Romina Gurashi

Dalla polvere al cyberspazio: come la terza ondata di modernizzazione sta riscrivendo le regole del conflitto

> Che la guerra non sia più necessaria non implica affatto condividere l'illusione che la guerra sia un retaggio atavico, tramandato dall'uomo delle caverne e di cui la nostra era illuminata si è alla fine liberata.
>
> Polanyi K., *Il significato della pace*, Bulletin, No. 3, 1938.

Abstract
Il contributo analizza la trasformazione dell'istituzione della guerra, avvalorando la tesi sempre più diffusa in campo sociologico dell'emergere di nuove forme di conflitto quali la cyberguerra, i conflitti cognitivi e i conflitti ibridi. In questo quadro, lo studio evidenzia l'esigenza di un approccio più strutturato per colmare le attuali lacune nella comprensione delle implicazioni su sicurezza, privacy, resilienza sociale e regolamentazione internazionale, ambiti in cui le conoscenze attuali restano frammentarie. Le conclusioni di questa ricerca offrono prospettive inedite sulle modalità con cui la terza ondata di modernizzazione sta riscrivendo le dinamiche conflittuali, ampliando i campi di battaglia fino a raggiungere il cyberspazio, e delineando nuove dinamiche di potere ed equilibrio. Tali conclusioni aprono nuove strade per interpretare e anticipare le sfide globali, evidenziando la necessità di adeguate politiche di difesa e collaborazione istituzionale internazionale in un contesto di crescente complessità.

Keywords: guerra; modernizzazione; cyberguerra.

1. L'evoluzione del conflitto: una questione di modernizzazione

Sebbene un numero crescente di studiosi abbia condannato la guerra come il flagello più distruttivo dell'umanità e invocato l'eliminazione dei conflitti armati come l'obiettivo più nobile delle società moderne (cfr. Walzer 1977; Galtung 1996), l'osservazione empirica dei cambiamenti avvenuti nei metodi di fare guerra nel corso dei secoli mostrano un gra-

Romina Gurashi, Sapienza Università degli Studi Internazionali di Roma, Italy, romina.gurashi@unint.eu DOI 10.61014/legamisocialiteoria/vol15/gurashi in *Oltre la seconda modernità*, F. Antonelli, A. M. P. Toti (a cura di), Published by Morlacchi Editore U.P., ISBN 978-88-9392-578-5 DOI 10.61014/legamisocialiteoria/vol15

duale ed inevitabile rafforzamento della sua presenza e vitalità. L'incursione militare della Federazione Russa in Ucraina, l'escalation del conflitto israelo-palestinese, le ostilità in Siria e il confronto armato nello Yemen, sono solo alcuni degli eventi più recenti che mostrano come, invece di scomparire, il conflitto abbia assunto nuove forme (cfr. Kaldor 1999; Scahill 2013).

La metamorfosi dalla guerra tradizionale – precedentemente caratterizzata principalmente dal confronto diretto tra gruppi militari su campi di battaglia geograficamente definiti – verso la guerra moderna segna una significativa evoluzione nelle sue manifestazioni. Le guerre odierne, infatti, si caratterizzano per l'integrazione di dimensioni quali la cyberguerra, il terrorismo, la guerra cognitiva e la guerra economica (cfr. Arquilla, Ronfeldt 1993; Singer, Friedman, 2014). Queste nuove forme di conflitto non sono solamente il riflesso degli avanzamenti tecnologici resi possibili dagli avanzamenti della scienza e della ricerca ma riflettono anche i cambiamenti nelle strategie politiche e nei paradigmi sociologici.

Nel suo saggio pionieristico *La terza ondata* (1980), Alvin Toffler propone una teoria della modernizzazione che si sviluppa attraverso tre distinte "ondate" evolutive caratterizzate da specifici salti qualitativi nelle strutture sociali, economiche e tecnologiche. Toffler colloca nell'ultima fase, quella della società post-industriale segnata dall'ascesa del capitalismo dell'informazione e della conoscenza come principali vettori di sviluppo, il contesto in cui la guerra si trasfigura in forme più elusive ma non per questo meno pervasive. Il lavoro di Toffler è stato ampiamente dibattuto e integrato da parte di altri studiosi (Castells 1996; Bell 1973) che hanno sottolineato come la società dell'informazione abbia radicalmente trasformato i contesti in cui il conflitto si manifesta.

L'applicazione del framework conoscitivo della "terza ondata di modernizzazione" all'analisi delle trasformazioni della guerra porta alla formulazione dell'ipotesi di ricerca di base secondo cui le tecnologie dell'informazione e della comunica-

zione non solo hanno ampliato il numero di coloro che possono innescare un conflitto su scala globale, ma hanno anche comportato un cambiamento delle strategie di guerra attribuendo nuova centralità della dimensione culturale-identitaria e un protagonismo inedito a nuovi attori che stanno contribuendo a riscrivere le regole e gli equilibri della conflittualità.

L'importanza di questa dimensione culturale-identitaria è stata già evidenziata da studiosi come Kaldor (1999), Duffield (2004), Malešević (2008), e assume ancor più peso oggi se si considera che, sempre più spesso, essa funge da strumento di guerra e, simultaneamente, anche da *casus belli*. Appare dunque importante riflettere su come la costruzione di narrazioni e l'affermazione di identità culturali non siano fenomeni nuovi nel panorama bellico e tuttavia, sulla scorta della digitalizzazione e della globalizzazione, stiano oggi contribuendo a cambiare il volto delle guerre radicalizzando le polarizzazioni etniche, religiose e culturali.

A questo proposito appare dunque imperativo domandarsi: in che modo la terza ondata di modernizzazione sta contribuendo a ridefinire i conflitti? Quali sono le implicazioni sociali e politiche di questo cambiamento? E, come le radicalizzazioni identitarie possano coniugarsi alla cyberguerra?

Alla luce di questi interrogativi, il presente articolo mira ad esplorare come l'impatto trasformativo su scala sociale e tecnologica della "terza ondata di modernizzazione" stia ridefinendo le regole del conflitto, spostando l'asse della guerra dai combattimenti sui campi di battaglia alla conflittualità ingaggiata nelle sfere digitale, cognitiva ed economica.

2. La terza ondata e il cambiamento dei paradigmi bellici

L'irruzione delle tecnologie dell'informazione e della comunicazione (TIC) nel dominio bellico ha determinato un'evoluzione paradigmatica che ha segnato la nascita di conflitti caratterizzati da obiettivi e modalità operative senza

precedenti. La prima e più importante conseguenza di questa transizione è stata lo spostamento dell'arena delle ostilità dallo spazio fisico, generalmente limitato e conosciuto, al cyberspazio, una dimensione virtuale governata da una logica che differisce significativamente da quella del mondo reale (Rid 2013; Libicki 2007). Questo spostamento ha avuto implicazioni non solo in termini di cambiamenti nella tecnica bellica, ma anche nella stessa definizione e riconcettualizzazione del campo di battaglia, che ora comprende una realtà virtuale ben più ampia in cui la guerra è un fenomeno ubiquo nello spazio e insidioso nei suoi effetti (Nissenbaum 2015).

La cyberguerra e la guerra informatica incarnano pienamente questa metamorfosi e dimostrano in maniera incontrovertibile come i progressi delle TIC abbiano ampliato, più o meno consapevolmente, il repertorio delle strategie belliche. Esempi specifici come l'invasione Russa dell'Ucraina e l'escalation del conflitto israelo-palestinese mostrano come i cyberattacchi abbiano assunto un ruolo centrale nella conduzione delle ostilità, influenzando direttamente l'esito dei combattimenti (Weimann 2015; Zetter 2016). Questi conflitti rivelano il potere del cyberspazio come teatro di operazioni che non si risolvono esclusivamente nel mondo virtuale ma si estendono, con conseguenze spesso devastanti, al mondo fisico impattando in modo diretto non solo su organizzazioni e istituzioni ma anche sui civili. Si pensi ad esempio all'attacco informatico lanciato da hacker russi ad Agosto 2022 contro la società Energoatom (Santora 2022), responsabile della gestione di tutti gli impianti nucleari dell'Ucraina, con il probabile scopo di causare un black-out in tutta la nazione[1] oppure all'attacco informatico condotto da hacker ucraini a Settembre 2022 contro il gruppo Wagner e che ha permesso loro di sottrarre dati e informazioni preziose sulle identità dei mercenari aderenti all'organizzazione (Ansa 2022).

1 La società era stata già oggetto di attacchi analoghi nel corso del 2015 e del 2016 e, in quelle occasioni, si erano verificati blackout diffusi.

Come questi avvenimenti hanno dimostrato, la spinta della modernizzazione ha cambiato radicalmente i contenuti del conflitto e, di conseguenza, anche gli attuali paradigmi di studio. Alcuni di questi nuovi contenuti sono:

- *Digitalizzazione e automazione del campo di battaglia*: per cui la guerra è diventata sempre più automatizzata e digitalizzata, con l'utilizzo di droni, sistemi autonomi, e cyber-operations (Singer e Friedman, 2014);
- *Cyberguerra*: vale a dire attacchi informatici condotti contro infrastrutture critiche nazionali e sistemi di informazione militari ai fini della conquista, della dissuasione, del conflitto e/o della competizione (Clarke, 2010);
- *Guerra ibrida*: ovvero l'integrazione di mezzi convenzionali, tattiche di guerriglia, attacchi cibernetici e guerra d'informazione, al fine di rendere meno chiara la distinzione tra stato di guerra e di pace (Hoffman, 2007);
- *Privatizzazione del conflitto*: con il crescente utilizzo di contractor, di società militari private o di gruppi criminali (Singer, 2008);
- *Etica e legislazione internazionale*: riguardanti le questioni etiche legate ai conflitti latenti, agli attacchi informatici cui non è possibile attribuire una responsabilità, all'uso dei dati e alla protezione dei civili (Walzer, 1977);
- *L'impatto dei media e dei social media*: che permette la manipolazione della percezione pubblica del conflitto, influenzando sia l'opinione pubblica che le decisioni politiche (Hoskins e O'Loughlin, 2010).

3. La cyberguerra e le sue implicazioni sociali

Nel quadro di questi cambiamenti paradigmatici della modernità, la cyberguerra merita quindi il posto d'onore.

Essa, infatti, rappresenta forse il fenomeno più emblematico della società post-industriale e rivoluziona le armi della guerra (ora digitali), i tempi (l'immediatezza) e i campi di battaglia (virtualmente infiniti e diversificati).

In virtù di questi caratteri e del suo *modus operandi* è possibile delineare una serie di costanti tipiche di questa forma di conflittualità. L'elemento forse più significativo e al contempo critico riguarda l'anonimato. In occasione di attacchi cibernetici, spesso risulta difficile se non addirittura impossibile individuare i responsabili dell'azione in assenza di rivendicazioni. Inoltre, a differenza dei conflitti tradizionali, che richiedono investimenti significativi in termini di risorse economiche e militari, la cyberguerra permette anche ad attori con risorse scarse o limitate (piccoli stati, gruppi non statali) di poter esercitare la loro influenza in ambiti specifici come, ad esempio, la manipolazione delle informazioni o di più ampia portata come la destabilizzazione sistemica di intere società (Rid, McBurney 2012). In questo senso, la cyberguerra può rappresentare sia uno strumento di *soft power* (volto ad influenzare l'opinione pubblica) sia di *hard power* (volto alla distruzione di infrastrutture strategiche), permettendo agli attori di esercitare la loro influenza in modi non convenzionali. Inoltre, la mancanza di un quadro legale internazionale chiaro e condiviso che regolamenti la liceità di determinate azioni, la loro eticità, i tipi di reazioni ammissibili, le relazioni tra gli attori, le modalità di azione (solo per citarne alcune) lascia spazio al far west delle interpretazioni e dei potenziali abusi.

In virtù degli strumenti tecnologici a disposizione, numerose sono le tipologie di attacco possibili. Tra queste è possibile enumerare senza avere la pretesa di essere esaustivi:

– *Malware*: vale a dire virus, worm, trojan, e ransomware progettati per infiltrarsi, danneggiare, o prendere il controllo dei sistemi informatici target;

– *Phishing e Social Engineering*: ovvero tecniche che mirano a ingannare gli utenti affinché rivelino informazioni

confidenziali, come password o dati di accesso, attraverso email ingannevoli, messaggi, o siti web falsificati;

- *Exploit e Zero-Day Attacks*: i primi sfruttano vulnerabilità note nei software per ottenere un accesso non autorizzato o per danneggiare un sistema, mentre i secondi sfruttano vulnerabilità non ancora note al pubblico o al produttore del software;
- *DDoS (Distributed Denial of Service)*: vale a dire attacchi che sovraccaricano i server o le reti con traffico fittizio, rendendoli inaccessibili agli utenti legittimi. Questi sono spesso realizzati attraverso reti di computer infetti (botnet);
- *APT (Advanced Persistent Threats)*: ovvero campagne di hacking mirate e sofisticate progettate per mantenere un lungo accesso clandestino a una rete per spiare o sottrarre informazioni sensibili;
- *Attacchi alla Supply Chain*: ovvero attacchi che mirano a compromettere i fornitori o i componenti di software e hardware al fine di accedere a reti o sistemi di destinazione più grandi e protette;
- *Spoofing e Man-in-the-Middle*: in altri termini, tecniche che intercettano o alterano la comunicazione tra due parti senza che queste se ne accorgano, permettendo agli aggressori di intercettare dati o inserire messaggi fraudolenti;
- *Hacking di dispositivi IoT (Internet of Things)*: ovvero attacchi a dispositivi connessi, come telecamere di sicurezza, termostati intelligenti, e veicoli, anche al fine di lanciare attacchi più ampi, spiare, o causare danni fisici.

A fronte della complessità di questi strumenti, le possibilità che un individuo, un gruppo o una intera società diventino vittima di violenza sono sempre più numerose. Un esempio emblematico di queste dinamiche si è verificato nel 2007,

quando l'Estonia ha subito una serie di attacchi DDoS che hanno colpito banche, media e istituzioni governative. Evento scatenante dell'attacco è stata la decisione del governo estone di rimuovere la statua del Soldato di Bronzo dal centro di Tallin per ricollocarla nel cimitero militare della città. Una scelta che aveva profonde implicazioni politico-sociali visto che la statua era stata eretta alla fine della Seconda Guerra Mondiale per commemorare i caduti sovietici dell'opposizione al nazismo e che si è tradotta in due giorni di guerriglia urbana alimentata dalla popolazione russofona, crisi diplomatica[2] e attacchi informatici probabilmente condotti da hacker russi (Del Re, 2009). L'evento ha spinto le istituzioni a riconsiderare il problema della sicurezza nazionale anche nella prospettiva della sicurezza digitale e ha rappresentato un vero e proprio spartiacque in termini di consapevolezza delle vulnerabilità cui sono esposte le società moderne.

Anche l'attacco al sistema di arricchimento dell'uranio iraniano mediante il worm "Stuxnet" nel 2010 ha rappresentato un momento di profondo ripensamento dei contenuti stessi della cyberguerra, dimostrando come, attraverso le tecnologie informatiche, sia oggi possibile non solo aggredire organizzazioni più o meno ampie e complesse, ma anche la più ampia capacità nucleare di uno Stato (Langner 2011). Il worm "Stuxnet", dopo essere stato inserito nel sistema tramite la pennetta usb di qualche dipendente, si è infiltrato in molti altri sistemi informatici e ha operato in tre fasi: scansione e bersaglio di reti e sistemi Windows, diffusione in tutta la rete e infine bersagliamento di sistemi specifici come gli impianti di arricchimento dell'uranio controllati da controllori logici programmabili (PLC). Si stima che questo worm possa aver distrutto 1000 centrifughe per l'arricchimento dell'uranio ovvero 30% dell'efficienza di arricchimento nucleare dell'Iran (Albright, Brannan, Walrond 2010).

2 Con la minaccia del Presidente della Federazione Russa, Vladimir Putin, di interrompere definitivamente le relazioni diplomatiche.

L'evento qui descritto è interessante per tre ordini di ragioni. In primo luogo, il cyberattacco agli impianti iraniani ha consentito di evitare un attacco militare tradizionale da parte di Israele che sentiva messa in discussione la sua sicurezza regionale, in secondo luogo, il successo dell'attacco operato congiuntamente da Stati Uniti ed Israele ha determinato la scelta del presidente americano Obama a incrementare il ricorso alle cyberarmi nella gestione di un grande numero di ulteriori situazioni delicate (Toniutti 2012), e, in terzo luogo, ha permesso per la prima volta di intravvedere un nuovo e ancor più preoccupante pericolo: la possibilità di perdere il controllo di infrastrutture vitali e di armamenti in grado di produrre effetti apocalittici. Uno spettro, questo, che unito a quello che aleggia sulla minaccia dell'uso di armi nucleari allo scopo della deterrenza, potrebbe incrementare i livelli di pericolo delle stesse popolazioni dei paesi che detengono o ospitano questo tipo di armamenti. Il paradosso che si potrebbe verificare è quindi quello per cui i paesi che detengono il maggior numero di armamenti tecnologici ai fini della sicurezza, in virtù della cyberguerra, possano divenire anche quelli maggiormente insicuri.

Come mostra l'analisi dello stato dell'arte sin qui svolta, l'attenzione del mondo accademico e scientifico è interamente proiettata verso lo studio dei caratteri tecnici dell'evoluzione della cyberguerra e delle conseguenti strategie di offesa e di difesa. A mancare, all'interno di questo quadro già di per se molto complesso e sfidante, è però la dimensione sociale, vale a dire l'attenzione alle implicazioni nella dimensione individuale e di gruppo.

È infatti innegabile che le costanti sin qui elencate possono avere delle importanti implicazioni in termini di:

– *Privacy e sicurezza dei dati*: la cyberguerra mette a rischio la privacy e la sicurezza dei dati personali dei cittadini, con potenziali ripercussioni sulla libertà individuale e sulla fiducia nelle istituzioni e nel digitale;

– *Accesso alle informazioni*: gli attacchi possono mirare a limitare l'accesso alle informazioni, manipolare o a censurare contenuti, influenzando la libertà di espressione e il diritto all'informazione;
– *Resilienza sociale*: la dipendenza dalle tecnologie digitali rende le società vulnerabili agli attacchi informatici, ed è quindi necessario stimolare lo sviluppo di una maggiore resilienza tramite l'educazione alla sicurezza informatica e la preparazione alle emergenze.

Le istituzioni si trovano quindi di fronte alla sfida di proteggere i cittadini non solo da potenziali danni fisici ma anche dal senso di insicurezza e vulnerabilità che accompagna la minaccia degli attacchi informatici.

4. Conclusioni

La natura evolutiva della cyberguerra, con le sue manifestazioni sempre più insidiose e raffinate, richiede un'urgente revisione della nostra interpretazione dei conflitti nell'ambito digitale. Le rivoluzioni indotte dalla "terza ondata di modernizzazione" hanno profondamente trasformato il panorama dei conflitti, sottolineando l'impellente bisogno di aggiornare le nostre strategie di difesa e sicurezza alle sfide emergenti in questo scenario inedito.

L'introduzione delle tecnologie informatiche e comunicative nel teatro di guerra ha notevolmente esteso le capacità di una vasta gamma di attori di innescare disordini, rivelando una dimensione bellica che, sebbene immateriale, produce conseguenze dirette e distruttive nel quotidiano di intere società. Gli attacchi informatici all'Estonia nel 2007 e l'operazione Stuxnet contro l'Iran nel 2010 rappresentano casi emblematici dell'impatto della cyberguerra sulla sicurezza nazionale e sull'equilibrio internazionale.

Di fronte a questa realtà, la prevenzione delle ricadute sociali dei cyberattacchi diventa una priorità. È fondamentale promuovere una cooperazione internazionale rafforzata e sviluppare normative e strumenti di controllo del comportamento degli Stati e degli attori non statali nel cyberspazio. Sebbene l'innovazione tecnologica sia una leva di progresso e benessere, essa incarna anche un rischio che non può essere contenuto esclusivamente tramite soluzioni tecnologiche. Sono necessari nuovi approcci politici, economici, sociali e culturali per circoscrivere l'influenza e l'ambito d'azione del cyberspazio.

In sintesi, la questione della cyberguerra sollecita una responsabilità collettiva nel riconsiderare la guerra e le sue ripercussioni nel mondo interconnesso di oggi. Rispondere efficacemente alle sfide presentate da questa modalità di conflitto esige un impegno comune a scala mondiale, mirato a costruire un avvenire in cui la tecnologia serva da baluardo per la pace e il benessere, invece che come mezzo di devastazione e divisione.

Riferimenti bibliografici

Albright, D., Brannan, P., Walrond, C.
2010, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*, Institute for Science and International Security Report, 22 Dicembre, documento disponibile al link: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (02/04/2024).

Ansa
2022, *Kiev: "Hackerato il sito del Gruppo Wagner, presi i dati dei mercenari"*, 19 Settembre, documento disponibile al link: https://www.ansa.it/sito/notizie/mondo/2022/09/19/kiev-hackerato-il-sito-del-gruppo-wagner-presi-i-dati-dei-mercenari_1a377ef5-0d60-4ea5-814a-7dc7536c648b.html (28/03/2024).

Arquilla, J., Ronfeldt, D.
1993, *Cyberwar is Coming!, Comparative Strategy*, Vol. 12, No. 2, pp. 141-165.

Bell, D.
1973, *The Coming of Post-Industrial Society*, Basic Books, New York.

Castells, M.
1996, *The Rise of the Network Society*, Blackwell Publishers, Singapore.

Clarke, R. A., Knake, R.
2010, *Cyber war: The next threat to national security and what to do about it*, Harper Collins, New York.

Del Re, E. C.
2009, *L'Estonia bloccata dal complesso della Russia*, «Limes. Eurussia, il nostro futuro?», No. 3, documento disponibile al link: https://www.limesonline.com/rivista/l-estonia-bloccata-dal-complesso-della-russia-14619321/ (28/03/2024)

Duffield, M.
2004, *Le guerre postmoderne. L'aiuto umanitario come tecnica politica di controllo*, Il Ponte, Bologna.

Galtung, J.
1996, *Peace by Peaceful Means: Peace and Conflict, Development and Civilization*, Thousand Oaks, Nuova Dheli, Sage Publications, Londra.

Hoffman, F. G.
2007, *Conflict in the 21st century: The rise of hybrid wars*, Potomac Institute for Policy Studies, Arlington.

Hoskins, A., O'Loughlin B.,
2010, *War and media: The emergence of diffused war*, Polity Press, Cambridge.

Kaldor, M.
1999, *Le nuove guerre. La violenza organizzata nell'età globale*, Carocci, Roma.

Langner, R.
2011, *Stuxnet: Dissecting a Cyberwarfare Weapon,* IEEE Security & Privacy, Vol. 9, No. 3, 49-51.

Libicki, M. C.
2007, *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, Cambridge.

Malešević, S.
2008, *The Sociology of New Wars? Assessing the Causes and Objectives of Contemporary Violent Conflicts*, International Political Sociology, Vol. 2, No. 2, 97-112.

Nissenbaum, H.
2015, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford.

Polanyi, K.
1938, *Il significato della pace*, Bulletin, No. 3.

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

Rid, T., McBurney, P., Cyber-Weapons
2012, *The RUSI Journal*, Vol. 157, No.1, 6-13.

Santora, M.
2022, *The operator of Ukraine's nuclear plants says it faced an ambitious cyberattack*, The New York Times, 16 Agosto, document disponibile al link: https://www.nytimes.com/2022/08/16/world/europe/the-operator-of-ukraines-nuclear-plants-says-it-faced-an-ambitious-cyberattack.html (28/03/2022).

Scahill, J.
2013, *Dirty Wars: The World is a Battlefield*, Nation Books, New York.

Singer, P. W.
2008, *Corporate warriors: The rise of the privatized military industry*, Cornell University Press, Ithaca.

Singer, P. W., Friedman, A.
2014, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, Oxford.

Toffler, A.
1980, *The Third Wave*, Bantam Books, New York.

Toniutti, T., Stuxnet
2012, *Israele e Usa dietro al virus. "Creato da noi, ci è sfuggito di mano"*, la Repubblica, 01 Giugno, documento disponibile al link: https://www.repubblica.it/tecnologia/2012/06/01/news/stuxnet_israele_e_usa_ammettono_creato_da_noi_ci_sfuggito_di_mano-36353500/ (28/03/2024)

Walzer, M.
1977, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, Basic Books, New York.

Weimann, G.
2015, *Terrorism in Cyberspace: The Next Generation*, Columbia University Press, New York.

Zetter, K.
Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Broadway Books, 2016.

Romina Gurashi, Ph.D. è Ricercatrice in Sociologia Generale (SPS/07) presso l'Università degli Studi Internazionali di Roma UNINT. Nell'ambito della European Sociological Association (ESA), è membro del Direttivo del Research Network 36 – Sociologia delle Trasformazioni: Oriente e Occidente mentre in Albania è Vicepresidente dell'Associazione Albanese di Sociologia (ALBSA). In Italia è membro del direttivo della sezione Teorie Sociologiche e Trasformazioni Sociali dell'Associazione Italiana di Sociologia (AIS). Tra i suoi temi di ricerca vi sono i processi di reciproca implicazione di pace e sviluppo sostenibile; macro, meso e micro processi di mutamento sociale legati alla sicurezza e la difesa; smart society e globalizzazione; conflitto e integrazione; teoria sociologica, anche classica; processi di riconoscimento sociale e identitario attraverso il Made in Italy.