ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

15
2022

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

15

ISSUE 1/2022

Milano 2022

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 1 – 15/2022

Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 978-88-9335-956-6

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

Russia-Ucraina: oltre la Guerra Ibrida, verso il Techno-Cognitive Warfare

Marco Lombardi

Marco Lombardi, director of ITSTIME research center, is full professor at the Catholic University of Sacred Heart, where he teaches Crisis management and risk communication, Mass Communication theory, Sociology, Intelligence and counter terrorism, Security policies. He is the director of the Dpt. of Sociology and member of the scientific board of the School of Doctorate, the masters in Cultural Diplomacy and the School of Journalism. He managed several EU founded research projects mainly focused on terrorism, security and crisis management. He co-operates with different institutional agencies involved on security both at national and international level.

Abstract

The Russian-Ukrainian conflict unexpectedly brought war to Europe.
At present (end of March 2022) I do not consider any conclusive scenario to be foreseeable: today the most optimistic forecast is contained in the uncertainty of an evolving event, for which everything is possible. But this brief note, which introduces others that follow dedicated to the conflict between Russia and Ukraine, focuses on what so far already constitutes predictably persistent results in the medium to long term.
Now we are at the Total Hybrid War in which the dimensions of the conflict overlap, interfere, produce an escalation of effects in different contexts: no conflict had yet unfolded in this articulated form, where they are no longer needed and the predictive and interpretative drivers of the scenarios fail. This is the first Total Hybrid War that has surpassed itself, paving the way for the now present Techno-Cognitive Warfare.
The characteristics of the Ukrainian Russian confrontation can be traced back to some emerging themes: the overlapping of the dimensions of the conflict; the centrality of strategic communication; the multiplication of actors in the field.
Although the conflict is still ongoing, however, some signs of permanent change are already evident. In the paper, I discuss only a few, which concern the change in the paradigm of the now techno-cognitive war, the broad re-modeling of the meaning of cyberspace, the central role of information and communication, and, also, a consequent different mode of negotiation between the parties to accelerate the peace process.
The conclusions add to the previous reflections two hopes.
The first concerns our capacity for de-escalation: wars, this one, in particular, has clearly shown how we can risk being stuck in a symmetrical process of escalation so that every action (in every dimension of the conflict) is answered with an action of a greater degree (in every other dimension of the conflict). It is a trap, also favored by technologies, which has configured an automatism, a practice of "taken for granted", which can only be interrupted by a conscious and responsible choice.

The second, which takes the form of advice, concerns the individual cognitive equipment that each one must assume for the governance of the flow of communication in which he is immersed. Therefore, I emphasize what I call the Principle of Maximum Protection:

- *any information is false until proven otherwise*.

and the Principle of Maximum Effectiveness:

- *every piece of information is true for its target audience*.

I expect a lasting more than ten years of the conflict that has just begun, albeit blanded and conveyed through actions that will focus on one or the other dimension (cyber, kinetic, economic, social, etc.) in an exclusive way, if those who will have to govern the confrontation will be able to avoid the simultaneous overlapping of the effects generated by the actions carried out in each dimension. In practice, we now need to learn to govern a widespread, subthreshold, and continuous global conflict: without surrendering to Cognitive Warfare as a replacement for "Peacefare".

Il conflitto russo-ucraino ha inaspettatamente portato la guerra in Europa.
Allo stato attuale (fine marzo 2022) non reputo prevedibile alcuno scenario conclusivo: oggi la previsione più ottimista è contenuta nell'incertezza di un evento in evoluzione, per il quale tutto è possibile. Ma questa breve nota, che ne introduce altre che seguono dedicate al conflitto tra Russia e Ucraina, si concentra su quanto finora già costituisce dei risultati prevedibilmente persistenti nel medio-lungo periodo.
Ora siamo alla Guerra Ibrida totale in cui le dimensioni del conflitto si sovrappongono, interferiscono, producono una escalation di effetti in contesti diversi: ancora non si era dispiegato in questa forma articolata alcun conflitto, dove non servono più e i driver predittivi e interpretativi degli scenari falliscono. Questa è la prima Guerra Ibrida Totale che ha superato sé stessa, aprendo la via all'ormai presente Guerra Tecno-Cognitiva.
Le caratteristiche del confronto russo ucraino possono essere ricondotte ad alcuni temi emergenti: il sovrapporsi delle dimensioni del conflitto; la centralità della comunicazione strategica; la moltiplicazione degli attori sul campo.
Benché a conflitto ancora in corso, tuttavia, alcuni segni di cambiamento permanente sono già evidenti. Nel paper mi soffermo solo su alcuni, che riguardano il cambiamento del paradigma della guerra ormai tecno-cognitiva, la ri-modellazione ampia del significato di spazio cibernetico, il ruolo centrale dell'informazione e comunicazione e, anche, una conseguente diversa modalità di negoziazione tra le parti per accelerare il processo di pace.
Le conclusioni aggiungono alle riflessioni precedenti due auspici.
Il primo riguarda la nostra capacità di *de-escalation*: le guerre, questa in particolare, ha mostrato con chiarezza come si possa rischiare di restare bloccati in un processo simmetrico di *escalation*, per cui a ogni azione (in ogni dimensione del conflitto) si risponde con una azione di grado maggiore (in ogni altra dimensione del conflitto). Il secondo, che assume la forma di un consiglio, riguarda l'attrezzatura cognitiva individuale che ciascuno deve assumere rispetto al governo del flusso di comunicazione in cui è immerso secondo il Principio di Massima Tutela e il Principio di Massima Efficacia.

Keywords

Hybrid Warfare, Cognitive Warfare, Cyberspace, Ukraine, Russia

1. Premessa

Il conflitto russo-ucraino ha inaspettatamente portato la guerra in Europa.

Allo stato attuale (fine marzo 2022) non reputo prevedibile alcuno scenario conclusivo: oggi la previsione più ottimista è contenuta nell'incertezza di un evento in evoluzione, per il quale tutto è possibile.

Ma questa breve nota, che ne introduce altre dedicate al conflitto tra Russia e Ucraina in questo volume di STS, si concentra su quanto finora già costituisce dei risultati prevedibilmente persistenti nel medio-lungo periodo.

Nessuno se lo sarebbe mai aspettato, anche se la Terza Guerra Mondiale era in corso da anni e definita a "capitoli" da Papa Francesco già nel 2014: finora, tuttavia, la percezione del conflitto era tenuta distante dalle opinioni pubbliche occidentali, perché gli "eserciti" si combattevano nelle terre espropriate ai cittadini: dalla Siria all'Afghanistan, dalla Libia all'Africa profonda le cosiddette Grandi Potenze si affrontavano quotidianamente via "proxy". Tutto questo era sufficiente a far sì che la distanza contenesse le paure delle rispettive popolazioni.

Improvvisamente, l'Ucraina è diventata la nuova terra di confronto ed essa è prossima, è di confine per l'Europa, non ci sono cuscinetti ad attutire il rombo dei cannoni. Così un drone che vola a 700 chilometri orari percorre in solitudine 1300km dall'Ucraina per schiantarsi in Croazia[1]: la facile mobilità di questi anni diventa protagonista di uno spazio minaccioso senza zone di mezzo che garantiscano distanze di sicurezza: oggi non basta uno stato serve forse un continente e un oceano a dividere blocchi di vecchia memoria.

Un'opinione pubblica che ha vissuto decenni di guerre lontane, percettivamente ed emotivamente filtrate dall'apparato mediatico, si rende improvvisamente conto che la guerra non ha a che fare con la giustizia ma con la sopravvivenza di chi si trova coinvolto, indipendentemente dalle ragioni.

A chi tocca gestire il conflitto è difficile rinunciare a interrogarsi sul "perché" della guerra, ma deve capire che, assumendo la necessaria prospettiva del crisis management, determinare le cause serve solo per comprendere meglio gli effetti da contenere non per attribuire colpe. Soprattutto adesso, che la costruzione della narrativa rassicurante – quella della guerra che non c'è perché lontana – è definitivamente crollata: per la prima volta abbiamo il completo spiegamento della Guerra Ibrida, finora teorizzata da alcuni, accettata da pochi, praticata diffusamente ma sempre dispiegando con discontinuità il suo potenziale. Furono così sia l'Afghanistan che la Siria, che la più articolata guerra al terrorismo, diffuso e connesso.

[1] https://www.ilfoglio.it/esteri/2022/03/11/video/un-vecchio-drone-militare-sovietico-si-e-schiantato-a-zagabria-in-croazia-3797541/

La Guerra Ibrida: più volte ho commentato questa definizione del conflitto, sostenendo – non da solo! – che si trattasse di un'evoluzione del modo di fare la guerra, caratterizzata da:

- incertezza delle norme che la regolano e, dunque, grande flessibilità tattica e strategica "oltre il limite";
- pluralità di attori (pubblici e privati) portatori di interessi specifici diversi e in conflitto tra loro per il successo, anche quando schierati dalla stessa parte;
- compresenza di asset concorrenti;
- essere una guerra delocalizzata, pervasiva e diffusa.

È proprio a partire dagli albori del conflitto Russo – Ucraino (2014) che si cominciò a definire questo scenario, spesso con grande difficoltà ad accettarlo sia a livello politico sia militare: in ogni caso esso spaventava perché, nella sua accezione, mostrava chiaramente come fosse già in corso una Terza Guerra Mondiale strisciante, cioè non riconoscibile utilizzando i canoni dei conflitti trascorsi, ma evidente negli obiettivi sottesi al confronto multidimensionale tra le potenze di questi anni.

Tutto questo era quanto avevamo definito Guerra Ibrida: senza regole, con una molteplicità di attori coinvolti e di asset impiegati. Ma oggi, le considerazioni iniziali che portarono ad elaborare questa definizione in sede NATO, non sono più sufficienti a contenere la varietà delle minacce. Finora, infatti, le diverse strategie si dispiegavano in "parallelo", attivando cioè interventi nella dimensione cyber piuttosto che in quella militare tradizionale, o ancora in quella comunicativa piuttosto che economica, con effetti che si manifestavano all'interno della dimensione originaria, adesso non è più così.

Ora siamo alla Guerra Ibrida Totale in cui le dimensioni del conflitto si sovrappongono, interferiscono, producono una escalation di effetti in contesti diversi: ancora non si era dispiegato in questa forma articolata alcun conflitto, dove le regole che finora sono servite per identificare il nemico (che non è necessariamente chi ti spara) non servono più e i driver predittivi e interpretativi degli scenari falliscono.

I segni della guerra russo-ucraina sono evidenti:

- Il primo segno, primo perché più banale, è nella presenza di tutte le dimensioni della guerra: terra, aria, mare, spazio e cyber. Queste dimensioni sono ormai simultaneamente presenti e reciprocamente interdipendenti nell'esercitarsi sul campo.
- Gli attori si sono moltiplicati a dismisura: gli eserciti ufficiali sono una piccola componente sul terreno. A questi si aggiungono milizie su base ideologica, religiosa, economica. E poi i volontari per costituire un corpo internazionale di risposta, in un campo che è condiviso da attori "*non conflict*" quali media e NGO. Ma soprattutto un attore è sempre più presente

da protagonista: la Pubblica Opinione, che è l'audience della guerra nella dimensione cyber.

- Il privato, nella forma dei nuovi super stati globali delle *major*, si schiera su più dimensioni per sfruttare i propri *asset*: le *major* della comunicazione adeguano i palinsesti alle diverse narrative e praticano forme di propaganda e di censura; altri limitano i servizi normalmente offerti, che possono essere utilizzati da parti in causa o, al contrario, le parti in gioco trovano inaspettate *backdoor* per un utilizzo creativo dei medesimi servizi: tutti in gioco.
- L'*asset* economico si è dispiegato con le sanzioni che colpiscono la quotidianità della vita di tutti, cercando di frantumare l'opinione pubblica russa, ma con effetti boomerang sulle opinioni nazionali. L'effetto complessivo dell'attacco economico ha ormai dato avvio a un nuovo assetto economico globale che sostituirà il precedente.
- La dimensione cyber, che finora era stata descritta come la Linea Maginot di difesa statica delle infrastrutture, finalmente si riconosce per le competenze multifunzione che implicano azioni che vanno dalla inibizione e distruzione dell'hardware primario, al sabotaggio nella erogazione dei servizi dipendenti dalla rete, fino all'impiego del cyberspazio, che in questa veste deve essere garantito operativo, per l'azione più massiccia di info-war mai dispiegata, che utilizza tutte le piattaforme digitali di comunicazione possibili.

Questa è la prima Guerra Ibrida Totale che ha superato sé stessa, aprendo la via all'ormai presente Guerra Tecno-Cognitiva.

2. Verso il Cognitive Warfare

2.1 Il sovrapporsi delle dimensioni

Come ho sostenuto, il conflitto ibrido finora si era mostrato nella sua complessità generata dal moltiplicarsi delle dimensioni: per esempio, da una parte l'incremento esplosivo del tipo delle formazioni combattenti e dall'altra le numerose strategie comunicative destinate alla conquista di "cuori e menti" dei pubblici.

Invece, di questa guerra si deve sottolineare non la simultaneità ma la sovrapposizione di dimensioni e *asset*, che richiede una strategia olistica e una interdipendenza profonda delle tattiche, governata da un sistema di comando che ha la sua competenza e forza nella dimensione cognitiva[2].

[2] https://www.itstime.it/w/guerre-future-la-nuova-centralita-dellintelligence-e-la-ridefinizione-dello-spazio-cibernetico-by-marco-lombardi/

La differenza tra le due prospettive è enorme. Se prima era difficile che una strategia di guerra comunicativa portasse a una reazione "*boot on the field*", adesso la sovrapposizione degli effetti (e l'aumento del rischio complessivo) è tale per cui a una narrativa può conseguire una risposta militare, in una sorta di reattività che sembra coinvolgere tutte le catene di comando e controllo. Eppure era atteso e scritto, da quando gli Stati Uniti avevano ben chiarito che un attacco a loro infrastrutture cibernetiche avrebbe potuto causare una reazione tradizionale (bombardamento) sull'origine della minaccia[3]. In perfetta sintonia con la Russia che, il 25 marzo 2022, ricorda con Andrei Krutskikh come "*un attacco informatico, sia esso accidentale o intenzionale, anche perpetrato sotto falsa bandiera, può facilmente portare a un'escalation, a uno scontro su vasta scala*"[4].

Questo significa che, in questo momento, non abbiamo nessuna sicurezza di poter sostenere che una minaccia, che per sua natura appartiene agli asset comunicativi della info-war del cyber, non possa trovare una risposta rapida in una azione che riguarda un *asset*/dimensione differente, per esempio sul campo.

Si tratta di una novità a cui il sistema politico e strategico è pericolosamente esposto perché ancora non c'è una dottrina adeguata a governare la Cognitive Warfare. Probabilmente per una pluralità di ragioni, non solo legate alla rapidità (costantemente invocata come causa) del cambiamento soprattutto delle tecnologie digitali, tra cui un conflitto generazionale nella catena di comando e controllo che contrappone i caratteri anagrafici dell'esperienza analogica ai *digital born*, giovani che anche non hanno nessuna consapevolezza del significato radicale di "Guerra Fredda", tornato ad avere senso interpretativo di questa realtà.

2.2 La comunicazione

Il paradigma della Guerra Ibrida, che aveva suggerito la persistenza di una Terza Guerra Mondiale in corso, aveva anticipato la prospettiva del *techno-cognitive confrontation* sottolineando la centralità della comunicazione nel warfare, evidenziata dalla sua autonomia rispetto alle altre armi: oggi la comunicazione non è corollario a un'azione di guerra ma è essa un'azione di guerra. Questa forma di conflitto, sperimentata oggi in Europa, arriva al "pubblico" nella sua forma mediata, cioè per gli effetti che ha sulla quotidianità prodotti

[3] https://www.itstime.it/w/guerra-ibrida-perche-avere-piu-paura-del-conflitto-russo-ucraino-by-marco-lombardi/

[4] https://www.ilgiornale.it/news/mondo/mosca-lancia-lallarme-garantire-sicurezza-informatica-2020898.html

dall'annientamento delle piattaforme di comunicazione e dalle capacità di interpretazione e comando, organizzata in una guerra di flusso (continua).

Ma questo è solo un aspetto in cui si declina la minaccia.

L'altro, a cui gli ultimi venti anni di terrorismo dovrebbero averci abituato, è lo scontro che avviene sfruttando e utilizzando il nuovo ecosistema digitale della comunicazione: in molti casi, si è già dimostrato, è controproducente attaccare l'infrastruttura che regge lo spazio cibernetico ma conviene penetrarla utilizzandola "ai limiti delle opportunità" per modificare i piani cognitivi e interpretativi sui cui si basa sia la presa di decisioni sia la produzione del consenso dell'avversario.

Questa logica è alla base della cyber war russo-ucraina che attacca infrastruttura e piattaforme, ruba identità e pone riscatti, promuove interpretazioni contro-dipendenti di realtà esclusivamente narrative: in questa guerra il ciberspazio ha cambiato forma, ampliandosi come luogo di opportunità anche per distribuire informazione "utile al nemico". Questa strategia si applica in un contesto favorevole perché come cittadini siamo più esposti, e perché come ogni situazione di incertezza richiede, ci offriamo più vulnerabili agli strumenti della comunicazione con il risultato di diventare fan e tifosi degli schieramenti, effetto cercato e voluto ovviamente dalle parti in conflitto: il mutarsi delle audience in tifoserie, per l'una o per l'altra squadra, modifica gli equilibri in campo e rende ben più difficile il negoziato.

L'obiettivo degli attori del conflitto è quello di costruire rappresentazioni nella Pubblica Opinione, che poi orienta la politica e le scelte. Russi e ucraini, pur con il medesimo scopo e con il medesimo uso strumentale della comunicazione, agiscono però in maniera diversa verso pubblici – *target audience* – diversi, ripetendo un format che ha il compito di consolidare lo zoccolo duro dei fan. Per alcuni, la maglietta militare del presidente ucraino diventa il simbolo della verità come per altri lo sono la cravatta e la maschera impassibile russa: si cade in trappola per il bisogno di avere qualcosa – qualcuno – a cui credere di fronte ad una realtà troppo complessa: vince il *brand*.

2.3 La moltiplicazione degli attori

Se la guerra ibrida è caratterizzata dalla molteplicità degli attori sul campo, lo schieramento in Ucraina supera ogni precedente storia: il combattimento, infatti, è ormai tra tanti gruppi, con la presenza di milizie straniere, tutti autonomi nel darsi le "buone ragioni" per il combattimento[5].

[5] https://www.itstime.it/w/ucraina-russia-ormai-e-troppo-tardi-by-gianluca-frinchillucci-e-marco-lombardi/

Il gruppo più conosciuto è sicuramente il Battaglione Azov, che fa parte dello schieramento ucraino, anche se le milizie di stampo neo-nazista sono varie[6]. Azov, con le sue parate e il suo stemma che ricorda Wolfsangel, ha dato il pretesto alla pubblicistica russa di definire gli ucraini nazisti. Ma non si tratta del solo gruppo con questa connotazione: per esempio sono anche emersi altri gruppi con riferimento alla divisione delle Waffen SS "Galizien".

Con l'Ucraina combatte anche una sorta di legione straniera con volontari provenienti da tutto il mondo e la Legione Georgiana, a cui ha aderito anche l'ex ministro della Difesa Irakli Okruashvili. Ma anche due battaglioni di ceceni, "Dzhokhar Dudaev" e "Sheikh Mansour", condividono la medesima parte dello schieramento.

Anche sul fronte russo ci si avvale di milizie che si ispirano per i simboli usati e per il linguaggio al Terzo Reich e al mondo del suprematismo bianco. Il Patriarca Kirill di Mosca e di tutte le Russie (lo scorso 6 marzo) nella Cattedrale di Cristo Salvatore nella capitale russa, ha sostenuto che: "*Siamo impegnati in una lotta che non ha un significato fisico, ma metafisico*". È con questa legittimazione che alcune milizie si ispirano proprio alla Chiesa Ortodossa Russa e combattono la loro battaglia contro gli ucraini, che sono l'avanguardia del corrotto mondo occidentale. Ma alle milizie ortodosse si aggiungono i mussulmani ceceni, guidati dal fanatismo religioso e dalla pratica terroristica in guerra, e i gruppi ultranazionalisti russi che si ispirano al movimento Pamyat. Tra i gruppi più attivi troviamo il Movimento Imperiale Russo che ha reclutato migliaia di volontari. Ma aggiungiamo, tra i vari, il Battaglione Sparta, una formazione armata che fa parte della Repubblica Popolare di Donetsk, e il Battaglione Svarozich, gruppo pagano di adoratori del dio slavo Svarog, poi assorbito dalla Brigata Vostok, nella quale si sono arruolati anche italiani, di varia estrazione ideologica. Questo agglomerato di combattenti, convive con una sorta di legione mercenaria in cui spicca la Wagner[7], ma a cui si aggiungono gli arruolamenti in corso in numerosi teatri di conflitto in cui la Russia è presente.

La domanda che sorge spontanea è: questa varietà reciproca di gruppi schierati sul campo in che modo risponde alla formale catena di comando e controllo? Quella stessa catena di comando che avrà il compito di "dichiarare la pace" e la fine dei combattimenti?

[6] https://www.itstime.it/w/wp-content/uploads/2022/02/Ukranian-Right-Wing-Armies.png

[7] https://wagnera.ru/

3. La lezione appresa

A conflitto ancora in corso, tuttavia, segni di cambiamento permanente sono già evidenti. Mi soffermo solo su alcuni, sui quali si dovrà tornare, che riguardano il cambiamento del paradigma della guerra ormai tecno-cognitiva, la ri-modellazione ampia del significato di spazio cibernetico, il ruolo centrale dell'informazione e comunicazione e una conseguente diversa modalità di negoziazione tra le parti per accelerare il processo di pace.

3.1 Techno-Cognitive Confrontation

Lo scenario del conflitto emergente è ormai quello del *techno-cognitive confrontation*, che ricorda la compresenza funzionale della dimensione tecnologica e di quella tipicamente umana della conoscenza e interpretazione e che esalta il ruolo del digitale: la capacità che esso ha di far transitare e trattare enormi quantità di informazioni massimizza il rischio che, bloccando l'infrastruttura si metta in crisi la catena decisionale. Questo scenario, è caratterizzato dalla variazione di velocità dei processi, che dunque richiederanno iper-rapidità nella presa di decisioni, e dalla enorme complessità dovuta all'aumento dell'informazione, ormai costituita da frammenti di bit correlati. Un'azione di adeguamento per governare efficacemente questo conflitto deve considerare lo spazio cibernetico come lo spazio di un nuovo ecosistema, superando la sintesi contenuta nell'idea di sistema socio-tecnico, per affermare quella più recente di eco-sistema digitale. Tutto questo non ha a che fare solo con la rapidità con cui si tramettono le informazioni, piuttosto con il processo interpretativo che necessita della consapevolezza della sua attuazione, nelle premesse e nelle conclusioni, per distinguersi dalla semplice reazione automatica all'evento. La domanda è come si ottiene questa capacità di simultaneità decisionale efficiente, intesa come una super velocità cognitiva e interpretativa, laddove esplode la compresenza di oggetti significativi: meno tempo, più segni deboli "che hanno senso in relazione tra loro", più modelli interpretativi possibili.

3.2 Un ciberspazio diverso

Il cyber warfare legato all'interpretazione della difesa delle strutture all'interno di un perimetro da tutelare è ampiamente superato, al punto che questa strategia finora prioritaria potrebbe rivelarsi controproducente in contesti che preferiscano una circolazione elevata di comunicazione pubblica. In questa prospettiva, il nuovo ciberspazio non è un'area tecnologica da perimetrare per massimizzarne la sicurezza ma è anche un'area da penetrare e utilizzare in quanto campo della comunicazione strategica: il bilanciamento tra queste

due prospettive è un aspetto del governo del conflitto nuovo ed emergente. Non solo: è assolutamente verosimile che, al di là di ogni accordo per la cessazione dei combattimenti "*on the field*" la guerra continui a lungo nella dimensione digitale[8]: proprio per questa primazia della comunicazione, nel mondo reticolarizzatto e iperconnesso, è opportuno cominciare considerare la persistenza di uno stato conflittuale da governare in continuum, che si esprime nel confronto tecno-cognitivo tra attori concorrenti.

3.3 Informazione e opinione pubblica

L'impiego delle strategie di info-war porta a due conclusioni che persisteranno.

La considerazione di partenza è che nel momento in cui il pubblico è convinto di partecipare a una guerra di informazione, rinuncia alla analisi in favore dello schieramento. Infatti, nelle situazioni di incertezza, la pluralità discordante di informazioni ne acuisce il bisogno riducendo la capacità interpretativa personale, favorendo invece l'appartenenza sulla base di emotività ed affettività. Infatti, il primo obiettivo per una strategia efficace di info-war è di convincere il pubblico di essere una vittima di "*fake news*": si tratta del primo passo per ancorarlo a rappresentazioni rassicuranti e persistenti, non necessariamente rappresentative della realtà, in cui la fiducia nel *brand* costituirà la ragione della propria appartenenza.

In questa prospettiva, dunque, la prima conclusione ci spinge ad abbandonare l'idea (fin troppo di moda in questi anni) di poter utilizzare il metodo OSInt (Open Source Intelligence) per acquisire informazioni utili in quanto tali, perché tutte le fonti risponderanno alle strategie dell'info-war. Le informazioni, in quanto dato di realtà, potranno in parte essere raccolte via HumInt e in SigInt. All'OSInt resta una diversa prospettiva: quella dell'analisi di "una pluralità di false narrative" per similitudini tra i medesimi oggetti tematizzati e per differenze tra gli oggetti delle narrative[9], non avendo l'obiettivo di raccogliere informazione ma di comprendere il "*mood*" che si vuole promuovere nell'opinione pubblica e le strategie comunicative dei contendenti.

[8] https://www.cybersecurity360.it/cybersecurity-nazionale/guerra-ibrida-biden-chiede-di-rafforzare-la-cyber-security-usa-quali-scenari/

[9] Non è obiettivo di questo paper discutere questo aspetto dell'OSInt nel contesto dell'info-war. Per chiarire la questione si può esemplificare: a) dando per scontato che l'informazione che circola è falsa; b) che è utile capire la diversità con cui gli attori in conflitto narrano i medesimi oggetti della comunicazione; c) quali siano per ciascun attore gli oggetti esclusivi della propria comunicazione; d) etc.. Tutto ciò con l'obiettivo limitato di comprendere per differenza/similitudine lo stato d'animo che si vuole produrre nell'opinione pubblica, da parte di ciascuna fonte, e non con l'obiettivo di raccogliere informazioni descrittive della realtà dei fenomeni.

La seconda conclusione afferma con forza l'Opinione Pubblica come uno strumento centrale del conflitto tecno-cognitivo: un importante protagonista che può essere sfruttato per esercitare pressione su *audience* diverse e sulla governance del conflitto e del quale si deve tener conto nelle pratiche diplomatiche di negoziazione.

La centralità della comunicazione in queste guerre permette di sostenere che la reputazione pesa come i cadaveri dei soldati e come la mancanza del pane: nel conflitto i tre fattori sono interlacciati: un attacco comunicativo produce la risposta di un carro armato o l'assalto al forno. E viceversa.

L'effetto di questa sovrapposizione definisce la qualità della vittoria o della sconfitta, perché non tutte le vittorie o le sconfitte sono uguali nelle loro conseguenze. Si tratta di dimensioni (comunicativa, economica, militare) che oltre che determinare la vittoria o la sconfitta in una guerra, soprattutto determinano la sopravvivenza politica dei sopravvissuti nel dopo guerra. Da questo la necessità, e l'urgenza, di utilizzare la comunicazione con la stessa attenzione delle tradizionali armi di distruzione di massa.

3.4 Nuove forme di negoziato

Nei prossimi anni ci si troverà davanti alle conseguenze dovute alla sostituzione delle due forme di conflitto: quello ibrido e quello tecno-cognitivo.

La moltiplicazione degli attori sul campo (Guerra Ibrida), schierati a combattere secondo interessi molteplici e diversi, rende assolutamente incerta la loro risposta alla catena di comando e controllo istituzionale con il risultato che, molto probabilmente, la dichiarazione di cessazione dei combattimenti sarà recepita funzionalmente da ciascuno sulla base degli interessi personali. È inevitabile che un teatro "ibridato" continui a essere interessato da un perdurante livello di conflitto "tra bande" sul campo.

Il protagonismo dell'Opinione Pubblica, destinataria delle strategie comunicative della guerra tecno-cognitiva, non permette di escluderla dalle pratiche diplomatiche di negoziato: l'attore protagonista (anche le vittime sono attori protagonisti) dell'info-war richiede una partecipazione propositiva fino all'ultima sequenza perché non può più rinunciare al ruolo che si è assunto nel conflitto: questo pubblico non può andare via in silenzio. È inevitabile, dunque, trovare nuovi processi e nuove formule negoziali partecipate che ridefiniscono le pratiche di formulazione dei trattati e della loro negoziazione.

4. Conclusioni

Anche se banale è utile ripetere che la guerra tra Russia e Ucraina ha sconvolto l'assetto globale del mondo. A queste brevi note, con cui ho voluto

cominciare per "fermare" alcuni punti di riflessione che stanno emergendo a conflitto ancora in corso, in quanto aspetti che caratterizzano il prossimo periodo di turbolenza dovuta a un confronto che perdurerà modellandosi per le opportunità che saranno offerte, aggiungo due auspici.

Il primo riguarda la nostra capacità di *de-escalation*: le guerre, questa in particolare, ha mostrato con chiarezza come si possa rischiare di restare bloccati in un processo simmetrico di *escalation*, per cui a ogni azione (in ogni dimensione del conflitto) si risponde con una azione di grado maggiore (in ogni altra dimensione del conflitto). Si tratta di una trappola, favorita anche dalle tecnologie, che ha configurato un automatismo, una pratica del "dato per scontato", che non può che essere interrotta da una scelta consapevole e responsabile.

Il secondo, che assume la forma di un consiglio, riguarda l'attrezzatura cognitiva individuale che ciascuno deve assumere rispetto al governo del flusso di comunicazione in cui è immerso. Dunque, sottolineo quello che io chiamo il Principio di Massima Tutela:

- *ogni informazione è falsa fino a prova contraria*.

e il Principio di Massima Efficacia:

- *ogni informazione è vera per la sua target-audience*.

Confido maggiormente nella responsabilità che affido a ciascuno con l'applicazione dei due principi proposti, che non in una strategia complessiva di *de-escalation*.

Piuttosto, mi aspetto un perdurare ultradecennale del conflitto da poco cominciato, seppur blandito e veicolato attraverso azioni che si concentreranno sull'una o sull'altra dimensione (cyber, cinetica, economica, sociale, etc.) in maniera esclusiva, se chi dovrà governare il confronto sarà capace di evitare la sovrapposizione simultanea degli effetti generati dalle azioni condotte in ciascuna dimensione.

In pratica, ormai abbiamo la necessità di imparare a governare un conflitto globale diffuso, sottosoglia e continuo: senza arrendersi al Cognitive Warfare in sostituzione del "Peacefare".

References

https://www.ilfoglio.it/esteri/2022/03/11/video/un-vecchio-drone-militare-sovietico-si-e-schiantato-a-zagabria-in-croazia-3797541/

https://www.itstime.it/w/guerre-future-la-nuova-centralita-dellintelligence-e-la-ridefinizione-dello-spazio-cibernetico-by-marco-lombardi/

https://www.itstime.it/w/guerra-ibrida-perche-avere-piu-paura-del-conflitto-russo-ucraino-by-marco-lombardi/

https://www.ilgiornale.it/news/mondo/mosca-lancia-lallarme-garantire-sicurezza-informatica-2020898.html
https://www.itstime.it/w/ucraina-russia-ormai-e-troppo-tardi-by-gianluca-frinchilluc-ci-e-marco-lombardi/
https://www.itstime.it/w/wp-content/uploads/2022/02/Ukranian-Right-Wing-Armies.png
https://wagnera.ru/
https://www.cybersecurity360.it/cybersecurity-nazionale/guerra-ibrida-biden-chiede-di-rafforzare-la-cyber-security-usa-quali-scenari/

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-9335-956-6

Euro 20,00