

Amnesty International (2023). Israele blocca le comunicazioni, rischio senza precedenti per i civili di Gaza, in *amnesty.it*, 28/10/2023, consultato il 19/12/2024 (https://www.amnesty.it/israele-blocca-le-comunicazioni-rischio-senza-precedenti-per-i-civili-di-gaza/).

Arrighi G. (1996). *Il lungo XX secolo: denaro, potere e le origini del nostro tempo*, Milano: Il Saggiatore.

Id. (1999). *I cicli sistemici di accumulazione: le trasformazioni egemoniche dell'economia-mondo capitalistica*, Soveria Mannelli (CZ): Rubbettino.

Id. (2008). *Adam Smith a Pechino: genealogie del ventunesimo secolo*, Milano: Feltrinelli.

Arrighi G., B. J. Silver *et al.* (2003). *Caos e governo del mondo: come cambiano le egemonie e gli equilibri planetari*, Milano: Bruno Mondadori.

Arquilla, J. (2021). *Bitskrieg: The New Challenge of Cyberwarfare*, Cambridge: Polity Press.

Arquilla J. and D. Ronfeldt (1997) [1993]. Cyberwar is Coming!, in J. Arquilla e D. Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica-Washington: RAND, pp. 23-60.

Consiglio dell'Unione europea (2022). Operazioni informatiche russe contro l'Ucraina: dichiarazione dell'alto rappresentante a nome dell'Unione europea, in *consilium.europa.eu/it*, consultato il 19/12/2024 (https://www.consilium.europa.eu/it/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/).

Cybermaterial, (2023). CyberAv3ngers Sells Israel Power Data, in *Cybermaterial.com*, 28/12/23, consultato il 19/12/2024 (https://cybermaterial.com/cyberav3ngers-sells-israel-power-data/).

Cyber Peace Institute, (2022). Case study: Viasat attack, in *cyberconflicts.cyberpeaceinstitute.org*, giugno 2022, consultato il 19/12/2024 (https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat).

Domingo A. (2023). Billboards in Israel Were Hacked to Display Pro-Hamas Content, in *Teachtimes.com*, 13/10/2023, consultato il 19/12/2024 (https://www.techtimes.com/articles/297488/20231013/billboards-israel-hacked-display-pro-hamas-content.htm).

Fadda D. e A. Longo (2022). HermeticWiper attacca l'Ucraina, allarme anche in Italia: come difendersi, in *cybersecurity360.it*, 24/02/22, consultato il 19/12/2024 (https://www.cybersecurity360.it/nuove-minacce/hermeticwiper-attacca-lucraina-allarme-anche-in-italia-come-difendersi/).

Filippini M. (2024). *Il realismo politico trasformativo*, Milano: Mimesis.

Gherasimov V. (2016) [2013]. The Value of Science Is in the Foresight, *MILITARY REVIEW*, January-February 2016, pp. 23-9.

Gramsci A. (2007). *Quaderni del carcere*. Torino: Einaudi.

Hoffman F. G. (2007), *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington: Potomac Institute for Policy Studies, consultato il 19/12/2024 (https://www.potomacinstitute.us/images/stories/publications/potomac_hybridwar_0108.pdf).

Human Rights Watch (2023), Meta: Systemic Censorship of Palestine Content, in *hrw.org*, 20/12/2023, consultato il 19/12/2024 (https://www.hrw.org/news/2023/12/20/meta-systemic-censorship-palestine-content).

Huntley S. (2023), La Nebbia della Guerra: come il conflitto in Ucraina ha trasformato il panorama delle minacce informatiche, in *Blog di Google Italia*, 24/02/2023, consultato il 19/12/2024 (https://blog.google/intl/it-it/notizie-aziendali/la-nebbia-della-guerra-come-il-conflitto-ucraino-ha-trasformato-il-panorama-delle-minacce-informatiche/).

IEP (2024), Global Peace Index 2024, in *economicsandpeace.org*, consultato il 19/12/2024 (link: https://www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf).

Kobialka (2023), Israel Cyberattacks: What MSSPs Need to Know, in *MMSPALER.com*, 10/10/2023, consultato il 19/12/2024 (https://www.msspalert.com/news/israel-cyberattacks-what-mssps-need-to-know).

Microsoft Threat Intelligence (2022). Report speciale: Ucraina, in *Microsoft | Security Insider*, 27/04/2022, consultato il 19/12/2024 (https://www.microsoft.com/it-it/security/security-insider/intelligence-reports/special-report-ukraine/).

Pearson J. (2022). Ukraine launches 'IT army,' takes aim at Russian cyberspace, in *Reuters*, 27/02/2022, consultato il 19/12/2024 (https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/).

Petkauskas V. (2023). Red Alert, Israel's rocket alert app, breached by hacktivists, in *Cybernews.com*, 15/11/2023, consultato il 19/12/2024 (https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas/).

Render-Katolik A. (2023). The IT Army of Ukraine, in *csis.org - Center for Strategic & International Studies*, 15/09/23, consultato il 19/12/2024 (https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine).

Rid T. (2013). *Cyber War Will Not Take Place*, Oxford: Oxford University Press.

Serhan Y. (2024), How Israel Uses AI in Gaza – And What It Might Mean for the Future of Warfare, in *Time*, 18/12/2024, consultato il 19/12/2024 (https://time.com/7202584/gaza-ukraine-ai-warfare/).

Singer P. W. (2015). Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons, *Case Western Reserve Journal of International Law*, 47 (1), pp. 79-86.

Sylvia N. (2024). Israel's Targeting AI: How Capable is It?, in *RUSI - The Royal United Services Institute for Defence and Security Studies*, 8/02/2024, consultato il 19/12/2024 (https://www.rusi.org/explore-our-research/publications/commentary/israels-targeting-ai-how-capable-it).

Wallerstein I. (1985). *Il capitalismo storico*, Torino: Einaudi.

Id. (1995). *Il sistema mondiale dell'economia moderna. III: L'era della seconda grande espansione dell'economia-mondo capitalistica, 1730-1840*, Bologna: Il Mulino.

Id. (1999). *Dopo il liberalismo*, Milano: Jaca Book.

Skocpol T. (1981) [1979]. *Stati e rivoluzioni sociali. Un'analisi comparata di Francia, Russia e Cina*, Bologna: Il Mulino.

Tidy J. (2022). Ukraine crisis: 'Wiper' discovered in latest cyber-attacks, in *BBC*, 24/02/2022, consultato il 19/12/2024 (https://www.bbc.com/news/technology-60500618).