CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Istituto Superiore di Stato Maggiore Interforze
25° Corso – 3ª Sezione – 12° Gruppo di Lavoro

La "socializzazione del conflitto" nel modern warfare

(AS-SMD-03)

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.

L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e cyber security; Giuridica.

L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.

L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche.

L'IRAD si avvale altresì per le attività d'istituto di personale qualificato "ricercatore della Difesa, oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato.

L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore dalla Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.

CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Istituto Superiore di Stato Maggiore Interforze
25° Corso – 3ª Sezione – 12° Gruppo di Lavoro

La "socializzazione del conflitto" nel modern warfare

(AS-SMD-03)

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dell'autore, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali l'autore stesso appartiene.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

Questo volume è stato curato dall'**Ufficio Studi, Analisi e Innovazione dell'IRAD**.

Direttore
Gen. B. Gualtiero Iacono

Capo dell'Ufficio Studi, Analisi e Innovazione
Col. AArnn Pil. Loris Tabacchi

Progetto grafico
1° Mar. Massimo Lanfranco – C° 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello

Revisione e coordinamento
C.V. Massimo GARDINI – S.Ten. Elena Picchi – Funz. Amm. Aurora Buttinelli – Ass. Amm. Anna Rita Marra

Autore
ISSMI – 25º Corso 3ª Sezione 12º Gruppo di Lavoro

Stampato dalla Tipografia del Centro Alti Studi per la Difesa

Istituto di Ricerca e Analisi della Difesa
Ufficio Studi, Analisi e Innovazione
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3205
e-mail: irad.usai.capo@casd.difesa.it

chiusa a gennaio 2024

ISBN 979-12-5515-075-6

CENTRO ALTI STUDI PER LA DIFESA

ISTITUTO SUPERIORE DI STATO MAGGIORE INTERFORZE

25° CORSO SUPERIORE DI STATO MAGGIORE INTERFORZE

3ª Sezione - 12° GdL

La "socializzazione del conflitto" nel *modern warfare*

TESI DI GRUPPO

Anno Accademico 2022 – 2023

COMPOSIZIONE DEL GRUPPO DI LAVORO

C.C. (MM)	ARA	Stefano	Presidente
C.F. (MM)	TORTORIELLO	Enrico	Segretario
Col. (MLI)	MARICO	Dassè	Membro
Ten.Col. (AM)	SGAMBATI	Daniele	Membro
Magg. (AM)	MORLANDO	Raffaele	Membro
Magg. (AM)	MONTICELLI	Antonio	Membro
C.C. (FRA)	W. JAUREGUIBERRY	Paul-A.	Membro
Magg. (EI)	COLELLA	Gianfabio	Membro
Magg. (EI)	NEGRI	Barbara	Membro
Magg. (EI)	GIACOIA	Gerardo	Membro
Magg. (EI)	NARDI	Marco	Membro
Magg. (EI)	SCULCO	Domenico	Membro

INDICE

ABSTRACT

La realtà nella quale ci troviamo appare purtroppo assai lontana da quella rappresentazione euforica del XXI secolo alla base del progetto di costruzione del "Nuovo Ordine Internazionale liberale", che immaginava quest'epoca quale il migliore dei mondi possibili della storia dell'umanità. L'implosione di questo processo ha lasciato sul campo un complesso quadro geostrategico caratterizzato da una fluidificazione della gerarchia con la creazione di spazi di opportunità per le potenze emergenti non più acquiescenti, con il risultato di un marcato riequilibrio del potere in chiave multipolare. Accanto a queste, emergono sempre più potenti ed influenti attori non statuali, quali organizzazioni non governative (ONG), aziende private, società di sicurezza, gruppi organizzati, singoli individui. Diffusi squilibri economici, migrazioni incontrollate spinte da sempre più marcati cambiamenti climatici, organizzazioni transnazionali di stampo terroristico tenaci e resilienti e la crisi endogena di Paesi tradizionalmente solidi stanno influendo sempre più nella società, frammentando la coesione interna e polarizzando gli schieramenti. Ne consegue una realtà fortemente instabile, inquieta, caratterizzata da un deciso aumento della conflittualità sia essa in forma di guerra tradizionale, fino a poco tempo fa ritenuta irripetibile, che di scontro non lineare, spesso sottosoglia.

La spinta propulsiva delle *Emerging and Disruptive Technologies* (EDTs), la rapida evoluzione delle tecnologie e la loro progressiva e capillare diffusione, hanno definitivamente esteso le aree del conflitto ai nuovi domini *cyber* e *space*. Il ruolo dirompente che le nuove tecnologie stanno rivestendo nelle ostilità moderne e la loro natura estremamente duale hanno facilitato la partecipazione di un numero consistente di individui, spesso comuni cittadini, in possesso di strumenti innovativi estremamente efficaci e potenzialmente determinanti. Chi possiede queste tecnologie, sia essa un consorzio privato o un'azienda guidata da un singolo individuo, diviene estremamente influente nell'orientare le sorti del conflitto. Questo coinvolgimento massivo della popolazione è il cosiddetto fenomeno della "socializzazione del conflitto".

Sempre più civili, dunque, prendono parte alle ostilità, come soggetti attivi e passivi e, attraverso l'uso delle nuove tecnologie dell'informazione, vengono attratti, informati, influenzati, addestrati e coinvolti. *Social media* e applicazioni digitali sono i nuovi spazi e i nuovi strumenti della propaganda; essi rivestono un'importanza strategica sia nell'orientare le masse, spingendole ad agire per una o l'altra parte in conflitto sia fungendo da canale alternativo per il coordinamento della resistenza e la diffusione di *intelligence*. Alle modalità

classiche della guerra tradizionale, ecco che uno Stato, grazie a queste tecnologie, si trova ad avere nuovi strumenti a cui attingere, in grado spesso di mantenere il confronto al di sotto dello scontro aperto, in cui ad operare possono essere soggetti terzi, rendendo poi difficile l'attribuzione della paternità dell'azione. Azioni convenzionali e asimmetriche vengono così accoppiate in quella che è definita guerra non lineare, all'interno della quale il *Cognitive Warfare* assume fondamentale rilevanza per influenzare la popolazione e destabilizzare la struttura su cui poggia il sistema avversario, alterando la maniera in cui esso pensa e agisce: nei cittadini è riconosciuta, infatti, la potenzialità di influenzare le politiche di uno Stato, di indirizzarne l'operato e, in definitiva, di determinare successi o fallimenti.

Le masse, in un contesto di conflitto diffuso, "socializzato", siano esse costituite dai propri cittadini, da quelli avversari o da terzi, appaiono dunque essere il vero e proprio ago della bilancia. La resilienza di un Paese è impensabile si basi solamente sulle proprie Forze armate, bensì è dal sistema Paese che esso tra la vera forza, concretizzata dall'insieme di tutte le risorse, le potenzialità e le capacità che solo un insieme coeso di cittadini può mettere assieme nel momento assume un ruolo attivo.

Dal conflitto russo ucraino emerge inequivocabile il ruolo chiave di una resistenza organizzata, votata alla causa, consapevole della propria identità valoriale e preparata alla minaccia.

Di fronte al ritorno in Europa di un sanguinoso conflitto come quello a cui stiamo assistendo, viene da chiedersi se l'Italia sia preparata ad affrontare una potenziale invasione nemica nel proprio territorio. Da un'attenta analisi ne scaturisce la necessità di orientare in maniera coordinata tutti gli sforzi del sistema Paese al fine di creare i presupposti per incanalare i contributi della società civile per la Difesa nazionale. Un'organizzazione efficace di resistenza deve infatti prevedere una partecipazione sentita e consapevole della popolazione che lasci da parte i propri individualismi a favore del bene comune. Per far ciò si rende necessario, quindi, per l'Italia aumentare la propria resilienza affiancando alle Forze armate professionistiche, gruppi di civili opportunamente addestrati ed in grado di condurre operazioni di resistenza. Nondimeno risulta fondamentale creare una base valoriale condivisa e una coscienza nazionale, capace di incidere in maniera positiva sulla resilienza e sulle motivazioni della popolazione a resistere che, come evidenziato dal recente conflitto russo-ucraino, insieme al supporto esterno, risultano cruciali per una resistenza di successo.

INTRODUZIONE

La “socializzazione del conflitto” va intesa come la partecipazione alle ostilità della società civile. Già durante la II guerra mondiale in Francia, dopo l’invasione tedesca, gruppi armati composti da cittadini presero parte agli scontri bellici con azioni asimmetriche. Alcuni di questi confluirono in partiti politici che governarono il Paese negli anni successivi alla cessazione del conflitto mondiale. La popolazione e le milizie non regolari sono state anche protagoniste di movimenti di resistenza e attività di guerriglia che negli ultimi due secoli hanno preminentemente interessato il continente africano e il Medio Oriente. In merito, la dottrina e la letteratura militare hanno cercato di descrivere e modellizzare il fenomeno: ne sono un esempio il testo “Guerriglia” del tenente colonnello Thomas Edward Lawrence o il libro “*Small Wars*” scritto dal generale dell’esercito britannico Charles Edward Callwell. Oggi si assiste, tuttavia, a una sempre più massiccia partecipazione della società ai conflitti e al propagarsi di minacce cosiddette ibride perpetrate da attori di diversa natura (statuali e non), che spesso si estrinsecano in lunghe e mutevoli conflittualità spesso combattute sottosoglia[1]. L’oggetto di questo elaborato è quello di descrivere il fenomeno odierno della “socializzazione del conflitto”, ponendosi l’obiettivo di documentare come le mutazioni della società, la fruibilità della tecnologia duale, l’avvento di Internet e delle piattaforme *social* abbiano contribuito alla proliferazione di conflitti con caratteristiche del tutto nuove. Viene meno il confine tra pace e guerra, tra interno ed esterno, tra pubblico e privato, tra attore civile e militare. Le componenti politiche, militari, economiche e sociali si intrecciano tra loro in maniera fluida e determinano la necessità per uno Stato di approcciare la guerra in ottica multi-dominio e multilivello, in cui gli obiettivi militari devono essere perseguiti tenendo in considerazione sia la natura dei partecipanti sia le esigenze della popolazione. Per far ciò si è deciso di procedere analizzando sia informazioni e dati da fonti *open source*, sia il documento di dottrina militare denominato *Resistance Operating Concept* (ROC), sviluppato dallo *Special Operations Command Europe* (SOCEUR), che ha come oggetto l’organizzazione di movimenti di resistenza nazionali preparati e motivati. In questa tesi, strutturata in quattro capitoli, si affronteranno dapprima i fattori che stanno generando profondi mutamenti e divisioni nelle società moderne, per poi analizzare il ruolo nelle ostilità di attori del tutto nuovi, appartenenti alla società civile. Verranno in seguito analizzate le tecnologie duali e i *social network,* che costituiscono un *booster* per la partecipazione dei cittadini ai conflitti, oltre a determinare profondi cambiamenti nella conduzione delle ostilità.

[1] L’obiettivo primario è poter vincere senza combattere, erodendo la determinazione, la volontà e il sistema di consenso dell’avversario, attraverso azioni che si pongono nella zona (cd. *grey zone vds Cambridge Dictionary*) posta al di sotto della soglia che indurrebbe una risposta di tipo militare o economica.

Infine, nei due capitoli finali, si esamineranno le tattiche non lineari russe, utilizzate a partire dall'invasione della Crimea del 2014 e come la dottrina militare occidentale abbia cercato di contrastarle attraverso l'elaborazione del ROC. Tutto ciò sarà funzionale a valutare come, nel *modern warfare,* le diverse parti della società interagiscono con gli attori statuali e non al fine di trarre spunti e considerazioni sulle opportunità che scaturiscono dalla crescente "socializzazione del conflitto".

CAPITOLO 1

Evoluzione della società moderna e interazione nei conflitti

1. Inquadramento geostrategico

Dopo la fine della Guerra Fredda, è comparso sulla scena globale il "Nuovo Ordine Internazionale liberale"[2], caratterizzato dallo strapotere degli Stati Uniti e dall'assenza di *competitor* e attori di tipo regionale che agissero con attivismo e assertività.

Negli ultimi anni, però, si sta assistendo a un radicale cambiamento nello scacchiere mondiale. L'impotenza della *multi-level governance* nella gestione della crisi, unita alla progressiva volontà degli USA di svincolarsi dagli impegni internazionali (*retrenchment*), ha creato le condizioni per la comparsa di nuovi attori alla ricerca di potere e prestigio (*status seeker*). I singoli Stati perseguono agende autonome e disomogenee, stringendo alleanze fluide, spesso dettate da interessi contingenti. Si assiste, in sostanza, alla graduale regionalizzazione dell'ordine mondiale, contraddistinto da elevata competitività e conflittualità[3].

Gli interessi delle maggiori potenze si intrecciano e si scontrano con le aspirazioni degli attori regionali dando vita ad una sorta di perenne contesa condotta per lo più attraverso azioni ostili sottosoglia, trasversali, con un approccio multi-dominio e multilivello.

Inoltre, le *Organized Crime Organization*, la pirateria e le *Violent Extremist Organization* (VEO)[4] continuano a costituire una minaccia reale, diffusa e imminente per le società e le economie dei Paesi.

Tra le regioni maggiormente instabili si annovera il Mediterraneo, epicentro globale di interessi geopolitici ed economici, anche per la presenza di importanti risorse energetiche. Un'altra regione particolarmente caratterizzata da un fragile equilibrio interno è il continente africano. In particolare, nel Sahel, la precaria situazione economica, istituzionale e sociale ha favorito il proliferare di gruppi terroristici di matrice jihadista che hanno approfittato dell'instabilità politica creatasi a seguito dei colpi di Stato in diversi Paesi della regione. La complessa situazione del continente africano rende difficile il processo di stabilizzazione e, sino ad ora, gli sforzi mossi dalle organizzazioni internazionali in tal senso sono risultati vani.

Nel Grande Medio Oriente, il ritiro delle missioni di *peace-keeping* in Iraq e Afghanistan ha riportato alla luce problemi irrisolti e conflittualità interne. I talebani, tornati al potere,

---

2 Cfr. - AA.VV., "Ordine globale: la fine di un'era", www.ispionline.it, 15 febbraio 2023

3 Cfr. - Marco Ghisetti, "Le fragilità ed il fallimento dell'ordine egemonico liberale", osservatorioglobalizzazione.it, (15 febbraio 2023)

4 Lo sviluppo del nuovo terrorismo di matrice islamica sta riacquistando una nuova rilevanza territoriale, un esempio è l'emirato di Idlib in Siria del gruppo Hay'at Tahrir al-Sham (HTS), un tempo conosciuto come "Fronte Al Nusra", braccio siriano di al-Qaeda.

hanno imposto leggi e restrizioni che vanno a erodere le precedenti conquiste in materia di libertà e diritti fondamentali della popolazione.

A complicare il quadro geostrategico si aggiungono le conseguenze dei cambiamenti climatici. Il riscaldamento globale, la desertificazione, i fenomeni meteorologici intensi e improvvisi stanno mettendo in risalto le fragilità dei Paesi più poveri, provocando l'aumento di situazioni di crisi e flussi migratori.

La dimensione virtuale e il dominio cibernetico sono fattori sempre più rilevanti nel conflitto, trainati dal rapido sviluppo delle EDTs (*Emerging Disruptive Technologies*). L'espansione delle ostilità nel cyberspazio, la fruibilità di tecnologie duali, la diffusione dei *social network*, hanno facilitato la partecipazione di attori terzi e non statuali all'interno delle ostilità, dando impulso al fenomeno della "socializzazione dei conflitti". Un collettivo organizzato autonomamente *online*, un'azienda o un'organizzazione a carattere internazionale può infatti inserirsi in un conflitto convenzionale e non, con conseguenze tangibili a livello politico e strategico.

Il cambiamento delle società moderne e le conseguenti asimmetrie, inoltre, stanno provocando la proliferazione di conflitti intrastatali dove si assiste alla comparsa di nuovi attori esterni, non controllati dagli Stati, che si aggiungono a quelli interni. Anche il recente conflitto russo-ucraino, che pur ha riportato in auge lo scontro di tipo convenzionale tra gli eserciti regolari, vede al contempo una consistente partecipazione di mercenari, milizie locali, gruppi *hacker* e aziende private. Nei paragrafi seguenti si andranno ad analizzare le cause esogene ed endogene di frammentazione delle società moderne e come la conseguente eterogeneità aumenti le conflittualità al suo interno. Si valuterà infine la crescita degli attori non statuali nella partecipazione alle ostilità e quale sia il loro inquadramento giuridico nel diritto internazionale e umanitario.

2. "Fattori esogeni" di mutamento sociale

Per "fattori esogeni" di mutamento sociale, si intendono elementi o fenomeni di varia natura, non ascrivibili ad un singolo Stato, che generando profondi cambiamenti e eterogeneità nelle società, spesso foriere di frammentazioni, divisioni e asimmetrie. Uno di essi è la globalizzazione. A partire dai primi anni 2000, essa ha generato la crescita di connessioni e relazioni tra i Paesi diventando al contempo, però, una delle principali cause esogene di frammentazione sociale. Le sue dinamiche comportano la creazione di *hub* con connessioni fluide di carattere sociale, economico e finanziario che rispondono al meccanismo della riduzione dei costi. La tendenza per chi si affaccia al mondo globale è quella di legarsi ad *hub* preesistenti che presentano già elevata densità di connessioni, con

la conseguenza che le strutture createsi presentano sia spiccati caratteri di inclusività sia di iniquità[5]. Basti pensare alla crescita delle multinazionali e alle difficoltà incontrate dalla classe media nella conduzione delle proprie imprese negli ultimi 20 anni. I lavoratori del mondo sviluppato, inoltre, si ritrovano a competere con mercati caratterizzati da manodopera a basso costo. L'industria dell'abbigliamento in Bangladesh, ad esempio, impiega circa quattro milioni di persone, con un salario mensile paragonabile a quello giornaliero di un lavoratore statunitense. Secondo gli studiosi, la globalizzazione ha comportato anche un deciso aumento del lavoro minorile con una conseguente descolarizzazione dei figli delle famiglie più povere e l'aumento delle disparità[6].

In un mondo globale, così strettamente interdipendente, anche le crisi assumono caratteri transnazionali: quella finanziaria statunitense dei *subprime* del 2008 si è propagata rapidamente in Europa e nel mondo, acuendo le sofferenze e le frammentazioni sociali.

La stessa pandemia da COVID-19 si è diffusa velocemente tra gli Stati e ha acuito le situazioni di crisi infrastatali e le differenze fra le componenti della società all'interno di uno stesso Paese. Il costo sociale del COVID-19 è stato elevato così come l'impatto sulla psiche della popolazione. Gli Stati come USA, Russia e Cina, invece di unirsi in strategie e progetti di ricerca condivisi, hanno preferito agire singolarmente, trasformando la ricerca per un vaccino in una vera e propria competizione. Chi ha pagato il prezzo più elevato della pandemia sono stati i Paesi più poveri, non potendo sostenere i dispendiosi progetti di ricerca né acquisire i vaccini occidentali. Anche negli Stati cosiddetti ricchi si sono verificate spaccature e conflitti sociali: le fasce deboli della popolazione sono state colpite più duramente dalla grave recessione economica allora in essere. Ciò ha sia acuito le asimmetrie sia esasperato tensioni sociali latenti.

Un altro "fattore esogeno" che concorre al mutamento sociale sono i rapidi cambiamenti climatici. Essi rappresentano l'effetto dell'intervento umano sull'ambiente, sul quale pesano gli enormi processi di globalizzazione, di industrializzazione e l'ampio uso di materie prime e fonti non rinnovabili per le produzioni di energia e beni.

L'incremento delle temperature e l'aumento di eventi estremi hanno portato il mondo accademico ad interessarsi sempre più ai cambiamenti climatici e alle sue possibili ripercussioni sulla società.

Oggi, più che nel passato, l'incremento senza precedenti, in numero e intensità, di fenomeni meteorologici ad insorgenza rapida, quali uragani, inondazioni, tempeste, siccità, carestie, ha portato a un aumento dei flussi migratori: nel 2020, ad esempio, secondo un

[5] Cfr. – Prof. Giovanni Tria, "La globalizzazione contemporanea: caratteristiche conseguenze e sfide".
[6] Cfr. – "*Effects of Economic Globalization"*, www.nationalgeographic.org, (07 febbraio 2023).

rapporto dell'*Internal Displacement Monitoring Centre,* i cambiamenti climatici hanno costretto 30,7 milioni di persone di ad abbandonare la propria terra d'origine[7] per rifugiarsi in altre aree della propria nazione o in Paesi limitrofi. A peggiorare la situazione, come riporta l'UNHCR, è la tendenza dell'86% degli sfollati a migrare in Paesi in via di sviluppo, che, a loro volta, presentano vulnerabilità dal punto di vista sociale, climatico e ambientale[8]. Infine, secondo il "*NATO Strategic Concept*" del 2022, il cambiamento climatico è un «*moltiplicatore di minaccia*» che può esacerbare l'instabilità politica nelle regioni a rischio: tale tematica assurge ad una rilevanza strategica, in ragione delle conflittualità dirette che è capace di innescare e che hanno un impatto non secondario sull'economia, sulle società e sulla sicurezza internazionale.

Un ulteriore "fattore esogeno" è rappresentato dalle organizzazioni transnazionali, soprattutto di stampo terroristico: esse si sono spesso incuneate in Stati con forti crisi istituzionali e d'identità, esacerbando divisioni e conflitti. In alcuni casi, sono andate oltre gli attacchi sporadici e il proselitismo, arrivando a conquistare e governare territori infrastatali all'interno dei quali si è presto instaurata una spasmodica ricerca del nemico, non solo rivolta all'esterno ma anche tra le componenti della società stessa, con il risultato di minarne la coesione. Ne è un esempio l'*Islamic State* (IS) che, con una repentina ascesa, è riuscito nel 2014 a costituire un califfato nel Medio Oriente (nei territori di Siria e Iraq). Sebbene sia stato sconfitto e non rappresenti più un'entità territoriale, il movimento ha assunto un'organizzazione decentralizzata e continua tutt'oggi, insieme ad altre VEO, ad avere seguito nel Medio Oriente e negli Stati africani (Sudan, Somalia, Niger, Ciad), aumentando le divisioni all'interno di società non omogenee ed in crisi da molti decenni[9].

3. "Fattori endogeni" di mutamento sociale

I "fattori endogeni" si differenziano da quelli "esogeni" in quanto generano mutamenti i cui effetti si riverberano principalmente all'interno della società di un singolo Stato. Tra i principali si annoverano le differenze culturali che determinano scissioni della popolazione in gruppi eterogenei dal punto di vista di usi, tradizioni, credenze e comportamenti. Il problema si pone quando questi gruppi diventano intransigenti verso i comportamenti altrui.

Anche gli squilibri economici possono acuire le differenze, specialmente quando portano gli individui a non poter far fronte neanche ai propri bisogni primari, provocando la

---

7 Cfr. – *Internal Displacement Monitoring Centre* (IDMC), " *Global Report on Internal displacement* 2021", *Norwegian Refugee Council* (NRC).

8 Cfr. – AA.VV, " UNHCR: La pandemia non ferma la fuga da guerre e persecuzioni: più di 82 milioni di profughi. Il doppio di dieci anni fa", www.repubblica.it, (10 aprile 2023).

9 Cfr. – Elena Alice Rossetti, "Le possibili traiettorie dell'IS nel 2022 in Iraq e Siria dopo l'attacco alla prigione di Al-Sina e la morte del leader Abu Ibrahim al-Hashimi al-Qurashi", www.geopolitica.info, (20 marzo 2023)

crescita di sacche di povertà ed emarginazione all'interno della società. Questo fenomeno è particolarmente evidente nelle periferie delle grandi città, dove si sono venuti a creare interi quartieri abitati da persone accomunate dal forte disagio economico.

Le differenze politiche rappresentano pure un "fattore endogeno" e causano profonde contrapposizioni tra gruppi sociali quando è presente una forte polarizzazione delle opinioni che non consente un normale dialogo tra le persone.

Infine, negli Stati sorti nell'era post-coloniale, dove i confini sono stati decisi senza tener conto delle peculiarità religiose, culturali ed etniche, si sono create delle miscele esplosive all'interno delle società che spesso si sono tramutate in scontri violenti e lotte di potere. Ne sono un esempio i conflitti ormai perenni negli Stati africani come il Congo, il Ruanda o la Somalia.

Per capire meglio come i "fattori endogeni" sopra esposti siano forieri di divisioni e ormai presenti in tutto il globo, si sono di seguito analizzati tre *case studies* di Paesi appartenenti a tre continenti diversi: Libia, Siria e Stati Uniti.

a) Il caso Libia

La Libia a partire dal XVI secolo ha subito dominazioni straniere (ottomana e italiana), raggiungendo l'indipendenza con la fine dell'era coloniale. Lo Stato creatosi nel 1951, riunisce al suo interno varie etnie, la cui convivenza non è mai stata priva di ostacoli e tensioni. In alcuni periodi, l'esistenza delle tribù berbere è stata messa in discussione e le minoranze etniche Tuareg e Tebu sono state spesso marginalizzate dal governo.

La Libia si divide in tre grandi macro-regioni, ciascuna di queste abitata da popolazioni con cultura, lingua e storia differenti: la Tripolitania è stata fortemente influenzata dalla cultura mediorientale, la Cirenaica da quella greco-romana, mentre il Fezzan ha subito influenze delle varie culture africane.

In seguito alla rivolta scoppiata nel 2011, l'elemento tribale interno alla popolazione libica è tornato ad avere un ruolo rilevante rispetto al mantenimento del controllo territoriale, mettendo così in luce sopite contrapposizioni tra le parti della società. È noto, infatti, che la popolazione risulta fortemente eterogenea dal punto di vista della composizione tribale e etnografica: gli *Imazighen* (o Berberi) sono concentrati soprattutto lungo i confini con l'Algeria, le tribù arabe dei *Warfalla* e dei *Al-Abaidat* in Tripolitania e Cirenaica, mentre i Tebu popolano il Fezzan. Durante il periodo del governo Gheddafi, alle tribù berbere e africane non erano riconosciuti gli stessi diritti rispetto a quelle arabe. I loro membri non possedevano la cittadinanza libica e venivano esclusi dalle cariche pubbliche.

La creazione di un sistema di privilegi familiari ed economici ha aumentato le ineguaglianze e minato la pacifica convivenza tra le parti. Si pensi, ad esempio, che l'assenza di politiche redistributive ha consentito solo a pochi di trarre vantaggio dallo sfruttamento delle ingenti risorse petrolifere[10]. Infine la presenza di vaste zone desertiche che circondano la Tripolitania e la Cirenaica, costituisce una barriera geografica che ostacola l'interazione e l'integrazione tra le parti sociali.

b) Il caso Siria,

La Siria è una nazione altamente diversificata che ospita varie comunità religiose ed etniche (ebrei, cristiani, alawiti e sunniti). La lora convivenza è stata tutt'alto che semplice, costellata da episodi di discriminazione ed emarginazione perpetrati dai governi.

Il regime del presidente Bashar al-Assad ha portato avanti una politica esclusiva e discriminatoria a favore della minoranza alawita e di alcuni settori dell'economia, come ad esempio quello mercantile, marginalizzando le altre comunità religiose ed etniche presenti nel Paese. Il malcontento crescente è sfociato in proteste di piazza durante le primavere arabe del 2011, represse nel sangue dal regime. Le manifestazioni si sono concentrate soprattutto nelle zone rurali. Il settore agricolo, che contribuiva per circa il 20% del PIL, infatti, stava vivendo una difficile situazione, dovuta alla persistente siccità[11]. Ciò aveva dato impulso alla migrazione di più di un milione di persone verso i centri urbani, bisognosi di assistenza alimentare. Tali spostamenti hanno inevitabilmente avuto delle ripercussioni sulla stabilità socio-economica del Paese, il cui governo era additato di aver peggiorato la situazione con delle politiche agricole sconsiderate[12]. Solo pochi e privilegiati investitori hanno potuto godere dei benefici di tali misure e sono venuti meno i principi socialisti del partito Ba'ath, incapace di tener fede alle promesse circa l'attuazione di politiche distributive. Il contesto iniquo e frammentato ha provocato così sanguinosi scontri tra le parti sociali che si protraggono ormai da più di dieci anni.

c) Il caso Stati Uniti

Dal 1979, i salari reali dei lavoratori hanno subito una crescente diminuzione, mentre il reddito delle famiglie più ricche è più che triplicato. Allo stesso tempo, la disoccupazione è aumentata colpendo in maniera maggiore giovani e gruppi etnici minoritari. Le differenze

[10] Cfr. – AA.VV., "Società libica: il ruolo del tribalismo", mondointernazionale.org, (05 marzo 2023).
[11] Cfr. – Stefano Torelli, "La Siria tra rivolte e depressione", Istituto per gli Studi di Politica Internazionale.
[12] In particolare, la decisione di sottoporre a coltura intensiva molte aree intorno all'Eufrate, prima destinate al pascolo, avrebbe accelerato l'esaurimento delle risorse idriche. Si veda International CrIS Group, Popular Protest in North Africa Land the Middle East (VI): The Syrian People's Slow-motion Revolution, in «Middle East/North Africa Report», 108, July 6,2011, p. 23

tra la comunità bianca e quella afroamericana e ispanica si riflettono anche nel minor grado di scolarizzazione con conseguenti difficoltà di poter accedere a incarichi di prestigio[13].

Gli Stati Uniti vivono in questo periodo una fase di forte polarizzazione politica che ha riflessi anche sulla società. I membri dell'*establishment* sono diventati sempre più riluttanti a cercare soluzioni conciliatorie e questo si ripercuote negativamente sui cittadini. Tra essi infatti, si sta facendo strada la cosiddetta *cancel culture*, definita dal dizionario australiano Macquaire come "l'atteggiamento all'interno di una comunità che richiede o determina il ritiro del sostegno a un personaggio", ossia una vera e propria forma di ostracismo, o boicottaggio di un individuo, reo di aver anche lontanamente espresso opinioni fuori dai canoni del *politically correct*[14]. A tal proposito un editoriale del New York Times di marzo 2022 "*America Has a Free Speech Problem"* riporta: "*Nonostante la tolleranza e la ragione della società moderna, gli americani stanno perdendo il controllo di un diritto fondamentale come cittadini di un Paese libero: quello di poter dire ciò che pensano e di esprimere le proprie opinioni in pubblico senza paura di essere infamati o isolati"*[15]*.* La *cancel culture* non si ferma solo alla libertà di espressione, ma porta avanti un revisionismo storico che tende a interpretare gli avvenimenti del passato con metodi e valori anacronistici; ne sono esempi le recenti rimozioni di bandiere e statue, icone della storia americana, da luoghi pubblici, poiché reinterpretate quali simboli di discriminazione razziale o accostate a valori non più condivisi.

Esempi di questo fenomeno si trovano già in *South Carolina*, quando la bandiera dei secessionisti che sventolava sulla cupola del parlamento locale è stata rimossa a seguito di una strage in una chiesa afroamericana o quando, nel 2021 è stata asportata la statua di uno dei padri fondatori degli USA, Thomas Jefferson, dal New York City Hall perché accostato al fenomeno dello schiavismo. Il governatore repubblicano *pro tempore* ha ritenuto intollerabile che rimanesse al suo posto, poiché simbolo di odio e sopraffazione nei confronti delle persone di colore. Tale pratica si è accanita financo sulle statue raffiguranti svariati personaggi storici. Nel 2021 è stata rimossa la statua di uno dei padri fondatori degli USA, Thomas Jefferson, dal New York City Hall a seguito di una petizione popolare proposta da consiglieri afroamericani e latinoamericani. Il terzo Presidente degli Stati Uniti è stato tacciato di essersi reso protagonista dello schiavismo, allora pratica comunemente accettata, poiché impiegò degli schiavi nella sua piantagione di Monticello[16].

---

[13] Cfr. – Cristina da Rold, " Il gap etnico dell'università oggi. La disuguaglianza negli Stati Uniti", www.ilsole24ore.com, (03 aprile 2023).

[14] Cfr. – Paola Rosa Ardagna, "Cancel culture, che cos'è davvero la "cultura della cancellazione", www.repubblica.it, (20 aprile 2023).

[15] Cfr. – Algadiscia Marocco, "Non si può più dire niente". Anche il New York Times si è redento dalla *cancel culture"*, www.huffingtonpost.it, (05 marzo 2023).

[16] AA.VV., "Usa, rimossa la statua di Thomas Jefferson dalla New York City Hall", www.tg24.sky.it, (05 marzo 2023).

Purtroppo la *cancel culture* non colpisce solo i monumenti, ma dilaga nelle università, nelle redazioni dei giornali e più in generale in tutti i settori pubblici e privati. Esprimere la propria opinione potrebbe scatenare orde di intolleranza, perpetrate con l'ausilio dei mezzi di comunicazione digitali e dei *social network*, che spesso e volentieri hanno comportato il licenziamento o le dimissioni di professori e giornalisti. Ne sono un esempio le dimissioni di James Bennet, responsabile degli editoriali del New York Times, accusato di razzismo per aver pubblicato l'articolo del senatore repubblicano Tom Cotton che invocava l'intervento dell'esercito per arginare i disordini e le violenze provocate da alcune frange del movimento *Black Lives Matter*[17].

In sostanza siamo di fronte a un paradosso: la società americana, simbolo di libertà, sta vivendo un periodo caratterizzato dalla censura esacerbata dalle pulsioni perbeniste. Ciò sta causando atti violenti e forti contrapposizioni di tipo etnico, economico e culturale all'interno della popolazione, che stanno mettendo a dura prova la tenuta democratica del Paese.

4. Crescita interazione attori esterni nei conflitti

Ci sono molti possibili attori esterni che possono essere coinvolti, a vario titolo e con diverse finalità, in un conflitto e tra questi si annoverano: Stati-Nazione, Organizzazioni Internazionali, gruppi militanti, organizzazioni non governative (OnG), aziende, individui e gruppi di pressione. È importante sottolineare che questi attori esterni possono avere interessi e obiettivi diversi, che potrebbero non essere necessariamente allineati con quelli delle parti in conflitto.

Quale nota metodologica, questo paragrafo si prefigge l'intento di compendiare taluni tra i più influenti attori esterni nell'attuale contesto, mentre le implicazioni tecnologiche che sottendono alle loro attività saranno più dettagliatamente illustrate nel capitolo 2.

Se la partecipazione di Stati e Organizzazioni Internazionali è frequente e quindi ben documentata nella letteratura dei conflitti armati e non rientrante direttamente nella narrativa del paragrafo, l'analisi degli altri soggetti appare particolarmente interessante per le implicazioni di "socializzazione del conflitto" che generano.

Con riferimento alle organizzazioni terroristiche paramilitari transnazionali di matrice islamica, come IS e al-Qaeda, appare importante evidenziare come il proselitismo e la propaganda siano state molto rilevanti. Il loro obiettivo consiste nel creare consenso e screditare il nemico occidentale, fomentando la levata in massa della popolazione musulmana contro l'invasore infedele. In taluni conflitti come Afghanistan e Yemen sono

[17] Ibid nota 16

state addirittura decisive per permettere di rovesciare i governi e impiantarne altri. Il ruolo delle Organizzazioni non Governative in un conflitto può risultare importante in quanto potrebbero consentire significativi vantaggi per una delle parti in contesa. Le ONG si attivano per la protezione dei diritti delle popolazioni in diversi momenti e a diversi livelli. Le strategie che adottano variano a seconda della natura dei loro obiettivi, siano essi specifici o generali, di lungo o breve termine, locali, nazionali o internazionali e così via. L'assistenza diretta per la tutela dei diritti umani, la raccolta di informazioni spesso utilizzate come evidenze probatorie nelle ricostruzioni delle responsabilità dei capi di governo che hanno innescato il conflitto e le campagne *in loco* per creare consenso e *lobbying*, sono solo alcuni tra gli strumenti utilizzati negli scenari di conflitto.

La partecipazione di attori esterni, in particolare individui o aziende private, è un fenomeno già presente in passato. Essa si sostanzia in una serie di attività effettuate da un soggetto o una comunità di soggetti o società che, di fatto, non hanno alcun legame diretto con un determinato conflitto, ma che, intervenendo in esso per motivazioni non sempre facilmente discernibili, mettono in campo competenza, capacità e mezzi, producendo importanti effetti a favore dell'una o dell'altra parte in contesa.

Il parallelismo, ad esempio, con la storia di M. E. Lepido nel I Sec A.C. ricchissimo romano poi politico, generale e triumviro, permette di intuire come un personaggio potente abbia potuto influenzare, in modo significativo, i conflitti politici e militari della Repubblica dell'antica Roma, mediante la sua enorme armata privata e costruire una vasta rete di clienti e alleati politici. Oggi però si assiste ad una crescita esponenziale in rilevanza, numero e eterogeneità di attori esterni nei conflitti, tra le cui cause possiamo annoverare l'aumento dei conflitti intrastatali e la crescita della velocità delle relazioni tra organizzazioni e tra individui, a seguito dei dirompenti sviluppi della tecnologia.

Tra gli attori esterni (individuali ma anche aziendali) possiamo elencare Elon Musk ed il suo sistema satellitare *Starlink*[18], messo a disposizione dell'Ucraina per assicurare continuità nella rete di comunicazione, anche per le attività operative in senso stretto, contro l'aggressore russo. Si tratta nello specifico di un facoltoso soggetto che, attraverso la sua organizzazione e la tecnologia di cui dispone, offre, a titolo gratuito, una serie di *asset* satellitari che possono, in qualche modo, essere d'ausilio per gli ucraini.

Il fatto di essere proprietario di *Twitter*gli conferisce, peraltro, anche un importante seguito con cui può essere influenzata parte dell'opinione pubblica costituita dagli innumerevoli fruitori. La politica di *Twitter*, ad esempio, è decisamente favorevole all'invio di

[18] Starlink è una costellazione satellitare che permette di accedere a internet con connessioni a banda larga. All'inizio della guerra Musk ha fornito terminali al governo ucraino per sopperire ai danni inferti dai russi alle reti di telecomunicazioni

armi in Ucraina in armonia con le politiche dell'amministrazione Biden, mentre si mostra critica verso le altre soluzioni proposte dai repubblicani di Trump. Un soggetto esterno che, da subito, ha guadagnato enormi porzioni di consenso, spostando verosimilmente taluni equilibri nei conflitti, è Mark Zuckemberg, che attraverso i suoi popolari *social (facebook, Instagram e Youtube)*, permeati da un progetto editoriale contrario alla politica aggressiva russa ha, a titolo di esempio, nel marzo 2022, estromesso la testata giornalistica *Sputnik* (ex Voice of Russia e RIA Novosti) considerata troppo filoputiniana[19].

Appare evidente che uno strumento di colossale seguito come Facebook (2,9 miliardi di utenti attivi mensili in tutto il mondo nel 2021[20]) possa spostare il consenso anche solo orientando gli algoritmi verso notizie pro-occidente.

Di contro, la Cina non rimane a guardare e, tramite l'azienda cinese *ByteDance* detentrice dell'app *Tik Tok*, gode di un seguito di circa un miliardo di utenti attivi e un valore di mercato stimato in circa 300 miliardi di dollari. La filosofia editoriale di *Tik Tok* è stata aspramente contestata dall'amministrazione Trump così come la gestione dei dati personali e la possibilità che tale *App* potesse inviare in Cina dati e dettagli anche sensibili[21].

Un soggetto che, invece, si può considerare normalmente trasversale, ma che nel conflitto Ucraino si è decisamente schierato apportando significativi vantaggi alla fazione occidentale, è *Anonymous*. Come noto, si tratta di un movimento decentralizzato di *hacktivismo* che agisce in modo coordinato per perseguire un obiettivo concordato. *Anonymous* che negli anni ha acquisito popolarità per aver rivendicato in modo spettacolare i propri attacchi informatici contro varie società e istituzioni governative, vanta una lunga trafila di attività *cyber operative* durante i conflitti. Si ricordano gli attacchi ad alcuni siti in Egitto (2011) per agevolare il rovesciamento di regime o quelli contro i siti di Israele a favore dei palestinesi (2012). Recentemente, nel 2022, ha dichiarato guerra "telematica" alla Russia a seguito dell'invasione dell'Ucraina, attaccando numerosi siti governativi, trasmettendo messaggi in televisione e oscurando, tra gli altri, il sito ufficiale di Russia *Today*. Il 2 marzo 2022 *Anonymous* ha addirittura dichiarato di aver *hackerato* il sito dell'agenzia spaziale russa Roscosmos, mettendo fuori uso alcuni satelliti spia. Tale notizia è stata tuttavia smentita dalle autorità russe ma è indicativa di come un soggetto esterno al conflitto, spesso in contraddizione con gli USA, sposi una causa facendo fronte comune con

[19] AA.VV. "Ucraina, ecco le purghe di Zuckerberg: oscurata la testata giornalistica Sputnik", www.ilcorriere.it, (21 marzo 2023)

[20] Biagio Simonetta, "Quanti utenti ha Facebook? Gli account doppi mettono in discussione i numeri ufficiali", www.ilsole24ore.com, (21 marzo 2023)

[21] Michela Rovelli, "Tik-Tok, perché Trump vuole bloccarlo e Microsoft vuole comprarlo", www.corriere.it, (21 marzo 2023)

l'Occidente contro l'aggressore russo, infliggendogli danni significativi attraverso *cyber* attacchi.

5. Inquadramento giuridico degli attori

Appare evidente che in un conflittoin cui vi siano elementi di complessità così significativi, è fondamentale, ancorché complicato, inquadrare il regime giuridico da applicare per le discendenti tutele del Diritto Internazionale Umanitario (DIU) ovvero dei principi generali del Diritto Umanitario (DU). In primo luogo è necessaria una qualificazione del conflitto.

In una situazione di ostilità tra Stati (attori statuali), al verificarsi del primo scontro a fuoco tra le reciproche Forze armate, sono presenti tutti gli elementi di diritto per definire il conflitto come Armato Internazionale (IAC).

Attraverso il DIU, quindi, coloro che prendono parte alle ostilità sono *lawful combatant* e godono dello *status* di combattenti privilegiati ai sensi degli artt.43 e 44 del I Protocollo Aggiuntivo alle Convenzioni di Ginevra (I PA), ricevendo, in caso di cattura, le tutele derivanti dallo *status* di "prigionieri di guerra" POW (art. 4-20 della III CG e art. 43-47 del I PA – II sez.).

Tali tutele consistono nella presunzione di attribuzione dello *status* di POW, fino a prova contraria, essendo la potenza detentrice responsabile del trattamento loro applicato secondo i criteri di umanità (art. 13 III CG), pena l'attribuzione di gravi infrazioni.

Una ulteriore *species* di combattenti è riferita a quei soggetti che, pur non facendo parte delle Forze armate di uno stato in conflitto, partecipano di fatto alle operazioni militari. Circa i citati soggetti, più in generale, con il I PA vi è stato un complessivo ampliamento della nozione di legittimo combattente. In sostanza tutti i belligeranti, regolari o irregolari, hanno un solo dovere fondamentale, quello di distinguersi dalla popolazione civile mentre sono impegnati in un attacco o in un'operazione militare preparatoria all'attacco. Se non lo fanno, essi perdono lo *status* di combattente legittimo e, quindi, non fruiscono del trattamento riservato ai prigionieri di guerra.

In caso di conflitti armati non-Internazionali (NIAC), non sussiste diretta affermazione nell'ambito del diritto internazionale umanitario (DIU) se non attraverso un ragionamento "*a contrariis*" rispetto al diritto positivo che definisce i conflitti armati internazionali (IAC).

Secondo l'interpretazione giurisprudenziale del tribunale per i crimini in ex Yugoslavia (ICTY) nel caso Tadic, per NIAC si intende una situazione di protratta violenza armata tra le autorità di governo e gruppi armati organizzati o tra questi ultimi all'interno del territorio di

uno Stato. Requisiti fondamentali sono la sussistenza di una significativa intensità degli scontri e un'organizzazione dei gruppi armati.

Attraverso la disciplina dei NIAC, le parti sono vincolate al rispetto del DIU e operano talune tutele particolari sia a favore della popolazione civile, sia a favore dei soldati che sono incapaci di svolgere le loro funzioni militari (*hors de combat*). Lo *standard* minimo di copertura dei diritti umani è garantito dall'art 3 "comune" della Convenzione di Ginevra, una norma consuetudinaria che impone l'inviolabilità dei principi fondamentali, nonché dal II PA del 1977.

Tracciato questo generale quadro normativo, occorre adesso verificare lo specifico inquadramento di quei soggetti che partecipano in modo attivo al conflitto.

Non appare inconferente, tuttavia, ai fini della narrazione e dell'inquadramento giuridico, evidenziare preliminarmente il concetto di occupazione o di territorio occupato per qualificare i comportamenti dei residenti nello stato occupato.

Un territorio è considerato come occupato quando di fatto si trova sotto l'autorità di una forza armata straniera, anche se l'occupazione non incontra alcuna resistenza militare. Il DIU si applica in qualsiasi situazione di occupazione, indipendentemente dal fatto che l'occupazione sia legittima o no. Esso disciplina i diritti della popolazione e i doveri delle forze di occupazione. Queste ultime devono provvedere a garantire l'ordine pubblico e la sicurezza nel rispetto, salvo un impedimento assoluto, delle leggi in vigore. Le forze di occupazione sono, inoltre, responsabili della fornitura di derrate alimentari e di medicinali alla popolazione.

Di seguito sono enucleate alcune fattispecie di interazione della popolazione civile con la potenza occupante, che, in relazione alla tipologia di intervento, può essere ricondotta ad uno specifico inquadramento nell'ambito del Diritto Internazionale.

a) Uso dello smartphone e disciplina dello spionaggio

L'uso dello *smartphone*, ormai, ha condizionato in modo talora decisivo l'andamento di un conflitto, in particolare in caso di occupazione. L'utilizzo improprio di tali mezzi di comunicazione da parte degli occupanti può consentire l'identificazione di postazioni militari grazie ad esempio alle dirette su Tiktok, ovvero la tracciabilità sui *social* dei percorsi di *footing* effettuati. Essi popolano il *web* di informazioni *open source* che, ormai da tempo, gli Stati hanno imparato a decriptare ed interpretare per fini prettamente bellici. Inoltre, una particolare categoria di soggetti è costituita, ad esempio, dagli abitanti dei centri urbani occupati, che invece procacciano tali informazioni (anche simulando altre tipologie di attività

*social c*ome ad es. dirette *web*, uso di *Instagram*, *Tiktok* etc), rendendo accessibile *online* la posizione delle truppe nemiche.

Dal punto di vista giuridico, l'inquadramento che sembra poter essere applicabile a questi soggetti, almeno in via analogica, in tali contesti è quello derivante dalla disciplina dello spionaggio da parte della popolazione civile. Durante un conflitto, i metodi di raccolta delle informazioni militari (ad esempio, quelli attuati attraverso l'esplorazione, l'osservazione e la ricognizione) sono considerati leciti, anche se effettuati in territorio nemico. Mentre per i soldati catturati quando svolgono tali compiti si applicano le tutele di POW, purché siano in uniforme, è invece considerato come svolgente attività di spionaggio chi raccoglie o cerca di raccogliere informazioni in un territorio controllato da una Parte avversaria senza uniforme (art. 46, I PA del 1977). Esiste tuttavia una "clausola di salvaguardia": in territorio occupato, non sarà considerato come spia chi, residente in detto territorio, raccoglie o cerca di raccogliere, per conto della Parte da cui dipende, informazioni di interesse militare, salvo che non agisca sotto falsi pretesti o in modo deliberatamente clandestino.

Da qui si trae la conclusione che non essendo lo spionaggio di per sé contrario al DIU, il soggetto in questione non perderà il diritto allo *status* di prigioniero di guerra e non potrà essere trattato come spia, se non nel caso in cui egli sia catturato mentre svolge attività in modo illecito.

b) Capacità di interferire nei sistemi di comunicazione mediante App e software commerciali

Sempre mediante una interpretazione di tipo analogico, i soggetti autori delle attività in titolo possono essere considerati alla stregua di sabotatori.

Anche il sabotaggio è consentito dal DIU, purché l'oggetto dell'azione sia un obiettivo militare (art. 52.2 I PA). I sabotatori, in genere, vengono identificati come combattenti che operano oltre le linee dell'avversario per distruggere o rendere inservibili determinati beni che contribuiscono effettivamente all'azione militare del nemico.

I sabotatori in uniforme sono considerati combattenti legittimi e, se catturati, godono dello status di POW. Nel caso in cui agissero non distinguendosi dalla popolazione civile non hanno diritto allo status di POW. Qualora catturati dal nemico, essi avranno comunque accesso alle garanzie previste dall'art. 75 I PA, analogamente a quanto previsto per le spie.

In entrambi i casi su descritti (spionaggio e sabotaggio) effettuati però da parte di civili, l'art. 5 della IV Convenzione di Ginevra del 1949 sancisce che "*se, in un territorio occupato, una persona protetta dalla Convenzione è arrestata come spia o per atti di sabotaggio, oppure perché giustamente sospetta di svolgere un'attività dannosa per la sicurezza della*

Potenza occupante, detta persona potrà, se la sicurezza militare lo esige in modo assoluto, essere privata dei diritti di comunicazione previsti dalla presente Convenzione". Quindi esiste un criterio di sicurezza militare che impone necessarie restrizioni dei diritti dei predetti soggetti. Il terzo capoverso del citato articolo recita: "*In ciascuno di questi casi, le persone, cui si applicano i capoversi precedenti, saranno comunque trattate con umanità e, in caso di procedimento giudiziario, non saranno private del loro diritto ad un processo equo e regolare, come è previsto dalla presente Convenzione. Esse recupereranno altresì il beneficio di tutti i diritti e privilegi che la presente Convenzione conferisce alla persona protetta, non appena ciò sia compatibile con la sicurezza, dello Stato e della Potenza occupante*".

La previsione generale dell'art.68 della predetta Convenzione, tuttavia, riferisce che quando una persona protetta commette un'infrazione unicamente nell'intento di nuocere alla Potenza occupante, ma quest'infrazione non colpisce la vita o l'integrità corporale dei membri delle forze o dell'amministrazione d'occupazione, non crea un serio pericolo collettivo e non danneggia gravemente i beni delle forze o dell'amministrazione d'occupazione o gli impianti da esse utilizzati, detta persona è punibile con l'internamento o la semplice prigione. La pena di morte non è prevista nei confronti delle persone protette, salvo nel caso in cui queste siano colpevoli di spionaggio, di gravi atti di sabotaggio degli impianti militari della Potenza occupante o di infrazioni intenzionali che abbiano cagionato la morte di una o più persone. Lo Stato occupante è titolato quindi a processare e punire con la massima pena coloro che ricadano nelle citate fattispecie reputate criminose.

c) Supporto di attori esterni al conflitto legati al mondo della finanza e dell'industria tecnologica

Il sostegno assicurato alle forze di Kiev da parte di Elon Musk nel conflitto russo-ucraino mediante la rete *Starlink* ha aperto nuovi e imprevisti scenari nell'ambito della guerra, con aspetti da sviscerare necessariamente anche dal punto di vista prettamente giuridico.

Il "fattore Elon Musk"[22] può essere inquadrato giuridicamente come un sostegno ad una parte del conflitto. Non essendo possibile identificarlo come attore statuale o gruppo armato, è qualificabile come un privato cittadino che fornisce assistenza e supporto ad una parte in guerra; si potrebbe applicare lo schema del "*contractor*" qualora vi fosse una remunerazione da parte dello Stato che beneficia dei servizi di tale attore.

[22] Secondo il politologo statunitense Iam Brenner, (vds. "*Elon Musk spoke Vladimir Putin before Ukraine peace plan report 2022*", www.businessinsider.com, (20 marzo 2023)

Si tratta quindi di persone giuridiche (es. *Space X*) formate da persone fisiche (soggette al DIU) che intervengono nel conflitto, anche solo quali "*Corporate warriors*" nel fornire servizi logistici, tecnici, di trasporto e supplementari.

Sappiamo, tuttavia, che lo Stato che incorpori formalmente i *contractors* (*de jure*) o fattualmente (*de facto*), fa sì che questi ultimi agiscano per conto dell'incaricante (cit. Art. 43 I PA). È chiaro, quindi, che vi debba essere una sottoposizione del *contractor* alla catena di comando dello Stato assoldante.

L'art.1 del I PA stabilisce che ogni soggetto non appartenente alle Forze armate di una delle parti in conflitto deve essere considerato civile. Essi non possono essere oggetto di attacco, ma non hanno neppure il diritto di prendere parte alle ostilità e l'uso delle armi è loro consentito soltanto per mera difesa di se stessi o di coloro i quali sono sottoposti alla loro responsabilità.

In termini generali, nell'eventualità in cui dei civili prendano parte ai combattimenti, si spogliano del loro *status* per acquisire quello di combattenti illegittimi: in tal caso potrebbero essere oggetto di un legittimo attacco nemico e non godrebbero di alcuna immunità per gli atti di belligeranza compiuti quand'anche fossero rispettosi del DIU. Va da sé che nel caso venissero catturati, non potrebbero neppure godere dei privilegi del prigioniero, spettando loro unicamente il diritto al trattamento umano ed all'equo processo.

Per poter tuttavia concludere che attori esterni come Elon Musk possano essere considerati combattenti illegittimi in un conflitto come quello Russo-Ucraino, non si può trascurare il fattore geografico. Una qualificazione di tale soggetto quale diretto partecipante alle ostilità si scontra con l'applicazione geografica del DIU, specialmente in un conflitto tradizionale tra Stati come quello attuale. Nell'ottica, quindi, di evitare un allargamento incontrollato del territorio del conflitto e degli attori coinvolti, la partecipazione di un attore "a distanza" (cioè non presente in zona di guerra) non può essere considerata "diretta" ai sensi dell"art. 51.3 del I P.A.; ragionando in senso contrario, infatti, si dovrebbe ammettere la possibilità per la Russia di colpire Musk in territorio statunitense, cosa -ovviamente- non consentita dal DIU.

Sul punto, tuttavia, non vi è una posizione dottrinale univoca.

Le esigenze di restrizione del concetto di partecipazione diretta, con cui si vuole proteggere la popolazione civile tenendola fuori dai pericoli delle ostilità, si scontrano con un'interpretazione estensiva finalizzata a scoraggiare il civile dal prendere parte nel conflitto.

Tuttavia è da rilevare che oggi la nozione stessa di conflitto armato stia attraversando un processo di cambiamento dovuto all'uso di nuove tecnologie come i droni o attacchi *cyber* che stanno lentamente cancellando i confini geografici dei conflitti, tagliando grandi distanze

e diminuendo la necessità di *“boots on the ground*”. In sintesi nel caso di specie sembra difficilmente inquadrabile Musk come contractor, salvo che non partecipi ad azioni territorialmente inquadrate nello scenario di conflitto.

CAPITOLO 2
LA TECNOLOGIA NEL *MODERN WARFARE*

1. Tecnologia duale nei conflitti

Con il termine *dual use* si fa riferimento a prodotti, inclusi *software* e tecnologie, che possono avere un utilizzo sia civile che militare. Questa commistione tra i due ambiti non è un fenomeno recente; la storia dell'uomo è ricca, infatti, di esempi di questo continuo scambio tra i due comparti e altrettanto evidente è il mutuo beneficio di cui entrambi hanno goduto. Emblematico è il caso della carriola: ora di natura assolutamente civile e dai risvolti pratici conclamati, nacque nel 100 a.C. dall'esigenza dell'esercito cinese di trasportare agevolmente materiale militare e si rivelò di tale valore strategico che l'imperatore ne vietò per anni la diffusione al di fuori dei ranghi. Compiendo un deciso balzo temporale in avanti, è convenzionalmente accettato che il primo esempio di tecnologia duale moderna sia l'ammoniaca. Questo composto, ampiamente impiegato in ambito civile nei primi del '900 quale base fondamentale per i fertilizzanti, si rivelò altrettanto dirompente quando utilizzato nel contesto della I Guerra mondiale, come arma chimica. La lista di materiali di natura duale è estremamente varia ed abbraccia tecnologie missilistiche, satellitari, nucleari, chimiche e biologiche.

Questa larga diffusione, sia temporale che tematica, è dovuta al riconoscimento di evidenti punti in comune tra gli interessi militari e quelli del mondo industriale civile. Da un lato il comparto militare, spinto dalla necessità di guadagnare o mantenere la supremazia tecnologica sull'avversario, è stato da sempre incline ad investire nella ricerca e nella produzione, sfruttando le capacità esprimibili dall'industria nazionale; dall'altro l'industria, grazie a questa *partnership*, ha compreso da subito i benefici nell'accedere a maggiori finanziamenti e a tecnologie avanzate e ad una rete composta da altre aziende, laboratori della Difesa e dipartimenti di ricerca universitari.

In questo connubio, la forza economica esprimibile dalla Difesa ne garantiva il ruolo trainante e le permetteva di dettare l'agenda: i prodotti e le tecnologie sviluppate erano, per natura, intrinsecamente militari e venivano successivamente adattate ad un uso civile. Negli anni '90, la progressiva riduzione del *budget* per la spesa militare e la crescita esponenziale del fatturato di alcune aziende e consorzi civili, hanno invertito il paradigma e le gerarchie tra i due ambiti. La Difesa pare, oggi, non più in grado di guidare il comparto civile imponendo i propri programmi, ma pare piuttosto costretta a colmare i propri *gap* capacitivi andando a pescare da un paniere di prodotti che le industrie sviluppano in base alle loro priorità.

Questa continua osmosi tra comparti, contraddistinta da una ininterrotta interazione tra sfera civile e militare, ha avuto riflessi non solo nello sviluppo capacitivo ma, in qualche modo, ha contribuito ad offuscare la separazione tra militare e civile, tra soggetto coinvolto attivamente nelle ostilità e non. Così come per alcune tecnologie, dove appare difficile capirne l'effettiva natura, allo stesso modo, per alcune parti della popolazione appare altrettanto complicato definirne l'appartenenza (civile o militare) e soprattutto l'agire (belligerante o meno).

Il ruolo dirompente che le nuove tecnologie emergenti stanno rivestendo nei conflitti moderni e la natura estremamente duale di queste ultime hanno -come conseguenza- esteso il conflitto al di là della tradizionale sfera militare, coinvolgendo un incredibile numero di persone che di questa tecnologia fanno uso, più o meno consciamente.

2. Implicazioni sull'uso della tecnologia duale (internet, droni, GPS, immagini satellitari)

L'uso duale della tecnologia sta influenzando in maniera consistente e difficilmente arginabile i conflitti moderni. Se *Internet*, droni, GPS, immagini satellitari e altre tecnologie sono strumenti usati da decenni dalle forze militari, convenzionali e non, per vari scopi, ora è la popolazione civile che diventa soggetto passivo delle loro implicazioni o l'attore che ne fa un uso autonomo e indipendente. In questo paragrafo verranno analizzate le diverse tecnologie e come queste vengono utilizzate contro la popolazione, o da essa stessa, negli scenari di guerra.

a) Internet

L'uso di *internet* ha subito negli ultimi decenni un'accelerazione vertiginosa nell'ambito dei conflitti: fine ultimo della rete è sovente stata la propaganda. D'altronde sono ben note le immagini trasmesse da *Daesh,* il sedicente califfato islamico, tramite siti *internet*, con contenuti che spaziavano dai proclami dei loro *leader*, alle esecuzioni di prigionieri o ancora gli spezzoni di addestramento dei propri miliziani. Ancora prima di *Daesh,* i Talebani e *al-Qaeda* usavano le stesse tattiche, attraverso i proclami dei loro esponenti, come Bin Laden, o filmando gli attacchi perpetrati dalle loro forze contro truppe USA e NATO, a scopo propagandistico. L'obiettivo era duplice: creare proselitismo, diretto o indiretto, mediante una reale affiliazione all'associazione terroristica o con la semplice emulazione (i cosiddetti *lupi solitari*), con lo scopo aggiuntivo di influenzare l'opinione pubblica occidentale, caratterizzata da un rifiuto per la guerra nella sua brutalità, tanto da mettere in discussione

l'impegno dei propri militari in lande desolate e apparentemente svincolate dalla realtà quotidiana.

Al-Qaeda ha sfruttato questo fenomeno durante il conflitto iracheno, beneficiando di combattenti stranieri, i cosiddetti *foreign fighters*, i quali, ammaliati dalla forza comunicativa del gruppo terroristico, arrivavano in Iraq pronti a combattere per il *jihad,* in difesa dei propri fratelli musulmani oppressi. Questo primo modo di usare *internet* fa leva sull'*appeal* delle immagini e delle parole trasmesse tramite la rete per arruolare nuovi combattenti. Non accade nulla di diverso rispetto a quanto fatto dalle Forze armate regolari, con la differenza che stavolta sono i terroristi gli emanatori del messaggio: non occorre più recarsi in un centro di arruolamento e presentare dei moduli. Il filtro di istituzioni ivi preposte è assente, con l'aggiunta della potenza amplificatrice di una causa sacra che coinvolge spesso coloro che sono ai margini della società, più inclini alla radicalizzazione.

Con l'IS anche il processo di arruolamento, con la costruzione della fascinazione per il *jihad*, attraversa una nuova fase. Per anni il cammino tra la radicalizzazione, l'arruolamento, il combattimento e il martirio era stato accompagnato dalla vita nell'ombra, dal silenzio e dal segreto. Dei *mujaheddin* conoscevamo i volti solo dopo il sacrificio, quando ormai si erano trasformati in *shahid*, in martiri. Oggi non è più così: in *internet* i combattenti discutono, postano i video della partenza verso il nuovo Stato, raccontano una loro quotidianità fatta d'indottrinamento e di modelli di vita alternativi a quelli da cui provengono. I nuovi combattenti trovano un palcoscenico in cui possono essere protagonisti già in questa vita, prima dei martiri. Gli *shahid* hanno una platea globale cui rivolgersi, una popolarità insperata, e quindi il loro viaggio, spesso senza ritorno, si colora di prospettive magnifiche di vite che alternano atti eroici a gioie quotidiane: questo è l'IS che viene raccontato nei loro video postati sul *web.* La rete è ora in grado di arruolare cittadini contro il loro stesso Stato, creando il mito di un ideale e di combattenti pronti a morire per esso.

Inoltre, la propaganda mira anche a creare degli emulatori, non formalmente affiliati con l'organizzazione terroristica, spinti a imbracciare le armi o qualsiasi altro mezzo contro i miscredenti. Stavolta la portata dell'indottrinamento è ancora più grande, perché non necessita di un contatto diretto tra il reclutatore e l'aspirante miliziano; occorre solo che l'idea venga assorbita per creare un attentatore pronto a morire, i cosiddetti *lone wolf.* La propaganda è divulgata nella rete sotto forma di video pronti a risucchiare nel vortice *jihadista* normali cittadini, attecchendo prevalentemente nei giovani delle classi più povere, spesso figli o nipoti di immigrati di prima generazione, che stanno negli strati più bassi della società. I filmati non contengono solo messaggi ideologici ma suggeriscono spesso la

modalità d'azione, come quando invitano a "*schiacciare gli infedeli con le automobili*"[23]. *Internet* è ora in grado di creare nuove armi, gli uomini stessi, i cosiddetti lupi solitari introvabili dalle *intelligence* mondiali perché non hanno nessun legame fisico o comunicativo con l'organizzazione terroristica e che diventano delle macchine di morte pronte a tutto. Essi sono disposti a perpetrare attacchi suicidi e sono in grado di usare coltelli, bombe rudimentali, armi da fuoco e autoveicoli. Il limite è solo nell'immaginazione, avendo *internet* dimostrato di poter trasformare normali cittadini in sanguinosi terroristi.

La propaganda non serve solo a favorire il proselitismo, ma anche a terrorizzare la popolazione, fungendo da megafono di attacchi compiuti: a volte le organizzazioni possono creare un clima di paura anche solo con le minacce, i proclami, le dimostrazioni, le esecuzioni. Proprio queste ultime, con le famose decapitazioni dei prigionieri da parte di *Daesh,* hanno avuto un forte impatto sulla popolazione occidentale. L'obiettivo è quello di terrorizzare attraverso la creazione di un prodotto mediatico di facile fruizione sia per la distribuzione (un breve video lanciato per ogni assassinio su tutte le piattaforme, comprese quelle mobili) sia per la comprensione, per quanto sia esplicito. Si tratta di una minaccia che si rivolge a tutti e che diventa necessariamente notiziabile dai media. Un altro tema ricorrente è come al *jihadista* piaccia la morte tanto quanto l'occidentale sia attaccato alla vita. I *jihadisti* cercano di dimostrare che essi sono pronti a commettere ogni atrocità per terrorizzare i loro nemici e indebolirne il morale. Anche quando mostra filmati o immagini in cui decapita cittadini occidentali, IS si assicura che la colpa venga attribuita all'Occidente, usando le stesse vittime per ripetere l'atto d'accusa prima dell'esecuzione.

L'uso di internet a scopi propagandistici non si limita ovviamente a organizzazioni terroristiche o paramilitari. La Russia, già anni prima dell'invasione dell'Ucraina del 2022, usava una *guerra digitale ibrida*[24]*,* modalità che verrà trattata nel dettaglio nel terzo capitolo, relativo alle tattiche di guerra non lineari. La popolazione civile, però, nei conflitti moderni ha evidenziato un'inclinazione che la fa discostare dall'immagine di mero soggetto passivo della propaganda o dell'influenza della comunicazione dell'avversario. La guerra russo-ucraina mostra come normali cittadini possano svolgere una funzione di contro-propaganda anche nei confronti di un regime, come quello di Putin, che applica un forte controllo sui media, bloccando ogni forma di dissenso. Subito dopo lo scoppio della guerra, *Anonymous* ha suggerito a tutti, ma in particolare agli ucraini che vivono per testimonianza diretta le vicende belliche, di utilizzare gli spazi dedicati alle foto e alle recensioni di tutti i luoghi di

[23] Cfr. - AA.VV., "Twitter e Jihad: la comunicazione dell'IS", www.ispionline.it (ultimo accesso 13/04/23)
[24] Maksymilian Czuperski, direttore del *Digital Forensic Research Lab.*

interesse russo (ristoranti, gallerie d'arte, pub e monumenti) in *Google Maps* per raccontare quanto stava avvenendo in Ucraina.

Questa iniziativa, tra le altre, serve in particolare per dare ai russi un nuovo mezzo di informazione, ben diverso da quelli di Stato, vassalli di Mosca, così da aggirare efficacemente la propaganda del Cremlino. L'invito è rimasto su *Twitter* fino al 28 febbraio 2022, quattro giorni dopo l'invasione, ma nelle ore successive gli utenti si sono impegnati a condividere informazioni e immagini. Molti utenti hanno risposto alla richiesta di *Anonymous* con grande entusiasmo. Il gruppo *hacker* ha anche aggiunto delle istruzioni sulla modalità con cui recensire: *"Se sono enti vicini al Cremlino, sentitevi liberi di votare una stella, altrimenti andate con le cinque, perché risulteranno più visibili e condividete ogni informazione possibile per sensibilizzare i lettori sul conflitto, magari scrivendo in russo"*[25]*.* Un ulteriore consiglio è stato quello di variare il contenuto delle «recensioni», perché la censura può facilmente rimuovere un gran numero di commenti sfruttando parole chiave in comune, così da operare in automatico. La contro-propaganda ucraina ha lo scopo di rispondere alla disseminazione di *fake news* operata dal Cremlino per rompere il muro della censura e inoculare nella popolazione russa i primissimi anticorpi di dissenso verso il regime.

b) Droni

Non solo i *Predator* o i *Reaper*, le sofisticate piattaforme senza pilota in possesso delle più equipaggiate Forze armate occidentali, rappresentano i droni del futuro. Droni più piccoli, ma capaci di svariate funzioni, che vanno dall'osservazione alla propaganda, da piccoli bombardamenti ad attacchi *kamikaze*, vengono costruiti e usati non più esclusivamente da forze regolari, ma da fazioni irregolari para-militari o dalla popolazione stessa. Dall'attentato al presidente del Venezuela Maduro nel 2018, ai ripetuti attacchi condotti dall'IS, i droni di derivazione civile stanno diventando sempre più diffusi negli scenari di combattimento.

Proprio *Daesh,* nella guerra in Iraq e Siria, ha portato l'impiego di droni a un livello che non si era mai visto prima. Gli scontri feroci nelle vie di Mosul ne testimoniarono l'uso efficace da parte dell'IS, che più volte aveva sorpreso le unità governative con attacchi con i droni. Gli apparecchi usati erano di due tipi: o commerciali, acquistati attraverso intermediari sul mercato civile in Turchia e nel Golfo, o costruiti nelle officine e nei laboratori creati all'interno di abitazioni. Alcuni erano costati poche centinaia di dollari, altri arrivavano a cifre significative oscillanti tra i 3 mila e gli 8 mila dollari[26]. Molti di questi terminali sono di

[25] Cfr. - Lorenzo Nicolao, "Anonymous sfida la censura di Putin con Google Maps: le recensioni di bar e locali raccontano la guerra", www.corriere.it (ultimo accesso 25/03/23)

[26] Cfr. - Olimpo Guido, "La guerra dei droni nuova minaccia IS", www.corriere.it (ultimo accesso 13/04/23)

origine cinese, e dispongono di un'autonomia sufficiente per sferrare un *raid*, *modus operandi* favorito dalle posizioni ravvicinate dei due schieramenti. L'offensiva per liberare la città si era trasformata in una battaglia strada per strada, dunque, gli islamisti poterono organizzare delle sortite con i velivoli, equipaggiandoli con piccole cariche, (di solito granate da 40 millimetri), modificate e dotate di alette «in coda» per aumentarne la stabilità. I droni raggiungevano le aree dove erano localizzati mezzi e truppe nemiche, per poi sganciare l'ordigno da una altezza di circa 300 metri[27]: mini-bombardamenti che colpivano fuoristrada, camioncini, nuclei di soldati. Un'evoluzione di quanto era già stato fatto sia dallo Stato Islamico, sia da altre fazioni coinvolte nel conflitto regionale: gli Hezbollah libanesi e un gruppo d'opposizione siriana ci hanno provato in alcune occasioni, a conferma di una tendenza che va oltre questo specifico teatro. I mini-droni dell'IS permettevano missioni diverse, tutte *low cost*, ed erano ovviamente facilmente trasportabili viste le dimensioni ridotte. Essi erano in grado di azioni dirette contro gli avversari, attraverso il bombardamento, ma anche di svolgere un ruolo guida per gli attentatori suicidi; il loro occhio elettronico ha aiutato i «martiri» a bordo dei mezzi, fornendo indicazioni utili su difese ed eventuali ostacoli; i droni erano usati anche come trappole, con micro-cariche destinate ad esplodere una volta finiti nelle mani degli avversari. Spesso erano delle armi esplosive *kamikaze*, che raggiungevano l'obiettivo e deflagravano.

Per contrastare tale minaccia, sia le autorità di sicurezza, sia gli eserciti sono al lavoro per trovare le opportune risposte. Il Pentagono ha stanziato venti milioni per la ricerca. Iracheni e alleati, durante la guerra con l'IS, avevano dotato gli uomini in prima linea di speciali «fucili» in grado di emettere onde per interrompere i collegamenti del drone, così come esistono sistemi che «confondono» il velivolo e possono provocarne la caduta. Anche gli iraniani hanno fornito apparati simili alle milizie amiche a Bagdad. In Europa alcune aviazioni hanno studiato tecniche che prevedono l'intervento di elicotteri. I francesi, imitando un progetto olandese, sperimentano una contromisura «naturale»: quattro aquile addestrate a ghermire il drone. Nella base di Mont de Marsan, nel sud del Paese, i militari hanno preparato i volatili che avrebbero dato risultati soddisfacenti. Nella guerra russo-ucraina la popolazione civile ha collaborato direttamente con le forze militari di Kiev, mettendo a disposizione i propri droni, pilotandoli, costruendoli o modificandoli. I civili impiegano questi dispositivi per l'osservazione e la raccolta informativa delle truppe nemiche. Anche in Ucraina, quindi, l'impiego di mini-UAV a scopo offensivo è sempre più massiccio. Le forze speciali di Kiev usano i droni per recapitare piccole munizioni con un carico esplosivo di poco superiore ai 2 chilogrammi per un raggio d'azione attorno ai 50 chilometri; vengono

[27] Ibidem

impiegati prevalentemente droni di dimensioni ridotte, economici, del tipo para-commerciale (ai quali vengono apportate più modifiche). Stiamo parlando di quadricotteri Matrice 300 o *Mavic*, entrambi prodotti in Cina, ma acquistati su canali paralleli dal momento che ogni azienda produttrice cinese ha preso le distanze dalla guerra. Dispositivi che una volta in prima linea vengono commutati in armi da battaglia per la guerra moderna. Si tratta di qualcosa di mai visto, solo teorizzato. Le forze speciali ucraine impiegano i *Mavic* con piccole lattine riempite di esplosivo e collegate a un sistema di sganciamento per farle cadere sul nemico, abbatterlo e sottoporlo ad una nuova sorta di guerra psicologica, dato che le lattine esplosive vengono impiegate anche sugli accampamenti russi, colpendo i soldati di Mosca nei momenti in cui si sentono più al sicuro. Un altro impiego dei droni da parte delle forze speciali è incentrato sull'osservazione del campo di battaglia. Piccole unità dotate di droni da ricognizione che hanno preso il nome di *"Ochi"* (Occhi), che vengono dispiegate su varie posizioni del fronte e attraverso i propri piccoli velivoli seguono gli spostamenti delle truppe russe dall'alto, e una volta individuate, inviano al proprio Comando le coordinate di postazioni nemiche, batterie d'artiglieria e sistemi da guerra sofisticati che "meritino" l'impiego di munizionamento guidato ucraino.

c) GPS

L'uso del GPS nelle guerre moderne è diventato imprescindibile. Che siano adoperati per la navigazione terrestre, per l'invio di coordinate a scopo difensivo (*MEDEVAC*, richiesta di rinforzi) o offensivo (per comunicare la posizione di truppe nemiche), i dati satellitari rappresentano una risorsa fondamentale per le forze militari. Oscurare i GPS dell'avversario e procurarsi le coordinate delle truppe della controparte tramite apparati di geolocalizzazione sono pratiche che sono state largamente usate nel conflitto russo-ucraino. La Federazione Russa ha usato le sue capacità di guerra elettronica non solo per bersagliare i GPS ucraini fin dal conflitto in Crimea nel 2014, ma anche per protezione interna: ad esempio quando Vladimir Putin si muove intorno a Mosca, come rivela un rapporto del *Center for Advanced Defence Studies* americano. I bersagli più delicati sono ritenuti gli aerei, i quali tuttavia possono usufruire di assetti dedicati, capaci di limitare i segnali elettronici di disturbo che risultano però efficaci soltanto a breve distanza. Diversa è la situazione per i ricevitori civili, più facili da alterare. I russi hanno attuato atti di oscuramento satellitari abbastanza regolarmente nella guerra contro il governo di Kiev, costringendo gli ucraini a continui aggiustamenti in termini di difesa cibernetica.

Ogni cellulare però può essere usato per inviare e individuare le coordinate di truppe. Se in zona di combattimento non vengono utilizzate procedure di sicurezza per disabilitare

la condivisione della propria posizione su determinati siti internet o la geolocalizzazione quando si scatta una foto, un semplice telefono può tradire la segretezza di un intero piano militare. Non è un caso che sia stato dato l'ordine alle unità russe al fronte di spegnere i cellulari non di servizio. Il quotidiano inglese *"The Sun"*[28] ha riportato la notizia di decine di profili di soldati russi sull'App di incontri *"Tinder"*, con tanto di geolocalizzazione e con foto che mettono in bella vista uniformi, insegne, armamento ed equipaggiamento vario. Le informazioni ricavate dalla App gratuita sono state condivise dai civili ucraini con i servizi di *intelligence*, e hanno aiutato a comprendere i movimenti delle forze russe sulla linea di combattimento.

d) Immagini satellitari

Il 2 maggio del 2011 le forze speciali americane, ad Abottabad, dopo un'azione diretta nella notte, neutralizzavano Osama Bin Laden. L'attacco non sarebbe stato possibile senza la sorveglianza attuata per mesi, attraverso immagini satellitari, del complesso dove il *leader di al-Qaeda s*i nascondeva. Era infattibile per l'*intelligence* americana avvicinarsi senza compromettersi e, per confermare l'identità dell'obiettivo, furono usati metodi comparativi delle ombre e dei movimenti. Anche *Google Maps* fu adoperato per avere un confronto della struttura con gli anni precedenti. I servizi d'informazione americani hanno usato in maniera continuativa le immagini satellitari per sorvegliare gruppi terroristici o sospetti affiliati.

Uno dei primi supporti, oltre che uno dei più consistenti, che gli USA hanno fornito agli ucraini dopo l'invasione riguarda proprio le immagini satellitari, per localizzare e tracciare i movimenti delle truppe russe. I funzionari ucraini hanno chiesto direttamente aiuto a tutti i *big* della tecnologia, compresi Tim Cook, ceo di *Apple*, ed Elon Musk, l'uomo più ricco del mondo, nonché l'imprenditore al comando di *Tesla* e di *Space X*. Mykhailo Fedorov, ministro responsabile del digitale in Ucraina, ha chiesto a Musk di fornire all'Ucraina le stazioni internet *Starlink*: "*Mentre voi cercate di colonizzare Marte, la Russia sta cercando di occupare l'Ucraina. Ti chiediamo di mettere a disposizione dell'Ucraina le stazioni Starlink e di arrivare ai russi sani di mente affinché prendano una posizione*"[29], ha dichiarato il ministro rivolgendosi all'imprenditore. Musk ha risposto all'appello di Fedorov il 25 febbraio 2022, affermando che un satellite *Starlink*, lanciato il giorno prima, era in posizione e che le stazioni di terra erano in viaggio verso l'Ucraina. Questo ha consentito all'Ucraina di disporre

[28] Parker Nick, "Russian soldiers bombard Ukrainian girls with flirty Tinder request, www.thesun.co.uk (ultimo accesso 3/03/23)

[29] Cfr. - Emiliano Ragoni, "Elon Musk mette a disposizione dell'Ucraina i satelliti di Starlink", www.corriere.it (ultimo accesso 3/4/23)

nuovamente del collegamento internet che, a seguito dell'*escalation* militare, era stato fortemente limitato.

3. Uso dell'informazione

La comunicazione globale si basa oggi su sistemi estremamente veloci, ma la maggior subordinazione alla tecnologia li rende contemporaneamente vulnerabili. Sono l'utilizzo delle informazioni e dei sistemi tecnologici collegati che consentono la superiorità informativa, prerequisito indispensabile per mantenere la propria libertà d'azione soprattutto nelle situazioni di crisi.

Il "sistema informativo" è dunque il luogo ove i sistemi umani e automatizzati osservano, orientano e prendono decisioni sulla base di tempestivi flussi informativi. I sistemi umani sono rappresentati dai responsabili dei processi decisionali, mentre i sistemi automatizzati sono i materiali e le strutture utilizzati per raccogliere, elaborare e disseminare le informazioni (reti, cyberspazio). Il sistema informativo è pertanto costituito da tre sfere correlate: fisica, informativa e cognitiva. Comprendere ed usare le informazioni in tutti i campi, da quello militare, a quello economico e diplomatico, ha sempre rappresentato un vantaggio imprescindibile. Ecco, quindi, l'incontestabile beneficio nel conseguire e mantenere il controllo dei sistemi e mezzi che sostengono tale flusso informativo da e verso i *decision makers*, garantendosi così l'*information superiority*.

I sistemi computerizzati costituiscono il nocciolo di tutti i sistemi di comando e controllo (C2) non solo militari; l'affidabilità degli stessi è fondamentale per quello che viene definito oggi C4ISR: Comando, Controllo, Comunicazione, Computers, Intelligence, Sorveglianza e Ricognizione. Internet infine rappresenta lo strumento più potente mai esistito per la divulgazione e circolazione dei dati, ad una velocità inconcepibile fino a pochi anni fa. Potente ma allo stesso tempo vulnerabile; in esso si diffondono notizie ed opinioni non controllabili, svincolate da ogni forma di esame della fonte attraverso le piattaforme *social*.

Le operazioni informative e di *intelligence online* non sono un fenomeno nuovo: molti esperti ritengono il conflitto Israele-Gaza del 2012 come la prima "guerra *Twitter*" al mondo, ma questi tipi di operazioni hanno assunto un ruolo davvero rilevante nel conflitto tra Russia e Ucraina. Nei primi giorni dell'invasione gli ucraini si sono dimostrati particolarmente abili nel veicolare il proprio messaggio attraverso *meme*, video e foto. Per l'Ucraina, mantenere l'attenzione dell'Occidente sul conflitto è stato fondamentale per sensibilizzare i governi e l'opinione pubblica, affinché fosse garantita una qualsiasi forma di sostegno. I giornalisti hanno descritto l'invasione dell'Ucraina come la "prima guerra *TikTok"*, la "guerra più accessibile a Internet della storia" e la guerra dei *social media* "più virale" di sempre.

Gli ucraini e i loro sostenitori hanno usato i *social media* per colpire, sminuire e demotivare i russi, cercando di incoraggiare i propri cittadini e, al contempo, fiaccare il morale degli invasori. Una grande quantità di video trasmessi in tempo reale su *Facebook, Telegram, TikTok* e *Twitter* ha smorzato la propaganda del Cremlino e ha radunato il mondo dalla parte dell'Ucraina mentre combatte per difendere la sua democrazia. La Russia è stata a lungo considerata abile nello sfruttare le opportunità offerte dalla rete: la sua macchina di propaganda ha usato per anni, ad esempio, i *social media* per screditare gli avversari e influenzare l'opinione pubblica. L'Ucraina, una volta attaccata, ha iniziato a fronteggiare la Russia sullo stesso terreno, attraverso una comunicazione costante e mirata per incoraggiare la resistenza e dar prova della propria resilienza sul palcoscenico globale.

Le tattiche rivelano come i *social media* abbiano aperto una nuova dimensione della guerra moderna, mostrando come Internet sia diventato non solo un territorio su cui combattere virtualmente, ma uno strumento per ottenere risultati concreti nel mondo reale.

La diffusione in rete di materiale video è risultata particolarmente efficace, contribuendo a trasformare storie locali di coraggio in leggende virali e, al contempo, a rendere pubblica una guerra che la Russia avrebbe preferito tener fuori dai riflettori.

Gli ucraini hanno pubblicato video di sé stessi mentre attaccavano carri armati avversari, sorvegliavano villaggi, preparavano *molotov* e le lanciavano contro i veicoli russi. Gli ucraini hanno anche utilizzato i *social media* per incoraggiare la levata in massa dei civili rimasti ancora esterni al conflitto. Rivolgendosi alla porzione femminile della popolazione, Kira Rudik, un membro del Parlamento, ha pubblicato su *Instagram* e *Twitter* una foto di sé stessa, a piedi nudi e con in mano un fucile Kalashnikov e seguita da una frase: "*Le nostre donne proteggeranno il nostro suolo allo stesso modo dei nostri uomini*". Altri *social* sono stati utilizzati, invece, come potenti strumenti di *intelligence:* un canale *Telegram* ucraino, ad esempio, ha esortato i suoi 400.000 abbonati a "filmare attentamente" e condividere video del passaggio delle truppe russe in modo che i combattenti ucraini potessero ingaggiarli; analogamente, lo stesso strumento ha permesso di condividere video e informazioni sui segnali in codice usati dai sabotatori russi.

I *social network* si sono rivelati anche strumento atto ad intimorire gli aggressori: in questo senso si deve leggere la diffusione di immagini raffiguranti i rottami carbonizzati dei veicoli militari avversari e dei corpi dei soldati russi deceduti.

Gli ucraini hanno anche condiviso istruzioni *online* su come evitare il fuoco dei cecchini, bloccare le strade e preparare *molotov*. A Kharkiv, il governatore ha usato *Telegram* per avvisare i residenti, consigliando loro di "*rimanere a casa e nascondersi durante la completa distruzione del nemico russo in città*". Il ministero dell'Interno ucraino ha utilizzato Internet

per stimolare il dissenso in Russia, pubblicando foto e video di soldati russi uccisi o catturati su un sito *web* e su un *account Telegram*, invitando i membri delle loro famiglie a chiedere a Putin di porre fine al conflitto.

L'invasione dell'Ucraina ha generato una miniera di dati digitali che potrebbero essere in futuro utilizzati per perseguire presunti crimini di guerra: attivisti e semplici cittadini si affidano agli *smartphone* per archiviare foto e video che documentano gli abusi.

In aggiunta, un'innovazione chiave nell'uso dell'informazione è stata rappresentata dallo sviluppo di App di *crowdsourcing* per fini militari. All'inizio del 2020, prima della guerra, l'Ucraina aveva lanciato l'*App Diia*, intesa come un'iniziativa di buon governo per rendere più facile per i cittadini rinnovare i permessi di licenza, pagare i biglietti del parcheggio e segnalare disservizi. Con l'invasione russa, il governo ucraino ha riproposto l'*App* per fungere da occhi e orecchie in prima linea per il proprio esercito. I cittadini possono inviare foto e video geolocalizzati di avvistamenti militari russi tramite l'*App* e segnalare persone ritenute filorusse. Questi dati sono quindi aggregati su una mappa e utilizzati dai funzionari dell'*intelligence*.

Nella battaglia del marzo 2022 per Voznesensk, una città del sud di 35.000 abitanti, i volontari ucraini hanno utilizzato invece l'*App* di messaggistica sociale *Viber* per inviare le coordinate dei carri armati russi e dirigere il fuoco dell'artiglieria. A tutto ciò si aggiunge che molte aree urbane stanno diventando "città intelligenti" in cui le tecnologie dell'informazione e della comunicazione contribuiscono ad aumentare l'efficienza dei servizi, condividere informazioni e migliorare il benessere dei propri cittadini.

La digitalizzazione tuttavia offrirà, al contempo, sempre maggiori opportunità agli avversari di interferire nelle aree urbane senza un gran dispiegamento di forze e risorse. I progressi tecnologici nell'elettronica accelereranno la proliferazione di sistemi autonomi con capacità *lethal* e *non lethal*.

L'uso dell'informazione nei conflitti in aree urbane può avere anche grossi risvolti inerenti la salvaguardia dei civili e del personale esterno al conflitto. Ne sono un esempio le battaglie di Mosul (Iraq) e Marawi (Filippine).

La liberazione di Mosul, nel luglio 2017, ha posto fine a nove mesi di intensi combattimenti urbani tra la coalizione a guida USA e un avversario ibrido rappresentato dall'IS. Attraverso mezzi di trasmissione, volantini, cellulari e Internet, si è cercato di diffondere informazioni vitali verso i civili e i gruppi di resistenza anti-IS all'interno della città. I tentativi di incoraggiarli ad andarsene prima dell'assalto della coalizione hanno avuto successo solo in parte, poiché l'IS teneva in ostaggio molti di loro. Più di 10.000 civili morirono durante la battaglia, di cui 2.300 vittime di danni collaterali.

Contrariamente a Mosul (44% di sfollati), a Marawi la strategia comunicativa messa in atto dal governo filippino si è rivelata molto efficace, garantendo al 98% della popolazione la possibilità di evacuare il campo di battaglia prima che si verificasse lo scontro a fuoco: furono così evitate pesanti perdite civili.

Una piccola citazione è necessaria circa una distorsione dell'uso di *internet* e di taluni sistemi di *editing* audio e video: il cosiddetto *deepfake.* I *deepfake* sono tecniche avanzate di manipolazione delle immagini e dei video, che possono essere utilizzate per creare contenuti audio e video falsi, apparentemente autentici, ma in realtà totalmente inventati.

Una ricerca congiunta del *Department of Psychology* della *Lancaster University* (UK) e del *Department of Electrical Engineering and Computer Sciences* dell'Università di Berkeley, in California, ha analizzato l'impatto dell'Intelligenza Artificiale sul meccanismo cognitivo che porta l'essere umano a fidarsi di più dei volti *deepfake* rispetto a quelli reali. Lo studio è stato pubblicato sulla rivista scientifica PNAS *(Proceedings of the National Academy of Sciences)*[30]. Ebbene, secondo il citato studio, una platea non adeguatamente preparata riconosce solo il 50% dei *deepfakes*, mentre un campione "formato" nel riconoscerli ha una precisione di appena il 60%. In media, quindi, ci si può aspettare che un *deepfake* possa scuotere le percezioni di almeno 4 persone su 10, generando influenze che possono rivelarsi di significativa importanza durante un conflitto. L'esempio della *fake news* dell'arresto di Donald Trump, riportato dalle maggiori agenzie di stampa internazionali[31], ha dimostrato (come si nota dai commenti sul *Tweet* dell'autore) che tali notizie hanno un seguito notevolissimo (circa 6,3 milioni di visite) e generano un dibattito acceso tra sostenitori dell'una o dell'altra tesi. Tale effetto, pantografato sulla popolazione, può creare una maggiore incertezza, portando a ulteriori problemi sociali e politici decisivi in epoca ad esempio di conflitto.

4. Uso della tecnologia in scenari di conflitto urbano

L'ambiente urbano rappresenta da sempre un nodo strategico sul quale i più importanti cultori dell'arte della guerra si sono interrogati. Lo fece Giulio Cesare sviluppando la "muraglia di scudi", tattica che consentiva ai legionari romani di difendersi dagli attacchi della popolazione, quando ingabbiati in un contesto urbano; Napoleone Bonaparte ideò, invece, la "linea di colonna", formazione stretta con la quale le sue truppe riuscivano ad operare in maniera agile adattandosi alle anguste strade cittadine; Georgy Zhukov, durante la battaglia di Stalingrado, ebbe la meglio sulle truppe del Reich grazie ad una strategia che prevedeva

[30] AA.VV., "Deepfake detection by human crowds, machines, and machine-informed crowds**",** www.pnas.org (20/03/2023)
[31] AA.VV., "'Trump arrestato', ma sono foto fake di una intelligenza artificiale", www.ansa.it (20/03/2023)

un impiego innovativo di carri armati ed artiglieria in un contesto urbano; John Warden, nel contesto della guerra del Golfo nel 1991, sviluppò la teoria dell'attacco aereo strategico, con l'uso di bombardamenti aerei mirati contro obiettivi specifici, come ponti, edifici e centrali elettriche, al fine di indebolire l'infrastruttura urbana nemica prima di attaccarla con forze di terra; David Petraeus, durante la guerra in Iraq, promosse tattiche che prevedevano il coinvolgimento della popolazione locale e delle istituzioni locali per cercare di instaurare un clima più permissivo, specie nei centri urbani, e guadagnare così libertà di manovra.

Considerando questo breve *excursus* storico, appare subito chiaro come un centro abitato rappresenti un ambiente del tutto particolare, da analizzare con attenzione, e nel quale le tecniche, le tattiche e le procedure vadano necessariamente riviste. L'impatto, infatti, del contesto cittadino sulle operazioni incide su diversi aspetti. In primo luogo, la densità del tessuto urbano limita di gran lunga la mobilità e la manovra; la presenza di numerosi edifici e strutture garantisce una larga gamma di opzioni per trovare riparo e copertura; la complessità dell'ambiente incide inoltre sulla *situational awareness*, rendendo difficile identificare una minaccia e coordinare adeguatamente un dispositivo. Più di tutto però, quello che rappresenta la variabile cardine dell'intero sistema di combattimento nel centro urbano, è la presenza della popolazione civile; la città rappresenta infatti un serbatoio di potenziali combattenti in grado di decidere le sorti di un conflitto sulla base della loro personale scelta di prendere le armi o meno e a favore di chi. Durante un conflitto armato i civili giocano un ruolo cruciale: essi possono rimanere neutrali ma, se qualcosa riesce a muovere le loro coscienze, sia questa paura, senso di rivalsa o patriottismo, possono da un momento all'altro decidere di schierarsi, apertamente o in maniera occulta, con la conseguenza, indipendentemente da quale sia la forma, di stravolgere i rapporti di forza.

Risulta altresì evidente come le città rappresentino i principali bersagli di attacchi militari e terroristici e siano sempre più teatro di violenze interne allo Stato e di conflitti armati, come si è visto di recente in Iraq, Siria, Libia, Yemen, Georgia e Ucraina. Tradizionalmente la sfida per le forze militari è costituita dallo sconfiggere le minacce radicate e diffuse all'interno della popolazione, senza causare danni collaterali. Invero, il complesso ambiente urbano può determinare un uso della forza spropositato per raggiungere l'*end state*, causando considerevoli perdite di vite umane.

Ciò premesso, al fine di contemperare le esigenze di protezione dei civili con l'intento di non inasprire gli animi della popolazione, l'impiego delle armi moderne e di talune tecnologie emergenti possono rivelarsi utili negli scenari di combattimento urbano. Tra queste, un ruolo significativo viene svolto dalle armi a guida di precisione con capacità di guida *Non-Line-of-Sight*: ne sono un esempio in particolare i mortai che spesso usano una

traiettoria alta per colpire il nemico in strade strette o dietro edifici. Oggi si stanno sviluppando sistemi autonomi, inclusi droni e *robot,* con molteplici capacità di rilevamento. Essi possono essere guidati da un operatore in avanscoperta allo scopo di fornire un allarme tempestivo prima di entrare in un potenziale imbuto letale. Altri, grazie all'utilizzo dell'intelligenza artificiale, potranno eseguire una mappatura completa per "ripulire" gli interni degli edifici o i percorsi sotterranei, prima che qualsiasi essere umano vi faccia il proprio ingresso.

Inoltre, le capacità ISR[32] dei moderni UAV[33] tattici, offrendo la scansione continua di vaste aree, forniscono la possibilità di indagare sugli eventi, valutare il comportamento del bersaglio, estrarre informazioni e determinare l'identità di un attacco. Per eliminare i danni collaterali, alcune di queste armi utilizzano testate con "effetti modulari", consentendo ai pianificatori della missione di concentrare l'effetto all'interno di una piccola area e lasciando intatti i locali o gli edifici vicini. Sebbene questo sia solo un elenco parziale delle capacità disponibili per supportare la guerra urbana, si evidenzia come il potenziale della tecnologia moderna possa incidere su di essa, fornendo agli eserciti moderni gli strumenti per esercitare la massima pressione sul nemico, riducendo al minimo i danni collaterali sulla popolazione.

Per di più, in questa battaglia di influenza, le tecnologie descritte nei paragrafi precedenti stanno svolgendo un ruolo sempre più significativo: internet e i *social media* vengono infatti usati come canali entro i quali convogliare i messaggi propagandistici nella speranza di arrivare ai cuori e alle menti della popolazione civile, spingendo i diversi soggetti neutrali a fare il primo passo verso l'una o l'altra fazione. Questa stessa tecnologia si sta rivelando oltremodo indispensabile anche in un secondo momento quando, a seguito della discesa in campo, si rende necessario coordinare le azioni di questi gruppi volontari.

L'ambiente urbano risulta così un facilitatore della socializzazione dei conflitti. Oltre che rappresentare l'abituale contesto residenziale di un gran numero di civili e dunque un luogo di immediato reclutamento, esso è anche il terreno di scontro nel quale le tattiche convenzionali si stravolgono e magnificano invece le capacità esprimibili da individui che non necessariamente devono essere numerosi, ben addestrati e ben equipaggiati.

Nel prendere la decisione se scendere in campo o meno, il civile è infatti ben conscio del fatto che, a differenza dello scontro in campo aperto, in un contesto urbano la sua efficacia non sarà legata ad un mero rapporto numerico con l'avversario. La sua conoscenza del territorio unita all'agilità di una formazione ridotta sono, infatti, elementi che in questo

[32] *Intelligence, Surveillance and Reconnaissance*
[33] *Unmanned Aerial Vehicle*

ambiente non solo colmano il gap con forze soverchianti, ma spesso ne garantiscono il deterioramento e la sconfitta. Allo stesso modo, il vantaggio proveniente dall'addestramento e dall'equipaggiamento viene in larga parte mitigato dalla complessità del contesto cittadino, dove rapidità di adattamento, velocità di ridispiegamento, capacità di canalizzare la manovra avversaria e utilizzo mirato di armi, non necessariamente di ultima generazione o pesanti, si sono rivelati fattori largamente efficaci.

La tecnologia oggi a disposizione della maggior parte della popolazione, rappresenta di per sé un ulteriore spinta al combattimento. Se, come detto, per i *leader* delle parti in conflitto, essa viene intesa come uno strumento con il quale esercitare un certo grado di influenza sulle masse, per il singolo cittadino la stessa rappresenta invece un vero e proprio moltiplicatore di effetti. Significativo a riguardo è riportare quanto emerso da un'intervista svolta da questo gruppo di lavoro al *Team* di *trainers* del *Joint Multinational Readiness Centre dello United States Army Europe and Africa*. Nel maggio 2022, l'unità statunitense, di stanza in Germania, è stata incaricata di svolgere l'addestramento a favore del personale ucraino all'utilizzo dell'obice M777. L'inesperienza da parte dei fruitori, spesso rappresentati da civili corsi alle armi a difesa del proprio Paese, ha comportato che in alcuni casi, al rientro in Patria, le procedure non fossero ancora ben interiorizzate. In questa situazione, una connessione *internet* ed un sistema di videochiamata, si sono rivelate tecnologie *dual use* di per sé fondamentali per mettere in contatto utilizzatori e istruttori, che pur operando a distanza, hanno potuto garantire un uso efficace del sistema d'arma. Ciò mette in risalto ancora di più come le tecnologie favoriscano la partecipazione della popolazione civile nei conflitti moderni.

5. Considerazioni sul C2 e coordinamento con le parti del conflitto

I sistemi di comando e controllo degli eserciti regolari sono sempre più sofisticati. Un centro di comando dispone di sistemi radio a più bande, capacità di comunicazioni satellitari, *datalink*, difese cibernetiche e sistemi di alimentazione dell'energia elettrica di riserva. Sono spesso protetti in dei *bunker*, occultati all'osservazione terrestre, aerea e spaziale e dotati di contromisure elettromagnetiche e sistemi di comunicazione criptati. Possono essere avanzati e arretrati, con vie di fuga da utilizzare nel caso in cui il nemico si avvicini e piani di contingenza per distruggere qualsiasi informazione possa cadere nelle mani dell'avversario. Tutto questo sembra quasi stonare quando lo si paragona ai mezzi di comando e controllo di organizzazioni terroristiche e paramilitari, che in molti casi riducono al minimo l'uso della tecnologia, vanificando gli elaborati mezzi convenzionali che avrebbero lo scopo di intercettarli e localizzarli. Bin Laden non si nascondeva, almeno non nella parte

finale della sua clandestinità, in qualche caverna isolata tra le montagne dell'Afghanistan. Il Califfo si era rifugiato ad Abottabad, a pochissima distanza dall'accademia militare pakistana. La CIA utilizzò i suoi migliori sistemi di osservazione e intercettazione per scovarlo e monitorlarlo, ma fino alla fine, nonostante tutte le tecnologie usate, non c'era alcuna certezza che fosse proprio Bin Laden l'uomo che risiedeva in quel comprensorio. Quando si paragona in che modo al-Qaeda disseminava le informazioni provenienti del suo *leader* alle metodologie iper-avanzate dell*'intelligence* americana, si ha quasi l'impressione di una contraddizione evidente: i terroristi usavano il passato invece che il futuro per eludere gli avversari. Nessuna radio o computer, ma passaggi di piccoli documenti su carta di mano in mano, che raggiungevano il destinatario, a scopi propagandistici, ma contenenti anche ordini e disposizioni per la struttura militare. Il corriere di Bin Laden, Abu Ahmed al-Kuwaiti, era l'unico a raggiungere il Califfo, per poi portare il messaggio al destinatario richiesto, non prima di una lunga catena di ulteriori messaggeri. La filiera della comunicazione era inconsapevole dell'identità dei livelli più alti da cui proveniva il messaggio, rendendo impossibile ogni forma di interrogatorio, in caso di cattura. Lo stesso Abu Ahmed accendeva il cellulare solo per chiamare la madre e lo faceva all'interno di un veicolo in movimento che transitava in un mercato affollato, girando lì attorno fino al termine della telefonata, rendendo ogni tentativo d'intercettazione vano. I terroristi trovarono nella negazione della tecnologia il miglior modo di combatterla e seppur alla fine la CIA sia riuscita nell'eliminazione di Bin Laden, se si esaminano gli anni impiegati dagli americani e le ingenti risorse di quella che è stata una delle più accanite "caccia all'uomo" della storia dell'umanità, si percepisce il successo che queste tattiche hanno avuto.

Le organizzazioni terroristiche e insurrezionali hanno saputo utilizzare anche metodi più moderni per comunicare, specie quando era necessaria la capillarità. In Afghanistan, ad esempio, semplici contadini con cellulari e radio avvisavano i Talebani dei movimenti dei convogli della NATO, cancellando l'effetto sorpresa di molte operazioni. L'uso dei civili per passare informazioni e comunicazioni non è certo nuovo; nella Seconda Guerra Mondiale i Partigiani italiani usavano staffette non militanti per recapitare messaggi di varia natura. Spesso usavano anche bambini: basti pensare a Oriana Fallaci che recapitava comunicazioni, in sella alla sua bicicletta, a soli quattordici anni. Ciò che cambia, nei conflitti moderni, è il canale con cui le informazioni sono veicolate, soprattutto i cellulari, attraverso messaggi, chiamate e *social network*. A meno di intercettazioni su larga scala, per quanto questi sistemi non siano criptati, risulta difficile individuare e tracciare le comunicazioni, necessitando di sforzi colossali che richiedono personale e risorse non indifferenti.

Anche in una guerra convenzionale come quella russo-ucraina la popolazione e i sistemi di comunicazione civili sono largamente usati e spesso inglobati nella struttura di comando e controllo. Il *Washington Post* conferma che, in Ucraina, l'esercito di Putin si è affidato con frequenza «sorprendente» a sistemi di comunicazione non protetti — *smartphone e walkie-talkie* — che stanno rendendo più vulnerabili le unità sul campo, già vittime di frequenti imboscate per opera della resistenza e così più facilmente localizzabili, ma che evidenzia anche i problemi di comando e controllo. I russi hanno a disposizione attrezzature moderne per le trasmissioni sicure ma, oltre ad aver danneggiato le infrastrutture per la comunicazione ucraine, i soldati fanno spesso ricorso a normali cellulari, al punto che — ha rivelato un anonimo funzionario di *intelligence* europeo[34] — i comandanti moscoviti sono stati in parecchie occasioni costretti a sequestrare il telefono personale dei loro subordinati per paura che potessero involontariamente rivelare la posizione della propria unità. Altri *report* hanno raccontato di radio ricetrasmittenti d'origine cinese, poco affidabili e non protette; una presenza attribuita a corruzione e carenze. Questa narrazione da un lato tiene certamente conto di quanto visto sul campo, ma dall'altro è usata dalla propaganda per sottolineare come Mosca avrebbe mandato i suoi «figli» allo sbaraglio. Insieme al cibo scarso e ai mezzi in avaria, ecco gli apparati per comunicare inadatti. Tutto può essere, tutto può accadere, basta ricordare che in ogni conflitto le valutazioni possono mutare spesso. Al tempo stesso è noto che Stati Uniti e alleati della Nato stanno fornendo a Kiev strumenti in grado di interrompere le trasmissioni russe, inducendo gli uomini di Putin a ricorrere a comunicazioni meno sicure che possono essere intercettate più facilmente. D'altronde, spiega al Post Kostas Tigkos, analista del *Janes Group*, un conto è costruire un ottimo sistema, come hanno fatto i russi, un altro è impiegarlo in battaglia per condurre operazioni complesse che coinvolgono migliaia di unità in movimento. Sono numerose le telefonate intercettate, anche da radioamatori, che sono state pubblicate online, su *YouTube* o sui *social*. Pur confermando alcuni dettagli, lo stesso Pentagono definisce questi episodi «aneddotici», ovvero frutto di informazioni dal campo non confermate. Molti analisti militari, inoltre, invitano a non generalizzare sui problemi di comunicazione; alcune unità possono averne avuti, altre no. Anche perché fra le prede belliche finite nelle mani ucraine ci sono pezzi sofisticati. Alcune foto hanno mostrato sistemi criptati in dotazione ai *commandos Spetsnaz*. Nella zona di Kiev è stato rinvenuto ad esempio un *container* militare abbandonato che gli esperti hanno riconosciuto essere parte del «modulo» Krasukha 4, usato per coprire i movimenti dell'Armata: il sistema serve a confondere i radar, i sensori degli aerei-radar e altre piattaforme simili usate dagli avversari. Qualche giorno dopo però un altro osservatore ha espresso riserve sul fatto che fosse davvero un «pezzo» così

[34] Cfr. – AA.VV., "L'aggiornamento militare sulla guerra in Ucraina: sistemi non criptati e cellulari rubati, tutti i problemi di comunicazione dei russi", www.corriere.it (5/2/23)

prezioso. Una conferma empirica del fatto che siamo su un terreno molle, fangoso, simile a quello che ha dato tanti guai ai generali dello zar. Eppure i russi sono sempre lì, a martellare l'avversario.

D'altra parte gli ucraini si sono ingegnati in modi sempre più originali per sfruttare tecnologia di derivazione non militare per implementare i sistemi di comando e controllo. Gli *smartphone*, per esempio, sono stati usati per capitalizzare la ricchezza di informazioni digitali che circolava in rete. L'Sbu (l'intelligence ucraina) ha creato un *chatbot*, ovvero un *software* automatico, opportunamente programmato, che funziona sui canali dell'App Telegram, la piattaforma che più di tutte ha occupato il centro della piazza digitale in questa guerra. Il bot, chiamato *"Stop Russian War"*, ha permesso di mandare in rete la posizione dei mezzi russi, con tanto di fotografie e video in tempo reale. In un secondo momento, i funzionari ucraini hanno reso ancora più facile per i cittadini caricare le posizioni dei nemici attraverso l'utilizzo di App governativa Diia (trattata nel para 3 capitolo 2). Le informazioni ricavate venivano verificate da droni militari prima di passare le coordinate all'artiglieria ucraina o all'aeronautica. I tantissimi video che mostrano resti carbonizzati di mezzi russi sulle strade di Bucha, Hostomel e Irpin, città non distanti da Kiev, sono diventate una conferma dell'efficacia della strategia di Kiev.

«Le persone intrappolate dietro le linee russe che usavano i *chatbot* hanno dato vita a una versione del XXI secolo dei partigiani che agivano dietro le linee naziste durante la seconda guerra mondiale»[35] ha detto, citato dal Financial Time, Mstyslav Banik, un alto funzionario del ministero della Trasformazione digitale che ha creato Diia.

Quando i russi si sono resi conto di quello che stava accadendo, hanno iniziato a girare di casa in casa per sequestrare *smartphone*, computer portatili e qualsiasi altro dispositivo, secondo testimoni citati dal *Financial Times*. Poi, per tagliare fuori gli ucraini nei territori occupati, le truppe di Mosca hanno cominciato a distruggere le antenne di trasmissione della rete 4G, ma questo ha reso impossibile agli stessi russi di utilizzare il loro sistema criptato, che lo necessita. La comunicazione tra le unità, di conseguenza, è diventata ancora più difficile, rendendo più complicato seguire il piano d'invasione stabilito.

Gli errori decisivi dei russi sono stati anche altri, come il danneggiamento della diga Kozarovychi sul Dnepr, che ha inondato la pianura, e il resto l'ha fatto l'accanita resistenza ucraina a Irpin e a Horenka, che se conquistate avrebbero spalancato la porta di Kiev ai russi. Tuttavia, è ormai lampante come oggetti che consideriamo banali e spesso futili, come i cellulari, hanno giocato un ruolo preziosissimo, per la prima volta nella storia militare di un conflitto convenzionale.

[35] Cfr. – Paolo Ottolina, "Smartphone (e tappetini di gomma di 2 euro): le armi a sorpresa per respingere l'attacco russo a Kyev", www.corriere.it (06/06/23)

Capitolo 3

La guerra non lineare (o ibrida) per la Federazione Russa

Il termine guerra non lineare (o ibrida) esprime un'ampia gamma di opzioni inclusive di stili e metodi complementari al tradizionale concetto di guerra convenzionale, in una sorta di accostamento di tattiche differenti, incluse quelle asimmetriche; il Colonnello americano *Frank Hoffman* la definì come la combinazione di nuove tecnologie e stili di combattimento nei quali la presenza statale tradizionale e l'osservanza delle regole, delle leggi e dei costumi di guerra perde decisamente di centralità[36].

La combinazione di metodi di guerra è in realtà tipica della maggior parte dei conflitti nella storia umana. Già in passato, come ad esempio durante la ribellione ebraica del 66 d.C., le guerre di indipendenza spagnole del XIX secolo, la Seconda guerra mondiale ed in Vietnam del Nord, forze con caratteristiche ibride impiegarono tattiche non convenzionali, combinate a campagne informative, per il raggiungimento dei rispettivi obiettivi. Dall'inizio del XXI secolo stiamo assistendo ad un incremento di conflitti ibridi condotti da attori statali e non, a tal punto che, nell'aprile 2017, l'Unione europea ha istituito il Centro europeo di eccellenza per il contrasto alle minacce ibride ad Helsinki, dove è stato ribadito che la minaccia principale per una Nazione risiede nella capacità avversaria di avviare un attacco multiforme prima che lo Stato preso di mira se ne renda conto. In tale contesto, caratterizzato da relazioni complesse e dinamiche, è richiesto non solo un nuovo modo di pensare alle sfide strategiche, alle minacce e alle opportunità, ma anche una presa di coscienza dell'importanza del dominio umano (psicologico e informativo) e una conoscenza dei metodi di accesso avversari a tale dominio[37].

La guerra ibrida prevede l'uso simultaneo di sistemi convenzionali e non, tra i quali anche elementi di natura irregolare o asimmetrica, come atti terroristici e *"criminal disorder"*, generalmente diretti e coordinati per ottenere effetti sinergici nelle dimensioni fisiche e psicologiche del conflitto[38].

A tale scopo sono utilizzate, ad esempio, le "*influence operations*" che cercano di minare la fiducia nel sistema *target* e di fungere da moltiplicatore di forze attraverso diverse azioni non cinetiche come la disinformazione, la coercizione, la corruzione, il *"Lawfare"*[39]*,* le *"DeepFakes*" e l'uso di reti terroristiche e criminali. La Federazione Russa si è dimostrata,

---

[36] Frank G. Hoffman, *"Hybrid Warfare and Challenges"*, Joint Force Quarterly 52, (2009).
[37] Frank G. Hoffman e James N. Mattis, *"Future Wars: The Rise of Hybrid Wars"*, (2005).
[38] Frank G. Hoffman, *"Conflict in the 21st Century: The Rise of Hybrid Wars"*, (Arlington: Potomac Institute of Policy Studies, 2007).
[39] Colonel Charles J. Dunlap Jr., *"Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts"* Humanitarian Challenges in Military Intervention Conference (November 2001).

fin dal 2014, particolarmente abile e spregiudicata nell'uso della propaganda e della disinformazione allo scopo di ottenere un ambiente e un'opinione pubblica favorevole a Mosca, non solo nei Paesi terzi ma anche negli stessi Paesi *target.*

L'impiego della forza sotto soglia, gli attacchi informatici, la coercizione economica e politica, la sovversione e la guerra dell'informazione possono essere singolarmente sviluppati in una campagna di guerra ibrida e concettualizzati come strumenti da tenere a disposizione in una sorta di "cassetta degli attrezzi". Questa strategia, definita "integrale" dai russi, che vede l'accoppiamento di azioni asimmetriche e convenzionali con il contributo delle tecnologie digitali (*cyber* e disinformazione), è chiamato "guerra non lineare", che è l'equivalente del concetto occidentale di "guerra ibrida".

Con particolare riferimento all'Unione Sovietica, questa sviluppò negli anni '20 il concetto di "guerra mascherata" (*maskirovka*) che comprendeva, accanto alle tattiche tradizionali, varie misure attive e passive progettate per ingannare un nemico e influenzare l'opinione pubblica occidentale[40]; questi strumenti dovevano essere adattati in funzione dello Stato obiettivo sfruttando a proprio vantaggio[41] legami commerciali, religiosi, etnici (panslavismo, minoranza di lingua russa, organizzazioni compatriote) e giuridici (neutralità)[42].

Di recente sviluppo tattico è il concetto di "*Lawfare*" che cerca di aiutare gli Stati a sviluppare una narrativa legalmente fondata che giustifichi le loro azioni e la loro aggressività. Un esempio è il caso della Crimea in cui la Russia ha affermato come il "*The Kosovo Precedent"* (la secessione del Kosovo dalla Serbia) abbia fornito un precedente legale internazionale[43] per la secessione dall'Ucraina.

Nell'ultimo ventennio sono presenti diversi esempi di applicazione di tecniche di guerra ibrida da parte di Mosca.

In Estonia, nel gennaio 2007, il governo aveva annunciato l'intenzione di spostare una statua di bronzo del periodo Sovietico dal centro della capitale Tallinn a un cimitero militare, contro il parere del governo russo[44]. L'Estonia, il "Paese più connesso" d'Europa subì attacchi informatici, condotti in maggioranza da *hacker* probabilmente reclutati dal governo russo, configurando i *cyber* attacchi più grandi e dirompenti a livello nazionale mai lanciati[45].

---

40 Merle Maigre, *"Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO"* The German Marshall Fund of the United States (12 February 2015).

41 Julio Miranda Calha, *"Hybrid Warfare: NATO's New Strategic Challenge?"* Draft General Report (Brussels: NATO Parliamentary Assembly (7 April 2015).

42 Vladislava Vojtiskova, Vit Novotny, Hubertus Schmid-Schmidsfelden, and Kristina Potapova, "*The Bear in Sheep's Clothing: Russia's Government Funded Organizations in the EU"* (Brussels: Wilfried Martens Centre for European Studies, 2016).

43 J. Dunlap, Jr., *"Lawfare: A Decisive Element of 21st Century Conflicts?"* JF Quarterly (July 2009).

44 Cfr. – Andreas Schmidt, *"The Estonian Cyberattacks",* www.researchgate.net (20/03/2023).

45 Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies" (Cybersecurity Interdisciplinary Systems Laboratory Sloan School of Management, Massachusetts Institute of Technology, May 2017).

In Georgia, tre settimane prima dell'incursione delle *Conventional Forces* russe dell'agosto 2008, venne messa in campo un'efficace campagna di guerra ibrida in cui vennero utilizzati attacchi informatici che impedirono agli *hacker* georgiani di sferrare il contrattacco[46], evitando così ai russi attacchi fisici più distruttivi e costosi.

Anche in Ucraina orientale e meridionale, le azioni della Russia hanno fatto largo ricorso all'impiego di SOF, agenti dell'*intelligence*, provocatori politici e rappresentanti dei media, nonché elementi criminali transnazionali e metodi che includono l'istigazione alla sovversione.

Alla luce di quanto detto, appare opportuno evidenziare il fatto che la guerra ibrida sia caratterizzata da una struttura operativa altamente flessibile, grazie all'uso di operazioni convenzionali e non all'interno delle cosiddette "*grey zone*", ossia aree sfocate in cui diventa sempre più difficile distinguere le azioni in tempo di pace da quelle in tempo di guerra e viceversa. Queste nuove caratteristiche dei conflitti pongono importanti sfide e rendono necessario uno sforzo di intelligence su vasta scala, al fine di contrastare le possibili minacce. A partire dal 2009, allo scopo di adeguarsi ai cambiamenti in corso, l'imponente struttura militare tradizionale russa è stata modificata e resa più agile e meglio preparata comprendendo un *pool* di forze di dispiegamento rapido costituite da *Special Operation Forces* (SOF) e truppe aviotrasportate. Inoltre, la conduzione di attività congiunte tra agenzie e ministeri è stata affidata al Centro di controllo della difesa, istituito nel 2014, facilitata anche dalla riforma normativa che ha semplificato l'impiego delle truppe all'estero.

1. Concettualizzazione teorica della guerra ibrida russa[47]

Nel 2013, il generale *Valery Gerasimov*, allora capo di stato maggiore della Federazione Russa, ha pubblicato un articolo basato sulle sue percezioni della Primavera araba e dell'*Euromaidan*[48]*. Gerasimov* ha messo in luce come i conflitti siano cambiati, prevedendo l'uso combinato di metodi diplomatici, economici, politici e altri non militari, insieme alla forza militare diretta[49].

Si prevedeva l'uso nascosto e non palese della forza, con il ricorso ad unità di ribelli paramilitari e civili e si sottolineava la necessità di fare affidamento su metodi asimmetrici e indiretti, sostenendo che le forze regolari dovevano essere utilizzate solo nelle ultime fasi

46 Max Gordon, *"Lessons From the Front: A Case Study of Russian Cyber Warfare"*, (December 2015).
47 Andras Racz, *"Russia's Hybrid War in Ukraine, Breaking the Enemy's Ability to Resist"* (Helsinki: The Finnish Institute of International Affairs, FIIA Report 43).
48 Robert Johnson, *"Hybrid War and its Countermeasures: A Critique of the Literature",* Small Wars and Insurgencies vol. 29, no. 1 (2018).
49 Valery Gerasimov, *"The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations"* translated by R. Coalson (Jan-Feb 2016).

del conflitto per il mantenimento della pace o per la gestione delle crisi[50]. Si riteneva, inoltre, che l'uso di metodi non militari come la propaganda e la sovversione potesse paralizzare uno Stato, anche in un lasso di tempo molto limitato, esponendolo al rischio di una condizione di disordine interno e di guerra civile, che avrebbero favorito l'intervento di forze straniere.

Sempre nel 2013 il Generale *Bogdanov* e il Colonnello *Chekinov* individuarono nello spazio delle informazioni il campo di battaglia principale[51]: la guerra psicologica e dell'informazione consentiva di schiacciare il morale delle truppe nemiche e della popolazione avversaria, spezzando così la loro volontà di combattere. Concepirono una fase iniziale, intensa e di lunga durata, priva di azioni cinetiche ma inclusiva di misure diplomatiche, economiche, ideologiche, psicologiche e informative, combinata ad un periodo seguente di ricognizioni su larga scala per raccogliere informazioni e localizzare unità militari nemiche, strutture governative chiave e infrastrutture critiche, a cui far seguire missioni sovversive per indebolirne l'efficacia. Lo scopo di questa fase era quello di distruggere i principali centri governativi e di controllo militare del Paese *target* per consentire poi nella successiva fase conclusiva alle forze irregolari degli attaccanti di entrare nel Paese per isolare e distruggere i rimanenti punti di resistenza. È possibile ritenere che la "strategia integrale" russa, di cui la guerra ibrida è una componente importante, sia stata arricchita dalla nozione di guerra "fuori dai limiti", concettualizzata dai colonnelli *Liang* e *Xiangsui* in *Warfare Beyond Bounds* (1999). La tesi sviluppata dai due colonnelli cinesi è che solo la combinazione di tutti i mezzi, militari e non, può permettere di raggiungere gli obiettivi politici desiderati, che è l'essenza della strategia integrale russa.

Questo approccio può essere descritto con il termine coniato durante l'era sovietica, "controllo riflessivo", progettato per indurre un "avversario più forte a scegliere volontariamente le azioni più vantaggiose per gli obiettivi russi".

Alcune combinazioni di questo stile di guerra potrebbero anche essere definite "guerra politica", facendola risalire a *Lenin* e all'inizio dell'Unione Sovietica[52].

2. La guerra ibrida russa

L'Istituto finlandese per gli affari internazionali ha descritto la guerra ibrida russa come composta da tre fasi principali: preparazione, attacco e stabilizzazione.

---

50 Racz, *Russia's Hybrid War in Ukraine.*

51 Sergey G. Chekinov and Sergey A. Bogdanov, *"The Nature and Content of a New-Generation War",* Military Thought (October-December 2013).

52 Zane M. Galvach, Thomas B. Everett, Matthew J. Mesko, Jeffrey V. Dickey, and Anton V. Soltis, *"Russian Political Warfare: Origin, Evolution, and Application"* (thesis, Naval Postgraduate School, 2015).

a) Fase preparatoria

In questa fase non vi è violenza e le misure adottate non devono oltrepassare alcuna soglia politica o giuridica che induca lo Stato bersaglio ad adottare contromisure. Si concentra sulla mappatura delle vulnerabilità strategiche, politiche, economiche, sociali e infrastrutturali del nemico e sulla creazione dei mezzi necessari per fare pressione sul governo, in maniera implicita e non necessariamente illegale, rendendo impossibile determinare se le misure russe per guadagnare influenza, possano servire come preparazione per un attacco ibrido.

La fase preparatoria della guerra ibrida, può essere suddivisa in tre periodi:

- **strategico**, esplorando i punti di vulnerabilità nell'amministrazione statale, nell'economia e nelle Forze armate;
- **politico**, incoraggiando l'insoddisfazione nei confronti delle autorità centrali nello stato obiettivo, anche rafforzando i movimenti separatisti locali e alimentare le tensioni etniche, religiose e sociali;
- **operativo,** avviando pressioni politiche, azioni di disinformazione unite alla mobilitazione delle Forze armate russe con il pretesto di esercitazioni militari.

b) Fase di attacco

Inizia con la violenza aperta, organizzata e armata, o la sua minaccia, attraverso unità che utilizzano uniformi, armi, veicoli e attrezzature russe, senza però alcun distintivo o simbolo, avendo come obiettivi prioritari quelli politici, allo scopo di paralizzare il processo decisionale.

Questa mancanza di segni distintivi ha consentito a Mosca, ad esempio in Crimea, di negare il proprio coinvolgimento, confondendo gli osservatori occidentali e guadagnando tempo, mediante una politica di negazione persistente; se applicato contro qualsiasi Stato della NATO altrettanto vulnerabile, potrebbe ritardare o impedire l'attivazione dell'articolo 5 del Trattato di Washington, poiché la maggior parte delle azioni rimarrebbe al di sotto della soglia della garanzia di difesa.

In questa fase risulta fondamentale sostenere la legittimità dei leader separatisti attraverso un costante sviluppo e rafforzamento da parte della diplomazia, dei media e dei discorsi pubblici russi con lo scopo di allontanare la popolazione dal vero governo sovrano e garantirsi il loro supporto.

Anche la fase di attacco può essere suddivisa in tre periodi:

- **Esplosione delle tensioni** mediante organizzazione di massicce proteste e rivolte antigovernative nello Stato utilizzando il sabotaggio condotto dalle forze speciali,

travestite da civili locali, i media per lanciare una campagna di disinformazione costituendo una minaccia imminente e schierando le forze regolari russe al confine, per rendere più difficile o impossibile il contrattacco;

- **Espulsione del potere centrale** disattivando il governo preso di mira, bloccando i media della nazione, monopolizzando la comunicazione e l'informazione, inibendo le Forze armate locali per fuorviare e disorientare l'opinione pubblica internazionale e screditare l'obiettivo;
- **Stabilire un potere politico alternativo** facendo riferimento a tradizioni di separatismo reali o inventate, sostituendo gli organi amministrativi e rafforzando la presunta legittimità attraverso l'impiego dei *media*.

Alla fine della fase di attacco, la capacità dello Stato di resistere con le sue forze militari convenzionali o altre forze di sicurezza interna viene meno.

c) Fase di stabilizzazione

Consiste nel consolidare i risultati raggiunti dalla guerra ibrida. Come possibili opzioni si possono avere l'annessione del territorio catturato oppure la permanenza del territorio all'interno del Paese di origine ma negando il controllo da parte del governo centrale, limitandone la libertà strategica di movimento. Esempi concreti di questi possibili sviluppi si sono avuti in Crimea e nel Donbass. Le unità russe di stanza in Crimea hanno esercitato pressioni sulle *élite* locali e sulla popolazione, organizzando il *referendum* di "indipendenza": dopo meno di un giorno intero di cosiddetta "autonomia", la Russia ha annesso la Crimea. Nel Donbass invece di stabilire un potere alternativo funzionante, la Russia ha creato un limbo politico, di sicurezza e sociale.

La fase di stabilizzazione può essere dettagliata in tre momenti:

- **Stabilizzazione politica del risultato,** attraverso un referendum e una decisione sulla secessione/indipendenza nello Stato bersaglio, con il forte supporto diplomatico e mediatico dello Stato attaccante;
- **Separazione del territorio catturato dallo Stato bersaglio,** annettendo il territorio catturato o stabilendo una presenza militare aperta o nascosta. Una possibile variante è rappresentata dall'invasione aperta con il pretesto del mantenimento della pace o della gestione delle crisi;
- **Limitazione duratura della libertà strategica di movimento degli Stati attaccati,** causata dalla perdita di territorio che si traduce in gravi conseguenze economiche, difficoltà e destabilizzazione politica interna, con risvolti sul grado di aderire a politiche o alleanze militari che richiedano l'integrità territoriale.

3. Il Cognitive Warfare

"In wartime, truth is so precious that
she should always be attended by a bodyguard of lies"[53]

Il *Cognitive Warfare* (CW) e le *Information Strategies* (IS) hanno da sempre fatto parte del tradizionale concetto di *Military Warfare* (MW); allo stesso modo, non è una novità il ricorso alla diffusione volontaria di informazioni false o fuorvianti per confondere l'avversario, tanto che lo stesso Sun Tzu afferma che "Tutta la guerra si basa sull'inganno"[54]. Tuttavia, fenomeni attuali quali la trasformazione digitale e la socializzazione dei conflitti, stanno ridefinendo la magnitudo e la portata dello strumento del CW.

Il dilagare del fenomeno dei *social media*, unito ad un uso ben pianificato degli stessi, ha permesso la diffusione di contenuti informativi ad una velocità e con una capillarità senza precedenti; la rivoluzione digitale ha, inoltre, consentito di estendere il *target* di quest'attività oltre i decisori politici e militari, arrivando direttamente alle masse. Nella popolazione è riconosciuta, infatti, la potenzialità di influenzare le politiche di uno Stato, di indirizzarne l'operato e, in definitiva, di determinare successi o fallimenti. È dunque al singolo cittadino che il moderno CW si rivolge e, per farlo, sfrutta le potenzialità dei nuovi *media* che hanno sconvolto i precedenti meccanismi comunicativi, permettendo la diffusione di un'enorme quantità di dati che vengono scambiati attraverso un sistema "*many to many*" tra milioni di utenti, senza filtri e senza grosse possibilità di controllo.

La letteratura moderna propone diverse definizioni di CW quali:

- *"Insieme delle manovre condotte nel dominio cognitivo per indurre una predeterminata percezione fra la target audience al fine di ottenere un vantaggio su un avversario"*[55];
- *"Manipolazione dell'opinione pubblica, da parte di elementi esterni, con l'intento di minare la coesione sociale o danneggiare la credibilità del sistema politico"*[56];
- *"Strategia che si focalizza nell'alterazione del pensiero pubblico attraverso lo strumento informativo al fine di modificare le azioni poste in essere dalla popolazione"*[57];

[53] Whiston Churchill, British National Archives.
[54] Sun Tzu, "L'arte della Guerra".
[55] Ottewell, 2020.
[56] Rosner e Siman-Tov, 2018.
[57] Oliver Backes e Andrew Swab, 2019.

- *"Strumento di uno Stato o di un gruppo sociale che permette di manipolare il meccanismo cognitivo di un avversario o dei cittadini di uno Stato ostile al fine di indebolirlo, penetrarlo, influenzarlo, soggiogarlo o addirittura distruggerlo"*[58]*;*
- *"Weaponization dell'opinione pubblica, da parte di un attore esterno, al fine di influenzare l'opinione pubblica e di destabilizzare le sue Istituzioni pubbliche"*[59]*.*

A fronte di una moltitudine di definizioni, emerge una caratteristica comune, costituita dallo scopo di quest'attività, che è quello di influenzare e destabilizzare la struttura su cui poggia il sistema avversario, alterando la maniera in cui esso pensa e agisce. Il CW è, in altre parole, un attacco rivolto al modo di pensare del rivale, alla maniera in cui la sua mente lavora e rielabora le informazioni per creare la propria visione del mondo.

Gli strumenti per influenzare e manipolare le decisioni e il comportamento avversario vengono tradizionalmente suddivisi in tre differenti macroaree: strumenti di influenza, di interferenza e di alterazione. Il primo gruppo comprende gli strumenti e le metodologie impiegabili per influenzare e manipolare, direttamente o indirettamente, il pensiero umano. Tali strumenti operano prevalentemente, ma non esclusivamente, attraverso l'ambiente informativo e la dimensione digitale, attraverso strategie di disinformazione e *digital influence* per orientare, dividere, polarizzare, sovvertire e radicalizzare.

La Federazione Russa, ben consapevole della rilevanza della competizione nella dimensione cognitiva, è da sempre molto attiva in materia e ha sviluppato un proprio caratteristico *modus operandi* per quanto riguarda l'attuazione di una propria strategia di disinformazione e propaganda.

4. Tattiche russe di disinformazione e propaganda

Con il termine *disinformation* si fa riferimento al processo di creazione, presentazione e diffusione volontaria di un contenuto fabbricato (completamente falso), manipolato (distorto), ingannevole o fuorviante; con *misinformation* viene invece definita la condivisione involontaria di un'informazione errata senza l'intenzione di influenzare il pubblico.

Le azioni perpetrate dalla Federazione Russa ricadono senza ombra di dubbio nel primo ambito e, addirittura, le attività di *disinformation and propaganda* (DP) rappresentano il *core tool* delle *"Active Measures"* utilizzate da Mosca nell'alveo dell'*Information Confrontation*, con la quale il Paese sfida gli avversari in quello che viene definito *Perpetual Conflict.*

[58] Underwood 2017.
[59] Bernal, Carter, Singh, Cao & Madreperla 2020.

Nell'ottica di aumentare la resilienza del proprio strumento e di porre in essere il concetto di *perpetual adversarial competition*, la Russia ha promosso lo sviluppo di un sistema di DP con caratteristiche di varietà e sovrapposizione sia degli strumenti che dei messaggi, che creano un vero e proprio ecosistema poggiante su 5 pilastri: *Official Government Communications, State Funded Global Messaging, Cultivation of Proxy Sources, Weaponization of Social Media e Cyber Enabled Disinformation*.

I vantaggi immediati che questa struttura offre alla Federazione Russa sono rappresentati dalla possibilità di:

- diffondere numerose variazioni della stessa narrativa, permettendo ai diversi pilastri dell'ecosistema di perfezionare il messaggio ingannevole adattandolo alle diverse *target audience;*
- sfruttare fonti non immediatamente riconducibili al governo russo; ciò permette a Mosca di prenderne le distanze all'occorrenza, ottenendo, tuttavia, ugualmente la diffusione del messaggio pernicioso;
- creare una camera di risonanza (*media multiplier effect)* tra i pilastri dell'ecosistema, aumentando la portata e la pervasività del messaggio malevolo.

La propaganda russa e le attività di disinformazione vengono così prodotte facilmente in grandi volumi e distribuite attraverso un ampio ventaglio di canali, sia *online* sia per il tramite dei *media* tradizionali. È interessante notare anche che, nello scenario informativo moderno, non sia la veridicità dell'informazione a rappresentare la chiave del successo per una sua efficace diffusione: recenti studi hanno infatti dimostrato che gli utenti tendono a rilanciare messaggi con contenuti ingannevoli *"farther, fuster, deeper and more broadly than the truth"*, specialmente quanto attinenti alla sfera politica.[60]

Il Cremlino, sfruttando l'ecosistema di DP, coniuga campagne di informazione (e disinformazione) "aperte" ad azioni invece non immediatamente riconducibili al governo russo, in una sorta di scambio simbiotico in grado di saturare l'ambiente informativo.

Per il primo filone, la Federazione russa opera attraverso i propri *account* sui *social media*. Mosca conta infatti 75 *account* su *Twitter*, con 7.3 milioni di *follower* che hanno raccolto 35.9 milioni di *retweet*, 29.8 milioni di *like* e 4 milioni di risposte e hanno *twittato* 157 volte tra il 25 febbraio e il 3 marzo 2022. Circa il 75% dei *tweet* riguardava l'Ucraina: molti di questi mettevano in discussione lo *status* dell'Ucraina come Stato sovrano, attirando l'attenzione sui presunti crimini di guerra di altri Paesi e diffondendo teorie del complotto[61]. Gli *account* governativi russi sono stati anche collegati ad attività di *"typosquatting"* (forma

[60] Vosoughi, Roy e Aral, 2018.
[61] Thompson and Graham, 2022.

di crimine informatico in cui gli *hacker* registrano domini con nomi di siti Web noti deliberatamente scritti in modo errato) volte a diffondere narrative false, spacciandosi per noti siti d'informazione[62].

Per quanto concerne invece le attività condotte in maniera che potremmo definire *"covert",* la Federazione Russa utilizza una serie di espedienti che non permettono una riconducibilità certa dell'azione al governo stesso. Una delle soluzioni largamente adottate è quella di ricorrere ai cosiddetti *trolls*, soggetti dediti a provocare discussioni, che partecipano a *chat* o *blog* in rete con il solo scopo di infastidire o attaccare altri utenti, con argomenti molesti, violenti o anche fuori luogo; il loro l'intento è di creare disturbo alla conversazione e irritare chi vi prenda parte, fomentando lo scontro e manipolando la percezione del contenuto. Ulteriore espediente di cui il Cremlino si serve per diffondere efficacemente dei contenuti ingannevoli nel sistema informativo è la creazione *ad hoc* di profili autorevoli: ad esempio, nel 2020, *Facebook* fu in grado di individuare una serie di falsi profili di utenti riconducibili a Mosca, che spacciandosi per giornalisti ucraini, erano usi introdurre false narrative ed incendiare i dibattiti sostenendo posizioni filorusse[63]. Tattiche simili sono state messe in atto costantemente durante le diverse fasi del conflitto russo – ucraino e dimostrano una continua evoluzione nelle TTPs[64] russe. Il governo britannico, per esempio, ha scoperto che alcuni *influencer* della nota piattaforma *TikTok* venivano pagati per amplificare le narrative filorusse[65]. Le attività di DP sono state perpetrate anche ricorrendo a meccanismi di intelligenza artificiale, in grado di selezionare messaggi autentici di utenti reali, coerenti con il punto di vista di Mosca, e di rilanciarli automaticamente nelle diverse piattaforme, con il risultato di aumentarne la diffusione e, al contempo, di eludere le misure di contrasto alla disinformazione. Tentativi di manipolazione dell'opinione pubblica sui *social media* hanno avuto luogo principalmente su *Twitter* e *Facebook*, ma ulteriori azioni malevole si sono registrate anche su *Instagram, YouTube* e *TikTok*. Esistono anche prove di campagne di DP che si sono svolte nelle sezioni "commenti" dei principali *media*[66]*.*

Di queste tattiche non si trovano tracce esclusivamente nello scenario *war* del recente confronto russo ucraino, bensì si possono riscontrare anche in altri ambiti della competizione sottosoglia. Nel 2017, ad esempio, *Facebook* ha denunciato come l'*Internet Research Agency*, un'organizzazione con sede in Russia, avesse esposto 126 milioni dei suoi utenti a disinformazione politica in vista delle elezioni statunitensi del 2016[67]. In merito, *Facebook*

62 Stefanicki, 2022.
63 Facebook, 2021.
64 *Tactics, techniques, and procedures*.
65 *The Guardian*, 2022.
66 *The Guardian*, 2022.
67 Dwoskin, 2021.

sostiene di aver scoperto, decine di campagne di DP condotte dalla Federazione Russa che hanno coinvolto più di 50 Paesi nel solo periodo 2017-2022, tra cui primeggiano, per frequenza degli attacchi subiti, Stati Uniti, Ucraina e Gran Bretagna.

A fattor comune, le campagne di DP messe in atto da Mosca, hanno come obiettivo quello di confondere e minare l'ambiente informativo. Da un lato esse cercano di creare confusione e complicare gli sforzi affinché le Istituzioni avversarie non possano operare efficacemente, dall'altro tendono ad accrescere il consenso interno ed esterno verso gli obiettivi nazionali. Una penetrazione così invasiva nelle dinamiche interne di un Paese rappresenta un rischio capitale per le fragili democrazie già provate da dinamiche storiche, sociali ed economiche complicate (come, ad esempio, l'Ucraina) ma, allo stesso tempo, costituiscono una minaccia grave, che non può e non deve essere sottovalutata, anche per le solide democrazie occidentali.

5. Considerazioni sul coinvolgimento della popolazione

Sebbene la guerra in Ucraina possa far pensare a un ritorno da parte della Russia al passato in termini di metodologie e tattiche impiegate, al contrario si può ritenere che sia stato un teatro caratterizzato da numerose operazioni inquadrabili all'interno dell'ambito della guerra ibrida, intesa secondo la concezione russa maturata già negli anni post Guerra Fredda e descritta nel 2013 dal generale russo Gerasimov. La guerra ibrida russa si propone, in contrasto alla visione della guerra tradizionale, di indebolire l'avversario agendo anche sulla popolazione mediante un'erosione graduale dei propri valori, della propria cultura e della propria volontà di resistere. Ciò consente di indebolire il potere politico e militare avversario e solo successivamente di distruggerne le forze di sicurezza.

Da ciò si intuisce come nella prima fase del conflitto le operazioni non convenzionali si concentrino nelle sfere della vita pubblica e quotidiana, andando ad identificare e sfruttare le vulnerabilità nel contesto politico, economico, sociale e culturale del Paese.

La Federazione Russa, ben consapevole dell'importanza della componente cognitiva per raggiungere i propri obiettivi, ha sviluppato e messo in atto una propria strategia di disinformazione e propaganda per confondere e minare l'ambiente informativo a proprio vantaggio, mettendo in difficoltà le istituzioni del Paese avversario e accrescendo il proprio consenso interno ed esterno. Tale strategia viene utilizzata anche contro la popolazione avversaria con lo scopo di intaccare e minare le idee e il punto di vista, generando confusione e disorientamento, togliendo i punti di riferimento nazionali.

In conclusione, appare evidente che la popolazione risulta un elemento chiave per il buon esito del conflitto, e pertanto bisogna porre in essere una serie di azioni per rafforzare

la resilienza che consenta di resistere ai tentativi avversari di minare la stabilità interna e la determinazione a resistere.

Tali metodi ibridi sfruttano principalmente l'accesso alla popolazione, quindi è necessario porre maggiore enfasi sul coinvolgimento del pubblico prima della crisi al fine di rafforzare la resilienza, elemento critico nella "trinità" della guerra di *Clausewitz*. Ciò potrebbe iniziare con instillare la fiducia nella popolazione, attraverso misure di resilienza interna ed un piano di difesa nazionale che includa la resistenza sotto l'occupazione, in grado di infondere fiducia popolare nei confronti di un potenziale avversario. La pianificazione e la preparazione della resistenza potranno configurarsi come forma di deterrenza, ed aumentare la probabilità di successo e di azioni tempestive di alleati e partner per ripristinare la sovranità perduta e l'integrità territoriale.

CAPITOLO 4
LA DOTTRINA CONTEMPORANEA OCCIDENTALE: GUERRA NON LINEARE E *RESISTANCE OPERATING CONCEPT* (ROC)

Il *Resistance Operating Concept* (ROC), elaborato dallo *Special Operations Command Europe* (SOCEUR) in collaborazione con gli Stati Baltici, Scandinavi e altri *partner* della NATO, nasce in risposta alle tattiche russe utilizzate per l'annessione della Crimea del 2014. Si fonda sullo sviluppo dell'azione governativa tesa, nel periodo antecedente la crisi, a promuovere la resilienza. Quest'ultima è intesa come la volontà e la capacità della società di resistere alle sollecitazioni esterne e di riprendersi dagli effetti provocati dalle stesse. L'approccio alla sicurezza del ROC è omnicomprensivo e prevede il coinvolgimento sia dell'intera struttura governativa sia di tutta la società. In tale contesto le Forze armate, l'apparato statale e la popolazione agiscono in maniera coordinata contro l'invasore per la Difesa Totale del Paese. L'intento di questo approccio è mobilitare tutto il supporto necessario, compresa la cooperazione con altri Stati sul territorio nazionale o all'estero. Inoltre, dato che la Difesa Totale richiede il dispiegamento di una capacità di resistenza preparata, risoluta e prolungata, essa funge anche da deterrente, in quanto un eventuale invasore dovrebbe mettere in conto un dispendio di risorse considerevole per poter avere la meglio sullo Stato sovrano. Nei paragrafi seguenti si partirà dall'analisi dei movimenti di resistenza della Seconda Guerra Mondiale per passare poi a definire quali siano le giuste metodologie per creare una società resiliente. Infine, verranno descritte le azioni necessarie che tutte le componenti dovrebbero mettere in pratica per rispondere all'invasore.

1. Evoluzione storica delle resistenze e "*lesson learned*"

Durante la Seconda Guerra Mondiale si diffusero i movimenti di resistenza in tutti i Paesi occupati. Dall'analisi delle dinamiche organizzative, sociologiche e operative con cui questi movimenti agirono contro gli invasori, nacque tutta la dottrina della guerra urbana del XX secolo.

In particolarein Francia, a seguito dell'invasione tedesca, si creò una situazione confusa e frammentata, che né il governo, né la popolazione erano preparati ad affrontare. In questo contesto, grazie al sostegno esterno degli alleati, il generale De Gaulle riuscì a organizzare le reti di resistenza, guidando gruppi armati e milizie in azioni di sabotaggio e guerriglia (rivolte soprattutto verso i connazionali che avevano aderito alla causa nazista). Il supporto militare e politico da parte degli alleati, in termini di armi, equipaggiamenti e finanziamenti, risultò fondamentale per il buon fine delle operazioni.

In Polonia la resistenza contro l'occupante tedesco e sovietico non ebbe successo, sebbene il Paese fosse riuscito in tempi rapidi a creare un governo in esilio capace di coordinare le attività dei vari gruppi armati che erano coesi e motivati. Gli alleati non diedero alcun sostegno in termini di armi ed equipaggiamenti, determinando l'inefficacia degli attacchi asimmetrici: l'azione dei movimenti di resistenza fu così limitata alla sola attività di *intelligence*.

Le Filippine, arcipelago sotto il controllo statunitense, non avevano sviluppato piani pre-bellici di resistenza. A seguito dell'invasione giapponese e del conseguente ritiro degli USA, molti militari americani e filippini si organizzarono in gruppi armati.

Essi riuscirono, nonostante l'assenza di coordinamento orizzontale, a condurre azioni efficaci. La chiave del successo fu, anche in questo caso, l'appoggio esterno che gli Stati Uniti offrirono sotto forma di forze "*stay-behind*" e rifornimenti (mezzi, armi, ecc…).

Negli Stati Baltici (Estonia, Lettonia e Lituania) durante l'occupazione sovietica si formarono movimenti di resistenza organizzata noti come i "*Forest Brothers*". Questi gruppi avevano un'organizzazione di tipo militare, strutturati in grandi unità ben equipaggiate. Dopo gli scontri di tipo simmetrico contro le forze sovietiche, dove subirono perdite consistenti, i "*Forest Brothers"* adattarono le proprie tattiche per un confronto di tipo asimmetrico ma, senza l'appoggio esterno, le loro azioni risultarono inconsistenti.

Dai casi analizzati in precedenza si possono delineare tre caratteristiche principali presenti, in tutto o in parte, nei movimenti di resistenza, che ne hanno determinato il successo o il fallimento: supporto esterno, organizzazione e asimmetria.

Quando presente, il supporto esterno è stato cruciale nella buona riuscita della resistenza, anche in assenza di piani pre-bellici. Una buona organizzazione dà la facoltà di reagire prontamente e in maniera coordinata all'invasore; tuttavia come nel caso polacco, l'assenza di rifornimenti, di idonei equipaggiamenti e di armi hanno determinato l'inconsistenza dell'azione dei gruppi di resistenza. L'asimmetria, infine, è la forma di conduzione delle ostilità più appropriata per contrapporsi alla soverchiante superiorità degli eserciti regolari (vds. caso paesi Baltici). In funzione delle caratteristiche sopra esposte, nel periodo della Guerra Fredda, i Paesi al confine dei due blocchi si sono dotati di organizzazioni di resistenza ben strutturate, basate, tra l'altro, sulla cooperazione e sulla mutua assistenza tra gli Stati.

2. Resilienza come base per la resistenza

a) Analisi dell'ambiente operativo

La gestione delle attività di resilienza costituisce per un governo una difficile sfida a causa dell'ambiente operativo altamente dinamico e complicato da fattori interni ed esterni. Internamente si profila un problema di comando e controllo (C2) in quanto le reti sociali, interconnesse tra loro, mettono in atto azioni eterogenee, non controllabili centralmente, complicando le dinamiche di potere e decisionali. Dal punto di vista esterno, l'intervento di vari soggetti (governi stranieri e attori non statali) potrebbe influenzare la popolazione minando alla base le fondamenta della resilienza.

Proprio a causa della complessità e molteplicità delle insidie per un governo, appare necessario disporre, attraverso processi di autovalutazione, di una mappatura di punti di forza e di debolezze che la propria società possiede, funzionale a discernere gli aspetti su cui concentrare i propri sforzi per costruire la resilienza.

Gli strumenti di analisi e di *problem solving* più largamente utilizzati dalla dottrina NATO per discriminare i predetti punti di forza e di debolezza sono i seguenti:

- DIMEFIL: viene scomposto il potere di un'intera nazione e opportunamente analizzato nei suoi sette elementi: diplomazia, informazione, potere militare, economico, finanziario, intelligence e diritto/forze dell'ordine;
- PMESII-PT: vengono individuate le caratteristiche dell'ambiente operativo della propria nazione e in cui il nemico andrebbe ad operare attraverso l'analisi di otto elementi distintivi: politica, apparato militare, economia, società, informazione, infrastrutture, ambiente fisico e tempo.

b) Costruire la resilienza

Una resistenza di successo necessita di una solida base di resilienza, che si può creare attraverso lo sviluppo di una forte identità nazionale accompagnata da attività preparatorie e formative pertinenti all'esigenza a favore della popolazione, nonché dalla creazione di idonee strutture politiche e istituzionali per superare eventuali crisi e contrastare/mitigare le minacce.

Identità nazionale

La coesione nazionale, intesa come forte identità e condivisione di valori, è un prerequisito per una resistenza perché mantiene e rafforza la resilienza e la motivazione della popolazione a resistere.

Un rafforzamento dell'identità nazionale si ottiene con misure di varia tipologia tra cui lo sviluppo della conoscenza storica e dell'educazione civica, l'attuazione di politiche inclusive per il coinvolgimento delle minoranze nella vita civile e istituzionale, l'organizzazione di eventi e attività sociali attraverso Organizzazioni non Governative (ONG) o altre realtà associative.

Consapevolezza Valoriale

Già prima dell'avvio della scolarizzazione e della contestuale educazione civica, la consapevolezza valoriale ha lo scopo di aiutare le classi più giovani a costruire una forte immunità alla propaganda nemica.

Tale coscienza, anche durante il conflitto, risulta fondamentale per mantenere alto il morale della popolazione. Ciò predispone la società a resistere all'occupante e a sostenere lo Stato.

Conoscenza e riduzione delle vulnerabilità

La conoscenza delle vulnerabilità di un Paese si perfeziona, come detto in precedenza, attraverso una mappatura completa dei punti di forza e delle debolezze. Esse riguardano tutti gli ambiti: identità, religione, economia, mancanza di libertà, corruzione, sfruttamento e mancanza di servizi essenziali.

La riduzione delle vulnerabilità richiede un approccio olistico che copra nella sua interezza gli elementi dell'ambiente operativo[68]. L'attenzione verso le aree di potenziale vulnerabilità è particolarmente importante nella fase iniziali per costruire una buona resilienza.

Identificazione potenziali minacce esterne

La conoscenza, a priori, delle potenziali minacce esterne consente di focalizzare e modellare l'organizzazione della resistenza rispetto ai vantaggi dell'ambiente operativo che il nemico è in grado di sfruttare.

Una volta individuate, vanno condivise verso l'esterno (per esempio verso i Paesi amici e la loro popolazione) con comunicazioni mirate.

[68] Tra le possibili azioni perseguibili si rilevano: il contrastare in modo proattivo i messaggi avversari, diversificare (per quanto possibile) e proteggere l'economia nazionale e le industrie/infrastrutture critiche, facilitare un quadro operativo comune tra le organizzazioni interessate, proteggere gli standard di vita di base, proteggere i confini, promuovere l'unità nazionale, adottare dati e misure di protezione informatica e garanzia delle informazioni, riducendo le vulnerabilità delle popolazioni chiave e mantenendo i vantaggi militari esistenti.

Preparazione contro la minaccia

La preparazione contro la minaccia di uno Stato, che si presume possa operare un'invasione e violare la sovranità nazionale, passa attraverso una serie di attività interne ed esterne che possono, tra le altre cose, fungere da deterrente. Solide relazioni con *partner* e alleati, in particolare, oltre a gettare le basi per un eventuale sostegno esterno alla resistenza, può disincentivare l'aggressione di un altro Stato. Lo strumento delle alleanze e degli accordi, oltre a codificare e talvolta definire ruoli e responsabilità prima della crisi, crea i presupposti per la legittimità in chiave internazionale del sostegno.

Tali accordi delineano la tipologia di quali supporti debba fornire ciascun alleato durante le diverse fasi e devono essere stipulati dai governi senza minarne la propria credibilità, in quanto ciò avrebbe effetti negativi in termini di consenso della popolazione.

Allo stesso tempo, la garanzia di un sostegno esterno, in particolare ma non soltanto[69] sotto forma di aiuti materiali e truppe, può accrescere la capacità e la volontà di condurre operazioni di resistenza.

Anche la comunicazione strategica è un elemento irrinunciabile per contrastare la narrativa propagandistica dello Stato aggressore, già ampiamente utilizzata dagli Stati baltici. Ne sono esempi la distribuzione di opuscoli di informazioni alla popolazione nel 2015 da parte del governo lituano su come prepararsi a sopravvivere alle emergenze e alla guerra. Il manuale forniva indicazioni su come osservare e inviare informazioni del nemico nel caso in cui la Russia avesse occupato parte del Paese. In sostanza la Lituania con un coinvolgimento "controllato" della popolazione si prefiggeva di creare un sistema di allerta precoce. Un altro esempio è l'emanazione di linee guida per l'informazione da parte del governo svedese su come prepararsi ad un eventuale attacco e su come contribuire alla Difesa Totale del Paese (vedasi approfondimento in "Annesso I"). In tutti gli opuscoli sopra citati oltre alle istruzioni furono inserite una serie di frasi ad effetto[70] e narrative eroiche per infondere motivazione e fiducia nella popolazione.

Un ultimo aspetto che sta assumendo sempre più rilevanza è il dominio *Cyber*. Resilienza e difesa della sovranità nazionale devono essere rivolte al massimo controllo possibile del cyberspazio, alla comprensione e al rilevamento degli attacchi perpetrati in questo dominio. Uno sforzo combinato di collaborazione e integrazione da parte dei militari, dei ministeri e delle altre agenzie governative con le organizzazioni civili può condurre alla mitigazione di questa nuova tipologia di minaccia.

---

[69] Ad esempio, l'alleato ricevente potrebbe dover stabilire un'indennità o una deroga all'interno del proprio quadro legale per determinate procedure doganali, autorizzazioni nazionali per consentire una rapida infiltrazione di forze e/o materiale durante i periodi di crisi prossima o effettiva.

[70] "Tutti sono obbligati a contribuire e tutti sono necessari" per la "Difesa Totale della Svezia" e se il Paese viene attaccato, "non ci arrenderemo mai. Quindi tutte le informazioni secondo cui la resistenza deve cessare sono false".

3. Progettare per la resistenza

a) Aspetti della pianificazione

Tutti gli sforzi di resilienza sopra riportati costituiscono le fondamenta della resistenza che, tuttavia, necessita di una approfondita pianificazione e progettazione per esprimersi in modo efficace.

Di seguito vengono individuate le attività necessarie alla progettazione della resistenza:

- *Pianificazione Strategica*

  La pianificazione deve essere completa, proattiva e omnicomprensiva. Dovrebbe includere aspetti come la comunicazione, l'organizzazione, la sicurezza e la supervisione. I meccanismi di controllo dell'avversario e l'identificazione dei metodi per minarne gli sforzi devono essere pianificati per tempo con la creazione e lo sviluppo di reti clandestine e ausiliarie strutturate, in cui ruoli e responsabilità siano chiari e definiti.

- *Pianificazione e organizzazione della componente di resistenza pre-crisi*

  In caso di destituzione o esilio, il governo deve anche prevedere una struttura di *leadership stay-behind*, che operi tra il popolo, per coordinare le operazioni di resistenza e contrastare il regime dell'invasore attraverso la creazione di una forma di governo. I soggetti individuati per tali compiti devono ricevere, in tempo di pace, la formazione e l'istruzione necessarie per adempiere ai propri doveri e per eventualmente migliorare l'organizzazione della resistenza.

A livello istituzionale deve essere creato un centro nazionale di gestione delle crisi all'interno del Ministero della Difesa o del Ministero dell'Interno con compiti di organizzazione, supervisione, pianificazione e preparazione della resistenza.

La pianificazione include l'identificazione degli incarichi operativi chiave e del personale per ricoprirli. Il governo deve inoltre individuare tra la popolazione i soggetti deputati a rimanere sul territorio e offrire supporto ausiliario alla resistenza e garantire la raccolta e la diffusione di informazioni sulle attività nemiche.

La struttura organizzativa della resistenza deve essere funzionale a supportare un governo clandestino. Le peculiarità politiche, fisiche e socioculturali, inoltre, sono determinanti per stabilire le dimensioni, la tipologia e la portata delle attività della resistenza. Parimenti importante risulta collocare le persone più idonee negli incarichi a maggiore responsabilità e garantirgli l'accesso a tutte le informazioni utili al loro operato. La

competenza e l'esperienza nei ruoli ricoperti all'interno della società civile possono essere validi elementi nel processo di selezione, ma bisogna evitare che vengano scelti soggetti con elevata esposizione mediatica. Ciò potrebbe incidere negativamente sul fattore della clandestinità. Si evidenzia che tutta la popolazione, anche la parte non inquadrata nell'organizzazione di resistenza, può agire con metodi passivi per fiaccare il morale del nemico. Tali metodi sono declinabili in molteplici attività o omissioni ovvero in una mancata collaborazione con il nemico.

- *Infrastrutture fisiche ed equipaggiamenti*

  Forniture come denaro, armi, munizioni, attrezzature mediche e apparecchiature di comunicazione necessarie per le operazioni di resistenza devono essere accentrate prima dell'emergere della situazione di crisi. Questi materiali, in tempo di pace, possono essere immagazzinati e mantenuti in luoghi prestabiliti, anche al di fuori delle strutture governative e militari. Il governo deve inoltre garantire finanziamenti e supporto logistico sufficiente a sostenere tutte le attività preparatorie.

  Le reti di resistenza sono di tipo multilivello e includono la logistica, la sanità, le comunicazioni, la finanza, l'istruzione, i trasporti, l'intelligence.

- *Processo di validazione/Esercitazione dei piani*

  Una volta terminato il processo di pianificazione della resistenza è opportuno che il governo organizzi esercitazioni per testarne l'efficacia e identificare i suoi punti di forza e di debolezza: il coordinamento e il sincronismo tra le principali parti interessate sono essenziali. Queste attività rappresentano anche l'opportunità di verificare l'interoperabilità con le forze di *partner* e alleati, individuare eventuali aspetti che necessitano di miglioramenti e standardizzazione, oltre a fungere come deterrente per i potenziali invasori. Una delle più grandi di queste esercitazioni si è svolta in Svezia nel giugno 2018: sono stati dispiegati tutti i 40 battaglioni della guardia nazionale (circa 22.000 soldati volontari). In linea con quanto esposto in questo paragrafo Stoccolma ha utilizzato l'esercitazione contro i potenziali aggressori per costringerli a considerare attentamente i rischi di attaccare il Paese. Per essere efficace, il deterrente deve essere credibile e visibile. La visibilità deve essere mantenuta attraverso un addestramento frequente ed esteso, soprattutto con le Forze armate di altri Paesi, che rendono appunto il deterrente più credibile.

b) Fattori di comportamento etico-organizzativo e considerazioni sul C2

In fase di pianificazione deve essere considerato l'impatto delle reti criminali sulle forze di resistenza e le possibili problematiche che ne derivano.

Gli elementi che per condizione e natura delle loro azioni agiscono isolati, senza il legittimo controllo e sostegno del governo, potrebbero, probabilmente, non attenersi ai codici etici e legali e mischiarsi con le reti criminali. Il coinvolgimento di quest'ultime, inoltre, potrebbe portare a vantaggi di breve periodo, ma data la loro poca affidabilità, il nemico potrebbe sfruttarle a suo favore per influenzare l'opinione pubblica interna ed internazionale.

La struttura organizzativa deve promuovere il comportamento etico dei suoi membri e controllare la violenza prevedendo anche un sostegno adeguato verso le loro famiglie: ciò costituisce un importante fattore attrattivo, oltre che motivazionale. Una struttura organizzativa efficace può aiutare la *leadership* a mantenere il controllo operativo e a gestire una potenziale *escalation* della tensione o della violenza. La resistenza deve trovare il giusto bilanciamento tra accentramento e decentramento. Il primo consente di coordinare, uniformare e standardizzare le azioni delle singole unità, ma allo stesso tempo aumenta il rischio che l'avversario scopra e destrutturi l'organizzazione della resistenza. Il decentramento pone sui singoli *leader* tattici la responsabilità delle operazioni in quanto possiedono una migliore capacità di comprendere i requisiti di sicurezza sul terreno. Il decentramento consente anche un adattamento più rapido agli imprevisti, ma richiede allo stesso tempo maggiore competenza e capacità di comando dei singoli *leader* tattici.

4. La resistenza

a) Attivazione

La resistenza è lo sforzo organizzato di una nazione e della sua società che comprende l'intera gamma di attività, da quelle non violente a quelle che implicano l'uso della forza, guidata da un governo legalmente costituito (potenzialmente esiliato/destituito o ombra) per ristabilire l'indipendenza e l'autonomia all'interno del suo territorio, a seguito dell'occupazione da parte di una potenza straniera.

Nell'eventualità di subire un'aggressione lo Stato si attiva per consolidare la propria resilienza e per pianificare le azioni per la Difesa Totale. Solo quando saranno chiare le intenzioni del nemico, verranno mobilitate le forze convenzionali e le forze di resistenza. Tuttavia, nella realtà non è sempre facile distinguere e discriminare l'entità e la pericolosità delle minacce, perciò il Paese dovrà monitorare con attenzione l'ambiente operativo ed attivare le proprie forze solo quando vi sia una chiara violazione della sovranità nazionale.

Lo Stato ricorrerà a tutte le proprie capacità in termini di *intelligence*, forze dell'ordine, forze militari convenzionali (CF), forze speciali (SOF) ed eventualmente anche della resistenza organizzata (vedi fig. 1). *L'intelligence* nazionale rappresenta lo strumento principale per identificare le azioni dell'aggressore e portarle a conoscenza del decisore politico.

Durante gli attacchi ibridi, le forze dell'ordine, supportate dall'*intelligence*, sono di solito le prime a entrare in contatto con coloro che intendono sovvertire la sovranità nazionale (vds. recentissimi esempi in Moldavia e Georgia), a differenza di quando il nemico opera tramite incursioni sul territorio. In quest'ultimo caso, saranno le forze militari convenzionali e speciali che per prime contrasteranno gli attacchi del nemico.

Nel caso in cui le CF soccombano, esse dovranno confluire nelle forze di resistenza, ovvero nelle Forze armate di Paesi alleati. Le SOF dovranno invece rimanere sul territorio in qualità di forza *stay-behind,* mimetizzandosi tra la popolazione e svolgendo attività asimmetriche (vds. fig.1).

Fig.1

Lo Stato aggressore concentrerà gran parte dei propri sforzi per fiaccare il morale della popolazione attraverso azioni coercitive. In quest'ottica risulta fondamentale l'attuazione di un piano di resistenza efficace che permetta di mantenere viva la speranza tra i cittadini di riacquisire la sovranità nazionale. Ciò favorirà inoltre il pervenire di aiuti da parte dei Paesi Alleati o addirittura l'ingresso delle loro forze convenzionali. Come si evince dai contenuti di questo capitolo il supporto esterno è un fattore essenziale per il successo dei movimenti di resistenza.

b) Le componenti della Resistenza e i loro compiti

Le organizzazioni della resistenza tipicamente sono composte da quattro componenti principali: le forze clandestine, di guerriglie, ausiliarie e la componente pubblica.

In particolare, le forze clandestine sono composte da personale in grado di svolgere compiti militari e politici, organizzate in cellule che operano nei centri urbani controllati dalle forze occupanti. I loro compiti includono attività di *intelligence* e controspionaggio, controllo di giornali, volantini, social media, televisione satellitare e pagine web, atti di sabotaggio, supporto logistico e copertura del personale ricercato.

Le forze di guerriglia si compongono di piccole unità di forze militari *stay-behind*, membri selezionati e addestrati della popolazione civile o una combinazione di entrambi. Le tecniche di guerriglia includono tradizionalmente incursioni, imboscate, sabotaggio e tecniche di disturbo per interdire i movimenti nemici, indebolirne il morale e degradarne la forza. Le operazioni dovrebbero essere guidate da obiettivi tattici e strategici, ricorrendo al sabotaggio in tutte le sue forme, con operazioni psicologiche e guerra informatica.

Le forze ausiliare rappresentano una componente abilitante che si attiva all'occorrenza e fornisce supporto di varia tipologia (compreso il supporto logistico). Si compone di diversi tipi di individui che svolgono funzioni specifiche all'interno di una rete urbana o di forze di guerriglia.

Le organizzazioni di resistenza hanno tradizionalmente richiesto, per il loro successo, componenti che operassero in ambiente urbano e rurale. In quest'ultimo le forze di guerriglia godono di minor libertà di movimento, perciò risulta fondamentale il supporto della componente clandestina e ausiliaria della resistenza. Inoltre grazie allo sviluppo tecnologico e ai sistemi satellitari è più semplice l'identificazione dei rifugi dei guerriglieri da parte del nemico mentre l'ambiente urbano offre la possibilità di potersi confondere tra la popolazione, beneficiando degli spazi affollati.

Infine, la componente pubblica si estrinseca nelle istituzioni createsi *post* occupazione. Qualora riconosciute e accettate dal nemico, costituiscono una risorsa importante nelle fasi negoziali in rappresentanza del governo, sia esso in esilio o destituito ovvero ombra. La modalità di come si debba formare il governo, anche in condizioni emergenziali, deve essere prevista nei piani elaborati prima che la resistenza venga attivata.

Sebbene non venga annoverato tra le componenti principali, il sostegno popolare risulta cruciale ai fini del successo delle operazioni, tenuto conto che le resistenze sono in gran parte formate dai cittadini e, al di là dell'appartenenza alle componenti, comunque concorrono con i cosiddetti metodi passivi (citati nei paragrafi precedenti) a ostacolare l'operato dell'occupante.

Per concludere, affinché la resistenza organizzata abbia successo serve una struttura di comunicazione funzionale a contrastare la narrativa delle forze occupanti, in grado di connettersi con la catena di comando nazionale e locale, ma anche con la popolazione e i Paesi alleati. Tuttavia, le comunicazioni sono l'aspetto più vulnerabile delle operazioni clandestine che può addirittura portare al fallimento delle stesse o alla distruzione dell'organizzazione di resistenza. L'uso di messaggi codificati, se individuati, possono comunque rivelare l'esistenza di una rete di resistenza, così come i segnali dei cellulari possono essere captati, geolocalizzati e quindi eliminati. Risulta fondamentale, pertanto, già in fase di pianificazione pre-crisi, trovare mezzi tecnici di comunicazione non rintracciabili e metodologie di contrasto delle moderne misure di sicurezza come droni e telecamere di sorveglianza.

5. FOCUS SULLA GUERRA IN UCRAINA

La resistenza è un'attività lunga, logorante e prolungata che richiede una ferrea volontà del popolo a resistere, oltre a un'adeguata pianificazione e organizzazione.

Il comandante delle forze speciali ucraine, il Generale Hryhoriy Halahan, a seguito dell'invasione della Crimea, aveva evidenziato l'urgenza dello sviluppo del movimento di resistenza subordinato alle SOF, sottolineando l'importanza di garantire ai membri e familiari dei combattenti protezione sociale e legale. Inoltre, secondo Halalan risultava altresì importante l'educazione militare-patriottica, mediante l'addestramento e la preparazione dei cittadini alle condizioni di vita nelle aree di conflitto.

Ciò avrebbe rafforzato l'efficacia dell'esercito ucraino, con le forze regolari poste a difendere, dopo un'invasione, i territori non ancora occupati e con i gruppi di resistenza, sotto la direzione delle SOF, impegnati a compiere azioni asimmetriche contro il nemico nei territori sotto il suo controllo.

In quest'ottica già nel maggio del 2021 fu presentato il Disegno di Legge N° 5557 sui "Fondamenti della Resistenza Nazionale", nel quale si palesava la volontà del governo di strutturare la resistenza in una più ampia strategia di Difesa Totale del Paese, in linea con i principi del ROC. Tale legge, entrata in vigore nel gennaio 2022, prevedeva la costituzione della *Territorial Defense Force*, un nucleo indipendente di 10.000 professionisti militari, con il compito di guidare una forza di 130.000 riservisti civili opportunamente addestrati per la lotta urbana e contro le tattiche ibride russe. Sebbene lo scoppio della guerra non abbia reso possibile il pieno sviluppo del progetto, l'Ucraina ha potuto comunque contare per la resistenza su un *pool* di combattenti esperti, in quanto circa 400.000 persone tra il 2014 ed il 2022 sono state impegnate in operazioni nel Donbass. I Paesi occidentali hanno

addestrato le forze SOF ucraine migliorandone le capacità e l'interoperabilità, tanto che le stesse ricevettero nel 2019 la relativa certificazione dalla NATO.

Nei primi giorni dopo l'invasione della Federazione Russa la resistenza si è manifestata con metodi non violenti. Le piattaforme *social* hanno avuto un ruolo fondamentale per la diffusione di una narrativa di una nazione disposta a resistere all'invasore, cruciale per consolidare morale e resilienza. Tra gli atti di resistenza non violenta messi in atto dalla popolazione si annoverano, ad esempio, la rimozione dei cartelli stradali o la formazione di catene umane e i blocchi per rallentare l'avanzata russa.

Col protrarsi del conflitto sono state adottate azioni asimmetriche sempre più violente e mirate: attività di identificazione di obiettivi militari per l'artiglieria ucraina, sabotaggio delle linee ferroviarie e attacchi contro figure e strutture collegate con le forze di occupazione.

Le celle delle forze di resistenza ucraine vengono tenute volutamente separate e isolate per evitare che i Partigiani catturati possano rivelare le identità dei loro membri durante gli interrogatori. Da un punto di vista di C2, le loro operazioni vengono coordinate da una *Task Force* inter-agenzia governativa e gestite sul campo dall'*intelligence* militare e dalle SOF. Queste ultime sovente compiono attacchi non convenzionali dentro le linee nemiche[71].

Fondamentale è stato ed è tutt'oggi l'appoggio esterno. Gli USA e l'Unione Europea hanno inflitto gravi sanzioni economiche alla Russia e continuano a inviare equipaggiamenti e armamenti verso l'Ucraina. Le aziende civili, come ad esempio Starlink di Elon Musk, hanno fornito un ulteriore contributo mediante i loro assetti abilitanti. Senza ciò, e senza la forte motivazione del popolo ucraino e delle milizie, la resistenza sarebbe risultata probabilmente inefficace ed incapace di esprimere appieno le proprie capacità organizzative e di resilienza.

[71] Andrew E. Kramer, *"Behind Enemy Lines, Ukrainians Tell Russians 'You Are Never Safe' - The New York Times"*, www.nytimes.com, (25/03/2023).

CONCLUSIONI E CONSIDERAZIONI

La realtà odierna appare come un sistema complesso, caratterizzato da un'evoluzione costante ed eccezionalmente rapida, dove attori eterogenei nascono, si confrontano e, a volte, si scontrano con una velocità impensabile in epoche precedenti. La frenesia con la quale avvengono queste interazioni sta comportando un sensibile aumento della conflittualità che si esprime quotidianamente in ogni dominio ed ogni livello dell'ambiente operativo e prende la forma di scontri convenzionali, non convenzionali, ibridi, sopra e sottosoglia.

In questo complesso quadro conflittuale, la crescita dirompente della globalizzazione, dei *social network* e delle tecnologie duali si rivela una spinta inclusiva nei confronti di quei soggetti un tempo estranei al conflitto, determinando una cosiddetta "socializzazione" dello stesso che finisce per investire la popolazione di un peso rilevante ai fini delle sorti dello scontro e di un ruolo più rilevante che in passato.

Oggi più che mai gli Stati devono dunque approcciare i conflitti in ottica multilivello cercando di portare a sé il consenso popolare, poiché in una società frammentata ed interdipendente, l'eterogeneità che viene a crearsi rende ancora più difficile influenzare e uniformare le intenzioni della popolazione.

Far convergere l'opinione pubblica attorno ai propri obiettivi, risulta infatti determinante sotto due aspetti: da un lato consolida il supporto interno facendo accettare ai propri cittadini i costi sociali, economici e finanziari che derivano dai conflitti, dall'altro può smuovere le porzioni incerte a schierarsi apertamente dando vita a quel fenomeno potenzialmente decisivo che prende il nome di resistenza.

Essa rappresenta un serbatoio sconfinato di potenzialità, risorse, *expertise* in grado di supportare e colmare le lacune del tradizionale strumento bellico costituito dalle Forze armate: l'attuale conflitto russo – ucraino ben ne dimostra efficacia ed attualità.

In conclusione, a nostro avviso, uno Stato che ponga in essere i presupposti per dotarsi di una resistenza preparata, organizzata e gestita si munisce di un potente strumento in grado di costituire un forte deterrente per potenziali aggressori e, al contempo, di un essenziale elemento (mezzo) per assicurarsi un certo grado di autonomia da alleati e *partner*.

Stimolato dai temi trattati nella tesi, il Gruppo di Lavoro ha deciso di profondere un ulteriore sforzo. Dopo aver delineato la situazione di partenza, si è cercato di indicare possibili iniziative volte a creare un ecosistema ideale allo sviluppo di una resistenza nazionale di successo, in grado di incanalare le forze eterogenee scaturenti dalla "socializzazione del conflitto".

Per farlo, si è adottato lo strumento del PMESII, già citato nel cap. IV, che ora ci permette di esporre le nostre considerazioni in maniera analitica, riferendole ai sei elementi del potere dello Stato:

- POLITICO
  - Situazione: Il contesto del post-guerra fredda, nel quale le ultime generazioni di leader politici si sono formate, non contemplava tra i principali punti di riflessione la possibilità di uno scontro simmetrico di grandi proporzioni sul territorio nazionale[72]. I temi della sicurezza e degli investimenti in Difesa sono dunque risultati spesso divisivi e secondari rispetto ad altri, ritenuti maggiormente rilevanti per il sistema Paese;
  - Proposte: nella considerazione che la Difesa rappresenti un valore e non un costo, si auspica un incremento degli investimenti in sicurezza. A ciò si dovrà accompagnare una promozione dell'identità nazionale al fine di diffondere una consapevolezza valoriale comune e aggregante, funzionale ad una presa di coscienza da parte dei cittadini circa la necessità del loro coinvolgimento attivo nella difesa del Paese.

- MILITARE
  - Situazione: Lo strumento appare funzionale ad operazioni di gestione delle crisi, che hanno caratterizzato gli ultimi decenni. Se immerso in un contesto di *warfighting* tradizionale, esso risulta sottodimensionato sia a livello quantitativo (centosessantacinque mila unità[73]) che qualitativo. Si pensi, ad esempio, al conflitto in corso tra Russia e Ucraina, dove l'agenzia di stampa "Reuters" stima i soldati caduti o feriti in trecentocinquantamila unità[74]. A seguito della sospensione della leva sono venute gradualmente a mancare le risorse economiche, infrastrutturali ed organizzative necessarie a sostenere un addestramento di massa;
  - Proposte: Si auspica un ripensamento della struttura organizzativa della Difesa, che sia in grado di inglobare porzioni della popolazione civile nel processo di formazione e addestramento. Si potrebbe pensare ad un'evoluzione del servizio di leva che preveda, ad esempio, un corso iniziale più breve seguito da continui aggiornamenti e partecipazioni ad esercitazioni congiunte con le Forze armate professionistiche.

---

72 Alessandro Colombo, "La crisi del "Nuovo Ordine Mondiale"", www.fondazionefeltrinelli.it, (16/04/2023).
73 Cfr. – Giovanni Martinelli, "Verso la revisione del modello di Forze armate?", www.analisidifesa.it, (16/04/2023).
74 Guy Falconbridge, *"Ukraine war, already with up to 354,000 casualties, likely to last past 2023 - U.S. documents"*, www.reuters.com, (23/04/2023)

- ECONOMICO
  - Situazione: Sin dal vertice del Galles del 2014, quando è stato posto l'obiettivo del 2% in difesa, il Paese non è riuscito a incrementare in maniera sostanziale la propria spesa. Nel 2014 l'Italia spendeva l'1,14% del PIL; nel 2022 la spesa è stata dell'1,51%, ancora ben al di sotto del livello concordato[75];
  - Proposte: Si auspica un grosso investimento iniziale strutturale che permetta di colmare le lacune evidenziatesi a seguito dell'evolversi del quadro geopolitico. Di questo, un'importante porzione dovrà essere destinata alla creazione di una struttura logistico–organizzativa adatta a formare e gestire un elevato numero di personale, funzionale all'inclusione di ampie porzioni della società nel sistema Difesa; peraltro, gran parte delle proposte scaturenti dall'analisi del PMESII prescindono necessariamente da un maggior e continuo sostegno economico.

- SOCIALE
  - Situazione: Figlia del benessere, la società odierna pare aver dimenticato i sentimenti di solidarietà e di aggregazione nazionale sperimentati nel periodo dei conflitti mondiali o del dopoguerra, dove la presenza di un nemico comune e le difficoltà quotidiane, fungevano da collante. Come descritto da Edward Luttwak nel saggio "*Toward Post-Heroic Warfare*", apparso su "Foreign Affairs" nel 1995, nelle società occidentali l'estremo sacrificio per la collettività, non viene più visto come un atto di eroismo, viene bensì classificato come spreco di vite umane[76]. Fenomeni di individualismo e localismo si sono gradualmente imposti su sentimenti di altruismo e amor patrio, creando un contesto nel quale l'individuo si sente sempre meno parte di una collettività e dunque è sempre meno incline a sacrificarsi per essa. A supporto di ciò è emblematico il sondaggio effettuato dalla società Izi, dove, tra gli intervistati circa la metà è favorevole alla reintroduzione della leva, ma solo il 3,5% di essi ritiene importante l'arruolamento di persone in caso di necessità[77] (vedasi approfondimento in "Allegato A");
  - Proposte: Al fine di creare la base per una resistenza, si avverte come necessario accrescere la coesione sociale. Si auspica dunque l'adozione di politiche inclusive che vadano ad avvicinare le diverse componenti che costituiscono la complessa società attuale ed una riforma del sistema d'istruzione che valorizzi le dinamiche di gruppo e l'interazione tra gli individui.

[75] Cfr. – Andrea Muratore, "La corsa dell'Italia alla spesa militare: perché deve raggiungere il target NATO", it.insideover.com, (16/04/2023).
[76] Cfr. – Michele Malincomi, "La guerra nell'era del post-eroismo", www.osservatorioglobalizzazione.it, (16/04/2023).
[77] Cfr. – AA.VV., "Reintroduzione della leva militare", www.izi.it, (16/04/2023).

- INFORMATIVO
  - Situazione: Nella classifica annuale sulla libertà di stampa del "*Reporters sens frontier*" (RSF), l'Italia occupa la 58ª posizione, penultima in Europa (ultima è la Grecia). Se si va ad approfondire la metodologia con la quale viene stata stilata tale classifica, si evince che i Paesi con i punteggi più bassi sono anche quelli dove le informazioni e la propaganda vengono spesso influenzate da agenti economici, politici e sociali[78]. Secondo il *RSF*, l'Italia è caratterizzata da un clima di forte polarizzazione delle opinioni, dove gruppi estremisti minano la libertà di espressione anche con metodi non ortodossi;
  - Proposte: Si auspica un coinvolgimento olistico di tutti i comparti della società al fine della creazione e della diffusione di una narrativa nazionale comune, slegata da interessi di nicchia e che miri a circoscrivere gli estremismi, in grado di accrescere la consapevolezza valoriale e di stimolare sentimenti di approvazione e condivisione attorno al tema della difesa nazionale.

- INFRASTRUTTURE
  - Situazione: Il ridimensionamento dello strumento militare ha comportato la razionalizzazione delle infrastrutture, con una conseguente perdita di capacità e capillarità sul territorio nazionale;
  - Proposte: Per conferire resilienza alla resistenza, sarebbe auspicabile la formulazione di un piano che preveda, a necessità, la rapida rimessa in funzione di strutture militari diffuse capillarmente su tutto il territorio.

Poter contare su una resistenza che, in caso di conflitto, concorra con le Forze armate alla difesa dello Stato è il frutto, dunque, di uno sforzo complesso e coordinato, che non può essere improvvisato nel momento del bisogno.

Per non farsi cogliere impreparati, si renderà dunque indispensabile, già in tempo di pace, promuovere a livello politico una riflessione sulle modalità di inclusione del cittadino nel sistema Difesa, coinvolgendo i diversi Dicasteri nella stesura di un piano di resistenza che contempli l'interazione tra civili attivi e militari, attraverso la definizione di procedure, modalità e l'individuazione di figure chiave.

La "socializzazione del conflitto" appare un fenomeno difficilmente arginabile: di fronte a ciò uno Stato può semplicemente limitarsi a monitorare l'evoluzione dello stesso, o può, come auspichiamo, promuovere un'analisi più attenta che miri a mitigarne i rischi e sfruttarne le opportunità, per costruire un Paese più sicuro, credibile e resiliente.

[78] Cfr. - rsf.org

BIBLIOGRAFIA

- "*Can technology transform future urban combat*", European Security and Defence, 2022 https://euro-sd.com/2022/03/articles/exclusive/25293/can-technology-transform-future-urban-combat/*2021", ed. 2021*
- *AA.VV, Unhcr: La pandemia non ferma la fuga da guerre e persecuzioni: più di 82 milioni di profughi. Il doppio di dieci anni fa, https://www.repubblica.it/esteri/2021/06/18/news/unhcr_-306592342/, (ultimo accesso 10/04/2023)*
- *AA.VV., "Effect on Economic globalization" https://education.nationalgeographic.org/resource/effects-economic-globalization/, (ultimo accesso 07/02/2023)*
- *AA.VV., "Ordine globale: la fine di un'era", https://www.ispionline.it/it/pubblicazione/ordine-globale-la-fine-di-unera-34141 (ultimo accesso 15/02/2023)*
- *AA.VV., "Twitter e Jihad: la comunicazione dell'IS", https://www.ispionline.it/it/pubblicazione/twitter-e-jihad-la-comunicazione-dellIS-12842 (ultimo accesso 13/04/23)*
- *AA.VV., L'aggiornamento militare sulla guerra in Ucraina: sistemi non criptati e cellulari rubati, tutti i problemi di comunicazione dei russi https://www.corriere.it/esteri/22_marzo_28/aggiornamento-militare-guerra-ucraina-sistemi-non-criptati-cellulari-rubati-tutti-problemi-comunicazione-russi-16d2d67c-aea9-11ec-89b4-33ef6a8626b0_amp.html (ultimo accesso 6/04/23)*
- *AA.VV., Società libica: il ruolo del tribalismo, https://mondointernazionale.org/focus-allegati/societ%C3%A0-libica-il-ruolo-del-tribalismo, (ultimo accesso 05/03/2023)*
- *AA.VV., Usa, rimossa la statua di Thomas Jefferson dalla New York City Hall, https://tg24.sky.it/mondo/2021/11/23/statua-thomas-jefferson-rimossa-new-york-city-hall, (ultimo accesso 05/03/2023)*
- *Alessandro Colombo, "La crisi del "Nuovo Ordine Mondiale", https://fondazionefeltrinelli.it/la-crisi-del-nuovo-ordine-mondiale/, (ultimo accesso 16/04/2023)*
- *Algadiscia Marocco, "Non si può più dire niente". Anche il New York Times si è redento dalla cancel culture", https://www.huffingtonpost.it/cultura/2022/03/24/news/new_york_times_cancel_culture-9029722/ (ultimo accesso05/03/2023)*

- *Andrea Muratore, La corsa dell'Italia alla spesa militare: perché deve raggiungere il target NATO, https://it.insideover.com/difesa/la-corsa-dellitalia-alla-spesa-militare-perche-deve-raggiungere-il-target-nato.html, (ultimo accesso 16/04/2023)*
- *Bartoccini Davide, "La guerra dei droni nei cieli dell'Ucraina", https://it.insideover.com/guerra/la-guerra-dei-droni-cieli-ucraina.html/amp (ultimo accesso 12/04/23)*
- *Bergen Peter, "Zero Dark Thirty: did torture really net bin Laden?", https://edition.cnn.com/2012/12/10/opinion/bergen-zero-dark-thirty/index.ht (ultimo accesso 10/04/23)*
- *Calha, Julio Miranda. "Hybrid Warfare: NATO's New Strategic Challenge?" Draft General Report (Brussels: NATO Parliamentary Assembly (7 April 2015).*
- *Caprara Giovanni, "La guerra e il rischio per i satelliti Gps. Ma i russi ancora non hanno scatenato l'offensiva", https://www.corriere.it/tecnologia/22_aprile_01/gps-terra-spazio-confronto-sistemi-militari-orbita-russia-occidente-98cd445e-af72-11ec-a232-b69d1c970bf4.shtml, (ultimo accesso 6/04/23)*
- *Chekinov, S.G. and S.A. Bogdanov. "The Nature and Content of a New-Generation War", Military Thought (October-December 2013).*
- *Cristina da Rold, "Il gap etnico dell'università oggi. La disuguaglianza negli Stati Uniti", https://www.infodata.ilsole24ore.com/2020/06/13/gap-etnico-delluniversita-oggi-la-disuguaglianza-negli-stati-uniti/, (ultimo accesso 03/04/2023)*
- David Kilcullen e Gordon Pendleton, *"Future urban conflict, technology, and the protection of civilians: Real-World Challenges for NATO and Coalition Missions"*, The Stimson Center, June 2021
- Drew Harwell e Rachel Lerman, "*How Ukrainians have used social media to humiliate the Russians and rally the world*" – The Washington Post, 2022, https://www.washingtonpost.com/technology/2022/03/01/social-media-ukraine-russia/
- *Dunlap, Charles J. Jr. "Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts" Humanitarian Challenges in Military Intervention Conference (November 2001).*
- *Dunlap, Charles J. Jr. "Lawfare: A Decisive Element of 21st Century Conflicts?" JF Quarterly (July 2009).*
- *Elena Alice Rossetti, "Le possibili traiettorie dell'IS nel 2022 in Iraq e Siria dopo l'attacco alla prigione di Al-Sina e la morte del leader Abu Ibrahim al-Hashimi al-Qurashi", https://www.geopolitica.info/possibili-traiettorie-IS-nel-2022-iraq-siria/, (ultimo accesso 20/03/2023)*

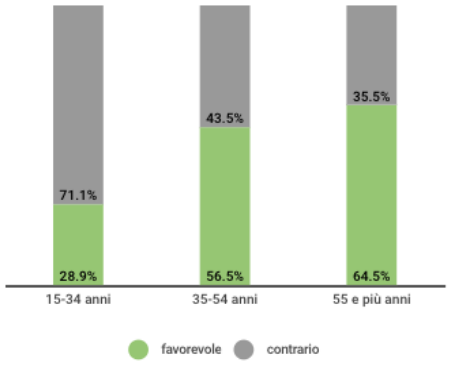
- *Galvach, Zane M., Thomas B Everett, Matthew J. Mesko, Jeffrey V. and Anton V Soltis. "Russian Political Warfare: Origin, Evolution, and Application" (thesis, Naval Postgraduate School, 2015).*
- *Gazula, Mohan B. "Cyber Warfare Conflict Analysis and Case Studies." Cybersecurity Interdisciplinary Systems Laboratory (CISL) Sloan School of Management, Massachusetts Institute of Technology. Submitted in partial fulfillment of master's degree requirements. May 2017.*
- *Gerasimov, Valery. "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations" translated by R. Coalson (Jan-Feb 2016).*
- *Gerasimov, Valery. "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations" translated by R. Coalson (Jan-Feb 2016).*
- *Giovanni Martinelli, "Verso la revisione del modello di Forze armate?", https://www.analisidifesa.it/2022/01/verso-la-revisione-del-modello-di-forze-armate/, (ultimo accesso 16/04/2023)*
- *Giovanni Tria, "La globalizzazione contemporanea: caratteristiche conseguenze e sfide", ed. 2019*
- *Gordon, Max. "Lessons From the Front: A Case Study of Russian Cyber Warfare", (December 2015).*
- *Guy Falconbridge, "Ukraine war, already with up to 354,000 casualties, likely to last past 2023 - U.S. documents", https://www.reuters.com/world/europe/ukraine-war-already-with-up-354000-casualties-likely-drag-us-documents-2023-04-12/, (ultimo accesso23/04/2023)*
- *Hoffman, Frank G and James N. Mattis. "Future Wars: The Rise of Hybrid Wars", (November 2005).*
- *Hoffman, Frank G. "Conflict in the 21st Century: The Rise of Hybrid Wars", (Arlington: Potomac Institute of Policy Studies, 2007).*
- *Hoffman, Frank G. "Hybrid Warfare and Challenges." Joint Forces Quarterly vol. 52, no. 1 (2009):*
- *https://mondointernazionale.org/en/focus-allegati/resistance-operating-concept-roc-alla-luce-della-guerra-in-ucraina (ultimo accesso 06/04/23)*
- *Internal Displacement Monitoring Centre (IDMC), "Global Report on Internal displacement*
- *International CrIS Group (ICG), "Popular Protest in North Africa and the Middle East (VI): The Syrian People's Slow-motion Revolution", 6 luglio 2011*

- *Johnson, Robert. "Hybrid War and its Countermeasures: A Critique of the Literature", Small Wars and Insurgencies vol. 29, no. 1 (2018).*
- *Johnson, Robert. "Hybrid War and its Countermeasures: A Critique of the Literature." Small Wars and Insurgencies vol. 29, no. 1 (January 2018).*
- *Khan Ilias M, "Who was the courier who led US to Osama Bin Laden?" https://www.bbc.com/news/world-south-asia-13300680.amp (ultimo accesso 11/04/23)*
- *Maigre, Merle. "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO" The German Marshall Fund of the United States (12 February 2015).*
- *Marco Ghisetti, Le fragilità ed il fallimento dell'ordine egemonico liberale, https://osservatorioglobalizzazione.it/osservatorio/fallimento-ordine-liberale/, (ultimo accesso 15/02/2023)*
- Marco Stoccuto, "*Le information operations: uno strumento per influenzare i processi decisionali"* – Informazioni della Difesa n. 4-2009
- *Michele Malincomi, "La guerra nell'era del post-eroismo", https://www.osservatorioglobalizzazione.it/osservatorio/guerra-post-eroismo/, (ultimo accesso 16/04/2023)*
- *NEW YORK TIMES (no author), "How Osama Bin Laden was located and killed", https://archive.nytimes.com/www.nytimes.com/interactive/2011/05/02/world/asia/abbottabad-map-of-where-osama-bin-laden-was-killed.html?mabReward=relbias%253Ar%252C&module=Search (ultimo accesso 12/04/23)*
- *Nicolao Lorenzo, "Anonymous sfida la censura di Putin con Goggle Maps: le recensioni di bar e locali raccontano la guerra", https://www.corriere.it/tecnologia/22_marzo_04/anonymous-putin-maps-ec2dba4e-9b9e-11ec-87e9-1676e8d33acb_amp.html (ultimo accesso 25/03/23)*
- *Olimpo Guido, "La guerra dei droni nuova minaccia IS", https://www.corriere.it/extra-per-voi/2017/03/03/guerra-droni-nuova-minaccia-IS-35361460-0055-11e7-92b1-e1f58b14debd.shtml (ultimo accesso 13/04/23)*
- *Otto C. Fiala, "Resistance Operating Concept (ROC), The JSOU Press, MacDill Air Force Base, Florida, 2020.*
- *Ottolina Paola, Smartphone (e tappetini di gomma di 2 euro): le armi a sorpresa per respingere l'attacco russo a Kiev, https://www.corriere.it/tecnologia/22_aprile_12/smartphone-tappetini-gomma-2-euro-armi-sorpresa-respingere-l-attacco-russo-kiev-256e60bc-ba3d-11ec-ac09-3ceafb137606_amp.html (ultimo accesso 21/03/23)*

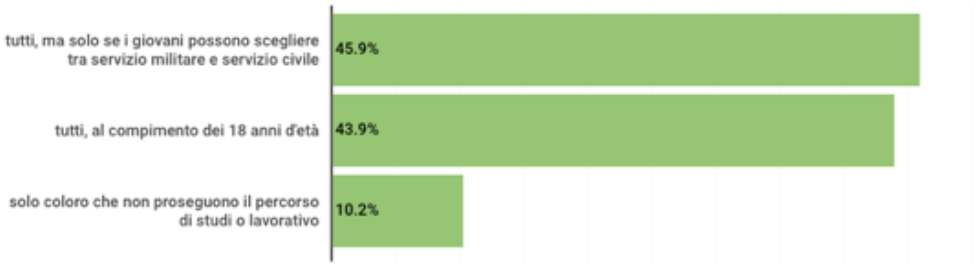
- *Paola Rosa Ardagna, "Cancel culture, che cos'è davvero la "cultura della cancellazione", https://www.repubblica.it/cronaca/2021/06/11/news/cancel_culture_le_parole_per_dirlo-304598775/, (ultimo accesso 20/04/2023)*
- *Parker Nick, "Russian soldiers bombard Ukrainian girls with flirty Tinder request, https://www.thesun.co.uk/news/17750041/russian-soldiers-tinder-ukraine/amp/ (ultimo accesso 3/03/23)*
- *Racz, Andras. "Russia's Hybrid War in Ukraine, Breaking the Enemy's Ability to Resist". Helsinki: The Finnish Institute of International Affairs, FIIA Report 43. June 2015.*
- *Ragoni Emiliano, "Elon Musk mette a disposizione dell'Ucraina i satelliti di Starlink", https://www.corriere.it/tecnologia/22_febbraio_27/elon-musk-mette-disposizione-dell-ucraina-satelliti-starlink-8e271cf0-97c1-11ec-97aa-535db4de4386.shtml (ultimo accesso 3/4/23)*
- *Schmidt, Andreas. "The Estonian Cyberattacks." (2013).*
- *Serarini Marta, "Osama Bin Laden, 10 anni fa veniva ucciso il leader di al-Qaeda", https://www.corriere.it/esteri/21_maggio_02/osama-bin-laden-10-anni-fa-veniva-ucciso-leader-al-qaeda-9b3b81e0-ab0b-11eb-a155-ccb2f12f7395.shtml (ultimo accesso 15/04/23)*
- *SOCEUR, "Resistance Operating Concept (ROC)", ed.2020*
- *Stefano Torelli, "La Siria tra rivolte e depressione" (Istituto per gli Studi di Politica Internazionale), ed. 2011*
- Steven Feldstein, "*Disentangling the digital battlefield: how the internet has changed war"* – 2022, https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/
- Vivek Wadhwa e Alex Salkever, "*How Elon Musk's Starlink Got Battle-Tested in Ukraine*", Foreign Policy Magazine, 2022 https://foreignpolicy.com/2022/05/04/starlink-ukraine-elon-musk-satellite-internet-broadband-drones/
- *Vojtiskova, Vladislava, Vit Novotny, Hubertus Schmid-Schmidsfelden, and Kristina Potapova, "The Bear in Sheep's Clothing: Russia's Government Funded Organizations in the EU" (Brussels: Wilfried Martens Centre for European Studies, 2016).*
- *www.izi.it*
- *rsf.org*

La reintroduzione della leva militare obbligatoria

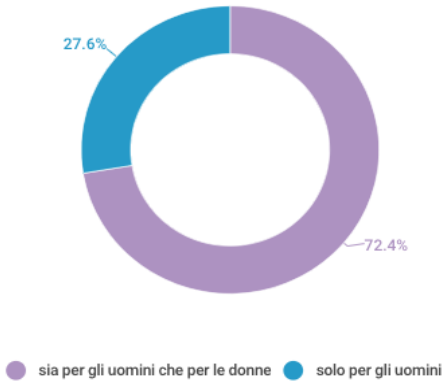
Lei è favorevole alla proposta di reintrodurre la leva militare obbligatoria in Italia (sospesa nel 2004)?



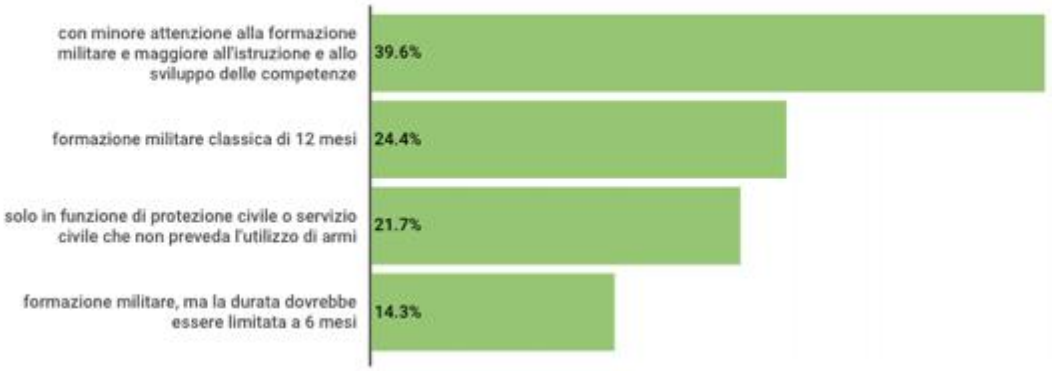
Se favorevole: chi dovrebbe essere soggetto al periodo di leva?



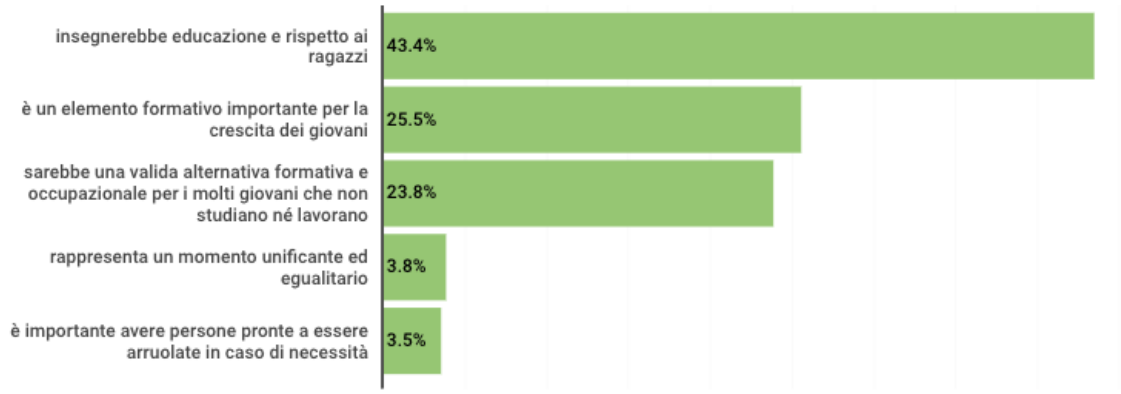
Se favorevole: per chi dovrebbe essere obbligatoria la leva militare?



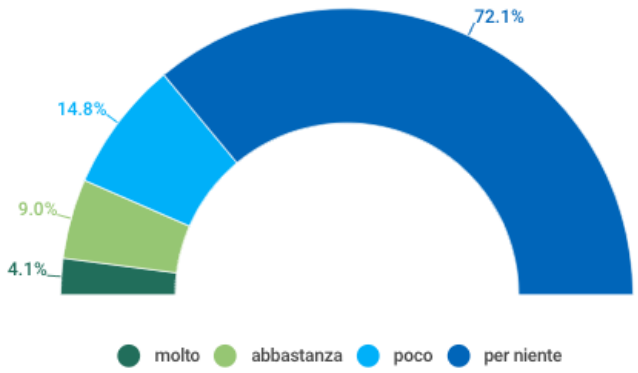
Se favorevole: con quale modalità dovrebbe svolgersi il periodo di leva?
(modalità prevalente, una sola risposta)



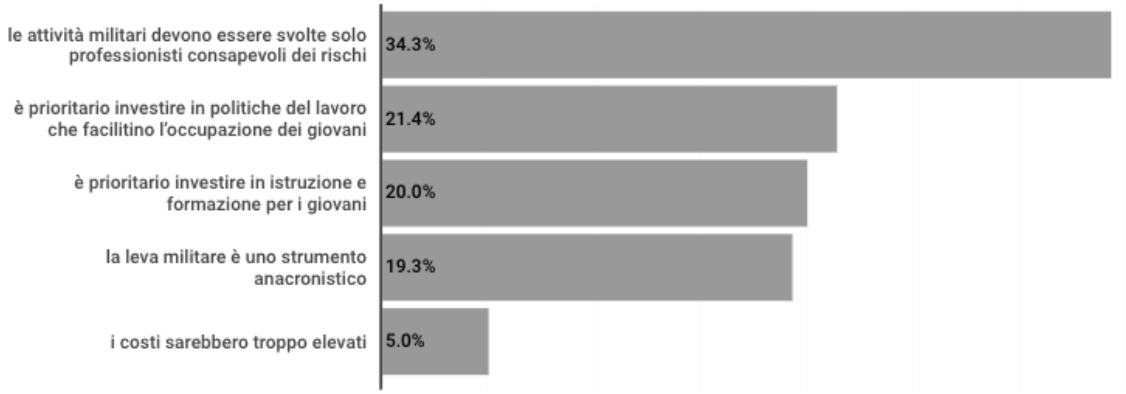
Se favorevole: perché è favorevole alla reintroduzione della leva obbligatoria?
(motivazione prevalente, una sola risposta)



Se favorevole: quanto la sua scelta è influenzata dalla guerra in Ucraina?



Se contrario: perché è contraria/o alla reintroduzione della leva obbligatoria?
(motivazione prevalente, una sola risposta)



Nota metodologica:
Popolazione di riferimento: popolazione residente in Italia
Campionamento: casuale stratificato per genere, classe d'età e macroarea geografica di residenza
Ponderazione: vincolata per sesso, classe d'età e regione di residenza
Metodologia: tecnica mista CATI-CAWI
Totale interviste: 1024, effettuate fra il 22 e il 23 agosto 2022

IMPORTANT INFORMATION FOR THE POPULATION OF SWEDEN

IF CRISIS OR WAR COMES

Emergency preparedness

Total defence

Warning systems

Contents

Emergency preparedness

Total defence

Warning systems

This brochure is available to download in several different languages at dinsäkerhet.se.

Questions and answers about the brochure can be found at dinsäkerhet.se.

MSB Swedish Civil Contingencies Agency

PEFC

MSB is a central government agency that works to improve Sweden's ability to prevent and manage accidents and emergencies. In the event of a serious accident or emergency, we provide support to those who are responsible.

Swedish Civil Contingencies Agency (MSB)
651 81 Karlstad
www.msb.se

Graphic design and production: Kreab AB
Illustrations: Arvid Steen
Printed by: Stibo Graphic A/S
Publ. no.: MSB1214 - May 2018
ISBN: 978-91-7383-836-8

For the population of Sweden

This brochure is being sent to all households in Sweden at the behest of the Swedish Government. The Swedish Civil Contingencies Agency (MSB) is responsible for its content. The purpose of the brochure is to help us become better prepared for everything from serious accidents, extreme weather and IT attacks, to military conflicts.

Many people may feel a sense of anxiety when faced with an uncertain world. Although Sweden is safer than many other countries, there are still threats to our security and independence. Peace, freedom and democracy are values that we must protect and reinforce on a daily basis.

Public authorities, county councils and regions, municipalities, companies and organisations are responsible for ensuring that society functions. However, everyone who lives in Sweden shares a collective responsibility for our country's security and safety. When we are under threat, our willingness to help each other is one of our most important assets.

If you are prepared, you are contributing to improving the ability of the country as a whole to cope with a major strain.

KEEP THIS BROCHURE!

3

Emergency preparedness

What would you do if your everyday life was turned upside down?

An emergency can result in society not functioning in the way we are used to. Climate change may mean that flooding and forest fires become more common. Incidents in the rest of the world may result in shortages of certain foodstuffs. Disruptions to important IT systems may have an impact on the electricity supply. In just a short time, your everyday life can become problematic:

- The heating stops working.
- It becomes difficult to prepare and store food.
- The shops may run out of food and other goods.
- There is no water coming from the taps or the toilet.
- It is not possible to fill up your car.
- Payment cards and cash machines do not work.
- Mobile networks and the internet do not work.
- Public transport and other means of transport are at a standstill.
- It becomes difficult to obtain medicines and medical equipment.

Think about how you and people around you will be able to cope with a situation in which society's normal services are not working as they usually do.

Your emergency preparedness

Your municipality is responsible for ensuring that services including care of the elderly, the water supply, the fire and rescure service and schools continue to function, even in the event of a societal emergency. As a private individual, you also have a responsibility. Preparing correctly can enable you to cope with a difficult situation, regardless of what has caused it.

In the event of a societal emergency, help will be provided first to those who need it most. The majority must be prepared to cope on their own for some time. The better prepared you are, the greater the opportunity you will also have to help others who do not have the same prerequisites.

What is most important is that you have water, food and warmth and are able to obtain information from the authorities and the media. You also need to be able to make contact with relatives. There are check-lists on pages 10 and 11 with foodstuffs and items that are good to have at home.

Think about what risks may affect you and your local area. Do you live in an area that is sensitive to landslides or flooding? Is there some sort of hazardous industry or something else in your area that may be good to know about?

Emergency preparedness

Be on the lookout for false information

States and organisations are already using misleading information in order to try and influence our values and how we act. The aim may be to reduce our resilience and willingness to defend ourselves.

The best protection against false information and hostile propaganda is to critically appraise the source:

- Is this factual information or opinion?
- What is the aim of this information?
- Who has put this out?
- Is the source trustworthy?
- Is this information available somewhere else?
- Is this information new or old and why is it out there at this precise moment?

- Search for information – the best way to counteract propaganda and false information is to have done your homework.
- Do not believe in rumours – use more than one reliable source in order to see whether the information is correct.
- Do not spread rumours – if the information does not appear trustworthy, do not pass it on.

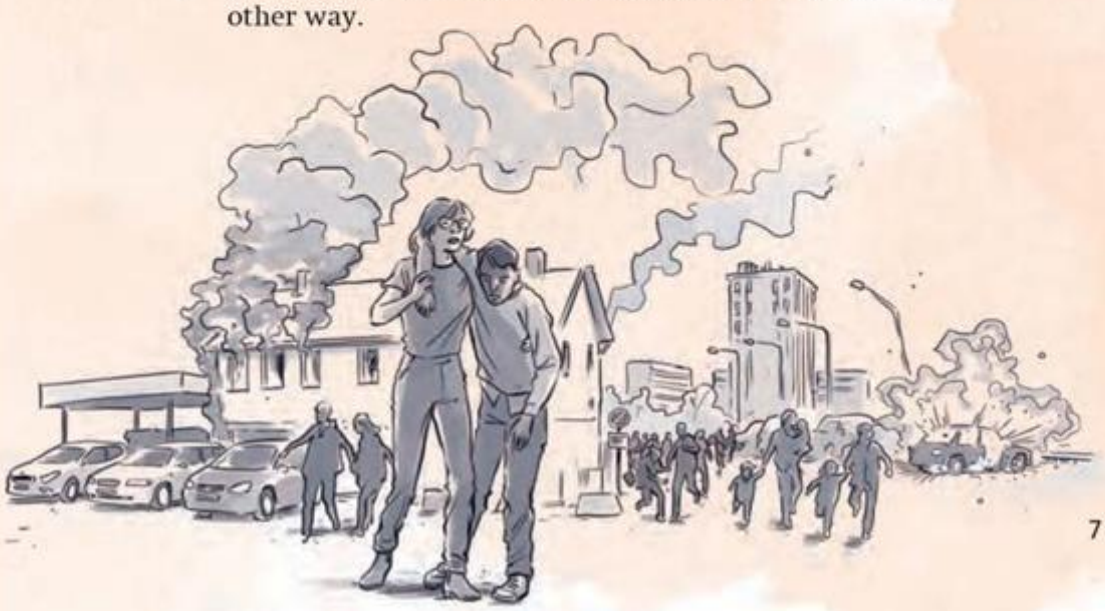
6

You can find more information at dinsäkerhet.se

In the event of a terror attack

Terror attacks may be targetted against individual people or groups, against the general public or against vital societal functions such as the electricity supply or the transport system. Even though there are many different ways to carry out a terrorist attack, there are some pieces of advice that may be applicable in most situations:

- Move to a safe place and avoid large groups of people.
- Call the police on 112 and inform them if you see something important.
- Warn those who are in danger and help those who are in need of assistance.
- Put your mobile on silent and do not call anyone who may be in the danger area. The sound of their phone ringing may reveal the location of someone who is hiding.
- Do not call anyone with your mobile unless you have to. If the network is overloaded, it may be difficult for vital calls to get through.
- Comply with requests from the police, the fire and rescue service and the authorities.
- Do not share unconfirmed information online or in any other way.



Emergency preparedness

7

Sweden's defences

Sweden's combined defences are in place to protect the country, our freedom and our right to live as we ourselves choose to. All of us have a duty to act if Sweden is threatened.

Total defence

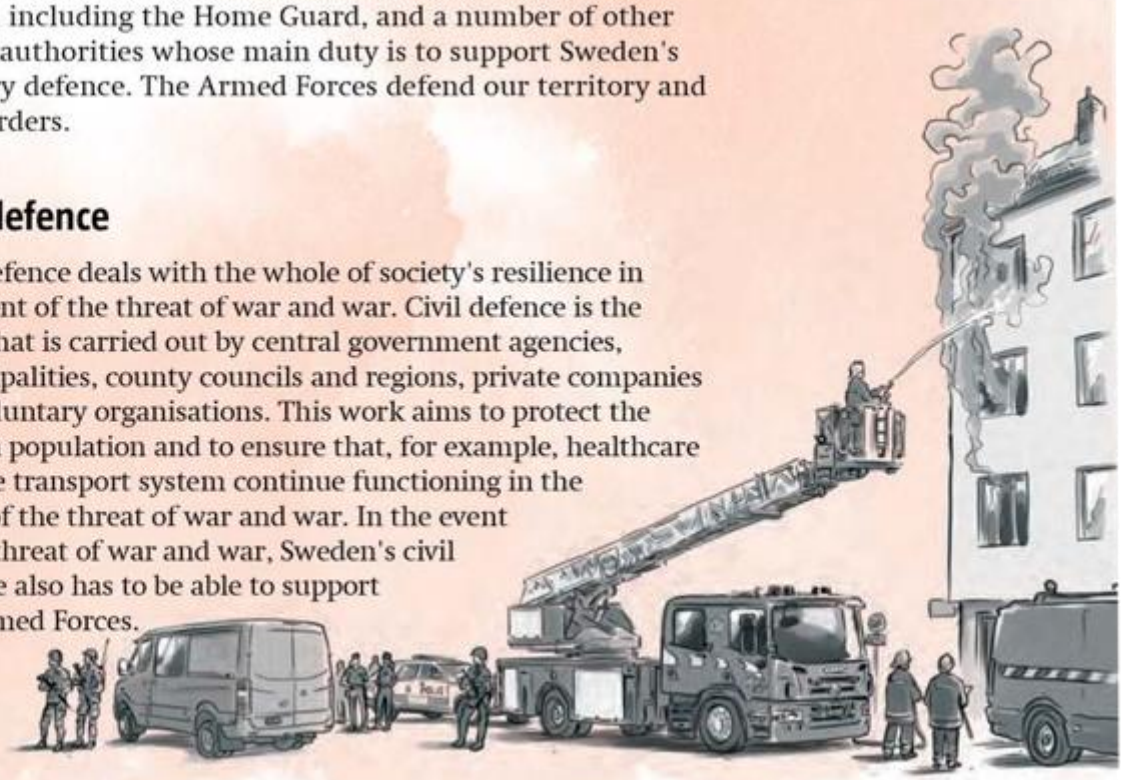
The term 'total defence' denotes all activities that are needed in order to prepare Sweden for war. Sweden's total defence consists of military defence and civil defence.

Military defence

Sweden's military defence consists of the Swedish Armed Forces, including the Home Guard, and a number of other public authorities whose main duty is to support Sweden's military defence. The Armed Forces defend our territory and our borders.

Civil defence

Civil defence deals with the whole of society's resilience in the event of the threat of war and war. Civil defence is the work that is carried out by central government agencies, municipalities, county councils and regions, private companies and voluntary organisations. This work aims to protect the civilian population and to ensure that, for example, healthcare and the transport system continue functioning in the event of the threat of war and war. In the event of the threat of war and war, Sweden's civil defence also has to be able to support the Armed Forces.



Total defence

8

Duty to contribute to Sweden's total defence

In Sweden there is a duty to contribute to total defence. This means that everyone who lives here and is between the ages of 16 and 70 can be called up to assist in various ways in the event of the threat of war and war. Everyone is obliged to contribute and everyone is needed.

The duty to contribute to total defence has three forms:

- **Conscription** into the Armed Forces.
- **Civil conscription** into organisations controlled by the Government.
- **General national service** involves serving in organisations that must function even in the event of the threat of war and war. This means that you continue to do your normal job, work in a voluntary organisation or are tasked by Arbetsförmedlingen with performing work that is of particular importance to Sweden's total defence.

Those compelled to contributed to Sweden's total defence can be given wartime postings. If you are given a wartime posting, you will have received wartime posting orders or another form of confirmation from your employer about this.

For many years, the preparations made in Sweden for the threat of war and war have been very limited. Instead, public authorities and municipalities have focused on building up the level of preparedness for peacetime emergencies such as flooding and IT attacks. However, as the world around us has changed, the Government has decided to strengthen Sweden's total defence. That is why planning for Sweden's civil defence has been resumed. It will take time to develop all parts of it again. At the same time, the level of preparedness for peacetime emergencies is an important basis of our resilience in the event of war.

Follow what is happening at **dinsäkerhet.se**

Total defence

9

Home preparedness tips

Your prerequisites and needs vary, for example, depending on whether you live in the countryside or in a built-up area, in a house or in an apartment. Here are some general home preparedness tips. Use that which is appropriate for you and those close to you. It is a good idea to share certain things and borrow from one another.

Food

It is important to have extra food at home that provides sufficient calories. Use non-perishable food that can be prepared quickly, requires little water or can be eaten without preparation.

- ☐ potatoes, cabbage, carrots, eggs
- ☐ bread with a long shelf-life, e.g. tortillas, hard bread, crackers, rusks
- ☐ cheese spread, soft whey cheese and other spreads in tubes
- ☐ oat milk, soy milk, milk powder
- ☐ cooking oil, hard cheese
- ☐ quick-cook pasta, rice, grains, instant mashed potatoes
- ☐ precooked lentils, beans, vegetables, hummus in tins
- ☐ chopped tomatoes to, for example, cook pasta in
- ☐ tins of bolognese sauce, makerel, sardines, ravioli, salmon balls, boiled meat, soup
- ☐ fruit purée, jam, marmelade
- ☐ prepared blueberry and rosehip soup, juice or another drink that can be stored at room temperature
- ☐ coffee, tea, chocolate, energy bars, honey, almonds, nuts, nut butter, seeds.

Water

Clean drinking water is vital. Allow for at least three litres per adult per day. If you are uncertain about its quality, you need to be able to boil the water.

If the toilet is not working, you can take strong plastic bags and place them in the toilet bowl. Good hand hygiene is important for avoiding infection.

- ☐ bottles
- ☐ buckets with lids
- ☐ Plastic bottles to freeze water in (do not fill to the top as the bottle will crack if you do)
- ☐ mineral water
- ☐ jerry cans, ideally with a tap, to collect water in. You can also have a couple of clean jerry cans that are filled with water as a reserve. These are to be stored in a cool, dark place.

Learn more about home preparedness at **dinsäkerhet.se**

10

Warmth

If the electricity goes off at a cold time of the year, your home will quickly become cold. Gather together in one room, hang blankets over the windows, cover the floor with rugs and build a den under a table to keep warm. Think about the risk of fire. Extinguish all candles and alternative heating sources before you go to sleep. Air the room regularly to let in oxygen.

- ☐ woolen clothes
- ☐ warm all-weather outdoor clothing
- ☐ hats, gloves, scarves
- ☐ blankets
- ☐ sleeping mats
- ☐ sleeping bags
- ☐ candles
- ☐ tea lights
- ☐ matches or fire-lighter
- ☐ alternative heat sources, e.g. LPG heaters, paraffin heaters.

Other

- ☐ spirit stove and fuel
- ☐ torch, head torch
- ☐ batteries

Communications

In the event of a serious incident, you need to be able to receive important information from the authorities, primarily Sveriges Radio's radio station P4. You also need to be able to follow how the media are reporting events, remain in contact with relatives and friends and be able to reach the emergency services in the event of an emergency.

- ☐ a radio powered by batteries, solar cells or winding
- ☐ a car radio
- ☐ a list of important telephone numbers on paper
- ☐ extra batteries/power bank for devices such as mobile phones
- ☐ mobile phone charger that works in the car.

- ☐ cash in small denominations
- ☐ medicine cabinet and extra medicines
- ☐ wet wipes
- ☐ hand sanitiser
- ☐ nappies and menstrual products
- ☐ paper printouts of information such as insurance policies, bank details, registration certificates
- ☐ fuel in the tank.

11

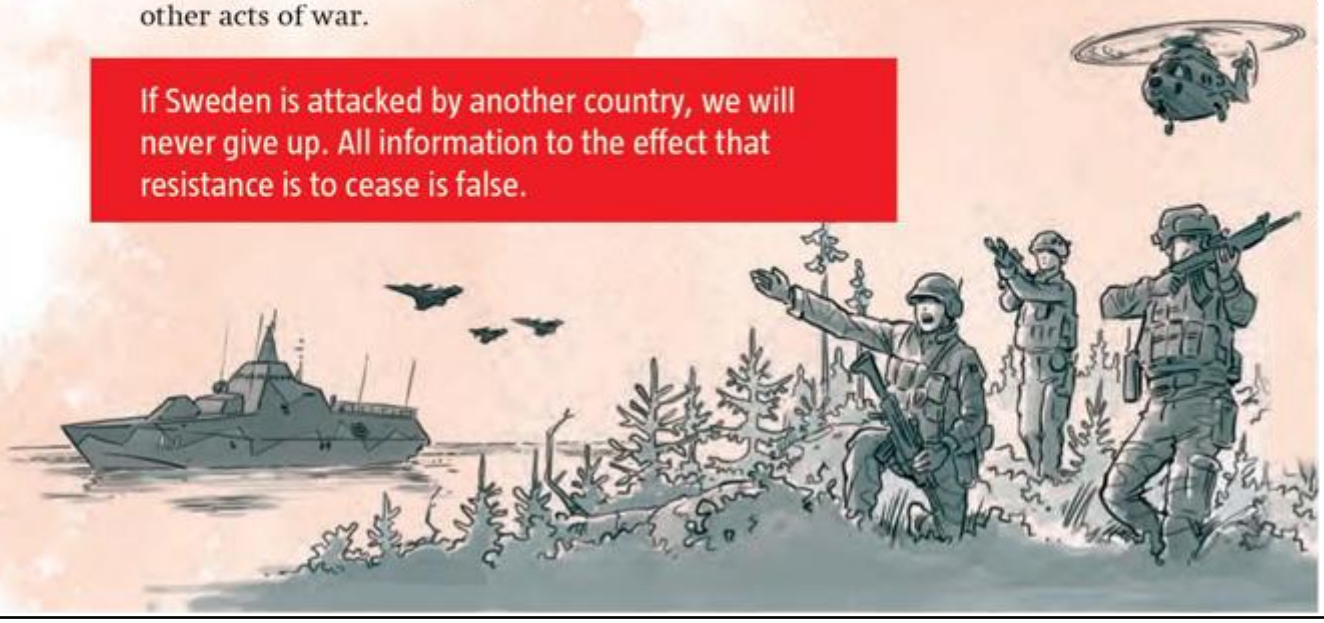
If Sweden is attacked, resistance is required

We must be able to resist various types of attacks directed against our country. Even today, attacks are taking place against our IT systems and attempts are being made to influence us using false information. We may also be affected by conflicts in our region. Potential attacks include:

- Cyberattacks that knock out important IT systems.
- Sabotage of infrastructure (e.g. roads, bridges, airports, railways, electricity cables and nuclear power stations).
- Terror attacks that affect a large number of people or important organisations.
- Attempts to influence Sweden's decision makers or inhabitants.
- Severed transport links that result in a shortage of foodstuffs and other goods.
- Military attack, for example airstrikes, rocket attacks or other acts of war.

Total defence

If Sweden is attacked by another country, we will never give up. All information to the effect that resistance is to cease is false.



12

Heightened state of alert

The Government can decide to put the country on a heightened state of alert in order to improve Sweden's chances of defending itself. In a heightened state of alert, peacetime laws apply, but other laws may also be used. For example, the state can requisition private property that is of particular importance to Sweden's total defence.

In a heightened state of alert, the whole of society has to gather its collective forces in order to ensure that which is most important functions. In a heightened state of alert, you may be called up to help in various ways.

Information about the heightened state of alert will be broadcast on radio and TV. Sveriges Radio's radio station P4 is the emergency channel.

Important public announcement

Signal 7 seconds – break 14 seconds

Danger over

Unbroken signal 30 seconds

Warning systems

Important public announcement

The warning and information system IPA (important public announcement) is used in emergency situations – for example in the event of emissions of hazardous substances, fires where there is a risk of explosion, forest fires and other natural disasters.

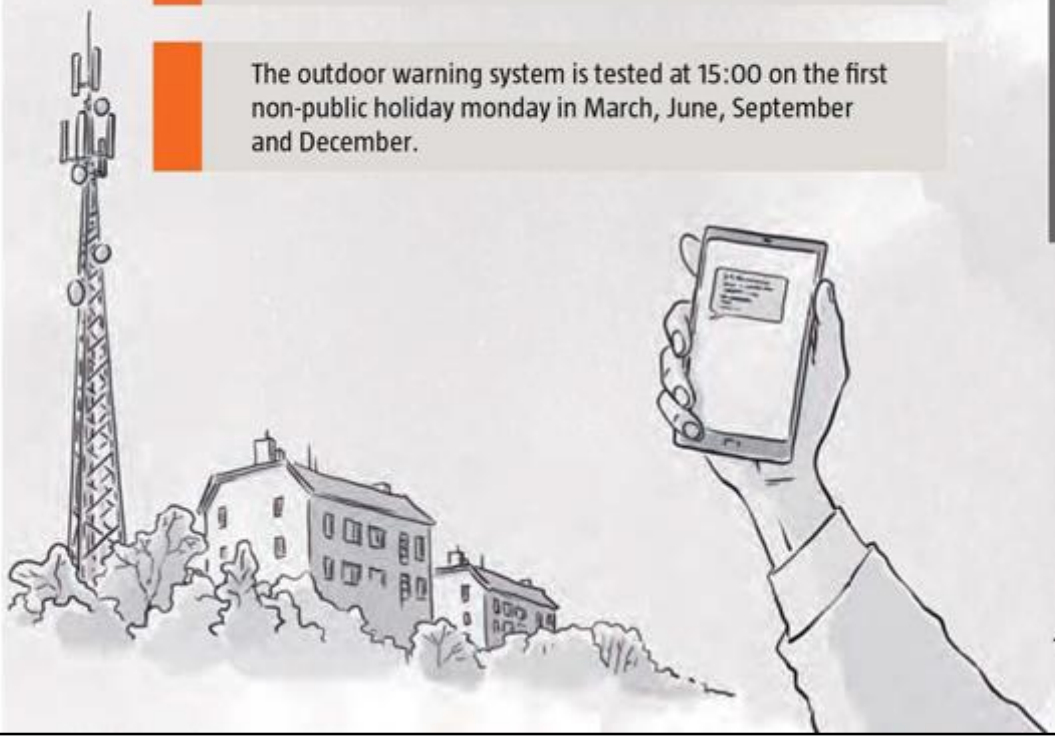
Important public anouncements are broadcast primarily on Sveriges Radio's radio stations, Sveriges Television's TV channels and SVT's teletext system. IPAs can also be sent as text messages to mobile phones within a specific area.

Outdoor warning

On rare occasions, the outdoor warning system is used ("Hesa Fredrik"). Facilities for the outdoor warning system are located in the majority of large built-up areas and around Sweden's nuclear power stations.

If you hear the signal: go indoors, close windows, doors and ventilation and listen to Sveriges Radio's radio station P4, which is tasked with providing public information.

The outdoor warning system is tested at 15:00 on the first non-public holiday monday in March, June, September and December.



Emergency alarm
Signal 30 seconds – break 15 seconds

Air raid warning
Signal with short bursts for one minute

Danger over
Unbroken signal 30 seconds

Emergency alarm and air raid warning

The emergency alarm is a way for the Government to announce that there is the imminent threat of war, or that the country is at war.

If you hear the signal, you have to go indoors immediately and listen to Sveriges Radio's radio station P4. Get ready to leave home with that which is most important, warm clothes, something to eat and drink and identification documents. If you have been given a wartime posting, you are to proceed immediately to the place you have been instructed to go.

The air raid warning means that you are to find shelter immediately, for example an air raid shelter or the cellar of the building in which you are located.

New ways to warn the population may be applicable.

Keep yourself up to date by visiting **dinsäkerhet.se**

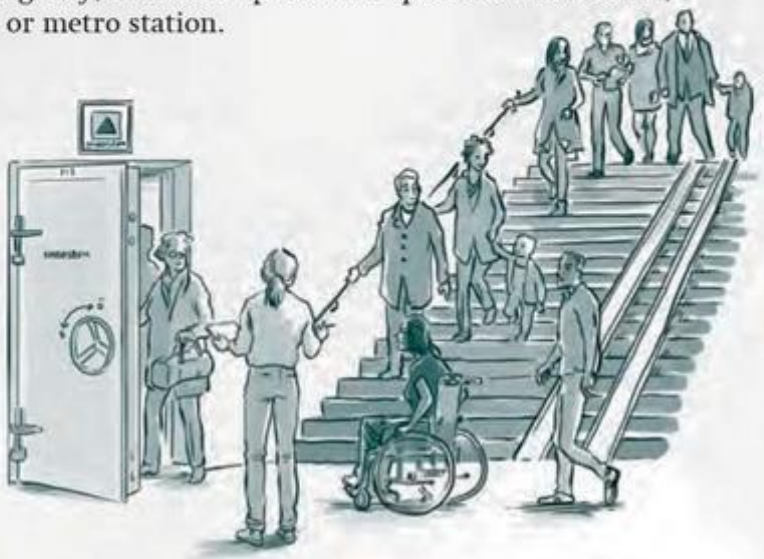
Warning systems

16

Shelters and other protective spaces

Shelters can provide protection to the population in the event of war. All shelters and buildings that contain shelters are marked with a sign. You do not belong to any specific shelter, you use whichever is nearest.

Find out the location of the shelters that are nearest to where you live and where you are during the daytime. In the event of an air raid alarm, go immediately to a shelter or, in an emergency, to another protective space such as a celler, tunnel or metro station.



Educate yourself!

Learn to provide first aid. Your knowledge can save lives. If you are the first on the scene after an accident or other serious incident, call SOS Alarm on the emergency number 112. Even if your pay-as-you-go SIM card has no credit, or your mobile has no SIM card, you can still call 112. SOS Alarm can provide advice about what to do at the site of the accident.

Get involved!

Many non-profit organisations and faith communities make important contributions to our collective security and preparedness. The voluntary defence organisations have specific duties as part of Sweden's total defence and offer both courses and training programmes. In the event of emergencies and heightened states of alert, their tasks include distributing important information to Sweden's population. You are needed and your contribution makes a difference!

18

IMPORTANT TELEPHONE NUMBERS AND WEBSITES

112

In an emergency situation that requires the immediate assistance of an ambulance, the fire and rescue service or the police.

113 13

To provide or obtain information about serious accidents or emergency situations.

114 14

All police matters that are not about crimes or incidents that are ongoing.

1177

Healthcare advice.

Dinsäkerhet.se

More detailed information about the contents of this brochure.

Krisinformation.se

Emergency information from Sweden's public authorities collected in one place.

Nota sull'IRAD[79]

L'Istituto di Ricerca e Analisi della Difesa (IRAD) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito come Centro Militare di Studi Strategici (Ce.Mi.S.S.) nel 1987 e riconfigurato come IRAD nel 2021 a seguito dell'entrata in vigore della Legge 77/2020 - art. 238 bis, l'IRAD svolge la propria opera avvalendosi di esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

[79] https://www.difesa.it/smd/casd/im/irad/


9 791255 150756