WORKING PAPER
APRILE 2022

L'INFORMATION WARFARE A SOSTEGNO DEGLI OBIETTIVI GEOPOLITICI DELLA RUSSIA

DOMENICO FRASCÀ

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

L'INFORMATION WARFARE A SOSTEGNO DEGLI OBIETTIVI GEOPOLITICI DELLA RUSSIA

Un'analisi di dottrina e teoria della guerra condotta dalla Russia con mezzi non lineari

Domenico Frascà

UNIVERSITÀ DEGLI STUDI FIRENZE

Working Paper

Aprile 2022

RIGUARDO L'AUTORE

Domenico Frascà svolge la libera professione fornendo consulenza alle imprese, istituzioni politiche ed enti del terzo settore, principalmente in: Analisi Geopolitica e Politico-Istituzionale, progetti di ricerca, monitoraggio di politiche e sviluppo di dossier. Ha conseguito un Master di II livello in Leadership ed Analisi Strategica presso l'IStituto di Scienze Militari Aeronautiche (ISMA) e Università degli Studi di Firenze (UNIFI). È laureato magistrale in Relazioni Internazionali e Studi Europei e laureato triennale in Scienze Politiche, presso la Scuola di Scienze Politiche Cesare Alfieri di Firenze (UNIFI). Ha frequentato il Corso di Perfezionamento in Intelligence e Sicurezza Nazionale dell'UNIFI in collaborazione con il Dipartimento delle Informazioni per la sicurezza (DIS). Ha seguito un corso di formazione su processi e tecniche di negoziazione delle Nazioni Unite presso Consules (Firenze, Roma e New York). Ha frequentato il corso intensivo Summer School 2015 "Il negoziato nelle crisi umanitarie" presso "Istituto per gli Studi di Politica Internazionale" (ISPI, Milano). È membro del Center for Cyber Security and International Relations Studies dell'UNIFI dal 2016, ha collaborato con Rivista Aeronautica, Agenda Digitale e Fondazione Luigi Einaudi. Si interessa principalmente di geopolitica, difesa e sicurezza.

L'INFORMATION WARFARE A SOSTEGNO DEGLI OBIETTIVI GEOPOLITICI DELLA RUSSIA

Indice

Abstract

La guerra dell'informazione è un tipo di minaccia transnazionale, che penetra i confini nazionali e incide sulla stabilità della società e, quindi, dello Stato, mirando ad influenzare la popolazione e sui leader, finanche a manipolare decisioni e azioni. Mosca esprime la sua politica di sicurezza nazionale in reazione alla percezione che la Federazione sia in un costante stato d'assedio da parte di operazioni di intelligence e di sfide alla sicurezza poste dagli avversari guidati dagli Stati Uniti al fine di sovvertire, influenzare e corrompere i valori e la cultura russa. Una pietra miliare della guerra non lineare Russa è emersa nel 2008, quando si sono riscontrate azioni di *InfoWar* russe in concomitanza con le operazioni militari russe in Georgia. La Russia ha adattato la sua strategia di confronto delle informazioni sei anni dopo (nel 2014) contro l'Ucraina, reclamando senza spargimento di sangue la Crimea e tenendo a bada i paesi da potenziali interventi. Sulla base dei suoi successi in Crimea, la Russia sta affinando l'*InfoWar* e sfruttando lo spazio informatico per rafforzare le sue capacità di propaganda, inganno e disinformazione a sostegno dei suoi obiettivi geopolitici.

Nota del Redattore

Questo è un elaborato ridotto, modificato e aggiornato della tesi magistrale, disponibile presso la biblioteca del Polo delle Scienze Sociali di Novoli, Firenze. Per un maggior approfondimento *Cfr*.: D. Frascà, *L'information Warfare a sostegno degli obiettivi geopolitici della Russia. Un'analisi di dottrina e teoria della guerra condotta dalla Russia con mezzi non lineari. Casi studio: Georgia, Ucraina e Crimea*, relatore Prof. Luigi Martino, Correlatori Prof.essa Francesca Ditifeci e Prof. Massimo Balducci, Università degli Studi di Firenze, Dipartimento di Scienze Politiche e Sociali, Corso di Laurea Magistrale in Relazioni Internazionali e Studi Europei, **luglio 2020**.

Sigle e Abbreviazioni

ASG	Accademia dello Staff Generale
ASM	Accademia di Scienze Militari
AVN	Akademiya Voyennykh Nauk - Accademia di Scienze Militari
C2	Command and Control
C2W	Command and Control Warfare
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CNO	Computer Network Operations
CSI	Comunità degli Stati Indipendenti
CST	Collective Security Treaty
DDoS	Distributed Denial of Service
DIME	Diplomatic Information Military and Economic
DoD	Department of Defence
EW	Electronic Warfare
FSB	Federalnaia Sluzhba Bezopasnosti – Servizio di Sicurezza Federale
GGE	Group or Governamental Experts
GGP	Grande Guerra Patriottica
GRU	Glavnoe Razvedyvatel'noe Upravlenie - Direttorato Principale per l'Informazione
ICT	Information and Communication Technology
IIA	Attività di Informazione e Influenza
IO	Influence/Information Operations

IO	Information Operations
IPW	Initial Period of War
IT	Information Technology
IW	Information Warfare
MILDEC	Military Deception
MTR	Military Technical Revolution
Nato	North Atlantic Treaty Organization
NCW	Network-Centric War
NGW	New Generation of War
NTW	New Type of War
OCS	Organizzazione per la Cooperazione di Shanghai
OSCE	Organizzazione per la Sicurezza e la Cooperazione Europea
Psy-Ops	Psycological Operations
RC	Reflexive Control
RMA	Revolution in Military Affairs
SEAE	Servizio Europeo per l'Azione Esterna
SIGINT	Signal Intelligence
SSA	Security Sector of Assistance
STRATCOM	Strategic Communications
SVR	Sluzhba Vneshnei razedki Rossiiskoi Federatsii – Servizio di Intelligence Estera
UAV	Unmanned Aerial Vehicle
UE	Unione Europea
UNHCR	United Nations High Commissioner for Refugees
URSS	Unione delle Repubbliche Socialiste Sovietiche
USA	United States of America
UW	Unconventional Warfare

WCIT	WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS

INTRODUZIONE

Per la Russia la guerra dell'informazione rappresenta una forma di potere politico e strumento geopolitico che consente un alto livello di manipolazione e influenza con una bassa probabilità di confronto militare[1]. Lo scopo è quello di promuovere un'agenda politica specifica dove la competizione internazionale si basa su differenze ideologiche e culturali[2]. Il politologo Dimitri Trenin insiste sul fatto che la guerra delle informazioni è diventata "accanto alla geoeconomia, uno dei principali campi di battaglia nel nuovo scontro tra Russia e Occidente"[3], con l'obiettivo ultimo di far crollare la fiducia del pubblico nei confronti dei sistemi politici degli Stati occidentali attraverso una combinazione di: attacchi informatici, disinformazione e propaganda[4]. Esistono modi differenti per raggiungere questo obiettivo, ed essi abbracciano canali diversi di propagazione.

Col fine di proiettare la potenza russa nello spazio terracqueo, in Occidente il concetto di *Information Warfare* è diventato oggetto di un improvviso acuto interesse quando ebbe inizio la crisi in Ucraina nel 2014[5].

---

[1] L.B. MONOV and M.L. KAREV, "Information Warfare Conceptual Framework", *International Journal of Recent Scientific Research*, Vol. 9, Issue, 5(F), maggio 2018, p. 26863, accessibile al seguente link: http://www.recentscientific.com/sites/default/files/10867-A-2018.pdf [ultima consultazione online: 16.04.22].
[2] *Ibidem*.
[3] D. TRENIN, *Information is a potent weapon in the new cold*, 17 settembre 2016, online: https://www.theguardian.com/commentisfree/2016/sep/17/hacking-politics-us-russia [ultimo accesso: 16.04.22].
[4] L.B. MONOV and M.L. KAREV, "Information Warfare Conceptual Framework", *op.cit*., p. 26864.
[5] K. GILES, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 3-5.

La guerra moderna, nella visione russa, deve colpire le menti dei belligeranti, a volte basta una notizia abilmente creata e supportata in modo credibile al fine di generare una distorsione semantica che a sua volta provoca un dissesto nella vita quotidiana di uno Stato; la vittoria o la sconfitta avviene nella psicologia dell'avversario[6].

Lo sviluppo della proiezione di potenza, dottrine e strategie di un paese, deve essere compreso e collegato a un contesto più ampio, basandosi su una serie di elementi e presupposti come esperienze storiche, minacce militari, tensioni geografiche, situazione economica, *background* ideologico e *standard* tecnologici, nonché le basi costituzionali del Paese. La Russia non fa eccezione. Lo Stato debole, ma potenza forte[7], del presidente Vladimir Putin ha influenzato le mentalità; con la fine della Guerra Fredda e la transizione attraverso gli anni di instabilità, il popolo russo si è sempre più orientato verso una società basata su una *leadership* forte[8]. L'esperienza della Russia moderna differisce da quella dei Paesi occidentali e ciò influisce anche sul suo pensiero militare in generale e, più specificamente, sul punto di vista della guerra dell'informazione[9].

Per quanto riguarda le minacce alla sua sovranità nazionale, la visione Russa è descritta in dottrine e documenti strategici come: la "dottrina militare"[10] e la "dottrina sulla sicurezza delle informazioni della

---

[6] U. FRANKE, *War by non-military means. Understanding Russian information warfare*, FOI, Swedish Reserch and Defence Institute, Stockholm, Sweden 2015, pp. 9-10.
[7] R. JACKSON, G. SØRENSEN, *Relazioni Internazionali*, Edizione italiana a cura di L. Bozzo, terza edizione, Egea, 2014, p.26.
[8] S. HANSON, "Putin and the Dilemmas of Russia. Anti-Revolutionary Revolution", Wilson Center, 2001. Accessibile online: https://www.wilsoncenter.org/publication/the-anti-revolutionary-revolution-russia [ultima consultazione online: 16.04.22]
[9] R. HEICKERO, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency (FOI). Stockholm, Sweden, March 2010, pp. 12-14.
[10] Dottrina militare approvata con decreto del Presidente della Federazione Russa n.706, 21 aprile 2000. Accessibile online: http://base.garant.ru/181993/#ixzz4qoOtOqe6 [ultima consultazione online: 16.04.22].

Federazione Russa"[11], entrambe del 2000[12] e approvate dal Consiglio di sicurezza della Federazione. Il documento che porta il nome di dottrina sulla sicurezza delle informazioni, individua e ipotizza minacce informative alla Russia e come lo Stato dovrebbe comportarsi al fine di mitigare le stesse e garantire la protezione d'informazioni strategicamente importanti[13]. Atro documento rilevante, approvato con decreto presidenziale il 2 luglio 2021, è indubbiamente la nuova "Strategia di Sicurezza Nazionale della Federazione Russa"[14].

Questo elaborato tenta di affrontare il tema *dell'Information Warfare* secondo la visione russa, analizzandone la dottrina attraverso gli elaborati, le dichiarazioni di ufficiali militari circa la guerra dell'informazione ed alcuni dei più noti articoli scientifici elaborati da studiosi della materia e del pensiero strategico della Federazione russa.

L'espressione "guerra dell'informazione", usata nel titolo è stata scelta come una semplice traduzione del concetto russo di *informatsionnaia voina*[15].

Al fine di organizzare lo studio dell'oggetto di questo elaborato, si è deciso di tentare di rispondere a tre domande: l'IW è un novo approccio alla guerra? L'IW viene condotta solo in tempo di guerra o anche in tempi di relativa pace? Perché la Federazione russa persegue i suoi obiettivi geopolitici attraverso l'IW?

---

[11] Il documento è tradotto e discusso, in D. CARMAN, "Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass media and the politics of identity". *Pacific Rim Law & Policy Journal Association*, 2002.

[12] Quella militare è stata successivamente rinnovata nel 2010 prima e, nel 2014 dopo, mentre quella sulla sicurezza delle informazioni nel 2016.

[13] R. HEICKERO, *Emerging Cyber Threats*, *op.cit.* p. 13.

[14] Strategia di Sicurezza Nazionale, approvata con decreto del Presidente della Federazione Russa n. 400, 2 luglio 2021. Accessibile online: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1 [ultima consultazione online: 16.04.22].

[15] Termini traslitterati da: "информационная война"; trad. in ligua iglese: "Information Warfare"; in italiano: "guerra dell'informazione".

Nel primo capitolo si tenta di inquadrare l'IW in un contesto di warfare e si cerca di capire da cosa nasce il bisogno di portare avanti questo tipo di attività esaminando anche i tipi di minacce che la Russia percepisce.

Nel secondo capitolo si cerca di analizzare i documenti ufficiali che la comunità scientifica ritiene strategicamente importanti. Tra i documenti ufficiali, *open source,* prodotti dal governo e da istituzioni militari che interessano l'oggetto di studio, troviamo: la "strategia di sicurezza nazionale"; la "dottrina militare"; le "opinioni concettuali riguardanti le attività delle Forze Armate della Federazione Russa nello spazio delle informazioni"; la "dottrina sulla sicurezza delle informazioni della Federazione Russa"; altri documenti in merito all'information security adottati nel contesto delle organizzazioni internazionali; infine, il "concetto per una *cybersecurity* russa".

Nel terzo capitolo, poiché le sole fonti primarie analizzate nel secondo capitolo lasciano trapelare solo alcune indicazioni, si è deciso di integrare quanto appreso dai documenti con un'analisi del concetto di IW russa seguendo gli studi della comunità accademica e militare – quasi esclusivamente facendo riferimento ad elaborati o dichiarazioni di ufficiali (anche ormai in congedo) militari della Federazione russa, attenendosi anche agli studi del tenente colonnello Timothy L. Thomas (emerito specialista statunitense nel campo del dominio delle operazioni informative russe) – che ci permette di comprendere meglio il significato del pensiero russo in merito all'oggetto di studio. Sempre nel terzo capito si tenta di analizzare anche due scuole di pensiero geopolitiche di due studiosi anch'essi russi (ritenuti estremamente importanti per il Cremlino) per cercare di comprendere meglio le motivazioni dell'approccio della Federazione nell'intraprendere l'IW.

Nel quarto capitolo, si tenta attraverso l'analisi di tre casi studio – Georgia, Crimea ed Ucraina – di fornire la base per un capitolo di sintesi che identifica gli attributi di spicco dell'IW e affina la comprensione di come agisce la Russia in questo spettro di conflitti e competizione. Infine, nel capitolo conclusivo si tenterà di rispondere, in base a quanto esaminato nel corso della ricerca, ai suddetti interrogativi che hanno mosso la curiosità della ricerca.

Si è selezionato questi tre casi perché i criteri di selezione includevano affinità tra gli obiettivi geopolitici russi e gli aspetti non lineari della conduzione dell'aggressione russa, ed inoltre, entrambi i Paesi non erano (e continuano a non esserlo) membri della NATO e nei momenti precedenti alle aggressioni russe hanno manifestato una palese volontà di inserirsi nella sfera di influenza occidentale. Quindi si è deciso di non inserire il caso estone del 2007 tra i casi studio, poiché non rientrava in questi criteri di selezione. Questo giudizio non vuole in alcun modo sminuire l'importanza degli attacchi perpetrati dalla Russia in Estonia nel 2007, ma questi, secondo varie riflessioni, meritano uno studio differente, più tecnico ed approfondito con altri mezzi di ricerca.

Inoltre, si precisa che, anche se l'elaborato è aggiornato (aprile 2022) non è presente una valutazione degli eventi attuali in merito all'aggressione russa in Ucraina, poiché il conflitto ancora in corso non permette uno studio scientifico e approfondito della situazione.

Per la traduzione dei documenti ufficiali in lingua russa, il redattore si è avvalso di una persona madrelingua, mentre per i documenti e gli elaborati in lingua inglese le traduzioni sono in capo al redattore.

INFORMATION WARFARE. VECCHIE ABITUDINI, NUOVE CAPACITÀ

Un quadro sull'*information warfare*

La guerra dell'informazione è un tipo di minaccia transnazionale, che penetra i confini nazionali e incide sulla stabilità della società e, quindi, dello Stato, mirando ad influenzare la popolazione e sui leader, finanche a manipolare decisioni e azioni[16].

L'ultima pubblicazione sul Dizionario dei militari e dei termini associati del Dipartimento della Difesa degli Stati Uniti definisce le operazioni di informazione come: "occupazione integrata, durante operazioni militari, di capacità relative alle informazioni di concerto con altre linee operative per influenzare, interrompere, corrompere o usurpare il processo decisionale degli avversari e dei potenziali avversari proteggendo nel contempo i propri"[17]. Inoltre, Il dizionario identifica come attività separate la guerra elettronica, l'inganno militare e le operazioni di supporto alle informazioni militari. Un'altra fonte, il Glossario dei termini e delle definizioni della NATO, parla delle attività d'informazione come: azioni progettate per influenzare le informazioni o i sistemi d'informazione[18]. Mentre, l'UE non accetta la guerra dell'informazione come un'unica entità. Essa definisce le campagne

[16] L.B. MONOV and M.L. KAREV, "Information Warfare Conceptual Framework", *International Journal of Recent Scientific Research*, Vol. 9, Issue, 5(F), maggio 2018, pp. 26859-26866 accessibile al seguente link: http://www.recentscientific.com/sites/default/files/10867-A-2018.pdf [ultima consultazione online: 16.04.22].

[17] DOD Dictionary of Military and Associated Terms, febbraio 2018, accessibile online: http://www.jcs.mil/Doctrine/DOD-Terminology/ [ultima consultazione online: 16.04.22].

[18] NATO Glossary of Terms and Definitions, AAP - 06 Edition, 2017.

d'informazione come: "una serie di attività che supportano gli obiettivi della strategia d'informazione sulle crisi"[19], quindi poco chiara e molto vaga.

La visione attuale, nel mondo accademico, della dell'*information warfare* (IW) è ampiamente estesa tra diverse categorie e aree di competenza[20]. Come strategia generale, la guerra dell'informazione include quattro tipi di operazioni chiaramente distinte, che dividiamo in due categorie: in primo luogo, si considerano le operazioni dei media tradizionali e la guerra elettronica che, ad esempio, comprendono atti che hanno una fonte chiara e usano approcci tradizionali per diffondere messaggi e ingaggiare. In secondo luogo, si considerano gli attacchi informatici e le operazioni sui *social media*; essi comprendono azioni che si basano su tecnologie moderne per coprire la fonte, rubare informazioni, danneggiare reti e risorse informatiche e mettere le comunicazioni giuste davanti alla persona giusta nel momento esatto[21]. Il dottor Cathy Downes descrive una situazione simile con due termini: "potere narrativo" e "potere dirompente", entrambi collegati come uno strumento di influenza strategica[22].

Un importante studioso, Sir Lawrence Freedman, insiste sul fatto che la capacità di Internet di condividere idee e narrazioni porta il conflitto al livello sociale della società e allo stato attuale delle cose, pone molteplici opportunità per gli Stati e gli individui di influenzare le percezioni della popolazione. La guerra dell'informazione potrebbe creare false impressioni al fine di costruire o rompere alleanze e simpatie. In altre parole, solleva tensione e attrito su questioni attuali

[19] European External Action Service (EEAS), European Union Military Committee (EUMC), EUMC *Glossary of Acronyms and Definitions Revision 2015*, febbraio 2016.
[20] L.B. MONOV and M.L. KAREV, "Information Warfare Conceptual Framework", op. cit.
[21] *Ibidem*.
[22] C. DOWNES, "Strategic Blind-spots on cyber threats", *The Cyber Defense Review*, Vectos and Campaigns, 2018, pp. 1-19.

tra diversi gruppi di persone e, quindi, le opinioni, determinando un certo grado di discordia nella società[23].

David Stupples considera l'*Information War* come una combinazione di tre tipi distintivi di guerra: in primo luogo, la guerra elettronica deve distruggere lo spazio elettromagnetico; poi, gli attacchi informatici devono influenzare la funzionalità dell'infrastruttura nazionale; infine, le *psy-ops* (*Psycological Operations*) per degradare i valori e minare le norme morali. La combinazione e l'utilizzo congiunto di questi, potrebbe causare instabilità e caos[24].

L'InfoWar russa

Helle Dale della *Heritage Foundation*[25] sostiene che, attraverso l'emittente televisiva "RT" di proprietà dello Stato russo, Mosca sta conducendo una guerra d'informazione, al fine di diffondere propaganda e disinformazione minando la credibilità degli Stati Uniti e dell'Occidente, mettendo in buona luce l'operato russo[26]. In effetti, il canale rappresenta un tipo di rete globale con l'obiettivo di manifestare la forza di Mosca e presentare prospettive alternative attraverso la trasmissione in Asia centrale, Europa orientale e centrale, più in generale in Occidente, compresi gli Stati Uniti. Altresì, se occorre adoperarsi con l'intento di manipolare una determinata situazione interna, lo scopo più importante, di questo tipo di guerra, è che l'obiettivo agisca contro i propri interessi; per quanto possa sembrare contorto il ragionamento, l'attaccante può usare i media di proprietà

[23] L. FREEDMAN, "The Future of War. A Hstory", *PublicAffairs*, New York, 2017.
[24] D. STUPPLES, *The next war will be an information war, and we're not ready for it*, novembre 2015, accessibile online: http://theconversation.com/the- next-war-will-be-an-information-war-and-were-not- ready-for-it-51218 [ultima consultazione online: 16.04.22].
[25] Per maggiori informazioni sulla Fondazione si rinvia al sito web: https://www.heritage.org/about-heritage/mission [ultima consultazione online: 16.04.22].
[26] L.B. MONOV and M.L. KAREV, "Information Warfare Conceptual Framework", op. cit. p. 26862.

statale per far avanzare la sua agenda politica e diffondere apertamente confusione e distrazione, così da creare un ambiente artificioso a lui apparentemente sfavorevole, ma fattualmente favorevole[27]. L'*information warfare* è una guerra narrativa che utilizza anche i *social media* con l'intenzione di manipolare i fatti, disperdere disinformazione e amplificare il rumore della stessa sulle più disparate questioni, con la potenziale conseguenza di erodere la fiducia e la credibilità delle istituzioni e di creare discordia nella società[28]. In questo senso, la guerra dell'informazione segue tre strade: in primo luogo, l'attaccante raccoglie informazioni su obiettivi e gruppi specifici al fine di comprenderne le differenze, le preferenze, i desideri e le debolezze, considera anche la diversità delle persone come posizione geografica, pregiudizi culturali, modelli comportamentali, deviazioni politiche e demografiche al fine di ampliare il divario tra le comunità e aumentare il livello di incertezza; in secondo luogo, crea e diffonde la narrazione al pubblico e agli individui *target* attraverso i canali multimediali disponibili, sfruttando i timori più grandi, instabilità interne alla società, fino a causare danni intenzionali alla fiducia nelle istituzioni, alle idee ed ai valori[29]; infine, aumenta la portata dei suoi sforzi con lo scopo di reclutare sostenitori e sollecitare risorse[30]. Attraverso una rete di sostenitori, personalità false, *botnet* e *troll*, l'aggressore intensifica il livello delle sue attività per creare un

[27] *Ibidem*.
[28] U. FRANKE, *War by non-military means*, op.cit., p. 10-20.
[29] Secondo il General Counsel di Facebook, durante le elezioni presidenziali del 2016 per circa due anni la rete ha fornito la piattaforma per la distribuzione di 3.000 annunci Facebook e Instagram che promuovevano circa 120 pagine Facebook. Inoltre, 29 milioni di persone hanno pubblicato contenuti provenienti dalle operazioni originate in Russia 80.000 post che hanno raggiunto circa 126 milioni di persone. *Cfr*., C. STRETCH, Hearing Before the United States Senate Commiteeon the Judiciary Subcommittee on Crime and Terrorism, ottobre 2016, accessibile online: https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf [ultima consultazione: 16.04.22].
[30] L.B. MONOV and M.L. KAREV, "Information Warfare Conceptual Framework", *op. cit.*

ambiente artificiale di opinioni diverse e per corrompere la credibilità delle informazioni[31].

Nella visione russa, l'informazione può essere archiviata ovunque e trasmessa con qualsiasi mezzo: stampa, televisione o nella testa di qualcuno, in quanto soggetto agli stessi concetti di *targeting* di quelli sul computer o sullo smartphone di un avversario. Allo stesso modo, la trasmissione o il trasferimento di queste informazioni possono avvenire attraverso l'introduzione di dati corrotti in un computer, tramite una rete o da una chiavetta USB, che non è concettualmente diverso dalla collocazione di una disinformazione attraverso media tradizionali o una performance eseguita da un *influencer* su canali di noti *social media*[32].

In linea con la più ampia comprensione russa dello *information space*, il termine *information warfare* ha un'applicazione sorprendentemente ampia; le *information weapons* possono essere utilizzate in molti più domini che non nel *cyber*, includendo in modo cruciale il dominio cognitivo umano[33]. Ma anche nelle *Computer Network Operations* (CNO), l'arma dell'informazione non deve necessariamente avere un effetto distruttivo nel mondo reale nello stile di *Stuxnet*[34]. In linea con gli obiettivi di *information warfare*, in generale, la distruzione fisica delle strutture dell'avversario non è necessaria per influenzare il trasferimento e l'archiviazione dei dati[35].

Riassumendo, gli obiettivi decisivi sono: produrre discordia nella società, interrompere il processo decisionale e degradare la libertà di azione senza o con poca distruzione fisica. Dal punto di vista della

---

[31] *Ibidem*.
[32] K. GILES, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 10.
[33] K. GILES e W. HAGESTAD II, *Divided by a Common Language*, *op. cit.* p. introduzione.
[34] Un virus informatico creato con lo scopo di sabotare la centrale nucleare iraniana di Natanz.
[35] K. GILES, *Handbook of Russian Information Warfare*, *op. cit.*, pp. 13.

sicurezza nazionale, questo può essere tradotto come il pericolo della distruzione di una nazione, delle sue idee e dei suoi valori.

La Cyber warfare come sottocomponente dell'infoWar

Nel 2012 alla Conferenza di Budapest sul ciberspazio e alla Conferenza mondiale sulle telecomunicazioni internazionali (WCIT) a Dubai, un consenso euroatlantico, su uno spazio internazionale per il libero scambio di informazioni, opinioni, idee, concetti e teorie, si è scontrato con un modello alternativo sostenuto da Russia, Cina e altri Stati dell'Est-Europa, sostenendo un approccio completamente diverso della gestione dei contenuti e del controllo nazionale dello spazio informativo ed informatico. A Budapest, le nazioni europee hanno evidenziato gli aspetti dei diritti umani in merito alla sicurezza informatica, basandosi sul loro intendimento della libertà di Internet come diritto fondamentale, portando persino un rappresentante cinese a chiedersi se fosse in una conferenza sulla *cybersecurity* o sui diritti umani; mentre, a Dubai, una nuova serie di regolamenti internazionali sulle telecomunicazioni, non ha ottenuto il sostegno di molte delle 151 nazioni delegate, dopo l'energica opposizione degli stati euro-atlantici guidati da una delegazione statunitense[36].

L'insufficienza di raggiungere un accordo sui principi fondamentali che riguardano il *cyberspace* indicava il fatto che, nonostante una maggiore volontà nel corso del 2012 da parte di USA, Regno Unito e altre nazioni di impegnarsi con Russia e Cina in merito alle questioni di sicurezza informatica – o *cybersecurity* se si preferisce il termine anglosassone –, questo impegno rimane estremamente difficile in assenza di concetti concordati di ciò che costituisce la sicurezza

[36] Cfr., E. BURCHIA, "La conferenza mondiale su Internet è stata un fiasco: a vincere è stato Internet", *Corriere Della Sera*, dicembre, 2012.

informatica. Una disconnessione che fino ad adesso ha ostacolato il progresso e il raggiungimento di una comprensione reciproca, deriva dal fatto che la dottrina russa e cinese evidenziano un insieme differente di sfide alla sicurezza rispetto a quelle che normalmente riguardano Stati Uniti, Regno Unito e più in generale i paesi occidentali[37]. Quindi, ancor prima di affrontare le divergenze nell'attitudine e nella percezione delle minacce, c'è il problema più basilare e significativo dell'assenza di una terminologia comune tra i principali attori del *cyberspace*. Le definizioni di termini come conflitto cibernetico, guerra cibernetica, attacco informatico, arma cibernetica, guerra dell'informazione o *Information Warfare* etc. Utilizzati da Regno Unito, Stati Uniti, Russia e Cina non coincidono. Inoltre, traduzioni dirette di termini specifici russi o cinesi che assomigliano ai termini della lingua inglese, e viceversa, possono complicare ulteriormente le cose dando un'impressione fuorviante di comprensione reciproca, mentre in realtà si riferiscono a concetti completamente diversi[38]. *Cyber warfare* nella scrittura russa descrive concetti e attività estere, di conseguenza, le ricerche condotte circa il dominio *cyber*, nelle fonti russe, fanno principalmente riferimento al pensiero e Dottrine occidentali; ne consegue che qualsiasi ricerca sulle capacità e intenzioni russe che include la parola *cyber* rischia di fornire risultati fondamentalmente fuorvianti[39]. Per estensione, la ricerca sul *Cyber Command*, sulla dottrina *cyber* e sulle capacità informatiche della Russia è spesso uno sforzo

[37] K. GILES e W. HAGESTAD II, *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English*, 5th International Conference on Cyber Conflict, K. Podins, J. Stinissen, M. Maybaum (eds), NATO Publications, Tallinn 2013, p. Introduzione.
[38] *Ibidem*.
[39] K. GILES, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 8-13.

indiretto, poiché queste entità e concetti, anche se esistono, non sono nominati o descritti in questi termini[40].

Invece del *cyberspace*, la Russia fa riferimento all'*information space*, e include in questo spazio sia l'elaborazione informatica che l'elaborazione delle informazioni umane, ovvero il dominio cognitivo[41]. Solo all'interno dello spazio dell'informazione, il pensiero russo giunge a separare le attività di *CNO* dalle altre[42].

Quindi possiamo affermare che generalmente i russi non usano i termini *cyber* (kiber) o *cyberwarfare* (kibervoyna), tranne quando si riferiscono a scritti occidentali o altri scritti stranieri sull'argomento.

Il termine, usato dai teorici militari russi, è un concetto olistico che include operazioni di rete di computer, guerra elettronica, operazioni psicologiche e operazioni d'informazione[43]. In altre parole, il *cyber* è considerato un meccanismo per consentire allo Stato, o ad attori non statali, di dominare il paesaggio informatico[44]. Generalmente deve essere impiegato come parte di un'intera operazione, insieme ad altre più tradizionali armi di guerra dell'informazione, comprese le operazioni di disinformazione, *PsyOps*, guerra elettronica, e sovversione politica[45].

Secondo la Dottrina Militare della Federazione Russa del 2010, una delle caratteristiche dei moderni conflitti militari è "la precedente attuazione di misure di guerra dell'informazione al fine di raggiungere

---

[40] J. R. CLAPPER, US, "Worldwide Threat Assessment of the US Intelligence Community", dichiarazione al Senato del comitato dei servizi armati, 26 February 2015. https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf [ultimo accesso online: 16.04.22]

[41] K. GILES, *Handbook of Russian Information Warfare*, op.cit., pp. 8-12.

[42] T. L. THOMAS. "Russian Information Warfare Theory: The Consequences of August 2008," in S. BLANK e R. WEITZ (eds.). *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle, US Army War College Strategic Studies Institute, 2010.

[43] M. CONNELL and S. VOGLER, *Russia's Approach to Cyber Warfare*, CNA Analysis & Solution, 2017, p. 3.

[44] *Ibidem*.

[45] T. THOMAS (Lt. Col., U.S. Army, Retired), *Nation-State Cyber Strategies: Examples from China and Russia*, accessibile online: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850 [Ultimo accesso online: 16.04.22].

obiettivi politici senza l'utilizzo della forza militare e nell'interesse di dare una risposta favorevole alla comunità mondiale sull'utilizzo della forza militare"[46].

Il generale Valery Gerasimov, capo dello Stato Maggiore della Federazione Russa, nel suo popolare articolo "Il valore della scienza nella previsione" spiega che nel XXI secolo le linee di divisione tra gli stati di guerra e pace, iniziano a sfumare. Le guerre non sono più dichiarate e, una volta iniziate, procedono secondo un modello non lineare; l'esperienza dei conflitti militari, comprendendo quelli legati alle cosiddette "rivoluzioni colorate"[47], confermando che uno Stato può trasformarsi, in pochi mesi o addirittura giorni, in un'arena di feroce conflitto armato, diventare vittima di un intervento straniero e sprofondare in una rete di caos, catastrofi umanitarie e guerra civile[48]. Il *cyber* offensivo è quindi relegato a un ruolo di sostegno, anche se significativo, nell'aiutare lo Stato a raggiungere il dominio dell'informazione in tutte le fasi del conflitto; in linea con le tradizionali nozioni leniniste di combattere le continue minacce provenienti dall'esterno e dall'interno, il confronto nell'*Information Space* è più o meno costante e senza fine, non conosce confini, fisici o temporali[49]. Ciò contrasta nettamente con le concezioni occidentali e in particolare statunitensi del *cyber*, che è visto come un dominio separato, distinto dalla guerra dell'informazione e dai suoi aspetti psicologici associati[50].

Secondo Stephen Blank, data l'ampia concezione di IW nella teoria russa, l'attenzione delle operazioni cibernetiche tende a essere di

---

[46] Dottrina militare della Federazione Russa, approvata con decreto del presidente della Federazione Russa, 5 febbraio 2010, accessibile online: https://www.justsecurity.org/7777/russias-2010-military-doctrine/ [ultima consultazione online: 16.04.22].
[47] Questo termine è stato usato per descrivere i movimenti sociali in Georgia (2003), Ucraina (2004) e Kirghizistan (2005), che hanno portato a cambiamenti socio-politici in questi paesi.
[48] M. CONNELL and S. VOGLER, *Russia's Approach to Cyber Warfare*, op. cit. p. 4.
[49] T. THOMAS (Lt. Col., U.S. Army, Retired), *Nation-State Cyber Strategies*, op. cit. p. 266.
[50] M. CONNELL and S. VOGLER, *Russia's Approach to Cyber Warfare*, *op. cit*. p. 2-6.

natura strategica, piuttosto che operativa o tattica[51] (ciò non preclude il fatto che possa essere usata in modo operativo o tattico). Questa enfasi strategica ha, a sua volta, influenzato il modo in cui la Russia ha organizzato e postulato le sue forze cibernetiche[52].

Martin Libicki, in uno dei suoi studi sull'*information warfare* del 1995, ha segnalato che la guerra delle informazioni sarebbe stato un campo significativo dove le nazioni si sarebbero confrontate e avrebbero convogliato i loro sforzi per perseguire un vantaggio competitivo[53]. Libicki, nel suo elaborato, definisce l'IW come un conflitto che coinvolge la manipolazione, la protezione, la degradazione e la negazione delle informazioni, inoltre sostiene che entrare nella testa del nemico, gli inganni di ogni sorta e le operazioni psicologiche in generale, sono pratiche antiche quanto la storia, altre, in particolare la guerra elettronica, hanno raggiunto la ribalta nella Seconda guerra mondiale[54]. Continua spiegando che la recente automazione del centro di comando, ha creato obiettivi più vulnerabili poiché raggiungibili attraverso *software* malevoli e scrive: "se le società si evolvessero nella dimensione virtuale, aumenterebbero notevolmente gli effetti, l'importanza e la frequenza dell'*hackerwar* [...], della guerra delle informazioni economiche e le operazioni psicologiche sarebbero notevolmente trasformate"[55]. Con rare eccezioni, ad esempio la concorrenza per il controllo dei media, le informazioni non rientrano in un concetto di gioco a somma zero, ovvero: "la padronanza di IW non impedisce a un

[51] S. BLANK, "Cyber War and Information War à la Russe", from *Understanding Cyber Conflict: Fourteen Analogies*, George Perkovich and Ariel E. Levite, Published by George Town University Press, 2017.
[52] M. CONNELL and S. VOGLER, *Russia's Approach to Cyber Warfare*, op. cit. p. 6.
[53] M.C. LIBICKI, *What is Information Warfare?*, Center for Advanced Command Concept and Technology, Institute for National Strategic Studies, National Defence University, Washington DC, Agosto 1995, p. introduzione.
[54] *Ivi*, pp. 96-104.
[55] *Ibidem*.

avversario di fare lo stesso"[56]. La guerra delle informazioni è estremamente difficile da condurre senza una conoscenza precisa e affidabile dell'architettura della parte avversaria, ad esempio: come i media e le informazioni influenzano le decisioni, la struttura burocratica del comando, l'infrastruttura di comunicazione di una nazione e persino i dettagli del *software* dei loro sistemi di informazione[57]. In un suo studio più recente sostiene che l'attenzione degli Stati Uniti, dovrà evolversi ad una più ampia attenzione alla minaccia sulla guerra dell'informazione, rispetto ai singoli attacchi cibernetici. Pertanto, date le circostanze odierne i vari elementi della guerra dell'informazione dovrebbero essere sempre di più considerati come elementi di un insieme più ampio, piuttosto che specialità separate che supportano individualmente operazioni militari cinetiche[58]. Questa affermazione è supportata da tre circostanze emergenti, spiega Libicki: innanzitutto, i vari elementi possono utilizzare molte delle stesse tecniche, a partire dalla sovversione di computer, di sistemi e di reti. In secondo luogo, come risultato parziale della prima circostanza, gli aspetti strategici di questi elementi stanno convergendo e questo rende più probabile che in circostanze in cui un elemento di IW possa essere utilizzato, anche altri elementi possano essere utilizzati in concomitanza. In terzo luogo, come risultato parziale della seconda circostanza, i Paesi, in particolare la Russia, ma anche in misura minore, Corea del Nord, Iran e Cina, stanno iniziando a combinare gli elementi di IW, come parte di un disegno strategico più ampio[59]. Se le tendenze della tecnologia dell'informazione continuano e, cosa ancora più importante, se altri

[56] *Ibidem*.
[57] *Ibidem*.
[58] M.C. LIBICKI, "The Convergence of Information Warfare", *Strategic Studies Quarterly*, spring 2017, p. 49 disponibile online al seguente link: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf [ultimo accesso: 16.04.22].
[59] *Ivi*, p. 50.

paesi iniziano a sfruttare queste tendenze, come regola generale, l'attenzione sulla minaccia cibernetica dovrà evolversi e concentrarsi su una più ampia minaccia dell'IW[60]. Le percezioni della guerra cibernetica dovranno probabilmente essere ripensate, poiché sta diventando molto meno plausibile immaginare una campagna di attacchi informatici non accompagnata da altri elementi della guerra dell'informazione[61].

Il rilancio dell'*information warfare* in Russia

Secondo la studiosa russa, Jolanta Darczewska, l'*information warfare* russa ha una lunga tradizione e, questa, deriva direttamente dalla teoria della *spetspropaganda* (propaganda speciale), insegnata per la prima volta come materia nel 1942 presso l'Istituto militare russo di lingue straniere[62]. Il programma *spetspropaganda* è stato sospeso negli anni '90 per essere poi reintrodotto nel 2000 dopo la riorganizzazione dell'istituto che è ora noto come Dipartimento di informazione militare e lingue straniere dell'Università militare del Ministero della Difesa della Federazione Russa con lo scopo di formare specialisti nel gestire le informazioni provenienti dall'estero e in comunicazione militare, così come in monitoraggio e analisi delle informazioni, sviluppo delle informazioni militari e giornalismo di guerra[63]. L'istituto ha subito una profonda riforma a seguito di un rapido aumento dell'interesse per le questioni di *information security* avviato dal lavoro sulla dottrina di sicurezza delle informazioni della Federazione Russa annunciato nel 2000[64].

---

[60] *Ibidem*.
[61] *Ibidem*.
[62] J. DARCZEWSKA, "The anatomy of Russian information warfare. The Crimean operation, A Case Study", *Centre for Eastern Studies*, volume 42, Warsavia, 2014, pp. 9-14.
[63] *Cfr*., il sito web ufficiale dell'Università militare del Ministero della Difesa della Federazione Russa: https://vumo.mil.ru/ [ultimo accesso 16.04.22].
[64] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p. 9.

La teoria russa della guerra dell'informazione ha tratti di una scienza interdisciplinare applicata, poiché copre una gamma molto ampia di azioni (politiche, economiche, sociali, militari, informative, controspionaggio, diplomatiche, propagandistiche, psicologiche, tecnologie di comunicazione, etc.)[65]. Dagli anni 2000 in poi sono stati creati numerosi centri di ricerca con lo scopo di affrontare questioni ben definite, come ad esmpio: l'*Information security institute*[66], istituito nel 2003 presso l'Università statale di Mosca *Lomonosov*, è specializzato nella sicurezza delle informazioni nell'ambito della cooperazione internazionale della Federazione. La forma organizzativa dell'istituto è adeguata alla natura interdisciplinare del tema trattato così come alla natura interministeriale dei compiti ad essa assegnati[67]. Le risorse umane necessarie per risolvere i problemi regionali sono addestrate dal "Centro di informazione e analisi per lo studio dei processi sociopolitici nell'area post-sovietica", che è stato creato come parte della cattedra di "Storia per l'estero" presso l'Università di Lomonosov. Oltre a studiare la storia politica ed economica contemporanea dei paesi emersi in seguito al crollo dell'URSS, le principali aree di ricerca del centro includono: lo studio della diaspora sulla lingua russa, i suoi partiti politici e movimenti sociali e il modo in cui co-operare con partiti e movimenti sociali russi, nonché con l'analisi storica delle questioni etniche post-sovietiche[68]. Inoltre, sempre per restare negli ambienti che svolgono attività di monitoraggio informativo e persuasione, vale la pena notare che Maxim Meyer, specialista in strategie mediatiche e dal 2007 ricopre il ruolo di

[65] Ivi, p. 10.
[66] Information Security institute, Università statale di Mosca Lomonosov in Russia, L'istituto è guidato da Vladislav Sherstyuk, ex direttore dell'Agenzia federale delle comunicazioni e delle informazioni governative (FAPSI), *Cfr*. http://www.ipib.msu.ru/ [ultimo accesso 16.04.22].
[67] *Ibidem*.
[68] *Ibidem*.

direttore esecutivo della *Russkiy Mir Foundation*[69], tiene regolarmente conferenze nei Paesi ex Unione Sovietica.

La maggior parte degli autori russi comprende la guerra dell'informazione come parte della rivalità tra i diversi sistemi di civiltà e, in questa competizione, al fine di influenzare le masse, vengono utilizzate "armi informative" che possono essere di varia natura[70]. Mescolano così l'ordine militare e non militare, la sfera tecnologica (spazio cibernetico) e quella sociale (spazio delle informazioni) e fanno riferimenti diretti alla "guerra psicologica" tra Oriente e Occidente[71]. Oltretutto il termine *information warfare* solitamente viene collocato, dai più, in due contesti: 1) come circostanza difensiva da possibili interferenze ai danni della sicurezza nazionale, proprio come la dottrina sulla sicurezza delle informazioni della Federazione Russa[72] illustra; 2) come rivalità tra Russia e Occidente[73], innestata in più dimensioni tra cui quella politica, ideologica, socio-culturale ed economica che, per facilitare la complessità, potremmo asserire più semplicemente ad un unico concetto, ovvero quello di rivalità geopolitica.

La Russia ha una lunga tradizione nel condurre campagne d'inganno e, con il termine "Maskirovka" (letteralmente, "metodi per l'inganno"), si intende un insieme di stratagemmi al fine di manipolare e controllare il nemico creando una falsa impressione della situazione reale, costringendolo ad agire in un modo prevedibile[74]. Da un punto di vista

---

[69] *Cfr*., il sito web della Russkiy Mir Foundation (essa ha il compito di sostenere i russi e russofoni che vivono al di fuori della Federazione Russia): https://russkiymir.ru/it/ [ultimo accesso 16.04.22].
[70] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p. 12.
[71] *Ibidem*.
[72] *Cfr*. "Dottrina sulla sicurezza delle informazioni della Federazione Russa" approvata con decreto dal Presidente della Federazione Putin, 9 settembre del 2000. Disponibile online sul sito dell'ITU al seguente link: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf [ultima consultazione online: 16.04.22]. Questa dottrina sarà trattata in modo più approfondito nel capitolo 2, paragrafo 2.4 di questo elaborato.
[73] Principalmente due attori, Stati Uniti e NATO.
[74] HEICKERO R., *Emerging Cyber Threats*, op.cit, p. 20.

russo, *Maskirovka* è una componente cruciale della guerra dell'informazione[75], con tale operazione si introduce misure ingegneristicamente interconnesse per ingannare l'avversario e proteggere i sistemi di comando e controllo[76]. Nello specifico: mira ad ingannare i servizi d'intelligence stranieri ed i centri di comando e controllo con lo scopo di indurre, e quindi influenzare, un avversario a prendere decisioni che vadano a beneficio delle forze russe[77].

Gli Stati Uniti usano il termine *Military Deception* (MILDEC), come una capacità fondamentale delle *Information Operations* (IO), per ingannare i *decision makers* di un avversario in una situazione di conflitto; mentre *Maskirovka*, è un tipo indipendente di supporto operativo per influenzare un avversario e si svolge su base giornaliera a tutti i livelli[78].

Riassumendo, *Maskirovka* comporta una serie di metodi, compresi gli aspetti sia psicologici che tecnici, a tutti i livelli di conflitto. È un'attività quotidiana diretta (principalmente) contro servizi e sistemi di intelligence nemici, ma anche verso sistemi di comando e controllo civili. L'obiettivo è ottenere effetti sia sintattici che semantici manipolando le informazioni ed i sistemi d'informazione.

L'origine dell'attuale strategia russa sull'*Information Warfare* risale agli anni '90, quando il Consiglio di sicurezza nazionale russo individuò la crescente necessità di prestare maggiore attenzione a forme di ingerenza occidentale di tipo informativo[79]; la manovra rivelatrice è

---

[75] T. THOMAS, *Manipulating the Mass Consciousness: Russian And Chechen "Information War" Tactics in the 2nd Chechen- Russian Conflict,* Foreign Military Studies Office, Fort Leavenworth, 2018, p. 12.
[76] HEICKERO R., *Emerging Cyber Threats*, op.cit, p. 21.
[77] *Ivi*, p. 22.
[78] *Ivi*, p. 23-26.
[79] C. COLLISON, Russia's Information War: Old Strategies, New Tools. How Russia Built an Information Warfare Strategy for the 21st Century and What the West can Learn from the Ukraine Experience, SL, 2017, accessibile online: https://jsis.washington.edu/ellisoncenter/wpcontent/uploads/sites/13/2017/05/collison_chris_Russia's-Information-War-Old-Strategies-New-Tools-How-Russia-Built-an-Information-Warfare-Strategy.pdf [ultima consultazione online: 16.04.22].

stata l'adozione da parte della Federazione di una dottrina sull'information security, presentata negli anni 2000[80]. L'obiettivo principale della dottrina, è quello di delineare delle azioni volte a garantire la protezione delle informazioni strategicamente importanti, ovvero mitigare l'ingerenza di attività straniere dirette contro gli interessi della Federazione russa nella sfera dell'informazione[81]. Questo ricco documento espone senza mezzi termini l'obiettivo del governo russo di rendere sicuro l'*Information space*[82]. Inoltre, sia questa dottrina che quella militare del 2010, sottintendono che le operazioni d'informazione sono delle operazioni da mantenere costanti in tempo di pace e da intensificare nel preludio alla guerra, piuttosto che solo una componente della guerra stessa[83]. L'ossessione per la sfera dell'informazione, la presunta influenza esercitata dai media stranieri al fine di delegittimare il governo e i costumi della Russia e i mezzi per incoraggiare, favorire e sostenere un'immagine positiva fuori e dentro i confini russi, mostrano che il Cremlino dà la priorità a una strategia multiforme che enfatizza l'informazione come mezzo per promuovere obiettivi politici.

Tattiche e strategie sviluppate e impiegate durante il periodo sovietico sono servite da base per stabilire nuove strategie che incorporano parte del repertorio, secolare, leninista e nuove tendenze come IW, come definito da Mosca, per lo svolgimento di una guerra

---

[80] "Dottrina sulla sicurezza delle informazioni della Federazione Russa" approvata con decreto dal Presidente della Federazione Putin, 9 settembre del 2000. Disponibile online sul sito dell'ITU al seguente link: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf [ultima consultazione online: 16.04.22].

[81] Il documento è tradotto e discusso in D. CARMAN, "Traduzione e analisi della dottrina della sicurezza informatica della Federazione russa: mass media e politica dell'identità". *Associazione Pacific Rim Law & Policy Journal*, 2002.

[82] T. THOMAS, (Lt. Col., U.S. Army, Retired), Nation-State Cyber Strategies: Examples from China and Russia, accessibile online: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-20.pdf [ultima consultazione online: 01.07.18]. Inoltre, Cfr. C. COLLISON, Russia's Information War, op. cit.

[83] R. HEICKERO, Emerging Cyber Threats, op.cit., pp. 18-21.

politica continua, contro obiettivi ostili. Sebbene alcuni osservatori russi e stranieri usino nuovi termini come guerra "non lineare" o di "nuova generazione" per descrivere la pratica della Russia, l'IW che la Russia conduce oggi segue le logiche della già passata guerra politica sovietica[84], ma sono cambiati i mezzi di cui la Federazione – così come altri Stati – dispone.

La percezione di assedio permanente nella mentalità russa

La Russia esprime la sua politica di sicurezza nazionale in reazione alla percezione che la Federazione sia in un costante stato d'assedio da parte di operazioni di intelligence e di sfide alla sicurezza poste dagli avversari guidati dagli Stati Uniti[85] al fine di sovvertire, influenzare e corrompere i valori e la cultura russa. Come scrivevano C. Andrew e V. Mitrokhin a proposito della costante mentalità del regime sovietico: "Tutti i regimi autoritari, poiché considerano l'opposizione fondamentalmente illegittima, tendono a vedere i loro avversari impegnati in una [continua] cospirazione sovversiva"[86].

In Russia, non vi è alcuna distinzione tra il periodo di pace o quello di guerra, piuttosto, data la sua percezione del conflitto permanente e protratto, la Russia si prepara ogni giorno alla guerra schierando tutti gli strumenti del potere statale per accrescere i suoi interessi e la sua sicurezza[87].

---

[84] S. BLANK, "Cyber War and Information War à la Russe", from *Understanding Cyber Conflict: Fourteen Analogies*, George Perkovich and Ariel E. Levite, Published by George Town University Press, 2017, p. 82.
[85] Ivi, p. 82-84.
[86] C. ANDREW, V. MITROKHIN, *The Sword AND the Shield: The Mitrokhin Archive AND the Secret History of the KGB*, Basic Books, New York, 1999, disponibile online: https://archive.org/details/TheSwordAndTheShieldTheMitrokhinArchiveAndTheSecretHistoryOfTheKGB/mode/2up [ultimo accesso: 16.04.22].
[87] S. BLANK, "Cyber War and Information War à la Russe", *op.cit.* p. 82-84.

Osservando le operazioni della Federazione russa ci possiamo accorgere che l'intero Stato partecipa alla guerra politica, poiché dai documenti ufficiali russi sulla sicurezza nazionale, dal 2009 si percepisce come vi siano piani per mobilitare l'intero Stato per un conflitto, la chiamata è rivolta a tutti i cittadini della Federazione[88].

Le attuali tendenze nell'ambiente di sicurezza dell'area post-sovietica non sono favorevoli alla Russia, che deve competere per l'influenza nella regione con gli Stati Uniti, l'UE, la Cina, la Turchia, l'Iran e altri attori. La maggior parte dei paesi della regione non si considera minacciata dall'esterno e quindi le richieste di unità nell'area di difesa strategica proposte da Mosca servono principalmente ai soli interessi della Russia[89]. Inoltre, l'area della *Comunità degli Stati Indipendenti* (CSI) oggi non costituisce una comunità geopolitica o di civiltà, e nel Caucaso meridionale la Russia ha perso in parte l'influenza sulla Turchia così come nell'Europa orientale verso l'Unione europea. L'economia russa, e in parte anche la sua influenza militare in tutta l'area, si sta erodendo a favore della Cina, le cui iniziative strategiche come *La Nuova Via della Seta* rendono la Cina un attraente centro di gravità. Eppure, la Russia continua a considerare il controllo della regione come un segno distintivo del suo status di potenza mondiale e un meccanismo per impedire i tentativi dei Paesi della regione di perseguire politiche multi-vettore e integrarsi con strutture che sfuggono al controllo di Mosca[90].

Sebbene la Russia sia chiaramente disposta ad esercitare l'uso della forza come in Georgia e Ucraina, queste operazioni militari rappresentano l'apogeo di una strategia basata su operazioni portate

---

[88] S. BLANK, "'No Need to Threaten Us, We Are Frightened of Ourselves: Russia's Blueprint for a Police State - the New Strategy," in S. Blank and R. Weitz (a cura di), *The RUSSIAN MILITARY TODAY AND Tomorrow: ESSAYS in Memory of MARY FITZGERALD*, Strategic Studies Institute, US Army War College, 2010, pp. 19-150.
[89] J. DARCZEWSKA, "Russia's Armed Forces on the Information War Front", Center for Eastern Studies, giugno 2016, pp. 29-36.
[90] *Ibidem*.

avanti per anni e che utilizzano strumenti integrati, militari e non, per sovvertire governi dall'interno. In altre parole, IW, che comprende la *cyber warfare*, le operazioni psicologiche etc., ha lo scopo di ottenere i risultati che altrimenti si dovrebbero conseguire con l'utilizzo della forza militare cinetica[91].

Basandosi sul brutale successo della seconda campagna cecena, Putin ha cercato di ripensare la guerra contemporanea e ricostruire un esercito efficace. L'attuale strategia, proprio come quella del 1921-1939, identifica forme surrogate di potere per compensare le carenze in armamenti sofisticati che possiedono gli Stati Uniti[92]. Pertanto, la guerra asimmetrica ha ottenuto con successo grandi sostenitori, poiché data l'inferiorità economica e le carenze militari della Russia, sembrava sempre più un'alternativa sicura e a costi molto più bassi, rispetto al confronto militare diretto con la NATO o gli Stati Uniti.

Una delle minacce principali che la Russia percepisce è che le campagne di *information warfare* contro la Federazione sono sviluppate dall'Occidente per compromettere la sovranità nazionale della Russia e facilitare il cambio di regime[93]. La minaccia percepita potrebbe essere esistenziale, ma in termini storici, questa visione ha qualche giustificazione nella misura in cui la dichiarazione di *glasnost,* di Mikhail Gorbachev, ha innescato processi che hanno portato al collasso dello Stato nella forma dell'Unione Sovietica, da allora questa libertà di "trasparenza" e di espressione può essere vista come una sfida diretta allo Stato russo[94].

---

[91] S. BLANK, "Cyber War and Information War à la Russe", *op.cit.* p. 82-84.
[92] *Ibidem*.
[93] GILES K., *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 33-40.
[94] *Ibidem*.

La distribuzione incontrollata e la riproduzione di informazioni online è stata fin dall'inizio considerata una minaccia per la Russia tanto quanto lo era, in precedenza, l'invenzione della fotocopiatrice[95]. Questo atteggiamento molto attento ha suscitato una forte resistenza iniziale da parte degli organismi di sicurezza statali russi in merito all'adozione di Internet. Alla fine del 1996, nelle audizioni parlamentari intitolate "La Russia e Internet: la scelta di un futuro", un alto funzionario dei servizi di sicurezza ha contrassegnato Internet in tutte le sue forme come una minaccia alla sicurezza nazionale russa[96]. L'argomento che alla Russia recava più preoccupazione era che l'adozione di Internet avveniva in un momento in cui le strutture di sicurezza erano in termini relativamente più deboli e quindi non erano in grado di garantire che il processo fosse guidato[97]. Esiste un conflitto diretto tra il concetto occidentale di Internet, che insiste nel considerare il flusso di informazioni come libero, illimitato e non governato, e la posizione promossa dalla Russia e dagli Stati affini, che insiste invece sul principio di sovranità nazionale, e quindi un deciso controllo statale, nel *cyberspace* e più in generale nell'*information space*.

I funzionari dei media russi si sono costantemente impegnati a "limitare i diritti e le libertà solo nell'interesse della sicurezza"[98].

Ma oltre alle informazioni provenienti dall'estero, anche le *app* e i *software* utilizzati per comunicare via Internet sono sospettati. Ci sono dichiarazioni e ordini del governo russo che hanno ripetutamente messo in evidenza i pericoli dell'uso di software di fabbricazione estera

---

[95] Come descritto audacemente in A. SOLDATOV, I. BOROGAN, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, PublicAffairs, London, 2015.
[96] "La Russia e Internet: la scelta di un futuro", Atti della Duma di Stato, 17 dicembre 1996, citato in GILES K., *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 33-40.
[97] GILES K., *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 33-40.
[98] "Щеголев: цензуры Интернета в России не допустят" (Shchegolev: la censura di Internet non verrà consentita in Russia), Interfax, 20 gennaio 2012, accessibile in lingua russa online: http://www.interfax.ru/print.asp?sec=1448&id=226823 [ultimo accesso: 16.04.22].

e di servizi Internet commerciali esteri, come i servizi di messaggistica istantanea, questo avrebbe permesso a servizi d'intelligence straniera di accedere sia a segreti in ambito economico che di difesa sia ai dati personali dei cittadini russi[99].

Nel 2016 in Russia il ministro della Cultura Vladimir Medinskiy afferma che il servizio di streaming video *Netflix* è finanziato dal governo degli Stati Uniti come un metodo per "entrare nelle menti di ogni abitante della Terra"[100]. Così anche *Pokémon Go*[101] è stato descritto nelle fonti ufficiali russe come una componente della guerra dell'informazione occidentale[102]; in aggiunta, il ministro delle comunicazioni e dei mass media Nikolay Nikirofov, suggerisce che il gioco virtuale sia stato creato con l'aiuto di alcune agenzie di intelligence, e che le medesime agenzie stanno raccogliendo informazioni video da territori in tutto il mondo[103]. In Russia, questo ricorda i tempi sovietici quando vi era la preoccupazione di fotografare luoghi di uso quotidiano come ponti o stazioni ferroviarie poiché avrebbe potuto fornire al nemico informazioni utili sulla capacità di logistica in caso di guerra[104].

La percezione della Russia è che le campagne di informazione rappresentano una minaccia seria e crescente per il paese, attuata e perfezionata dagli Stati Uniti e dall'Occidente. La conferenza del 2007

---

[99] "Foreign special services step up online operations targeting Russia - top security official," RT, 15 giugno 2016, online: https://www.rt.com/russia/346772-foreign-special-services-step-up/ [ultimo accesso: 16.04.22].

[100] "Мединский обвинил власти США в попытке «залезть в каждый телевизор» через Netflix" ("Medinsky accusa le autorità statunitensi di aver tentato di infiltrarsi in ogni televisione tramite Netflix"), RNS, 22 giugno 2016, online: https://www.dp.ru/a/2016/06/22/Medinskij_obvinil_SSHA_v_p/ [ultimo accesso: 16.04.22].

[101] un gioco di realtà virtuale ampiamente popolare nel momento dell'uscita, ma forse effimero come del resto sono tutte le mode.

[102] J. MASHIRI, "An Absurd Signal: Pokémon Confirms Russia's War Footing" ("Un segnale assurdo: i Pokémon confermano il piede di guerra della Russia"), 19 luglio 2016, online: https://blogit.apu.fi/somesotilas/an-absurd-signal-pokemon-confirms-russias-war-footing/ [ultimo accesso: 16.04.22].

[103] "The Devil has arrived through this mechanism. The Russian authorities weigh in on Pokémon Go Five quotes", Meduza, 18 July 2016, online: https://meduza.io/en/feature/2016/07/18/the-devil-has-arrived-through-this-mechanism [ultimo accesso: 16.04.22].

[104] GILES K., *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 33-40.

dell'Accademia delle scienze militari (AVN) ha messo in luce l'emergere di minacce non militari. Secondo l'allora Capo di Stato Maggiore Yuriy Baluyevsky, sulla base dell'esperienza del crollo dell'Unione Sovietica e della Jugoslavia, e sugli esempi delle rivoluzioni colorate in Georgia, Ucraina, Kirghizistan e altrove, si può chiaramente vedere che esistono grandi minacce oggettive e che sono implementate non solo da mezzi militari, ma principalmente con metodi segreti e palesi di influenza politica e diplomatica, economica ed informativa, varie azioni sovversive ed interferenze negli affari interni di altri paesi. A questo proposito Baluyevsky afferma che gli interessi di sicurezza russi richiedono non solo di valutare queste minacce, ma anche di stabilire le misure appropriate per rispondere ad esse[105].

***Political warfare* o *hybrid warfare* russa?**

Il termine "guerra politica" è spesso attribuito al famoso diplomatico americano George Kennan, che scrisse del fenomeno nelle prime fasi della guerra fredda[106]. Kennan immaginava una battaglia di vasta portata per influenza, usando tutte le leve del potere nazionale[107].

La comunità scientifica ha sollevato almeno tre obiezioni sostanziali al termine. Anzitutto, alcuni hanno portato obiezioni in merito alla parola "politica"[108]. Come notoriamente notò Clausewitz, "la guerra è la continuazione della politica con altri mezzi"[109], il che implica che tutte le

---

[105] Conferenza del 2007 dell'Accademia delle scienze militari, *Cfr*. per una trascrizione del discorso in lingua russa: http://old.redstar.ru/2007/01/23_01/2_04.html [ultimo accesso: 16.04.22], *Cfr*. per un commento giornalistico: http://nvo.ng.ru/nvo/20070122/1_enemies.html [ultimo accesso: 16.04.22]

[106] G. F. KENNAN, "The Inauguration of Organized Political Warfare", Archivio digitale del programma di storia e politiche pubbliche, ottenuto e contribuito da A. Ross Johnson, aprile 1948, disponibile al seguente link: https://digitalarchive.wilsoncenter.org/document/114320 [ultimo accesso: 16.04.22].

[107] S. J. CORKE, "George Kennan and the Inauguration of Political Warfare," *The Journal of Conflict Studies*, Vol. 26, n. 1, estate 2016, pp. 101-20.

[108] F. HOFFMAN, "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks*, 28 luglio 2014, online: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ [ultima consultazione: 16.04.22].

[109] C. V. CLAUSEWITZ, *Della guerra*, Mondadori Oscar Classici, II edizione, versione integrale, 2017, p. 42.

guerre, non solo alcuni sottogruppi, sono guerre politiche. In secondo luogo, altri si sono interrogati sull'applicazione del termine "guerra", poiché l'atteggiamento "offensivo" sarebbe avviato senza una dichiarazione formale di ostilità, contro amici o avversari, dove spesso non viene impiegata la violenza fisica[110]. Infine, la definizione di Kennan può includere praticamente ogni forma di interazione statale, quindi risulta molto vago.

Grazie a questi problemi sollevati in merito alla definizione, molti strateghi hanno rinunciato all'utilizzo del termine "guerra politica" a favore di altri termini come ad esempio guerra ibrida, o *hybrid warfare* qualora si preferisse il termine anglosassone.

Come ha osservato il Professor Carnes Lord, il problema nasce dalla tendenza generale ad usare i termini "guerra psicologica" e "guerra politica" in modo interscambiabile per designare il fenomeno generale, per non parlare di una varietà di termini simili: guerra ideologica, guerra delle idee, comunicazione politica e altro ancora[111]. L'esperto di contro-insurrezione David Galula equipara i due termini: "la guerra rivoluzionaria è una guerra politica", e sosteneva che in entrambi "la politica diventa uno strumento operativo attivo"[112], quindi oltre ad essere lo scopo – secondo i dettami Clausewiziani – è anche lo strumento. Allo stesso modo, il colonnello francese Roger Trinquier ha usato il termine "guerra sovversiva", quasi nello stesso modo in cui Kennan ha usato "guerra politica", per descrivere un sistema interconnesso di azioni politiche, economiche, psicologiche e militari che mirano al rovesciamento dell'autorità stabilita in un paese e la sua

---

[110] F. HOFFMAN, "On Not-So-New Warfare", *op.cit.*
[111] C. LORD, "The Psychological Dimension in National Strategy," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, C. LORD and F. R. BARNETT, (a cura di), National Defense University Press, Washington, D.C.,1989, p.16.
[112] D. GALULA, *Counterinsurgency Warfare: Theory and Practice*, Fredrick Praeger, New York, 1964, pp. 6-7.

sostituzione con un altro regime[113]. Più recentemente, alti funzionari della difesa ed esperti, incluso Frank Hoffman della National Defense University, hanno suggerito che "guerra ibrida" potrebbe essere un termine migliore rispetto a quello di "guerra politica"[114].

Tuttavia, come comunemente usato, la guerra ibrida connota una combinazione di tattiche militari non cinetiche o irregolari con mezzi militari convenzionali, piuttosto che una combinazione di strumenti militari e civili per ottenere gli effetti desiderati.

La prevalenza degli strumenti nella guerra politica è di natura non cinetica, ma la loro combinazione con mezzi militari convenzionali costituisce l'aspetto "ibrido"; quindi, la guerra ibrida è certamente un fenomeno delle guerre attuali, ma sarebbe più appropriato definirla in talo modo nel momento in cui, in guerra, iniziano ad essere impiegati mezzi militari cinetici assieme a quelli non cinetici.

Altri strateghi hanno cercato di dare una "precisione politica" più adeguata della definizione originale di Kennan. Ad esempio, lo storico Paul Smith cerca di legare il termine alla guerra psicologica, affermando che la guerra politica è l'uso di mezzi politici per costringere un avversario ad eseguire la propria volontà; e per "politica" si intende descrivere un rapporto intenzionale tra popoli e governi che incidono sulla sopravvivenza nazionale. Quindi, la guerra politica può essere combinata con violenza, pressione economica, sovversione e diplomazia, ma il suo aspetto principale è l'uso di parole, immagini e idee, ovvero propaganda e guerra psicologica[115].

Eppure, sebbene vi sia un ampio consenso sul fatto che la guerra psicologica sia un aspetto della guerra politica, la maggior parte vede la

---

[113] R. TRINQUIER, *Modern Warfare: A French View of Counterinsurgency*, Pall Mall Press, London, 1964, p.6.
[114] F. HOFFMAN, "On Not-So-New Warfare", *op.cit.*
[115] P.A. Jr. SMITH, *On Political War*, National Defense University Press, Washington, D.C., 1989, p. 3.

guerra politica come un termine più ampio e comprensivo[116]. Carnes Lord e Frank Barnett hanno sintetizzato: "La guerra politica è un termine che è meno ben definito nell'uso e nella dottrina, ma che sembra utile per descrivere una gamma di attività palesi e segrete progettate per sostenere la politica nazionale e obiettivi militari"[117]. Nella definizione di Lord e Barnett, la guerra politica rappresenta un paniere di tattiche – non solo propaganda – e sebbene probabilmente meno intellettualmente soddisfacente, forse, è la definizione che è più in linea con la concezione originale di Kennan, che combinava la guerra psicologica con altri strumenti che vengono utilizzati per raggiungere scopi politici[118].

Più di recente, il *white paper* del marzo 2015 del Comando delle operazioni speciali dell'esercito degli Stati Uniti afferma che "La guerra politica comprende una serie di attività associate all'impegno diplomatico ed economico, l'assistenza al settore della sicurezza (SSA), nuove forme di guerra non convenzionale (UW) e attività di informazione e influenza (IIA)"[119].

Sulla base delle molteplici reazioni al termine, possiamo iniziare a delineare cosa sia o meno la guerra politica. Da un lato, comprende tutti gli strumenti del potere nazionale: diplomatico, informativo, militare ed economico; e a seconda del caso, alcuni di questi strumenti possono avere una maggiore o minore rilevanza, ma tutti sono possibili

---

[116] S. LUCAS e K. MISTRY, "Illusions of Coherence: George F. Kennan, U.S. Strategy and Political Warfare in Early Cold War 1946–1950", *Diplomatic History*, Vol. 33, n. 1, gennaio 2009, p. 40.
[117] R.F. BARNETT, e C. LORD (a cura di), "Afterword-Twelve Steps to Reviving American PSYOP," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, National Defense University Press, Washington, D.C., 1989, p. Introduzione.
[118] L. ROBINSON, T.C. HELMUS, R.S. COHEN, A. NADER, A. RADIN, M. MAGNUSON, K. MMIGACHEVA, *Modern Political Warfare. Current Practices and Possible Responses*, RAND Corporation, Santa Monica, California, 2018 p. 5.
[119] United States Army Special Operations Command, "SOF Support to Political Warfare White Paper", 10 marzo, 2015, p. 2. Disponibie online: http://orchestratingpower.org/lib/LIC/PW/2015,03,10%20arsoc%20support%20to%20PW.pdf [ultimo accesso: 16.04.22].

strumenti di guerra politica[120]. Inoltre, si può denotare che cosa non sia la guerra politica, vale a dire né regolari interazioni diplomatiche ed economiche né guerre convenzionali tra Stati[121].

In base a quanto detto sin qui, possiamo concludere che l'*information warfare* viene intrapresa sia in tempo di pace che in tempo di guerra ed essa può essere inserita sotto il cappello della *political warfare*, ma essa cambia cappello nel momento in cui si passa da un tempo di pace ad un tempo di guerra per indossare quello dell'*hybrid warfare*.

[120] L. ROBINSON, T.C. HELMUS, R.S. COHEN, A. NADER, A. RADIN, M. MAGNUSON, K. MMIGACHEVA, "Modern Political Warfare", op.cit., p. 6.
[121] *Ibidem*.

L'*INFORMATION WARFARE* NEI DOCUMENTI UFFICIALI RUSSI

Tra i documenti ufficiali, *open source,* prodotti dal governo e da istituzioni militari che interessano l'oggetto di studio, troviamo: la strategia di sicurezza nazionale[122]; la dottrina militare; le opinioni concettuali riguardanti le attività delle Forze Armate della Federazione Russa nello spazio delle informazioni; la dottrina sulla sicurezza delle informazioni della Federazione Russa; altri documenti in merito all'information security adottati nel contesto delle organizzazioni internazionali; il concetto per una *cybersecurity* russa.

Questi documenti sono sviluppati sotto gli auspici del Consiglio di Sicurezza Nazionale, il quale coordina un gran numero di agenzie governative coinvolte nel processo di produzione dei documenti di interesse nazionale. Il Consiglio di Sicurezza Nazionale è un'istituzione tra le più autorevoli nella Federazione Russa ed è presieduta direttamente dal presidente Putin. I suoi 13 membri permanenti – tra cui il primo ministro, il ministro della difesa, il ministro degli affari esteri e i capi del servizio di sicurezza, il servizio di sicurezza federale (Federalnaia sluzhba bezopasnosti, FSB), il servizio di intelligence estera (Sluzhba vneshnei razedki Rossiiskoi Federatsii, SVR) ed il direttorato principale per l'informazione (Glavnoe razvedyvatel'noe upravlenie, GRU) – si incontrano su base settimanale[123]. I documenti ufficiali non

[122] U. FRANKE, *War by non-military means*, *op.cit.* p.11.
[123] *Ibidem*.

coordinati a questo livello, ma rilasciati da singole agenzie governative, hanno un peso inferiore[124].

La strategia di sicurezza nazionale

La *strategia di sicurezza nazionale* della Federazione Russa, del 2009[125], del 2015[126] e in quella aggiornata del 2021[127], pongono le basi per la visione russa sull'*information warfare* e, inoltre, si apprende come i russi percepiscono alcuni eventi mondiali. Si segnala un'intensificazione dell'attività di *information warfare* e si sancisce che l'informazione è uno strumento che gli Stati possono impiegare per migliorare la loro sicurezza nazionale. Questo può avvenire implementando misure d'IW insieme a misure politiche, diplomatiche, militari ed economiche, per una strategia di deterrenza che possa permettere la mitigazione di minacce e di azioni distruttive da parte di uno stato (o coalizione di Stati) attaccante. Inoltre, si asserisce che esistono minacce che vanno al di là della sfera militare, bensì si concentrano a danneggiare la sfera culturale russa. Si individuano minacce *cyber* in merito alla sicurezza dei sistemi informatici, delle

---

[124] Per una lettura più approfondita sulla gerarchia dei documenti ufficiali nell'area della politica di sicurezza, *Cfr.* G. PERSSON, "Security Policy and Military Strategic Thinking", In J. HEDENSKOG, e C. VENDIL PALLIN (Eds.), *Russian Military Capability in a Ten-Year Perspective*, FOI, the Swedish Defence Research Agency, Stockholm, 2016.

[125] La "strategia per la sicurezza nazionale della Federazione Russa fino al 2020" è stata approvata con decreto del Presidente della Federazione Russa e pubblicata il 12 maggio del 2009 n.537. *Cfr*. sito internet del "NATO Cooperative Cyber Defence Centre of Excellence", document disponibile in versione inglese al seguente link: https://ccdcoe.org/library/strategy-and-governance/?search=russia [ultima consultazione online: 16.04.22].

[126] Strategia di Sicurezza Nazionale della Federazione Russa, editto presidenziale della Federazione Russa, 31 dicembre 2015 n. 683, Cfr. il "Portale Internet ufficiale informazioni legali Sistema statale di informazione" legale per la versione ufficiale in lingua russa: http://publication.pravo.gov.ru/Document/View/0001201512310038 [ultima consultazione online: 16.04.22], *Cfr*. anche il Centro superiore per gli studi sulla difesa nazionale spagnolo per il documento tradotto in inglese http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf [ultima consultazione online: 16.04.22].

[127] Strategia di Sicurezza Nazionale, approvata con decreto del Presidente della Federazione Russa n. 400, 2 luglio 2021. Documento ufficiale consultabile online in lingua russa: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1 [ultima consultazione online: 16.04.22].

strutture di ICT e più in generale alle infrastrutture critiche del Paese. In questi documenti la Russia si focalizza sull'aumento della sua influenza e del prestigio nazionale. Individua i suoi nemici nella figura degli USA e dei suoi alleati (NATO), tracciando un perimetro di minacce che posso provenire anche dagli Stati confinanti con la Federazione Russa. Un tema ricorrente è la difesa dei valori morali e spirituali tradizionali russi, minacciati dalla cultura occidentale e da estremisti e terroristi. Si enfatizza il fatto che la Federazione tenta di assicurare la sovranità culturale della Russia proteggendo la società da campagne informative distruttive ed impatti psicologici negativi; quindi, si legittima ad effettuare un controllo informativo statale per salvaguardare la propria sovranità e sicurezza della popolazione. Nell'ultimo piano strategico il Cremlino conferma che la difesa è preparata per garantire la protezione armata del Paese, tanto più la sua sovranità e l'integrità del suo territorio.

La dottrina militare

Le *dottrine militari* del 2010[128] e del 2014[129] hanno risposto a pieno ai compiti di difesa nazionale nell'ambito della strategia di sicurezza nazionale. La Federazione russa abbraccia l'*information warfare* come strumento di sicurezza nazionale. Si enfatizza il passaggio da un esercito di mobilitazione di massa ad un esercito professionale e altamente qualificato, in grado di affrontare le moderne minacce alla sicurezza nazionale ed i nuovi canoni che rientrano in un concetto di *Modern*

[128] Dottrina militare della Federazione Russa, approvata con decreto del presidente della Federazione Russa, 5 febbraio 2010, accessibile online: https://www.justsecurity.org/7777/russias-2010-military-doctrine/ [ultima consultazione online: 18.12.19].
[129] La dottrina militare della Federazione Russa del 2014 è stata approvata con decreto n. 2976 del Presidente della Federazione Russa, dicembre 2014. Disponibile online, sul sito dell'ambasciata russa in UK, al seguente link: https://rusemb.org.uk/press/2029 [ultima consultazione online: 16.04.22].

Warfare. Durante i conflitti moderni l'IW sarà essenziale per modellare lo spazio politico prima del conflitto. L'IW può essere utilizzata sia in tempo di pace che di guerra, sia come strumento solitario sia in combinazione con altri mezzi di difesa o d'attacco.

Le opinioni concettuali sulle attività delle Forze Armate della Federazione Russa nell'*Information Space*

Nella *visione concettuale* del 2011[130], definita da K. Giles una "proto-dottrina cibernetica militare russa", troviamo la prima dichiarazione esplicita del ruolo delle Forze Armate russe nel *cyberspace*[131]. Questo documento definisce i termini operativi da una prospettiva militare incentrata sull'informazione e risulta essere un documento strategico militare, ma non un manuale operativo. Qui si comprende che nella visione militare russa l'IW abbraccia elementi dell'intelligence, inganno a livello operativo, guerra elettronica, comando e controllo, gestione delle informazioni tra il personale, la difesa di sistemi di informazione da guerra elettronica e operazioni di rete di computer. Ci spiega inoltre che l'IW è un modo per risolvere i conflitti tra Stati o all'interno di essi, che può essere intesa come una lotta fra due o più Paesi all'interno dell'*information space* e che lo spazio delle informazioni e quello spazio dove avvengono le attività per influenzare singoli individui, società, infrastrutture e le informazioni stesse.

---

[130] Ministero della Difesa della Federazione Russa, "opinioni concettuali sulle attività delle forze armate della Federazione Russa nello spazio informazioni", 2011. Documento disponibile online al seguente link: http://www.pircenter.org/media/content/files/9/13480921870.pdf [ultima consultazione online: 16.04.22], *Cfr*. anche il sito del Ministero della Difesa russo al seguente link: http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle [ultima consultazione online: 16.04.22].

[131] K. GILES, "Russia's public stance on cyberspace issues" in *4Th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2012, p. 67.

La dottrina sull'*Information Security* della Federazione Russa

L'*information security* del 2000[132] e del 2016[133], principalmente catalogano minacce alla sicurezza delle informazioni e le contromisure previste per far fronte a queste minacce. Si parla anche in questi documenti di area spirituale da dover difendere da operazioni psicologiche che vengono utilizzate dall'attaccante per suscitare discordia nella società stanziata su di un determinato territorio; si enfatizza la politica dello Stato di mettere la sicurezza davanti alle libertà civili; ed infine, fornisce un quadro istituzionale di attori che gestiscono la sicurezza dell'informazione e gli attori che potrebbero essere coinvolti in attacchi.

Le Risoluzioni ONU

Nel contesto delle organizzazioni internazionali, dal 1998, la Russia ha sponsorizzato una serie di risoluzioni in seno all'Assemblea generale delle Nazioni Unite[134], ha invitato i Paesi membri a prevenire, in campo internazionale, le minacce informatiche e ha invitato i membri a fornire le loro opinioni sulla sicurezza delle informazioni in generale, ovvero sulle definizioni e sull'opportunità di sviluppare principi internazionali per affrontare il terrorismo e la criminalità dell'informazione. Attraverso

[132] Dottrina sulla sicurezza delle informazioni della Federazione Russa, approvata con decreto dal Presidente della Federazione Putin, 9 settembre del 2000. Disponibile online sul sito dell'ITU al seguente link: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf [ultima consultazione online: 16.04.22].

[133] Dottrina sulla sicurezza delle informazioni della Federazione Russa, approvata con decreto dal Presidente della Federazione Putin, 5 dicembre del 2016, disponibile online, *Cfr.* il "Portale Internet ufficiale informazioni legali Sistema statale di informazione legale" http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1 [ultima consultazione online: 16.04.22]. *Cfr*. anche il Ministero degli Affari Esteri della Federazione Russa per una versione in inglese https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 [ultima consultazione online: 16.04.22].

[134] UN GA, "Developments in the field of information and telecommunications in the context of international security", risoluzione adottata dall'Assemblea Generale delle Nazioni Unite [sulla relazione del primo comitato (A / 53/576)], 1999. Disponibile online sul sito delle Nazioni Unite nella sezione "documenti" al seguente link: https://undocs.org/en/A/RES/53/70 [ultima consultazione online: 18.12.19].

le definizioni date di protezione dell'informazione dei dati, proposte in seno a queste sessioni di dialogo internazionale, si comprende come vi sia una tensione tra modi fondamentalmente diversi di affrontare il ruolo del libero flusso di informazioni su Internet tra i paesi Occidentali e la Russia.

Il Concetto di Strategia per una cybersecurity russa

Nel *concetto di strategia per una cybersecurity russa*[135], si comprende come l'uso russo del termine "*cybersecurity*" è stato principalmente un modo per partecipare al dialogo internazionale e allo sviluppo normativo e di *policy* in merito alla *cybersecurity*. Il documento offre una definizione di cibersicurezza che differisce dalla sicurezza delle informazioni. In estrema sintesi, il *cyberspazio* è esplicitamente considerato un sottoinsieme di uno spazio informativo più ampio.

Riassumendo

Tutti i documenti ufficiali russi analizzati dipingono un'immagine di un periodo storico delle relazioni internazionali dove la complessità delle minacce è in forte mutamento. Sottolineano all'unanimità un concetto molto ampio di guerra delle informazioni, che va dalle operazioni psicologiche contro individui o intere popolazioni ad attacchi alle reti informatiche e/o infrastrutture critiche, ma soprattutto si percepisce un'influenza insidiosa dei *mass media* stranieri pronti a screditare l'operato della Federazione russa agli occhi della popolazione internazionale.

[135] *Cfr*., "concetto per una strategia di cybersecurity russa", Consiglio Federale russo, 2014, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [ultimo accesso: 16.04.22].

L'unica voce contraria a questo flusso di realismo politico è "il concetto di strategia di *cybersecurity*", che sottolinea gli aspetti positivi derivanti dalle opportunità nate con la moderna società dell'informazione. Ma che comunque, anche in questo documento si sottolinea che, queste opportunità che generano benefici alla società vanno protetti da minacce ed influenze esterne che avrebbero conseguenze indesiderabili.

In linea con il tradizionale pensiero russo, l'indirizzo che i documenti ufficiali offrono al lettore risulta essere di carattere puramente difensivo. Si rivelano poche informazioni su come la Russia conduce l'*information warfare* contro altri paesi, anche se si può leggere molto tra le righe. Per poter capire meglio come la Federazione Russa sfrutta il suo *know-how* nel campo dell'*information warfare*, occorrerà studiare il pensiero militare russo analizzando teorie e dichiarazioni di ufficiali militari che operano all'interno delle Forze Armate russe.

L'Information Warfare nella teoria militare ed accademica russa

Nei documenti ufficiali, le politiche in merito all'argomento sono dichiarate appena e con un velo di non facile lettura. Pertanto, è utile studiare anche il ragionamento della teoria militare russa in cui si possono trovare logiche, pensieri e riflessioni su cui poter avviare valutazioni il più appropriate possibile. In Russia, il Ministero della Difesa pubblica "Voennaia mysl"[136], una rivista ufficiale di teoria militare che finanzia la ricerca presso l'Università Militare[137]. Sebbene da una parte, le opinioni espresse negli articoli e nelle tesi di ricerca siano quelle degli autori e non rispecchiano le posizioni ufficiali della Federazione; d'altra parte, è lecito asserire che – le linee di pensiero così espresse in un contesto ufficiale come quello di un'Università militare, con finanziamenti diretti da parte del Ministero della Difesa – siano indirizzate direttamente od indirettamente all'attenzione dell'establishment militare russo.

Principalmente, l'approccio russo si basa su due aree per ciò che concerne la guerra dell'informazione, ovvero: l'area informativa tecnica e quella psicologica dell'informazione[138]; a conferma di questa logica ci viene in aiuto anche un autorevole libro (russo), in cui si afferma che i due principali filoni della guerra dell'informazione nel pensiero russo

[136] trad. Pensiero militare.
[137] U. Franke, *War by non-military means*, *op.cit.* p. 23.
[138] T. Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", *The Journal of Slavic Military Studies*, vol. 27, 2014, p. 101-130.

sono: la *guerra psicologica*, con lo scopo di colpire il personale delle forze armate e la popolazione (questa viene condotta in condizioni di competizione naturale, cioè permanentemente); e la *guerra tecnologica dell'informazione* per incidere sui sistemi tecnici che ricevono, raccolgono, elaborano e trasmettono informazioni (condotta durante guerre e conflitti armati)[139].

L'*infoWar* "à la Russe"[140] si differenzia dalle pratiche occidentali

La Russia considera il domino cyber in maniera diversa rispetto alle controparti occidentali, dal modo in cui i teorici russi definiscono la guerra informatica a come il Cremlino utilizza le sue capacità informatiche[141]. Nel dominio cibernetico, cogliere e comprendere il comportamento degli antagonisti, può spesso risultare avviluppato e macchinoso e le sfide concettuali associate al dominio *cyber* sono spesso analizzate da una prospettiva puramente tattica e/o difensiva. I problemi di attribuzione degli attacchi cibernetici, l'ingegnosità della guerra informatica, la sua rapida evoluzione e i metodi segreti tendono ad adombrare le motivazioni e le strategie degli attori coinvolti. I *reportage* dei media e l'analisi forense, solitamente, si concentrano sulle origini e sui vettori degli attacchi informatici, sulle tecniche e gli strumenti che usano, sul loro impatto e su come i loro effetti possono essere difesi o mitigati. Domande strategiche più ampie, come ad esempio il motivo per cui l'avversario conduce attacchi nell'*information*

---

[139] V. KVACHKOV, Спецназ России (trad. Teoria delle operazioni speciali), Voyennaya Literatura, 2004. Vladimir Kvachov è un ex ufficiale del GRU, la cui "teoria delle operazioni speciali", comprese le operazioni d'informazione, è stata adottata come base per il materiale di istruzione e addestramento militare russo (nota in K. GILES, *Handbook of Russian Information Warfare*, op.cit., p.9).

[140] Espressione ripresa da: S. BLANC, "Cyber War and Information War à la Russe", From *Understanding Cyber Conflict: Fourteen Analogies*, George Perkovich and Ariel E. Levite, Published by Georgetown University Press, 2017.

[141] M. CONNELL and S. VOGLER, *Russia's Approach to Cyber Warfare*, CNA Analysis & Solution, 2017, pp. 1-2.

space, come individuare l'obiettivo dell'attacco o come l'avversario percepisce il rischio e l'escalation nel *cyberspace* o ancora, il come ed il se, gli attacchi possono essere scoraggiati. Questi interrogativi vengono spesso trascurati e/o trattati in modo meno approfondito.

All'indomani della Guerra Fredda, a causa della mancanza di risorse e di vincoli di bilancio durante gli anni '90, gli scienziati russi dedicarono più tempo alla teoria dell'IO, rispetto ai loro colleghi occidentali, concentrandosi sulla teoria e sulla pratica[142].

Secondo lo studioso James Wirtz, la Russia, più di ogni altro attore, sullo scacchiere cyber, pare che sia riuscita ad escogitare un modo per integrare la guerra cibernetica in una grande strategia in grado di raggiungere obiettivi politici[143]. Al fine di contrastare questa strategia, i *policy makers* e gli apparati militari occidentali dovrebbero comprendere in che modo la Russia integra i concetti della guerra informatica nelle sue più ampie strategie militari e di sicurezza nazionale[144].

La Russia vede la superiorità in questa ampia applicazione della guerra dell'informazione come fattore chiave per la vittoria nel conflitto attuale e futuro:

> "Le guerre saranno risolte da una sapiente combinazione di misure militari, non militari e speciali non violente che saranno sottoposte a una varietà di forme e metodi attraverso una miscela di misure politiche, economiche, informative, tecnologiche e ambientali, principalmente sfruttando la superiorità dell'informazione. La guerra dell'informazione nelle nuove condizioni sarà il punto di partenza di ogni azione ora chiamata il nuovo tipo di guerra, o guerra ibrida, in cui si farà ampio uso dei mass media e, laddove possibile, delle reti informatiche globali"[145].

---

[142] R. HEICKERO, *Emerging Cyber Threats*, op. cit, pp. 12-17.

[143] J.J. WIRTZ, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power Into Grand Strategy", in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications: Tallinn, 2015, accessibile online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf [ultima consultazione online: 16.04.22].

[144] M. CONNELL AND S. VOGLER, *Russia's Approach to Cyber Warfare*, CNA Analysis & Solution, 2017, pp. 1-2.

[145] CHEKINOV e S. A. BOGDANOV, "The Nature and Content of a New-Generation of War", *Military Thought*, versione in inglese di East View information services, Vol. 22, n.4, 2013, pp. 13-24. Sergey Chekinov è citato più volte, ciò riflette sia la sua vasta gamma di pubblicazioni su questo argomento, sia la sua posizione di

Questa fusione e coordinamento tra diversi strumenti informativi è una caratteristica distintiva di come la Russia aspira a perseguire la guerra dell'informazione, mentre i critici del *modus operandi* della NATO suggeriscono che all'interno dell'Alleanza, questo coordinamento è al contrario evidente per la sua assenza; secondo una valutazione della NATO:

> "C'è ancora una mancanza di consenso quando si tratta di definire tutti gli elementi che costituiscono l'applicazione strategica del potere nel dominio delle informazioni. Per quanto riguarda l'uso di termini come Information Warfare (IW), Psychological Operations (PsyOps), Influence Operations (IO), Strategic Communications (STRATCOM), Computer Network Operations (CNO) e Military Deception (MILDEC), c'è molta confusione poiché esistono numerose definizioni contrastanti e questi termini sono usati in contesti diversi per descrivere obiettivi e azioni diversi"[146].

Nel contesto russo, tutte queste diverse discipline formano il concetto onnicomprensivo di *Information Warfare*[147].

Insieme ad altri strumenti, con lo scopo di proiettare la potenza russa nello spazio terracqueo, il concetto di *Information Warfare* è diventato oggetto di un acuto interesse improvviso nell'Occidente, quando ebbe inizio la crisi Ucraina nel 2014[148]. Tuttavia, agli occhi degli studiosi della materia, non sembra essere un fenomeno nuovo, bensì ampiamente ignorato dalla fine dell'Unione Sovietica; piuttosto, secondo K. Giles, e altri esponenti militari occidentali, riflette i principi permanenti dell'approccio russo alla competizione tra Stati, ampiamente aggiornato e rinnovato, come parte dei recenti preparativi della Russia per il conflitto in condizioni di inferiorità generale complessiva[149]. Come descritto dal presidente Vladimir Putin, "Dobbiamo tenere conto dei

---

capo del Centro per la ricerca strategica militare dell'Accademia dello Stato Maggiore russo e quindi come un indicatore affidabile delle attuali tendenze di pensiero all'interno dello Stato Maggiore.

[146] P. BRANGETTO e M. A. VEENENDAAL, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in N.Pissanidis et. al. (eds.), *8th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, giugno 2016.

[147] K. GILES, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, pp. 6-7.

[148] *Ivi*, pp. 3-5.

[149] *Ibidem*.

piani e delle direzioni di sviluppo delle forze armate di altri paesi [...] Le nostre risposte devono essere basate sulla superiorità intellettuale, saranno asimmetriche e meno costose"[150].

Nella visione russa, la guerra dell'informazione non è un'attività limitata alla guerra ormai scoppiata, bensì ha una natura olistica e onnicomprensiva ed è sia il soggetto che il mezzo del conflitto[151]. Non è nemmeno limitato alla fase iniziale delle ostilità, dove generalmente, include la preparazione d'informazioni utili in merito al campo di battaglia[152]. Invece, viene considerata un'attività costantemente in corso, a prescindere dallo stato delle relazioni con l'avversario[153]. Alla voce "Information Warfare" (*informatsionnaya voyna*), in un glossario di termini per la sicurezza delle informazioni prodotto dall'Accademia militare dello Stato Maggiore, viene riportata una chiara distinzione tra, la definizione russa, ovvero ampia e non limitata alla guerra e, quella occidentale che descrive le operazioni d'informazione come tattiche, limitate e svolte durante le ostilità[154].

L'*Information Warfare* può coprire una vasta gamma di diverse attività e processi che cercano di rubare, impiantare, interdire, manipolare, distorcere o distruggere le informazioni ed i vettori; i metodi disponibili per farlo coprono una gamma altrettanto ampia, inclusi computer, smartphone, dichiarazioni di leader o celebrità, campagne online di

---

[150] V. PUTIN, "Солдат есть звание высокое и почетное" (trad. Il soldato è un grado onorevole e rispettato), discorso annuale all'Assemblea federale della Federazione russa, Krasnaya zvezda, 11 maggio 2006. Disponibile online sul sito ufficiale del Presidente della Federazione Russa: http://kremlin.ru/events/president/transcripts/23577 [ultimo accesso: 16.04.22].

[151] K. GILES, *Handbook of Russian Information Warfare*, *op.cit*., pp. 3-5.

[152] P. ANTONOVICH, "Cyberwarfare: Nature and Content," *Military Thought*, versione in inglese di East View information services, Vol. 20, n.3, 2011, pp. 35-43.

[153] HEICKERO R., *Emerging Cyber Threats*, *op.cit,* p. 20.

[154] Словарь терминов и определений в области информационной безопасности, Voyennaya Akademiya (trad. Dizionario dei termini e delle definizioni sulla sicurezza delle informazioni), General'nogo Shtaba, 2nd Edition, Moscow Voyeninform, 2008.

troll[155] financo ad arrivare a trasmettere popolari video su YouTube rivolti ad una pluralità di individui oppure approcci diretti a singoli obiettivi[156].

L'effetto complessivo di questi strumenti nel settore dell'informazione è ripetutamente descritto nelle fonti "ufficiali" russe[157] come in grado di affrontare compiti strategici molto ambiziosi.

Timothy Thomas, studioso statunitense dei principi di guerra dell'informazione russa asserisce, nel 1998, che i diversi prismi della Russia possono offrire conclusioni totalmente diverse sull'intento, lo scopo, la letalità o l'intrusione di un'operazione di informazione; questa logica può portare a nuovi metodi per attaccare obiettivi in modi del tutto non tradizionali e creativi[158]. Le armi informatiche sono una forma di moltiplicatore di forza che cambia il paradigma della stabilità strategica[159].

L'approccio occidentale alla difesa informatica si è tipicamente concentrato sulle risposte tecniche alle minacce tecniche, ignorando in gran parte l'interfaccia con la guerra dell'informazione; questo approccio è del tutto appropriato per alcune minacce, ma non sempre sufficiente per un orientamento olistico come quello adottato dalla Russia[160].

La guerra dell'informazione russa rappresenta una forma di *potere politico* e uno *strumento geopolitico* che consente un alto livello di

---

[155] Nel gergo di Internet, utente di una comunità virtuale, solitamente anonimo, che intralcia il normale svolgimento di una discussione inviando messaggi provocatori, irritanti o fuori tema.
[156] K. GILES, *Handbook of Russian Information Warfare*, *op.cit*., pp. 3-5.
[157] Qui si fa riferimento ai documenti come, ad esempio, le Dottrine militari già citate nel secondo capitolo di questo elaborato.
[158] T. THOMAS, "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations", *Journal of Slavic Military Studies*, Vol.11, n.1, 1998 pp. 40-62.
[159] Per un approfondimento su studi di strategia *Cfr*. L. BOZZO, Studi di strategia. Guerra, politica, economia, semiotica, psicoanalisi, matematica, EGEA Editore, Collana Alfaomega, 2012.
[160] P. MALDRE, *The Many Variants of Russian Cyber Espionage*, Atlantic Council, agosto 2015, online: www.atlanticcouncil.org/blogs/natosource/the-many-variants-of-russian-cyber-espionage [ultima visualizzazione online: 16.04.22].

manipolazione ed influenza, con una bassa probabilità di confronto militare.

Indubbiamente, molti attori che operano ad alti livelli d'imprenditoria, hanno fatto ricorso a tecniche di marketing digitale utilizzando l'analisi dei *Big Data* per scoprire schemi, relazioni e dipendenze per vendere i propri prodotti; nell'area della competizione strategica c'è una fessura ben definita delle opportunità che i *Big Data* forniscono per la classificazione comportamentale di individui e gruppi di persone[161]. Considerando ciò, uno Stato malintenzionato o un attore non statale può esercitare in modo non determinabile un certo tipo d'influenza su una grande porzione di persone e controllarne il comportamento [elettorale, ad esempio][162].

Analisi delle teorie sull'*InfoWar* nel pensiero militare russo

Il punto di vista russo su l'IW è stato influenzato dal dibattito sulla *Revolution in Military Affair* (RMA) [163] durante gli anni '80 e '90, così come dalla costruzione di alcuni concetti, ad esmpio quelli di *Network-Centric War* (NCW) ed *Hybrid Warfare*.

Gli strateghi di tutto il mondo studiano non solo le cause dei conflitti passati ma anche come prevederne e prepararne di nuovi[164]. La previsione della forma di guerre future aiuta a determinare quali capacità le nazioni richiedono per contrastare i potenziali avversari e

[161] V. OVCHINSKY, S. LARINA, & KULIK, Russia and the Challenges of the Digital Environment, *Russian International Affairs Council (RIAC)*, Mosca, 2015.
[162] *Ibidem*.
[163] M. MOWTHORPE, "The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views", *University of Hull*, vol. 5, n. 2, estate 2005. Gli elementi del RMA possono essere riassunti come attacchi di precisione, concetti di guerra guidata dalle informazioni, guerra di comando e controllo, e dominio dell'informazione sul campo di battaglia.
[164] T. THOMAS, *Russian Military Thought: Concepts and Elements*, MITRE Corporation, agosto 2019, p. 123.

quali problemi far emergere per inserirli ad una voce all'interno del bilancio. I pianificatori russi della guerra futura introducono nella loro analisi tendenze contemporanee che portano a previsioni specifiche su come potrebbe svolgersi una guerra futura e quali potrebbero essere i suoi contenuti[165]. Queste previsioni sono ulteriormente modellate dalla logica del contesto situazionale, come le condizioni geopolitiche o il potenziale di sfruttamento delle risorse, e vengono quindi prese in considerazione delle scelte, dei metodi e delle forme nuove per combattere conflitti futuri spesso col fine di determinare la correlazione tra tattiche, strategia e probabilità di vittoria[166].

Le previsioni sono la chiave per la pianificazione della guerra futura perché si traducono in scenari probabili da dover fronteggiare, ovvero valutarli nel tentativo di evitare i percorsi che non portano da nessuna parte e nell'accettare quelli che aiutano a evitare errori[167].

Reflexive control theory

L'uso della teoria del controllo riflessivo o *reflexive control* (RC), può essere usata contro processi decisionali sia umani che informatici[168]. Il concetto di RC esiste da molto più tempo rispetto al concetto russo di IW e di quello NATO di operazioni di informazione; infatti, è apparso nella letteratura militare sovietica 30 anni fa con V. A. Lefebvre, che definì il controllo riflessivo come un mezzo per trasmettere a un partner o un avversario informazioni che sono appositamente preparate per renderlo incline, volontariamente, a prendere la decisione

[165] *Ibidem*.
[166] *Ibidem*.
[167] S. G. CHEKINOV e S. A. BOGDANOV, "A Forecast of the Character and Content of a Future War: Problems and Judgements", *Military Thought*, versione in inglese di East View information services n. 10, 2015, p. 49.
[168] T. THOMAS, "Russia's 21st century information war: Working to undermine and destabilize populations", in *Defence Strategic Communications journal*, NATO Strategic Communications Centre of Excellence, vol. 1, n.1, inverno 2015, p. 14.

predeterminata e desiderata dall'iniziatore dell'azione. Questo può comportare l'uso di un falso pretesto per ottenere una risposta specifica da una terza parte e quindi ottenere una giustificazione per ulteriori azioni pianificate[169].

Nel 2011 è stato offerto un riferimento di una definizione militare in qualche modo nascosta di RC in un documento ufficiale del Ministero della Difesa Russo, intitolato "Visione Concettuale sulle attività delle forze armate della Federazione Russa nello spazio informazioni"[170]. In questo documento il termine "guerra dell'informazione" è stato definito come segue:

> "Conflitto tra due o più Stati nello spazio informazioni con l'obiettivo di infliggere danni a sistemi, processi e risorse di informazione, nonché a strutture e altre strutture di importanza critica; minare i sistemi politici, economici e sociali; realizzare campagne psicologiche di massa contro la popolazione di uno Stato al fine di destabilizzare la società e il governo; oltre a costringere uno Stato a prendere decisioni nell'interesse dei suoi avversari."[171]

L'ultima riga, "costringere uno Stato a prendere decisioni nell'interesse dei suoi avversari" è la chiave. Non vi è alcuna differenza tra questa affermazione e quelle delle definizioni offerte da molti teorici nel tempo. Nel 1974, ad esempio, K. V. Tarakonov affermò che "RC è inteso come il processo di una delle parti nel fornire ragioni al nemico da cui può logicamente dedurre la propria decisione, predeterminata dalla prima parte"[172].

RC è ampiamente utilizzato nella teoria della deterrenza[173]. Nel 2003 tre accademici dell'Accademia Russa di Scienze Militari[174] hanno notato che il controllo riflessivo dell'avversario mentre prende decisioni nel corso di un conflitto diventa una componente significativa dei concetti

---

[169] *Ivi*, p. 15.
[170] Documento analizzato in § 2 di questo elaborato.
[171] *Ibidem*.
[172] C. Reid, "Reflexive Control in Soviet Military Planning", in Brian D. Daily and Patrick J. Parker (a cura di), *Soviet Strategic Deception*, Lexington Books, 1987, p. 294.
[173] *Ibidem*.
[174] Gli autori sono: S. Yu. Malkov, V. I. Kovalev, e B. Konyakhin.

nucleari; lo scopo del controllo è convincere l'avversario dell'inutilità del ricatto nucleare e delle pressioni militari sul paese, dove la vittima si sforza di far capire all'aggressore che anche la parte attaccante subirà le conseguenze di un attacco[175].

Nel 2008, I. N. Vorobyov e V. A. Kiselev hanno scritto che le moderne operazioni strategiche stanno sottolineando il ruolo crescente del supporto psicologico-informativo alle forze armate, che accolgono come strumento strategico l'uso del controllo riflessivo impiegando complesse misure militari-politiche e diplomatiche per ingannare il nemico[176].

Le forze armate sovietiche e russe hanno studiato a lungo l'uso della teoria del controllo riflessivo, in particolare a livello tattico e operativo, sia a fini d'inganno e disinformazione sia per controllare potenzialmente i processi decisionali del nemico[177]. Un'importante teorico del controllo riflessivo nel settore militare è il Maggiore Generale N.I. Turko, un ex istruttore dell'Accademia dello Stato Maggiore della Federazione Russa[178] e, proprio Turko, ha menzionato il controllo riflessivo come metodo per raggiungere la superiorità geopolitica e come mezzo per i negoziati sul controllo degli armamenti[179].

Il maresciallo Nikolai Orgakov

Il maresciallo Nikolai Orgakov, capo di Stato Maggiore (sovietico) negli anni '80, e stato una delle prime persone a richiamare l'attenzione sul cambiamento della guerra, usando il termine *Military Technical Revolution* (MTR) al fine di descrivere il cambiamento fondamentale dagli

[175] T. THOMAS, *Russian Military Thought: Concepts and Elements*, MITRE Corporation, agosto 2019, p.140-144.
[176] I. N. VOROBYOV e V. A. KISELEV, "The Evolution of the Principles of Military Art", *Military Thought*, versione in inglese edita da Eastview Publications, n. 3, 2008.
[177] T. THOMAS, "Russia's 21st century information war", *op.cit.* p. 16.
[178] *Ibidem*.
[179] *Ibidem*.

eserciti di massa in operazioni guidate dalla tecnologia, soppiantato poi dall'uso di RMA da parte dei funzionari del Pentagono[180].

Alcuni analisti militari russi, in linea con la visione del maresciallo Orgakov, hanno riconosciuto che le tecnologie dell'informazione potrebbero essere utilizzate come formidabili armi del secolo XXI, perfino paragonabili alle armi di distruzione di massa[181]. La Guerra del Golfo del 1990-91 venne dichiarata come la prima operazione tecnica; usando la guerra di comando e controllo, le forze della coalizione riuscirono a distruggere totalmente le infrastrutture di comunicazione irachene. È stato il campanello d'allarme, suonato alla Russia, per cambiare le Dottrine in essere, dato che gran parte dell'equipaggiamento militare iracheno era di fabbricazione sovietica[182].

La guerra in Afghanistan del 1979-89, la guerra in Cecenia del 1994-96 e quella del '99 hanno influenzato la mentalità russa e hanno portato a conoscenze pratiche ed approfondimenti sull'approccio russo all'IW[183]. Da un punto di vista psicologico della guerra, la Russia ha sofferto gravi problemi in Afghanistan e non è riuscita a influenzare i suoi avversari[184].

Il maggiore generale Ivan Vorobyev

Facendo un salto in avanti per arrivare a tempi più recenti[185], troviamo un articolo del maggiore generale in pensione Ivan Vorobyev,

---

[180] M. MOWTHORPE, "The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views", *University of Hull*, vol. 5, n. 2, estate 2005.
[181] HEICKERO R., *Emerging Cyber Threats*, *op. cit*, pp. 12-17.
[182] *Ibidem*.
[183] T. THOMAS, *Manipulating the Mass Consciousness: Russian & Chinese information war. Tactics in the second Chechen–Russian conflict*, aprile 2003, accessibile online: http://call.army.mil/fmso/fmsopubs/issues/chechiw.htm [ultimo accesso online: 16.04.22].
[184] Yu. SEROOKIY, "Psychological-Information Warfare: Lessons of Afghanistan", *Military Thought*, versione in inglese edita da Eastview Publications, vol. 13 n. 1, 2004.
[185] Si salta l'analisi del pensiero militare sovietico e quello dei primi anni del 2000 poiché non è oggetto di questo studio ricreare il processo storico del pensiero militare russo, ma per approfondimenti in merito, si rimanda alle seguenti letture: *Cfr*. I. A. KOROTKOV, *The History of Soviet Military Thought*, Mosca, 1980, *Cfr*. anche F. F. GAIVORONSKY e M. I. GALKIN, *The Culture of Military Thought*, Mosca, 1991.

pubblicato nel 2007[186]. I suoi contributi in merito alla teoria militare sono stati ampiamente elogiati dai suoi colleghi di *Military Thought*[187], quindi non si è avventati nell'affermare che la prospettiva avanzata da Vorobyev ha molto peso nella comunità militare russa.

Qualificando la moderna guerra dell'informazione, Vorobyev fa riferimento alla guerra del Golfo del 1991 per sostenere quanto sia importante una preventiva ed acuta valutazione dei sistemi di comando e del controllo del nemico assieme ai sistemi d'arma al fine di trovare un "ventre molle" da attaccare sia per via cinetica che elettronica[188]. Vorobyev è un sostenitore di una mentalità molto tradizionale e strettamente militare, che non tiene conto degli attori civili o degli aspetti economici e sociali nell'equazione militare. Per Vorobyev, l'aspetto nuovo e importante è che il nemico può essere combattuto non solo con un attacco cinetico e una manovra spaziale, ma anche negandogli l'accesso alle informazioni corrette[189].

Per fare questo, Vorobyev definisce un concetto triplice di attacco o shock di informazioni [informatsionnyi udar][190]:

1- attacco psicologico, disinformazione e inganno del nemico;
2- attacco psicotropico, che colpisce la psiche del nemico con mezzi speciali;
3- attacco informatico, che colpisce i computer nel sistema di comando e controllo del nemico.

---

[186] I. N. VOROBYEV, "The information shock operation", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2007, pp.14–21. Vorobyev è considerato, dai più, un uomo che ha dato un importante contributo alla teoria militare russa. Egli ha insegnato e fatto ricerca su tattiche e arte operativa per decenni, a seguito di una illustre carriera militare.
[187] Cfr. *Military Thought,* versione in inglese edita da Eastview Publications, n. 6, 2012.
[188] I. N. VOROBYEV, "The information shock operation", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2007, pp.14–21.
[189] U. FRANKE, *War by non-military means*, *op.cit.* p. 23.
[190] I. N. VOROBYEV, The information shock operation. *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2007, pp.14–21.

È interessante osservare qui che l'opinione proposta da Vorobyev è sorprendentemente simile a quella proposta della NATO circa 20 anni fa, ma da allora, la visione della NATO si è evoluta e ora distingue l'attuale concetto di "operazioni di informazione" dalla "guerra di comando e controllo" C2W: "Info Ops non è né una continuazione di Command and Control Warfare (C2W), né sostituisce C2W. [...] C2W è un tipo specifico di operazione – Info Ops è una funzione del personale"[191].

Egli afferma: "Dato che ci sono molte forze di diverso tipo coinvolte nella conduzione della guerra dell'informazione, è necessaria un'organizzazione per un coordinamento preciso"[192]. È evidente che ciò che Vorobyev ha in mente è una guerra convenzionale simmetrica tra attori statali, ed in effetti, il concetto di "Information Troops" avanzato da alcuni esperti, in primis K. Giles, sulla scia della guerra georgiana nel 2008, era probabilmente orientato proprio verso questo tipo di guerra dell'informazione[193].

Il maggiore generale Saifetdinov

Nel luglio 2014 il maggiore generale in pensione Saifetdinov[194] ha pubblicato un articolo che indaga sulla guerra delle informazioni nel regno militare[195]. Saifetdinov osserva che nel mondo moderno, le informazioni possono essere utilizzate per raggiungere obiettivi politici, economici, militari e di altro tipo, e concorda ampiamente con i documenti ufficiali – ad esempio la dottrina militare del 2010 – secondo

[191] U. FRANKE, *War by non-military means*, *op.cit.* p. 23.
[192] I. N. VOROBYEV, "The information shock operation". *Op.cit.* pp.14–21.
[193] K. GILES, "Information Troops – A Russian Cyber Command?" in *3rd International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2011, pp. 45-60.
[194] Dopo la sua carriera come ufficiale di artiglieria, egli ha prestato servizio presso l'Accademia militare dello stato maggiore e ha diretto il 27° Istituto centrale di ricerca e sviluppo del Ministero della difesa, supervisionando gli impegni di ricerca sui sistemi di comando e controllo e esercitazioni militari assistite da computer.
[195] K.I. SAIFETDINOV, "Information warfare in the military realm", *Military Thought*, versione in inglese edita da Eastview Publications, n. 7, 2014, pp. 38–41.

cui l'uso della guerra dell'informazione insieme alle tradizionali operazioni militari sta diventando più comune. Ad esempio, cita non solo la guerra del Golfo del 1991 e l'Operazione Iraqi Freedom nel 2003, ma anche gli eventi in Ucraina nel 2014. Saifetdinov, inizia elencando nel suo articolo gli effetti che possono essere raggiunti dalla guerra delle informazioni, e lo fa seguendo due principi: in primo luogo, i sistemi di comando e controllo possono essere degradati, interrompendo la capacità della leadership politica e militare di lavorare insieme e ingannando la loro percezione in modo che non siano in grado di agire come responsabili delle decisioni; in secondo luogo, le operazioni psicologiche possono essere condotte contro la popolazione in generale o contro i singoli decisori[196].

Egli tende a far emergere non solo che la guerra di informazione, consapevolmente guidata, sia un fattore decisivo in un conflitto militare, ma anche che, l'uso dell'*information warfare* può essere un modo per evitare conflitto militare aperto.

L'Ufficiale in pensione sostiene inoltre, che: "la guerra delle informazioni deve essere condotta continuamente in tempo di pace, in periodi di crescenti minacce e in tempo di guerra con tutte le forze disponibili"[197].

L'uso di tutte le forze disponibili sottolinea il fatto che la guerra dell'informazione non è esclusivamente di competenza del militare, ma piuttosto richiede un approccio multi-vettore. In effetti, la necessità di uno stretto coordinamento è al centro della visione di Saifetdinov sui principi su come raggiungere gli obiettivi della guerra delle informazioni. In tempo di pace, sostiene Saifetdinov, la guerra dell'informazione deve

[196] *Ibidem*.
[197] *Ivi*, p. 39.

sostenere gli obiettivi fissati dal livello politico ed essere condotta per "aumentare l'efficacia dei mezzi politici, diplomatici, economici, legali e militari per garantire la sicurezza nazionale della Federazione Russa, ed è di primaria importanza per assolvere il compito di deterrenza strategica"[198].

Aleksandr Gorbenko

Di contrasto risulta essere utile analizzare la prospettiva operativa principalmente militare di Vorobyev e Saifetdinov con la prospettiva strategica più ampia, offerta da Aleksandr Gorbenko nel 2009 nella sua tesi di dottorato presso l'Università militare[199]. Il suo argomento di tesi era: "la guerra dell'informazione nella politica degli stati moderni"; egli identifica cinque aree nell'ambito dell'arena dell'informazione:

1- i sistemi per prendere ed eseguire decisioni governative;
2- le risorse informative delle agenzie governative e dei mass media;
3- lo stato morale e psicologico della popolazione in generale e di coloro che prestano servizio nel settore della sicurezza in particolare;
4- l'infrastruttura informativa (reti, nodi di comunicazione ecc.);
5- i sistemi di informazione, comunicazione e controllo (ad es. in impianti industriali). Ancora una volta, questo ricorda il punto di vista espresso nei documenti ufficiali[200].

[198] *Ivi*, p. 40.
[199] A. N. GORBENKO, *Informatsionnoe protivoborstvo v politike sovremennykh gosudarstv* (trad. *Guerra dell'informazione nella politica degli stati moderni*), Tesi di dottorato, Università Militare, Mosca, 2009. Disponibile online: http://www.dslib.net/polit-instituty/informacionnoe-protivoborstvo-v-politike-sovremennyh-gosudarstv.html [ultimo accesso: 16.04.22].
[200] *Ibidem*.

I colonnelli Sergei Bazylev, Igor Dylevskii, Sergei Komov e Aleksandr Petrunin

Un altro contributo è offerto dai colonnelli Sergei Bazylev, Igor Dylevskii, Sergei Komov e Aleksandr Petrunin[201]. Gli autori si attengono molto accuratamente al documento circa le "Opinioni concettuali sulle attività delle forze armate della Federazione Russa nello spazio delle informazioni". Il loro articolo è essenzialmente una versione abbreviata delle opinioni concettuali.

Bazylev et al. identificano due effetti principali della guerra delle informazioni. In primo luogo, gli attacchi a sistemi di infrastrutture critiche come ad esempio l'industria, la finanza, l'energia ed i trasporti, possono portare al collasso del sistema finanziario o a crisi economiche a livello di sistema. In secondo luogo, gli attacchi possono essere utilizzati per far crollare la leadership politica e/o militare, demoralizzare, corrompere o imbrogliare la popolazione creando caos generalizzato[202]. Ancora una volta, questo articolo riprende gli argomenti trattati nelle dottrine analizzate nel capitolo precedente. Un punto ancor più interessante è quanto dichiarano gli autori in merito alle armi di distruzione di massa. Non sorprende, sostengono Bazylev et al., che i capi di Stato dell'Organizzazione per la Cooperazione di Shanghai (OCS) abbiano dichiarato che l'uso di armi informative può avere conseguenze alla pari con l'uso di armi di distruzione di massa[203].

---

[201] S. I. BAZYLEV, I. N. DYLEVSKII, S. A. KOMOV, e A. N. PETRUNIN, "Activities of the Armed Forces of the Russian Federation in the information space: principles, rules, confidence building measures", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2012, pp. 25–28. Bazylev lavora presso la direzione delle operazioni principali dello Stato maggiore, Dylevskii, Komov e Petrunin sono esperti assegnati al ministero della Difesa, operando nel settore della sicurezza internazionale delle informazioni.
[202] *Ibidem*.
[203] *Ibidem.*

Il colonnello Anatolii Streltsov

Considerando che Vorobyev, Saifetdinov e Bazylev et al. tutti discutono della guerra delle informazioni in un contesto militare, il colonnello in pensione Anatolii Streltsov adotta un ambito strategico più ampio, simile al pensiero di Gorbenko[204]. Streltsov, non solo è stato assegnato al Consiglio di Sicurezza Nazionale russo dal 1995, ma è anche autore di numerosi libri autorevoli sulla strategia di sicurezza delle informazioni del governo e consulente presso l'Istituto per le questioni di sicurezza delle informazioni dell'Università statale di Mosca (Lomonosov). È una figura molto influente ed inoltre punto di riferimento per l'establishment della sicurezza nazionale russa in merito alla guerra dell'informazione[205].

L'articolo del 2011 di Streltsov è una dichiarazione completa e autonoma della visione russa della guerra strategica delle informazioni e pur attenendosi strettamente ai documenti ufficiali, per quindi ribadire tali posizioni, Streltsov tenta anche di offrire loro basi legali, filosofiche e di scienze sociali.

In partenza egli enfatizza una visione del mondo intrisa di realismo politico, una visione che ricorda la già citata "strategia di sicurezza nazionale del 2009"[206]. Streltsov sostiene che in un mondo con crescenti tensioni, colmo di disparità economiche e con un uso preponderante della tecnologia dell'informazione, la guerra informatica globale [globalnoe informatsionnoe protivoborstvo] diventa uno dei fenomeni

---

[204] A. A. STRELTSOV, "The main tasks for government policy in information warfare". *Military Thought*, versione in inglese edita da Eastview Publications, n.5, 2011, pp.18–25.
[205] U. FRANKE, *War by non-military means*, *op.cit.* p. 26.
[206] La "strategia per la sicurezza nazionale della Federazione Russa fino al 2020" è stata approvata con decreto del Presidente della Federazione Russa e pubblicata il 12 maggio del 2009 n.537. *Cfr*. sito internet del "NATO Cooperative Cyber Defence Centre of Excellence", document disponibile in versione inglese al seguente link: https://ccdcoe.org/library/strategy-and-governance/?search=russia [ultima consultazione online: 16.04.22].

più importanti degli affari internazionali[207]. Streltsov Continua affermando che esiste una contraddizione tra: l'interesse nazionale dei paesi a cercare di influenzare i processi decisionali politici di altri paesi in modo favorevole a sé stessi e i principi di indipendenza e sovranità consacrati nella Carta delle Nazioni Unite[208]. Non sorprende che le c.d. "rivoluzioni colorate", avvenute in alcune delle ex repubbliche sovietiche, siano menzionate come esempi di tale ingerenza illegittima da parte di forze esterne negli affari di altri paesi. Da questo ragionamento, Streltsov propone di sancire come prioritarie le politiche del governo nella guerra dell'informazione in merito alla sicurezza nazionale, "sulla base di generalizzazioni da scienze politiche ed esperienza pratica"[209].

Il principale compito del governo nella guerra dell'informazione, sostiene Streltsov, è quello di contrastare i tentativi di attori illegittimi di utilizzare l'ambiente dell'informazione [informatsionnaia sfera] per influenzare la politica nazionale in modo illegale; ovvero utilizzando due modi: la guerra dell'informazione senza l'uso forzato della tecnologia, vale a dire nell'area dell'ideologia politica [nella sfera cognitiva]; e la guerra dell'informazione con l'uso della tecnologia, cioè nell'area della tecnologia dell'informazione [nel ciberspazio]. Questi due modi sono realizzati attraverso tre direttrici operative che vengono delineate nell'articolo[210]:

1- la guerra delle informazioni politiche;
2- la guerra delle informazioni tecniche;

---

[207] A. A. STRELTSOV, "The main tasks for government policy in information warfare". *Military Thought*, versione in inglese edita da Eastview Publications, n.5, 2011, pp. 18-19.
[208] *Ibidem*.
[209] *Ibidem*.
[210] *Ibidem*.

3- l'approvvigionamento di informazioni sulla politica del governo.

La guerra di informazione politica [politicheskoe informatsionnoe protivoborstvo] comporta innanzitutto la neutralizzazione o la riduzione del pericolo di diffusione di convinzioni ideologiche o religiose dannose, oppure minacce in merito alla disinformazione sulla politica statale nella sfera pubblica nazionale o internazionale[211]. La guerra dell'informazione politica, secondo Streltsov, è esercitata nell'ambito del c.d. *soft power* [miagkaia sila]. Nel contesto internazionale, questo termine è stato originariamente coniato da J. Nye nel suo celebre articolo del 1990[212], ma l'uso russo del termine è chiaramente diverso e più aggressivo. È interessante notare che il termine *miagkaia sila* potrebbe ugualmente tradursi in forza dolce, un termine che potrebbe riflettere più accuratamente la percezione russa.

Streltsov elabora un elenco di tre compiti principali da seguire per mitigare i danni della guerra delle informazioni politica:

1- identificare e fermare la propaganda ideologica dannosa;
2- stimolare la società civile a contrastare la propaganda ideologica dannosa;
3- fermare la disinformazione sulla politica statale.

Per quanto riguarda la guerra delle informazioni tecniche, osserva che l'obiettivo principale di questa pratica è quello di costringere gli

[211] *Ivi*, p. 20.
[212] J. NYE, "Soft Power", *Foreign Policy*, n. 80, autunno 1990, pp. 153-171. Disponibile online: https://www.jstor.org/stable/1148580?seq=1#metadata_info_tab_contents [ultimo accesso: 16.04.22].

attori politici illegittimi ad osservare e quindi ad ottemperare al diritto internazionale, più precisamente alla non ingerenza[213].

Per quanto riguarda l'approvvigionamento di informazioni sulla politica del governo, egli la definisce come il supporto delle informazioni alla politica del governo [informatsionnoe obespechenie gosudarstvennoi politiki] che comporta il conseguimento del sostegno della società nazionale e della comunità internazionale per le attività nell'ambito di tale politica e la cooperazione nella sua attuazione. Streltsov suddivide questo compito in due sotto-compiti:

1- mantenere un'immagine positiva dello stato [obespechenie pozitivnogo imidzha gosudarstva];
2- assicurarsi che la comunità sia informata delle azioni intraprese nell'ambito della politica statale[214].

Gli aspetti importanti del mantenimento di un'immagine positiva internamente includono l'immagine dei suoi leader, ciò che viene insegnato nelle scuole, non ultimo per quanto riguarda la forma del dibattito pubblico; mentre per la questione di come lo Stato viene percepito all'estero, vi include ancora le opinioni di persone influenti in altri paesi, da come viene insegnata la storia e altre materie all'interno delle discipline umanistiche e da come viene trattato lo Stato nei media stranieri. Mantenere la comunità informata sulle azioni intraprese, significa secondo Strelsov: ancora una volta la costruzione di un'immagine positiva della storia nazionale, ma anche la dimostrazione di come la leadership politica abbia effettivamente risolto problemi

[213] A. A. STRELTSOV, "The main tasks for government policy in information warfare". *Military Thought*, versione in inglese edita da Eastview Publications, n.5, 2011, p. 22.
[214] *Ibidem*.

specifici. Se questo compito viene risolto con successo, i sentimenti positivi della comunità nazionale e internazionale aiuteranno a mantenere la stabilità sociale all'interno della popolazione[215]. Al fine di diffondere il messaggio di politiche governative di successo, le agenzie che dipendono dal governo ed i funzionari dovranno cooperare intimamente con i mass media e la società civile[216].

Streltsov conclude il suo articolo ribadendo che i compiti così definiti sono necessari per l'indipendenza e la sovranità nazionale nella moderna società globale dell'informazione[217].

Il colonnello Chekinov ed il tenente Bogdanov

È interessante notare come la guerra dell'informazione può essere collocata in un contesto più ampio, ovvero: Il colonnello Chekinov ed il tenente Bogdanov affrontano la guerra dell'informazione utilizzando il concetto di approccio indiretto [nepriamye deistviia][218]. Gli autori sono entrambi affiliati al *Center for Military Strategic Studies of the General Staff*[219], che è diretto da Chekinov[220]. Secondo l'analisi dei due, l'approccio indiretto sta diventando sempre più importante nel mondo moderno, essi sostengono che: mentre l'approccio indiretto è stato storicamente secondo a quello diretto della forza e delle armi, nel mondo attuale l'approccio indiretto sta diventando sempre più il primo e principale strumento dello stratega principale[221]. Non sorprende che il loro primo esempio sia la politica degli Stati Uniti e di altri paesi NATO,

---

[215] *Ibidem*.
[216] U. FRANKE, *War by non-military means*, *op.cit.* pp. 28-29.
[217] A. A. STRELTSOV, "The main tasks for government policy in information warfare", *op.cit.*, pp. 25.
[218] S.G. CHEKINOV, e S.A. BOGDANOV, "The influence of indirect actions on the character of modern war", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2011, pp. 3–13.
[219] *Cfr*. il sito online del centro di studi: http://militaryarticle.ru/voennaya-mysl/2010-vm/10353-centr-voenno-strategicheskih-issledovanij [ultimo accesso: 16.04.22].
[220] Stando così le cose, si comprende bene che la loro analisi dovrebbe avere un peso considerevole quando si tenta di comprendere la prospettiva russa sulla guerra dell'informazione.
[221] S.G. CHEKINOV, e S.A. BOGDANOV, "The influence of indirect actions on the character of modern war", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2011, pp. 3–13.

descritta come: obiettivi aggressivi che vengono mascherati dietro la pretesa di diffondere democrazia, proteggere i deboli o contrastare il terrorismo internazionale[222].

L'approccio indiretto in guerra può essere approssimativamente descritto come segue. Non attaccare il nemico dove è più forte, ma dove è più debole, fallo con sorpresa e manovre rapide, cercando continuamente opportunità inattese per l'attacco[223]. Chekinov e Bogdanov descrivono l'idea riferendosi a Sun Tzu e Napoleone, ma prima di tutto citano il generale britannico Liddell Hart, a cui di solito viene attribuita l'idea moderna di *indirect approach*, se si preferisce il termine anglosassone. Liddell Hart sosteneva che una guerra con manovre e attacchi inaspettati diretti – con azioni sia psicologiche che cinetiche – alle debolezze nemiche, avrebbero portato alla vinttoria della battaglia prima che iniziasse[224]. Chekinov e Bogdanov sostengono che, mentre l'inganno è sempre stato usato in guerra, nel mondo moderno, i mezzi di influenza delle informazioni [sredstva informatsionnogo vozdeistviia] si sono sviluppati al livello in cui possono effettivamente svolgere compiti strategici da soli[225]. Infatti, mentre Liddell Hart confina l'azione indiretta principalmente all'interno del tradizionale contesto militare[226], Chekinov e Bogdanov esplorano il suo uso nel più ampio contesto delle relazioni internazionali in senso lato, facendo eco alla formulazione dei documenti ufficiali, sostengono l'importanza della guerra dell'informazione[227]: l'esperienza delle guerre locali e dei conflitti

---

[222] *Ibidem*.
[223] U. FRANKE, *War by non-military means*, *op.cit.* pp. 38-39.
[224] *Ibidem*.
[225] S.G. CHEKINOV, e S.A. BOGDANOV, "The influence of indirect actions on the character of modern war", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2011, pp. 3–13.
[226] A. DANCHEV, "Liddell Hart and the Indirect Approach", *The Journal of Military History*, Vol. 63, n. 2 aprile 1999, pp. 313-337. Accessibile online: https://www.jstor.org/stable/120646 [ultimo accesso: 16.04.22].
[227] S.G. CHEKINOV, e S.A. BOGDANOV, "The influence of indirect actions on the character of modern war", *op.cit.*, p 6.

armati degli ultimi decenni mostra che la guerra dell'informazione strategica [strategicheskoe informatsionnoe protivoborstvo] svolge un ruolo importante nel perturbare la leadership militare, quella di governo, i sistemi di difesa aerei e spaziale, fuorviando il nemico, formando opinioni pubbliche controllate, organizzando attività contro governi e condurre altre misure per ridurre la volontà dell'avversario di resistere[228].

In particolare, Chekinov e Bogdanov sostengono che i fattori combinati della globalizzazione e l'avvento della moderna tecnologia dell'informazione hanno creato legami economici strettamente integrati – compresi i flussi globali di risorse, tecnologia, denaro, informazioni, ecc. – tra paesi diversi e, mentre questa interdipendenza viene spesso considerata come un fattore che favorisce la pace e la stabilità, Chekinov e Bogdanov la vedono [giustamente] piuttosto come una minaccia alla sicurezza nazionale[229]. La globalizzazione e l'IT aprono nuove strade per le operazioni d'influenza. Oltre all'approccio indiretto, nell'importante rivista militare russa *Military Thought*, nel 2013, Bogdanov e il. Chekinov hanno posto la loro attenzione sul concetto di *New Generation of War* (NGW)[230]. La loro discussione è stata ampia e profonda, essi descrivevano chiaramente NGW come un modo in cui altre nazioni stavano conducendo una guerra contro la quale la Russia doveva essere pronta a rispondere[231]. Bogdanov e Chekinov sembravano riaffermare molti dei pensieri del tenente generale in pensione (ora deceduto) Vladimir Slipchenko, che fu la forza trainante del nuovo pensiero in

[228] *Ibidem*.
[229] U. FRANKE, *War by non-military means*, *op.cit.* p. 40.
[230] CHEKINOV e S. A. BOGDANOV, "The Nature and Content of a New-Generation of War", *Military Thought*, East View information services, n.4, 2013, pp. 13-24.
[231] *Ivi*, p. 18-19.

Russia negli anni '90 e nella prima parte del secolo successivo[232]. Egli scrisse spesso su quella che chiamava "guerra di sesta generazione", o guerra senza contatto, che si sarebbe basata su armi ad alta tecnologia e sistemi in grado di essere manovrati da piccoli gruppi di persone[233]. nel 2013, l'articolo di Slipchenko è apparso postumo nella rivista militare russa, dove discuteva la descrizione di Slipchenko sulla guerra planetaria e di molti altri concetti di guerra di nuova generazione[234].

Il generale Kartapolov

Tuttavia, poiché il termine NGW è quasi completamente scomparso dalle pubblicazioni militari russe, è necessario concentrarsi maggiormente sul lavoro dei membri più importanti del Generale Staff: Kartapolov e in particolare modo sul gen. Gerasimov. Essi utilizzano un termine differente, ovvero *New type of War* (NTW) che sembra descrivere il carattere in evoluzione della guerra, mentre NGW potrebbe essere più probabilmente un riferimento a un metodo di guerra (l'esercito russo considera i "metodi" come composti da armi e arte militare)[235].

Kartapolov ha descritto la NTW come qualcosa che sia l'Occidente che la Russia stavano studiando e per quanto riguarda la Russia, ha osservato che sono in fase di sviluppo forme e metodi non regolari per l'impiego delle Forze Armate e che questi sviluppi, renderanno possibile livellare la superiorità tecnologica del nemico[236]. Questo è uno dei motivi se non il motivo principe per pensare ad una condotta della guerra di nuovo tipo che utilizza metodi "asimmetrici" per affrontare il nemico, privilegiando il periodo iniziale della guerra se non addirittura

---

[232] T. THOMAS, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking", *Journal of Slavic Military Studies*, Vol. 29, n. 4, 2016, pp. 555-556.
[233] *Ibidem*.
[234] *Ibidem.*
[235] *Ibidem.*
[236] *Ibidem*.

il periodo di pace[237]. Bogdanov e Chekinov hanno discusso dell'importanza di ottenere la superiorità delle informazioni su l'avversario, specialmente se si vuole avere un vantaggio generale nel periodo iniziale di guerra (IPW) con l'intenzione di vincere la guerra prima ancora che si scateni il conflitto[238], proprio come sosteneva lo stratega Sun Tzu parecchi anni addietro, con due citazioni significative: "I guerrieri vittoriosi prima vincono e poi vanno in guerra, mentre i guerrieri sconfitti prima vanno in guerra e poi cercano di vincere"; "Il meglio del meglio non è vincere cento battaglie su cento bensì sottomettere il nemico senza combattere."[239]

Mentre l'enfasi dello Stato Maggiore fa apparire che la NTW abbia preso il primato nel pensiero militare russo, il concetto di NGW dovrebbe essere sempre presa in considerazione, poiché i due ufficiali hanno espresso in modo molto adeguato l'importanza delle informazioni e degli aspetti economici della conduzione del futuro guerra.

Il generale V. Gerasimov

Per quanto riguarda il generale V. Gerasimov possiamo dire che ha guidato un ringiovanimento del pensiero militare in Russia, motivando professori e istruttori a formare ufficiali dell'Accademia dello staff generale (ASG) in modo da usare le loro conoscenze per sviluppare nuovi concetti nell'arte militare, nelle forme e nei metodi di combattimento[240] ma, in somma, ha seguito la linea dettata dal piano che il presidente Putin ha ideato e attuato con decreto nel maggio

[237] *Ibidem.*
[238] CHEKINOV e S. A. BOGDANOV, "The Nature and Content of a New-Generation of War", *op.cit.,* pp. 13-24.
[239] SUN TZU, *L'arte della guerra,* prima ed. Neri Pozza Editore, Vicenza 1999, Nona ed. 2013.
[240] T. THOMAS, *Russian Military Thought: Concepts and Elements*, MITRE Corporation, agosto 2019, p.150-152.

2012[241]. Gli sviluppi prioritari di Putin, nell'ordine in cui sono stati elencati nel decreto erano: le forze dissuasive nucleari; i sistemi di difesa aerea e spaziale; i sistemi di comunicazione, ricognizione, comando e controllo e guerra elettronica; i veicoli aerei senza equipaggio (UAV); i sistemi di attacco robotizzati; la moderna aviazione di trasporto; le armi di precisione e mezzi per combatterle; i sistemi per la protezione individuale del personale di servizio[242].

Si può notare come il generale Gerasimov si sia attenuto al decreto del maggio 2012 attraverso l'analisi dei suoi discorsi tenuti nel corso degli anni. Discorsi che tra febbraio e marzo si tengono annualmente in forma di assemblea generale presso l'Accademia di Scienze militari russa (ASM) dove, il presidente dell'Accademia e generale dell'esercito Makhmut Gareyev apre la conferenza e Valery Gerasimov è, sempre, l'oratore in primo piano[243].

Gerasimov ha comandato distretti militari, prestato servizio in Cecenia, organizzato e guidato operazioni in Ucraina e Siria, ha stimolato il corpo degli ufficiali, i professori e gli accademici per aggiornare il pensiero militare, identificare tendenze e quindi minacce alla Russia, proposto nuove teorie di strategia e guerra asimmetrica, ha parlato di un nuovo tipo di guerra, e si è riferito alla guerra ibrida solo quando si parlava di Occidente e, in particolare, Stati Uniti. I numerosi discorsi tenuti dal generale Gerasimov presso l'Accademia di Scienze Militari, offrono una panoramica del pensiero militare russo in merito all'*information warfare*, e ci sono numerosi aspetti che riprendono le

---

[241] Decreto del Presidente della Federazione Russa n. 603 "Sull'attuazione di piani (programmi) per la costruzione e lo sviluppo delle Forze armate della Federazione Russa, altre truppe, unità e corpi militari e la modernizzazione del complesso militare-industriale" n. 603, 05.05.2012, *Cfr*. il "Portale Internet ufficiale informazioni legali Sistema statale di informazione" legale per la versione ufficiale in lingua russa: http://publication.pravo.gov.ru/Document/View/0001201205070021 [ultimo accesso: 16.04.22].

[242] *Ibidem*.

[243] T. THOMAS, *Russian Military Thought: Concepts and Elements*, MITRE Corporation, agosto 2019, p.150-152.

linee guida dei documenti ufficiali. In questi discorsi pubblici il generale Gerasimov ha richiesto lo sviluppo di nuove forme e metodi di guerra, sia che si tratti di affrontare le capacità di guerra ibrida dell'Occidente che di azioni terroristiche. Inoltre, ha sottolineato la necessaria collaborazione con il complesso militare-industriale poiché occorre sviluppare armi basate su nuovi principi fisici che serviranno sia da contrapposizione alle armi ad alta tecnologia di un avversario che ad assicurare l'implementazione di una deterrenza strategica non nucleare per la Russia rispetto ai potenziali avversari.

L'InfoWar nelle scuole di pensiero russe di geopolitica

La guerra dell'informazione ed il contesto geopolitico sono strettamente correlati, poiché la dottrina geopolitica tratta le informazioni come un'arma pericolosa: è economica, è un'arma universale, ha una portata illimitata, è facilmente accessibile e permea tutti i confini degli stati senza restrizioni[244]. Le lotte informative e di rete, ma più frequentemente la lotta psicologico-informativa, sono mezzi che lo stato usa per raggiungere i suoi obiettivi nella politica internazionale, regionale e domestica, per ottenere un vantaggio geopolitico[245]. I rappresentanti russi del pensiero geopolitico divulgano questo argomento e, partecipano in prima persona alla guerra dell'informazione come tecnologi politici[246] e *opinion leader*[247]. Ciò riguarda in particolare i rappresentanti chiave delle due scuole

[244] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p. 13.
[245] *Ibidem*.
[246] Un tecnologo politico è uno specialista nell'applicazione pratica di tecnologie politiche, gestione politica, campagne di costruzione di immagini e campagne elettorali. "Tecnologia politica" - un termine ampiamente sconosciuto in Occidente - è l'eufemismo comunemente usato negli ex stati sovietici per quella che è ormai un'industria altamente sviluppata di manipolazione politica. Per un maggior approfondimento sulla materia, *Cfr*. A. WILSON, *Virtual Politics: Faking Democracy In The Post-Soviet World*, Yale University Press, 2005.
[247] Ad esempio *Cfr*. I. PANARIN, "Information War against Russia", RT, 30 dicembre 2011, disponibile: http://rt.com/politics/information-war-russia-panarin-009/ [ultimo accesso: 16.04.22].

geopolitiche russe[248]: Igor Panarin[249] e Aleksandr Dugin[250], insegnanti accademici e mentori delle giovani generazioni di geopolitici russi[251]. Hanno collegamenti evidenti ai servizi segreti e vedono le mosse dell'avversario come azioni organizzate e più sofisticate di quelle usate durante il periodo della Guerra Fredda; sono sia teorici che professionisti della guerra dell'informazione: prendono parte attiva a programmi di analisi politica su Channel One, Rossiya, NTV, Ren-TV e TV RT[252], e anche alla radio (Panarin, per esempio, è ospite fisso in due radioprogrammi "Politica globale" e "La finestra sulla Russia" trasmessi dalla stazione radio *Voice of Russia*, dove commenta gli affari correnti nella politica internazionale)[253].

La scuola di pensiero "Panarin"

I primi scritti del professor Igor Panarin dell'Accademia Diplomatica del Ministero degli Affari Esteri della Federazione Russa[254] hanno posto

---

[248] *Cfr*. O. FREEDMAN, "The Russian Perspective on Information Warfare: conceptual roots and politicisation in russian academic, political, and public discourse", *Defence Strategic Communications Journal*, NATO Strategic Communications Centre of Excellence, Lettonia, Vol. 2, 2017, pp. 61-87.

[249] Igor Panarin, nato nel 1958, ha conseguito un dottorato in scienze politiche ed uno in psicologia, membro dell'Accademia di scienza Militare della Federazione Russa e numerosi altri organi di esperti associati al presidente e al Consiglio della Federazione. Ha iniziato la sua carriera professionale nel KGB dell'Unione Sovietica nel 1976. Dopo il 1991, ha lavorato presso la FAPSI. Nel 1999–2003 è stato a capo del dipartimento analitico del Comitato elettorale centrale. Attualmente è professore all'Accademia Diplomatica del Ministero degli Affari Esteri della Russia. Insegna anche presso MGIMO e l'Accademia presidenziale russa di economia nazionale e pubblica amministrazione. ha pubblicato più di 20 libri e centinaia di articoli, commenti e interviste, la maggior parte dei quali si concentra sulle sfaccettature psicologiche della guerra in generale e sulla guerra dell'informazione in particolare.

[250] Aleksandr Dugin, nato nel 1962, politologo, geopolitico, filosofo e storico della religione. Agli inizi degli anni '90 è stato caporedattore delle riviste Elementy e Milyi Angel e direttore del manifesto della casa editrice Arctogeia. professore presso il dipartimento di sociologia e filosofia dell'Università Lomonosov di Mosca (è stato rimosso dalla sua posizione all'Università dopo aver chiesto l'uccisione di nazionalisti ucraini), direttore del Center for Conservative Studies dell'Università di Mosca. Ha scritto più di dieci libri e centinaia di articoli pubblicati sulla stampa russa e straniera. È un rappresentante di spicco della geopolitica russa. Ha ricoperto diversi incarichi di consulenza senior nell'establishment politico russo ed è il principale ideologo del tradizionalismo integrale, dell'eurianesimo, del neoimperialismo, del bolscevismo nazionale e del conservatorismo russo. Tutte le teorie che lancia condividono la tesi geopolitica sottostante dell'esistenza di due "civiltà superiori": le civiltà della Terra e del Mare, che sono condannate alla rivalità. È il fondatore dell'Unione dei giovani eurasiatica e del Movimento eurasiatico internazionale.

[251] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. pp. 13-14.

[252] Per avere un'idea della loro attività e della loro massiccia presenza sui media basta digitare sul motore di ricerca Google il nome, ad esempio, di Dugin associato ad uno dei canali televisivi citati.

[253] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. pp. 13-14.

[254] *Cfr.* "Психологичекие аспекты обеспечения национальной безопасности России (ч. 1, 1995; ч. 2, 1996)"; "Психологическая безопасность войск (1996)"; "Информационная война и Россия (2000)". Trad.

le basi per la geopolitica della sicurezza delle informazioni della Federazione Russa[255] e, secondo la studiosa J. Darczewska, le opere successive[256] dello studioso hanno fornito motivi per giustificare la necessità della Russia di contrastare l'Occidente sul fronte dell'informazione[257]. Il professor Panarin distingue due grandi ondate di aggressione informativa contro la Russia: la prima è iniziata con la *perestrojka* e si è conclusa con il crollo dell'URSS; e la seconda, all'inizio di questo millennio che, secondo la sua opinione, durerà fino a quando non vincerà il bene, ovvero l'idea eurasiatica russa.

Mentre Dugin si concentra sulla lotta tra Occidente e Russia dal punto di vista della filosofia politica, Panarin si è concentrato sulla guerra dell'informazione come il dominio principale di questa lotta, sostenendo che: "Sin dall'antichità, la stabilità del sistema politico di qualsiasi paese si basava sulla rapidità e completezza con cui le élite politiche ricevono informazioni [...] e con quale velocità rispondono [...], è una lotta informativa sul controllo delle menti delle élite e di [altri] gruppi sociali"[258].

Analizzando la lunga storia della guerra, Panarin sostiene che la dimensione informativa ha sempre avuto uno dei ruoli più decisivi nel conflitto umano[259]. È importante notare che quando Panarin menziona questa dimensione, non si riferisce ad attività politiche, diplomatiche,

---

"Aspetti psicologici per garantire la sicurezza nazionale della Russia" (parte 1, 1995; parte 2, 1996); "Sicurezza psicologica delle truppe", 1996; "The Information War and Russia", 2000.

[255] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p.15.

[256] *Cfr.* "Технология информационной войны (2003); Информационная война и Третий Рим (2005); Информационная война и дипломатия (2004), Информационная война и геополитика (2006); Первая информацион- ная война. Развал СССР (2010)." Trad. La tecnologia della guuerra delle informazioni, 2003; La guerra delle informazioni e la terza Roma, 2005; Guerra dell'informazione e diplomazia, 2004, Guerra dell'informazione e geopolitica, 2006; La prima guerra dell'informazione. Il crollo dell'URSS, 2010.

[257] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p.15.

[258] I. PANARIN, *Informatsionnaya voyna i mir*, Mosca, 2006, p. 165. In cirillico: И. Панарин, Информационная война и геополитика, Поколение, Моська, 2006, п. 165. Disponibile su: https://books.google.it/books [ultimo accesso: 16.04.22]

[259] O. FREEDMAN, "The Russian Perspective on Information Warfare: conceptual roots and politicisation in russian academic, political, and public discourse", *Defence Strategic Communications Journal*, NATO Strategic Communications Centre of Excellence, Lettonia, Vol. 2, 2017, p 74.

economico-finanziarie o militari, ma piuttosto alla manipolazione delle loro immagini informative al fine di ottenere il controllo intenzionale dell'opinione pubblica, in modo che si possano ottenere determinati benefici politici[260]. Secondo Panarin, il controllo può essere ottenuto mediante manipolazione delle informazioni, fare disinformazione, fabbricare informazioni, fare attività di lobbying, ricattare o qualsiasi altro modo possibile per estrarre le informazioni desiderate; o semplicemente negando l'informazione all'avversario; pertanto, quando una guerra di informazione è condotta da uno Stato contro un altro, afferma Panarin, "mira a interrompere l'equilibrio di potere e raggiungere la superiorità nella dimensione informativa globale" prendendo di mira "i processi decisionali dell'avversario" manipolando intenzionalmente l'opinione pubblica nazionale[261].

Panarin definisce tre fasi principali della guerra dell'informazione: la prima fase è l'analisi politica strategica, che comprende la raccolta, aggregazione e scambio di informazioni su avversari e alleati allo scopo di condurre azioni attive; il secondo stadio, l'influenza informativa, si basa su infiltrazioni di commenti negativi e disinformazione nel dominio informativo dell'avversario, nonché sulla soppressione dei tentativi dell'avversario di ottenere le informazioni di cui ha bisogno; e la terza fase, ovvero la difesa informativa, avviene bloccando la disinformazione dispersa e infiltrata dall'avversario[262].

Nei suoi elaborati bibliografici, Panarin afferma che tutte le cosiddette "rivoluzioni colorate" nell'area della CSI e la "Primavera araba" sono un prodotto della tecnologia di controllo sociale e dell'aggressione, nella sfera delle informazioni, da parte degli Stati

---

[260] *Ibidem*.
[261] *Ibidem*.
[262] *Ibidem*.

Uniti[263]. A suo avviso, anche il movimento di protesta in Piazza Bolotnaya a Mosca è stata una manifestazione di questa aggressione: un risultato dell'operazione occidentale denominata "Anti-Putin" controllata dall'estero[264]. In pratica si tratta di operazioni di influenza, come ad esempio: influenzare la società; controllo intenzionale del pubblico col fine di ottenere determinati benefici; manipolazione delle informazioni (autentiche); disinformazione, come per es. diffondere informazioni fabbricate[265].

Secondo Panarin, uno degli aspetti più importanti della guerra delle informazioni è il fatto che prende di mira le menti dell'élite politica e della popolazione in generale, creando un'opinione pubblica favorevole e, quindi, influenzando l'intero processo decisionale politico dell'avversario[266]. Simile a Dugin, Panarin suggerisce che, negli ultimi secoli, la politica internazionale è stata dominata da una lotta tra due principali civiltà: una talassocratica, ovvero l'Impero britannico e gli Stati Uniti, ed una tellurocratica, ovvero l'Eurasia[267]. Inoltre, Panarin afferma che, durante il XX secolo, l'Occidente dominava la guerra dell'informazione e che questo dominio ha portato alla dissoluzione dell'Unione Sovietica poiché la "causa principale della catastrofe geopolitica del 1991 fu una sconfitta nella guerra informativa, che durò per 48 anni"[268].

Per evitare il ripetersi degli eventi che portarono alla sconfitta dell'URSS nella guerra dell'informazione contro l'Occidente, Panarin suggerisce di formare una nuova élite politica in grado di dare una

---

[263] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p.15.
[264] K. GEERS, *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015.
[265] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p.16.
[266] O. FREEDMAN, "The Russian Perspective on Information Warfare", *op.cit*. p. 76.
[267] *Ibidem*.
[268] I. PANARIN, *Informatsionnaya voyna i mir*, *op.cit*. pp. 20-21.

risposta adeguata alle sfide globali del XXI secolo, e questa élite, secondo lui, dovrebbe basarsi su intellettuali delle arti e delle scienze sociali, sull'alta dirigenza dei servizi di sicurezza e militari e sui grandi imprenditori; lo scopo strategico di questa élite dovrebbe essere la formazione di un'opinione pubblica globale positiva della Russia[269].

Panarin ha annunciato il suo progetto geopolitico nel suo libro, "Information of Warfare and Geopolitics" pubblicato nel 2006, analizzando la storia russa dal punto di vista geopolitico, ha concluso che il successo di tutti i progetti di politica internazionale era indissolubilmente legato all'avanzamento della guerra dell'informazione[270]. Sia l'impero americano che quello britannico ha avuto un vantaggio informativo, ma negli ultimi decenni Panarin crede che questo impero stia sprofondando nell'abisso ed è destinato a crollare e propone una nuova unione di stati, che si estende dall'Egitto alla Cina, come contrappeso a questo impero che cade, dove la Ruthenia eurasiatica sarebbe al centro di questa unione di stati[271].

La scuola di pensiero "Dugin"

Dugin, mette in evidenza diverse idee che hanno contribuito alla politicizzazione del concetto di guerra dell'informazione nel discorso accademico russo, è sempre stato uno dei sostenitori più ferventi dell'idea di una civiltà eurasiatica russa che ha caratteristiche socioculturali uniche, storia e ruolo nell'arena globale[272].

Per Dugin: "gli Stati Uniti [sono] la somma dell'Occidente, la sua avanguardia politica, religiosa e ideologica [...] l'incarnazione

[269] O. FREEDMAN, "The Russian Perspective on Information Warfare", *op.cit*. p. 77.
[270] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p.17.
[271] *Ibidem*.
[272] O. FREEDMAN, "The Russian Perspective on Information Warfare: conceptual roots and politicisation in russian academic, political, and public discourse", *Defence Strategic Communications Journal*, NATO Strategic Communications Centre of Excellence, Lettonia, Vol. 2, 2017, pp. 71.

dell'Occidente, del capitalismo occidentale, il suo centro e asse, la sua essenza"[273]. Secondo Dugin , la Russia è sempre stata uno dei nemici più vigorosi dell'Occidente; la lotta tra la civiltà protestante occidentale, guidata inizialmente dall'impero britannico e poi dagli Stati Uniti, e la civiltà eurasiatica ortodossa russa, può essere rintracciata attraverso centinaia di anni di confronto, fin dai tempi antichi: "dalla metà del XX secolo il duello geopolitico, che è stato rintracciato dai geo-politici fino agli antichi conflitti tra Atene e Sparta, Roma e Cartagine, ecc., si è finalmente cristallizzato nella collisione tra il mondo occidentale (il USA e Europa occidentale) e URSS, con satelliti in Europa e in Asia"[274].

Un altro aspetto delle idee di Dugin, più rilevante per l'idea della guerra dell'informazione, è come, secondo lui, l'Occidente (principalmente gli Stati Uniti) abbia condotto un'offensiva contro la Russia nel corso del XX e all'inizio del XXI secolo.

Nel 2007, Dugin ha pubblicato il suo libro *Geopolitika Postmoderna*, in cui ha presentato la sua interpretazione del concetto di guerra incentrata sulla rete[275], introducendo il termine guerre *net-centriche* nel discorso accademico e politico russo. Secondo Dugin, l'establishment militare americano ha sviluppato una nuova strategia militare, una guerra incentrata sulla rete, che si verifica in quattro aree interconnesse di attività umana: fisica, informatica, cognitiva e sociale[276]. Dugin definisce la rete come la dimensione informativa, in cui vengono sviluppate le principali operazioni strategiche, nonché il loro supporto mediatico, diplomatico, economico e tecnico, e afferma che lo scopo principale degli Stati Uniti è quello di stabilire e controllare tale rete, nel

[273] *Ibidem*.
[274] A. DUGIN, *Geopolitika Postmoderna*, 2007. Disponibile: https://it.scribd.com/document/45497425/Aleksandr-Dugin-Geopolitika-Postmoderna [ultimo accesso: 16.04.22].
[275] A. DUGIN, *Geopolitika Postmoderna*, *op.cit.* p. 16.
[276] *Ivi*, p. 246.

tentativo di ottenere il controllo completo e assoluto su tutti i partecipanti di attività militari effettive e possibilmente la loro totale manipolazione in tutte le situazioni: sia durante il periodo di guerra che in quello pace[277]. Secondo Dugin, il controllo è assoluta superiorità nella dimensione informativa, e lo scopo principale della guerra *net-centrica* americana è di impressionare le menti delle popolazioni, innestando l'idea che la competizione militare con gli Stati Uniti sia inutile e dovrebbe essere evitata. Dugin afferma che attraverso la dimensione informativa, Washington tenta di:

> "Costruire un sistema di dominio globale degli Stati Uniti su tutto il mondo, cioè l'analogia postmoderna del colonialismo e della sottomissione, eseguita in nuove condizioni, in nuove forme e con nuovi mezzi. Non è necessaria un'occupazione diretta, un massiccio dispiegamento di forze o una conquista territoriale. [...] La rete è un'arma molto più flessibile, manipola con la violenza e il potere militare solo in casi estremi, [mentre] i risultati principali sono raggiunti dall'influenza contestuale in un'ampia aggregazione di fattori: informativo, sociale, cognitivo, ecc."[278]

Riassumendo le idee di Dugin sulle guerre incentrate sulla rete: gli Stati Uniti stanno conducendo un'offensiva persistente e attentamente pianificata contro la Russia nel campo informativo come parte della sua strategia incentrata sulla rete per dominare il mondo nell'era informativa postmoderna. Per resistere a questo attacco, Dugin sostiene che la Russia deve adottare il "modello eurasiatico", che dovrebbe essere simmetricamente in opposizione al "modello atlantico-americano" e creare una propria rete, orientata esattamente nella direzione opposta. Secondo Dugin questa rete eurasiatica offrirebbe una risposta simmetrica all'interno della dimensione informativa e si baserebbe su: un gruppo speciale – composto da alti funzionari, servizi segreti, intellettuali, scienziati, politologi e giornalisti orientati al

[277] *Ivi*, p. 241-244.
[278] *Ivi*, p. 248-249.

patriottismo e attivisti della cultura – volto a promuovere il patriottismo e la cultura russa[279].

In altre parole, secondo Dugin, lo scopo della guerra dell'informazione è di influenzare una rete di persone, istituzioni, organizzazioni internazionali, ecc. Che promuovono in modo intuitivo un certo insieme di idee per raggiungere determinati obiettivi politici.

La politicizzazione di Dugin sulla guerra dell'informazione come una guerra incentrata sulla rete condotta dagli Stati Uniti contro la Russia è stata adottata da un folto gruppo di scienziati politici russi, che trovano interessante la sua interpretazione della storica lotta est-ovest[280].

Le "rivoluzioni colorate" sono state viste in Russia come processi artificiali, di "net-war", tracciati in Occidente volti a destabilizzare intere regioni nell'area post-sovietica[281].

Per quanto riguarda invece l'ideologia del neoconservatorismo, proposta da Dugin nel suo libro "La quarta teoria politica"[282], può essere sintetizzata come segue: c'è solo una ideologia dominante in Occidente, e questa ideologia è il liberalismo che si basa sull'individualismo, la tecnocrazia e il globalismo[283].

La quarta teoria, al contrario del liberalismo, del comunismo e del fascismo, che erano le ideologie predominanti nel XX secolo, dovrebbe istituire un super-Stato con ideologia post-liberale neoconservatrice. "La Russia è una forza rivoluzionaria post-liberale che lotta per un mondo multipolare, per autentica dignità e libertà e nella sua guerra al liberalismo la Russia difenderà la tradizione, i valori conservatori e la

---

[279] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p. 19.
[280] O. FREEDMAN, "The Russian Perspective on Information Warfare", *op.cit.* p. 73.
[281] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p.18.
[282] A. DUGIN, *La Quarta Teoria Politica*, Nuova Europa, seconda edizione, 2017.
[283] J. DARCZEWSKA, "The anatomy of Russian information warfare", *op.cit*. p. 19.

vera libertà"[284]. Arrivati a questo punto, si potrebbe citare Pierre Nord: "il tempo di pace non esiste mai per il governo di Mosca", scrisse lo studioso francese nel 1971[285].

Secondo Dugin, la Russia è stata incessantemente impegnata nell'*infowar* contro l'Ucraina per anni e questa guerra ha un background geopolitico. La Federazione, mentre costruiva l'Eurasia come sua vasta sfera di influenza con Mosca al centro, ha affrontato il problema di un'Ucraina sovrana lasciata sospesa tra Oriente e Occidente. Dugin crede che le differenze culturali non coincidano sempre con le divisioni territoriali e in questo caso la linea di divisione culturale taglierà il territorio; Mosca desidera che questa linea sia il più vicino possibile a ovest, mentre i geopolitici di Washington stanno cercando di trovare un modo per spingerlo il più possibile verso est[286].

Dugin in un suo articolo espone tre possibili scenari per la situazione Ucraina, basandosi sulla corrente del realismo delle teorie delle relazioni internazionali, sottolineando che questi scenari non siano particolarmente conformi alle norme ed alle consuetudini di correttezza diplomatica[287]:

Il primo scenario: la spartizione dell'Ucraina. L'Ucraina all'interno dei suoi confini attuali non ha una tradizione storica consolidata e le contraddizioni politiche che la lacerano riflettono il suo carattere artificiale. Creare un'idea nazionale comune che possa unire una

---

[284] *Ivi*, p. 20. Per una recensione del libro *Cfr*. il sito web de'*l'intellettuale dissidente*, al seguente link: https://www.lintellettualedissidente.it/controcultura/letteratura-2/aleksandr-dugin-quarta-teoria-politica/ [ultimo accesso: 03.04.20].

[285] *Cfr*. P. NORD, "L'intoxication par un intoxicateur". in V. VOLKOFF, *La désinfor- mation – arme de guerre*, L'age d'homme, Paris 1986. Le parole di Nord, specialista in disinformazione e intossicazione psicologica, sembrano essere ancora valide oggi.

[286] Cfr. Per un commento giornalistico sull'intervista a Dugin: https://geopolityka.net/prof-dugin-kwestia-podzialu-ukrainy-jest-juz-przesadzona/ [ultimo accesso: 03.04.20].

[287] A. DUGIN, "Progetto Euroasiatico e il problema Ucraina", disponibile in lingua russa: http://www.odnako.org/magazine/material/evraziyskiy-proekt-i-ego-ukrainskaya-problema/ [ultimo accesso: 16.04.22].

nazione sulla base di due civiltà reciprocamente esclusive è estremamente difficile. La volatilità della politica ucraina, il suo carattere grottesco e quasi perdente, è collegata a questo. I promotori dello sviluppo dell'idea nazionale sono gli zapadent[288], ma le loro formulazioni sono ostinatamente respinte dalle società dell'est e del sud dell'Ucraina. Pertanto, è possibile prevedere il crollo di questo paese in due zone: quella occidentale e quella sud-orientale. Questa probabilità, dice Dugin, negli ultimi anni si è ripetutamente palesata arrivando sull'orlo del conflitto civile, specialmente dopo la Rivoluzione arancione[289].

Il secondo scenario: Convincere il governo ucraino ad accettare il progetto di integrazione sotto la pressione delle circostanze o tenendo conto di benefici politici, economici ed energetici seri e tangibili. Questo scenario potrebbe essere privo di sangue, e la probabilità che avvenga aumenta nella misura in cui l'Ucraina deve affrontare difficoltà socioeconomiche molto gravi. La crisi economica e il caos crescente nelle economie europee e globali creano condizioni favorevoli per questo scopo. Ad un certo punto, Kiev potrebbe trovarsi in una situazione in cui semplicemente non avrà altra scelta che l'integrazione eurasiatica. Per attuare questo scenario, i servizi diplomatici dovrebbero essere messi in allerta, si dovrebbe avviare un progetto in stretta collaborazione con le élite ucraine, implementare processi di *netwar* in Ucraina, simili a quelli occidentali, ma con un segno geopolitico inverso, ovvero verso l'integrazione e il riavvicinamento con la Russia. Il fattore di pressione energetica, economica e legale svolgerebbe sicuramente un ruolo significativo in questo, ma non dobbiamo

[288] "zapadentsy" ("западенцы", cioè gli "occidentali").
[289] A. DUGIN, "Progetto Euroasiatico e il problema Ucraina", *op.cit.*

dimenticare altre opportunità multifattoriali di influenza: progetti sociali, scientifici, culturali, informativi e di altro tipo. Dovrebbe essere una vera battaglia per l'Ucraina, che coinvolge il personale più dotato della Russia[290].

Il terzo scenario – il più all'avanguardia considerato da Dugin – è quello di impegnarsi a stretto contatto con il nucleo del nazionalismo occidentale ucraino, che ideologicamente, per definizione, non possono pienamente concordare con i valori culturali di liberalismo, individualismo, tolleranza, multiculturalismo, ideologia dei diritti umani e altri standard della società occidentale. Il nazionalismo ucraino è il principale ostacolo all'attuazione del progetto di integrazione eurasiatica. Ma, dice Dugin, "si potrebbe provare a trasformare il veleno in una medicina e il nemico in un amico". L'Unione euroasiatica dovrebbe essere considerata come un modello che preserva le tradizioni e le caratteristiche culturali di società, gruppi etnici e gruppi organici. Di conseguenza, l'Ucraina come identità può sopravvivere solo in questa dimensione, mentre in una società europea individualista e liberale, l'identità collettiva subirebbe rapidamente l'erosione[291].

Tra queste tre strategie, Dugin afferma che se ne potrebbero perseguire due contemporaneamente e, con una certa abilità nel padroneggiare gli strumenti di politica estera, si potrebbe tentare addirittura di avanzare simultaneamente in tutte le direzioni lungo il modello americano: "Se a questo si applica volontà, mente e perseveranza, è del tutto possibile contare sul successo"[292].

Riassumendo le politiche di Dugin e Panarin sulla guerra dell'informazione, risulta essere importante evidenziare i loro quattro

---

[290] *Ibidem*.
[291] *Ibidem*.
[292] *Ibidem*.

aspetti comuni: in primo luogo, entrambi affermano che l'Occidente – prima l'Impero britannico, poi gli Stati Uniti – ha continuamente e deliberatamente tentato di intervenire e minare l'establishment politico russo prima, durante e dopo la guerra fredda; in secondo luogo, la principale strategia dell'Occidente è stata la guerra delle informazioni, che ha influenzato l'opinione pubblica russa ed internazionale contro l'élite politica russa, manipolando il flusso di informazioni su affari politici, diplomatici, economico-finanziari e militari; il terzo aspetto è l'affermazione di entrambi gli studiosi che, oltre alla manipolazione delle informazioni dall'esterno, la strategia occidentale mira a creare una "quinta colonna"[293] all'interno della Russia nel tentativo di destabilizzarla dall'interno[294]. E infine, come risposta a queste nuove e vecchie minacce, entrambi gli studiosi sostengono che la Russia dovrebbe alimentare la sua nuova élite politica, che dovrà essere patriottica ed entusiasta di mettere in un angolo la guerra net-centrica/informativa occidentale, rendendo la Russia centro politico, culturale, economico e militare della civiltà eurasiatica.

[293] Una quinta colonna è un'organizzazione a carattere militare (più o meno informale) che opera clandestinamente all'interno di una nazione o città per favorire l'invasore o il nemico.
[294] O. FREEDMAN, "The Russian Perspective on Information Warfare", *op.cit*. p. 76

COME LA TEORIA SI APPLICA NELLA PRATICA, CASI STUDIO: GEORGIA, CRIMEA E UCRAINA SUD-ORIENTALE.

Per cercare di comprendere meglio se e come, la teoria si collega alla pratica, dopo l'analisi dei documenti ufficiali russi e della teoria militare, trattati nei precedenti capitoli, si passa adesso ad analizzare due noti casi di studio – il caso della Georgia del 2008 e quello dell'Ucraina tra il 2013-2014 – introducendo il capitolo con un breve, ma il più esaustivo possibile, resoconto geopolitico che servirà a contestualizzare i casi studio.

Contesto geopolitico

Durante gli anni '90, la Russia ha combattuto una guerra di vecchia data contro i separatisti in Cecenia, nel mentre ha suscitato insurrezioni etniche in luoghi vicini come l'Ossezia del Sud e l'Abkhazia, due regioni separatiste della Georgia[295] [*vedi allegato n. 1*]. Dopo la caduta dell'Unione Sovietica nel 1991, la Georgia dichiarò nulla la sua costituzione sovietica, questo scatenò una serie di rivolte lungo la sua periferia per una maggiore autonomia[296]. A bloccare questi sentimenti etno-nazionalisti fu il primo presidente della Georgia indipendente, Zviad Gamsakhurdia[297], innescando un intervento militare russo a

[295] L. BEEHENER, et al., *Analyzing the Russian Way of War. Evidence from the 2008 Conflict with Georgia*, The Modern War Institute, 2018, p. 13.
[296] Quando la Georgia ottenne l'indipendenza, le aree lungo la frontiera georgiana erano piene di minoranze etniche che spingevano per una maggiore autonomia.
[297] R. D. ASMUS, *The Little War That Shook the World*, Palgrave Macmillian, New York, 2008, p.60.

nome dalla parte dei separatisti. Dopo che le guerre furono lasciate irrisolte, la Russia lasciò un battaglione di "peacekeeper" russi schierati in Abkhazia (circa 2.300 soldati) e Ossezia del Sud (500)[298]. Per il resto del decennio, l'entroterra della Georgia divenne un bastione di criminalità, signori della guerra, contrabbando e corruzione[299].

Gli osseti non sono etnicamente georgiani, ma più vicini ai persiani e, dal tempo degli zar ai bolscevichi, hanno avuto legami più stretti con Mosca che con Tbilisi[300]. Nel 1990, l'Ossezia del Sud lanciò una campagna per riunirsi con l'Ossezia del Nord dopo che Tbilisi spogliò l'Ossezia del Sud della sua indipendenza scatenando sporadici combattimenti tra georgiani e osseti, sfollando circa sessantamila persone e provocando un cessate il fuoco nel 1992 sponsorizzato dall'OSCE[301].

Durante gli anni '90 la Georgia sotto Shevardnadze si dedicò principalmente alla costruzione della nazione, mentre la Russia sotto Boris Eltsin cercò di mantenere una zona di influenza nel Caucaso meridionale[302]. Mosca stanziò le sue forze in quattro basi in tutta la Georgia sotto la forma di agenti di peacekeeping, con il chiaro sospetto georgiano di percepire questa iniziativa come un modo per Mosca di mantenere la sua egemonia imperiale nella regione[303]. Sotto Shevardnadze, la Georgia ha adottato una politica amichevole nei confronti della Russia, da una parte per paura di agitazioni e di suscitare

---

[298] A. LAVROV, "Timeline of Russian-Georgian Hostilities in August 2008." *In the Tanks of August*, Centre for Analysis of Strategies and Technologies, Ruslan Pukhov, Moscow 2010, p. 37.
[299] K. MARTEN, *Warlords: Strong-Arm Brokers in Weak States*, Cornell University Press, New York, 2012, p. 20.
[300] T. GOLTZ, "The Paradox of Living in Paradise: Georgia's Descent into Chaos", in *The Guns of August 2008: Russia's War in Georgia*, E. Svante, e S. Starr (a cura di), Sharpe, New York, 2008, p. 18.
[301] K.H. BACON, E M. LYNCH, "The Plight of Displaced Persons in the Caucasus", *World Policy Journal*, vol. 19, n 4, 2002, pp. 66–71.
[302] L. BEEHENER, et al., "Analyzing the Russian Way of War", *op.cit.*, p. 14.
[303] *Ibidem*.

risentimenti etnici nelle sue aree periferiche, dall'altra era per inerzia diplomatica[304].

La Georgia era strategicamente importante, data la sua posizione tra l'Unione Sovietica e il Medio Oriente e il suo status di corridoio tra i bacini ricchi di energia del Mar Caspio e del Mar Nero. Il gasdotto Baku-Tbilisi-Ceyhan [*vedi allegato n. 2*], un mezzo per pompare il greggio caspico verso i mercati europei, è stato anche un importante punto di svolta per la sovranità georgiana e far storcere il naso a Mosca[305].

Verso la fine degli anni '90 e l'inizio degli anni 2000, la Georgia era diventata il principale destinatario degli aiuti statunitensi su base pro capite, aveva rinunciato al *Collective Security Treaty* (CST) e aveva avviato la rimozione di tutte le forze russe[306]. La rivoluzione delle rose del 2003 ha creato un dilemma spinoso per il Cremlino, riguardava tanto la costruzione dello Stato quanto il ripristino della democrazia in Georgia e la strategia di sicurezza nazionale del nuovo premier riformatore Saakashvili, che si articolava in tre punti: a) ripristinare i confini territoriali della Georgia e riportare le sue province separatiste sotto il gregge di Tbilisi; b) stabilizzare la più grande regione del Caucaso e del Mar Nero; c) garantire lo status della Georgia attraverso il redditizio corridoio di transito dell'energia[307]. Per il neo-premier, ripristinare l'integrità territoriale della Georgia era una priorità vitale, persino esistenziale, che si sarebbe dimostrato disposto a combattere al fine di raggiungere tale obiettivo[308].

Saakashvili rivolse la sua attenzione verso l'interno del Paese, cercando di riformare la politica georgiana, stringendo legami più stretti

---

[304] *Ibidem*.
[305] *Ivi*, p.15.
[306] *Ibidem*.
[307] V. TSELUIKO, "Georgian Army Reform under Saakashvili Prior to the 2008 Five Day War", in *The Guns of August 2008: Russia's War in Georgia*, E. Svante, e S. Starr (a cura di), Sharpe, New York, 2008, p. 12.
[308] L. BEEHENER, et al., "Analyzing the Russian Way of War", *op.cit.*, p. 19.

con Washington, tanto è che Bush fece della Georgia parte del suo programma di promozione della democrazia, tenendo un discorso nel centro di Tbilisi nel 2005[309]; nel 2007 Putin pronunciò il suo discorso ampiamente riportato a Monaco[310], dove si scagliò contro gli Stati Uniti e denunciò quello che veniva comunemente definito un "mondo unipolare"[311]. Due giorni dopo Saakashvili annunciò che la Georgia avrebbe aderito alla NATO entro il 2009, ma molti analisti sostengono che la vera goccia che ha fatto traboccare il vaso sia stata l'indipendenza concessa al Kosovo all'inizio del 2008[312]. Per capire come e perché questi territori esplosero nell'estate del 2008, bisogna guardare indietro di un decennio, partendo dalle conseguenze disordinate della caduta dell'Unione Sovietica e i destini poco chiari dei gruppi etnici sfollati lungo la sua periferia.

La Russia ha lanciato la guerra contro la Georgia nell'agosto 2008 per obiettivi strategici e geopolitici di grande valore, tra cui l'annessione di fatto dell'Abkhazia, l'indebolimento o il rovesciamento del regime di Mikheil Saakashvili e la prevenzione dell'allargamento della NATO[313] [*vedi allegato n. 3*]. Le élite politico-militari russe si concentrarono sulla Georgia fin dai tempi della presidenza di Eduard Shevardnadze[314]. Le cose peggiorarono solo dopo che Mikheil Saakashvili, orientato verso Occidente (NATO e UE), venne eletto presidente. Dal 2006 l'operazione

---

[309] *Cfr*. Corriere della Sera, "Bush in Georgia: «Medierò con la Russia»", disponibile online; https://www.corriere.it/Primo_Piano/Esteri/2005/05_Maggio/10/bush.shtml [ultimo sccesso: 16.04.22].
[310] M. ALLEVATO, "Così Putin ha riportato Mosca al centro del Grande Gioco", *AG*I, 26 febbraio 2017, disponibile online: https://www.agi.it/estero/cos_putin_ha_riportato_mosca_al_centro_del_grande_gioco-1529516/news/2017-02-26/ [ultimo accesso: 16.04.22].
[311] L. BEEHNER, "U.S.-Russia Interests on Collision Course", *Council on Foreign Relations*, 14 febbraio 2007, disponibile online: https://www.cfr.org/backgrounder/us-russia-interests-collision-course [ultimo accesso: 16.04.22].
[312] L. BEEHENER, et al., "Analyzing the Russian Way of War", *op.cit.*, p. 21.
[313] A. COHEN, R. E. HAMILTON, *The Russian Military and the Georgia War: Lessons and Implications*, U.S. Army War College, Strategic Studies Institute, Carlisle, giugno 2011, p. sommario.
[314] *Ibidem*.

militare russa divenne rapidamente la questione del "quando", non del "se".

L'Ucraina, anch'essa come la Georgia, svolge da tempo un ruolo importante nello scacchiere internazionale e, ormai lo possiamo definitivamente affermare, che la Russia prima con l'annessione della Crimea e dopo con l'aggressione in Ucraina, ha scatenato la più grande crisi in Europa dopo la fine della Guerra Fredda, con logiche che alimentano ricordi del secolo precedente. L'ex consigliere per la sicurezza nazionale degli Stati Uniti Zbigniew Brzezinski, all'inizio del 1994 su *Foreign Affairs*[315], scrisse che un'Ucraina sana e stabile come contrappeso critico alla Russia dovrebbe essere il perno della nuova grande strategia degli Stati Uniti dopo la guerra fredda: "Non si può sottolineare abbastanza fortemente che senza l'Ucraina la Russia cessi di essere un impero, ma con l'Ucraina sottomessa e poi subordinata, la Russia diventa automaticamente un impero". Venti anni dopo, con la conquista della Crimea da parte della Russia, il ripristino e il rafforzamento della sovranità ucraina sono riemersi tra le principali priorità della politica estera degli Stati Uniti e dell'UE.

L'Ucraina era un territorio fondamentale per l'Unione Sovietica ed era, dietro solo alla Russia, la Repubblica sovietica più popolosa e più potente dell'Unione; produceva gran parte delle risorse agricole dell'URSS ed era anche un grande bacino per le industrie della difesa, contribuiva con un apporto considerevole di unità militari, tra cui la flotta del Mar Nero e parte dell'arsenale nucleare[316].

---

[315] Z. BRZEZINSKI, "The Premature Partnership", *Foreign Affairs*, marzo/aprile 1994, disponibile online: https://www.foreignaffairs.com/articles/russian-federation/1994-03-01/premature-partnership [ultimo accesso: 16.04.22].

[316] J. MASTERS, "Ukraine: Conflict at the Crossroads of Europe and Russia", *Council on Foreign Relations*, 5 febbraio 2020, disponibile online: https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia [ultimo accesso: 16.04.22]. Dopo la caduta dell'Unione Sovietica l'arsenale nucleare presente nei territori ucraini, così come quelli di stanza in Bielorussia e Kazakistan, venne trasferito in Russia, *Cfr*. E. SINELSCHIKOVA, "Perché dopo il crollo dell'Urss tutte le armi nucleari sono rimaste solo alla Russia?", *Russia*

Nelle recenti elezioni[317] i cittadini ucraini hanno manifestamente segnalato che considerano con distinto piacere il loro futuro nell'Unione Europa[318].

Nei suoi quasi sei lustri di indipendenza, il Paese ha cercato d'intraprendere il proprio percorso come stato sovrano, cercando di allinearsi più intimamente con le istituzioni occidentali, sia con l'Unione Europea che la NATO. Tuttavia, Kiev ha faticato a bilanciare le sue relazioni estere e a colmare profonde divisioni interne; poiché il popolo nazionalista di lingua ucraina – stanziato principalmente nella parte occidentale della nazione – è sempre stato incline a sostenere un percorso di integrazione con l'UE, mentre la comunità di lingua russa – stanziata prevalentemente nella parte sud-orientale – vedeva con favore un avvicinamento ed un legame più stretto con la Russia[319]. L'Ucraina occidentale ha trascorso secoli sotto il controllo mutevole di potenze europee come la Polonia e l'impero austro-ungarico; ciò, in una certa misura, aiuta a spiegare perché i cittadini ucraini della parte Nord-occidentale hanno teso a sostenere politici più vicini all'Occidente. Inoltre, La parte della popolazione che vive nel Sud-Est è in maggioranza ortodossa, mentre la fetta di popolazione del Nord-Ovest ha influenze cattoliche protestanti più marcate[320].

Beyond,19 giugno 2019, disponibile online: https://it.rbth.com/scienza-e-tech/82917-perché-dopo-il-crollo-dellurss [ultimo accesso: 16.04.22].

[317]Le elezioni parlamentari in Ucraina si sono tenute il 21 luglio 2019 per i membri della Rada. Inizialmente programmate per la fine di ottobre, esse sono state anticipate dopo che il nuovo presidente Zelensky durante il suo insediamento il 21 maggio 2019, aveva sciolto il parlamento. Rispetto alle precedenti elezioni, le circoscrizioni e i votanti sono inferiori a causa dell'annessione della Crimea avvenuta a marzo 2014 da parte della Russia e dall'aprile 2014 dell'occupazione dei separatisti di parti di Donetsk Oblast e Luhansk Oblast.

[318] *Cfr*. B. CAPELLI, "Elezioni parlamentari in Ucraina: volti nuovi e voglia di cambiamento", *Vatican News*, 20 luglio 2019, disponibile online: https://www.vaticannews.va/it/mondo/news/2019-07/ucraina-voto-elezioni-anticipate-europa-russia.html [ultima consultazione: 16.04.22].

[319] M. KOFMAN, K. MIGACHEVA, B. NICHIPORUK, A. RADIN, O. TKACHEVA, J. OBERHOLTZER, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, RAND Corporation, Santa Monica, 2017, pp. 48-49, disponibile online: https://www.rand.org/pubs/research_reports/RR1498.html. [ultimo accesso: 16.04.22].

[320] E. CONANT, "Come la storia, la geografia aiutano a spiegare la crisi politica dell'Ucraina", *National Geografic*, 31 gennaio 2014, disponibile online: https://www.nationalgeographic.com/news/2014/1/140129-protests-ukraine-russia-geography-history/ [ultimo accesso: 16.04.22].

L'Ucraina è diventata un campo di battaglia nel 2014 quando la Russia ha annesso la Crimea e ha iniziato ad armare e favorire i separatisti nella regione del Donbas [*vedi allegato n. 4*]. Durante i conflitti hanno perso la vita quattordicimila persone, vincendo così il premio della guerra più sanguinosa in Europa dai tempi dalle guerre balcaniche degli anni '90[321].

L'Ucraina è fondamentale per l'identità e la visione della Russia di sé stessa nel mondo, essa ha profondi legami culturali, familiari, economici e politici con l'Ucraina. Fu a Kiev tra l'XIII e nel IX secolo che il Cristianesimo fu portato da Bisanzio ai popoli slavi. Ed è stato il cristianesimo che è servito come ancoraggio per Kievan Rus, il primo Stato slavo da cui i moderni russi, ucraini e bielorussi traggono il loro lignaggio[322].

Secondo un articolo dell'Istituto Italiano di Studi Politici Internazionali (ISPI), "Il 17,3 per cento della popolazione [...] è di etnia russa, mentre la quota della popolazione di lingua russa è del 24 per cento. Questa percentuale nel corso del XX secolo è progressivamente aumentata in favore della presenza russa soprattutto nelle regioni meridionali e orientali, che per questo vengono chiamate *Novorossiya*[323]. Si tratta di un dato nevralgico per il nuovo *soft power* di Mosca, fondato sul suo ruolo di protettrice delle popolazioni russe, russofone e ortodosse (il cosiddetto *Russkiy Mir*, che tradotto significa il mondo russo)"[324] [*vedi allegato n. 5*]. Da qui si comprende da dove derivino le preoccupazioni della Russia nel garantire il benessere dei russi etnici che vivono in

[321] J. MASTERS, "Ukraine: Conflict at the Crossroads of Europe and Russia", *op.cit*.
[322] *Ibidem*.
[323] Trad. "Nuova Russia", un termine che risale alla Russia imperiale del XVIII secolo.
[324] A. F. BIAGINI, "Quanto conta l'Ucraina per la Russia. Quanto conta la Russia per l'Italia", *Istituto Italiano di Studi Politici Internazionali (ISPI)*, 16 aprile 2015, disponibile online: https://www.ispionline.it/en/node/13099 [ultimo accesso: 16.04.22].

Ucraina e, quindi, il perché rivendica il dovere di proteggere queste persone[325].

Dopo il crollo sovietico, in tanti tra l'establishment politico e militare russo hanno guardato con disappunto il distaccamento con l'Ucraina, definito come un errore storico ed una chiara minaccia in merito alla posizione della Russia come grande potenza sul palcoscenico mondiale. Lasciar gravitare l'Ucraina nell'orbita occidentale è stato considerato dai più, un duro colpo al prestigio internazionale della Russia[326].

Nel 1954, il primo segretario generale del Partito comunista da poco eletto Nikita Krusciov, trasferì la Crimea, di potestà russa, all'Ucraina al fine di intensificare e rafforzare il legame fraterno tra il popolo ucraino e russo. Dalla caduta dell'URSS, molti nazionalisti russi, sia in Russia che in Crimea, hanno bramato fervidamente un ritorno alla proprietà Russa, uno sbocco estremamente necessario per la proiezione di potenza russa nelle acque del Mediterraneo. Sebastopoli è il porto di origine della flotta russa del Mar Nero, e dalla cessione del '54 la Russia ne ha sempre fruito grazie a degli accordi di affitto tra le parti interessate[327].

Fino all'annessione della Crimea, la Russia forniva la maggior parte degli approvvigionamenti energetici (gas principalmente) all'Ucraina per poi andare a scemare nel 2016, anno in cui si sono fermate del tutto le esportazioni di gas a Kiev; tuttavia, la Russia si affida ancora ai gasdotti ucraini per pompare le sue risorse energetiche in Europa centrale e orientale, pagando miliardi a Kiev. Questo potrebbe cambiare nel momento in cui il *Nord Stream 2*[328] [*vedi allegato n. 6*] - che attraversa il Mar Baltico - venisse terminato, anche se la Russia ha un contratto con

---

[325] J. MASTERS, "Ukraine: Conflict at the Crossroads of Europe and Russia", *op.cit*.
[326] *Ibidem*.
[327] M. KOFMAN, K. MIGACHEVA, B. NICHIPORUK, A. RADIN, O. TKACHEVA, J. OBERHOLTZER, "Lessons from Russia's Operations in Crimea", *op.cit*. pp. 48-49.
[328] *Cfr*. Il sito web dedicato al *Nord Stream 2*, disponibile al seguente link: https://www.nord-stream2.com/en/pdf/document/124/ [ultimo accesso: 16.04.22].

l'Ucraina per diversi altri anni ancora. Il ripiegamento sul Nord Stream 2 potrebbe essere fatale per le entrate di Kiev e sicuramente darà a Mosca una leva politica economica in più da sfruttare a suo favore[329].

A seguito del continuo allargamento della NATO dopo la guerra fredda, crescono nella Russia sentimenti di crescente allarme per la sua sicurezza. Nel 2004, la NATO ha aggiunto sette membri – la sua quinta espansione e la più grande fino ad oggi – tra cui le ex repubbliche sovietiche baltiche: Estonia, Lettonia e Lituania. Quattro anni dopo, quando la NATO dichiarò la sua intenzione di voler corteggiare l'Ucraina e la Georgia, la Russia chiarì che era stata superata una linea rossa[330]. Nelle settimane precedenti il vertice della NATO del 2008, il presidente Vladimir Putin avvertì i diplomatici statunitensi che far aderire l'Ucraina così come la Georgia nell'alleanza sarebbe considerato un atto ostile nei confronti della Russia[331]. Qualche mese dopo, la Russia entrò in guerra con la Georgia, mostrando apparentemente la volontà di Putin di usare la forza per proteggere gli interessi della Russia[332].

Alla fine del 2013, il presidente Yanukovich, agendo sotto la pressione dei suoi sostenitori a Mosca, mise da parte i piani per formalizzare una più stretta relazione economica con l'UE e allo stesso tempo, la Russia spinse l'Ucraina a unirsi all'Unione economica eurasiatica non ancora formata. Molti ucraini hanno percepito la decisione come un tradimento da parte di un governo profondamente corrotto e incompetente, e ha innescato proteste in tutto il paese conosciute come *Euromaidan*.

---

[329] J. MASTERS, "Ukraine: Conflict at the Crossroads of Europe and Russia", *op.cit*.
[330] *Ibidem*.
[331] Askanews, "Putin: chi vuol Georgia, Ucraina nella Nato, non pensa [alle] conseguenze. Irresponsabili, ha detto Putin: Reagiremo proporzionalmente", Giovedì 19 luglio 2018, disponibile online: http://www.askanews.it/esteri/2018/07/19/putin-chi-vuol-georgia-ucraina-nella-nato-non-pensa-conseguenze-pn_20180719_00108/ [ultimo accesso: 16.04.22].
[332] J. MASTERS, "Ukraine: Conflict at the Crossroads of Europe and Russia", *op.cit*.

Information warfare in Georgia nel 2008

Nell'agosto 2008, il conflitto armato tra Russia e Georgia scoppiò sul territorio delle regioni separatiste della Georgia: l'Ossezia del Sud e l'Abkhazia[333]. La campagna militare pianificata dalla Russia durò 5 giorni fino a quando le parti, il 12 agosto, raggiunsero un accordo preliminare di cessate il fuoco mediato dall'UE guidata dalla presidenza di turno francese. Dopo aver firmato l'accordo, la Russia ritirò la maggior parte delle sue truppe dai territori georgiani, ma istituì zone cuscinetto attorno all'Abkhazia e all'Ossezia meridionale. Il 26 agosto 2008, la Russia riconosce l'indipendenza dell'Ossezia del Sud e dell'Abkhazia, rendendole parte di quella che il presidente Dmitry Medvedev ha definito la "zona di interesse privilegiata" di Mosca e da allora ha dispiegato cinque basi militari sul territorio georgiano occupato[334].

Le tensioni tra i due paesi erano aumentate negli anni precedenti a causa sia della politica estera della Georgia, diventata sempre più filo-occidentale sotto il presidente Mikheil Saakashvili, che a causa delle relazioni corrotte tra la Georgia e le repubbliche separatiste dell'Ossezia del Sud e dell'Abkhazia[335]. L'intervento militare della Georgia nell'Ossezia del Sud, il 7 agosto, apparentemente per impedire il bombardamento osseto del territorio georgiano, scatenò l'intervento della Russia l'8 agosto e mentre le forze militari russe si trasferivano nell'Ossezia del Sud, una serie di attacchi DDoS colpirono le reti ICT della Georgia, interrompendo le comunicazioni e danneggiando i siti web del governo; insieme alle infrastrutture del governo fu colpito anche il

[333] A. COHEN, R. E. HAMILTON, *The Russian Military and the Georgia War: Lessons and Implications*, U.S. Army War College, Strategic Studies Institute, Carlisle, giugno 2011, pp. 20-22.
[334] *Ibidem*.
[335] M. CONNEL M. E S. VOGLER, *Russia's Approach to Cyber Warfare*, CNA Analysis & Solution, 2017, p. 17.

comparto finanziario georgiano, le compagnie di trasporto ed i fornitori privati di telecomunicazioni, interrompendo così i servizi essenziali[336].

Sotto la costante raffica di informazioni delle *botnet*[337], la Georgia è stata sottoposta a un cyber-blocco e naturalmente il governo russo, ha negato il coinvolgimento attraverso un portavoce dell'ambasciata russa che affermò che, probabilmente, individui in Russia o altrove si fossero presi la briga di iniziare gli attacchi in forma indipendente[338]. In alcuni casi, gli attacchi erano anche allineati geograficamente alle operazioni convenzionali russe, ad esempio: gli hacker russi hanno attaccato siti Web governativi nella città di Gori nella Georgia orientale, insieme a siti web di notiziari, poco prima degli attacchi aerei russi sulla città[339]. Tuttavia, il governo georgiano è stato in grado di reindirizzare la maggior parte del suo traffico attraverso server in altri paesi, tra cui Stati Uniti, Estonia e Polonia.

La Russia e la Georgia hanno gareggiato per controllare il flusso di informazioni diretto alla comunità globale durante il loro breve conflitto nel 2008[340]. Entrambe le parti hanno impiegato offensive cinetiche (attacchi militari convenzionali e movimenti di truppe) e non cinetiche (attacchi informatici, propaganda e inganno). L'analisi a posteriori e le critiche della Russia ai suoi sforzi nel conflitto, hanno portato ad alcune serie riforme militari migliorative nel suo più ampio apparato di difesa,

---

[336] E. TIKK, K. KASKA E L. VIHUL, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia 2010, pp. 33-34.
[337] Una botnet è un gruppo di computer su Internet (chiamati "bot" o "zombi") che sono stati infettati da un software noto come malware. Il malware consente a un server di "comando e controllo" del computer di inviare comandi a questi robot. Spesso, le botnet lanciano e-mail di spam.
[338] J. MARKOFF, "Before the Gunfire, Cyberattacks", *NYT Online*, 12 agosto 2008, accessibile online al seguente link: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 [ultimo accesso: 16.04.22].
[339] M. CONNEL M. E S. VOGLER, Russia's Approach to Cyber Warfare, *op.cit.*, p.18.
[340] E. J. IASIELLO, "Russia's Improved Information Operations: From Georgia to Crimea", *Innovations in Warfare & strategy*, The US Army War College Quarterly Parameters, Vol. 47 n. 2, estate 2017, p.52

che poi si sarebbero riversate, queste migliorie, nell'intervento in Ucraina del 2014[341].

Nonostante la mancanza di una connessione sostanziale tra gli orchestratori degli attacchi informatici e il governo russo, è stata la prima volta che gli attacchi informatici e le operazioni militari convenzionali hanno lavorato insieme[342]. La Russia si è anche impegnata in operazioni informative psicologiche simultanee, tra cui campagne di propaganda, controllo delle informazioni e disinformazione, con risultati diversi, soprattutto in contrasto con gli sforzi della Georgia nelle stesse aree[343]. La Russia si è concentrata sul far ricevere dei temi chiave alla comunità internazionale, ovvero che: a) la Georgia e Mikheil Saakashvili, il suo presidente, erano gli aggressori; b) la Russia era costretta a difendere i suoi cittadini; c) né gli Stati Uniti né i suoi alleati occidentali avevano alcuna base argomentativa per criticare la Russia, poiché loro avevano intrapreso azioni simili in altre aree del mondo, in particolare in Kosovo[344]. Utilizzando filmati televisivi e interviste quotidiane, la Russia controllava il flusso di informazioni internazionali e cercava di influenzare le popolazioni locali dettando notizie, condividendo i progressi delle truppe russe a protezione dei cittadini russi e propagandando le atrocità georgiane[345]. Un sondaggio della CNN condotto all'epoca segnalò che il 92% degli intervistati credeva che la Russia fosse giustificata per l'intervento[346]. Nel corso della crisi, invece di restare inermi ed attoniti alla campagna di *InfoWar*

---

[341] *Ibidem*.
[342] D. HOLLIS, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, vol.7, n. 1, gennaio 2011, p.56.
[343] E. J. IASIELLO, "Russia's Improved Information Operations", *op.cit.*, p. 54.
[344] A. COHEN, R. E. HAMILTON, "The Russian Military and the Georgia War", *op.cit.*, p. 47-48.
[345] K. PAINE, "Reputation Redux: Russia Invades Georgia by Land and by Server," *PR News*, 25 agosto 2008, disponibile online: http://www.prnewsonline.com/reputation-redux-russia-invades-georgia-by-land -and-by-server/ [ultimo accesso: 16.04.22].
[346] Y. LEVINE, "The CNN Effect: Georgia Schools Russia in Information Warfare", *The eXiled Online*, 13 agosto 2008, disponibile online: http://exiledonline.com/the-cnn-effect-georgia-schools-russia-in -information-warfare/ [ultimo accesso: 16.04.22].

della Russia, i georgiani hanno lanciato un'aggressiva campagna di controinformazione impiegando la propria disinformazione e manipolando i media[347]. La Georgia richiese assistenza a società di pubbliche relazioni per riuscire a promuovere la sua narrazione e, per limitare l'andamento positivo a favore delle notizie russofile, riferì di raid aerei russi su obiettivi civili, diventando così vittima di un'invasione militare russa sconsiderata e criminale[348]. La Georgia conquistò i cuori e le menti della comunità globale[349].

Sebbene la guerra sia iniziata il 7 agosto 2008, la missione russa di minare l'ambiente dell'informazione della Georgia è probabilmente iniziata quasi due anni prima[350]. Alcuni esperti hanno scoperto che molti dei domini e gli acquisti di hosting per l'hub principale di distribuzione di malware, StopGeorgia.ru, erano stati registrati mesi prima dello scoppio delle ostilità[351] e, la società di hosting utilizzata per registrare il sito era segnalato da siti di monitoraggio del malware quasi due mesi prima dello scoppio del conflitto[352]. Gli attacchi informatici contro la Georgia e la loro capacità di rallentare la narrazione del governo georgiano si adattano bene alla dottrina militare della Russia del 2010, definita quindi dopo la guerra del 2008, che descrive l'importanza dell'"l'utilizzo integrato di forze militari e risorse di carattere non

---

[347] *Ibidem*.
[348] T. EROFEEVA, "Georgia-Russia War: An Information Control Story", *Prezi*, 6 maggio 2014, disponibile online: https://prezi.com/i4fk4qprev0s/georgia-russia-war-an-information-control-story/ [ultimo accesso: 16.04.22].
[349] A. TSYGANOK, "Informational Warfare - a Geopolitical Reality", rivista online della *Strategic Culture Foundation*, 5 novembre 2008, disponibile online al seguente link: https://www.rbth.com/articles/2008/11/05/051108_strategic.html [ultimo accesso: 16.04.22]. Cfr. anche P. WILBY, "Georgia Has Won the PR War", *The Guardian*, 17 agosto 2008, disponibile online: https://www.theguardian.com/media/2008/aug/18/pressandpublishing.georgia [ultimo accesso: 16.04.22]; *Cfr*. anche "Independent International Fact-Finding Mission on the Conflict in Georgia", *Council of the European Union*, Report, vol. 1, Bruxelles, settembre 2009, disponibile online: https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf [ultimo accesso: 16.04.22].
[350] L. BEEHENER, et al., *Analyzing the Russian Way of War. Evidence from the 2008 Conflict with Georgia*, The Modern War Institute, 2018, p. 60.
[351] J. CARR, *Inside Cyber Warfare*, O'Reilly Media, seconda edizione, dicembre 2011, pp. 17-18.
[352] L. BEEHENER, et al., Analyzing the Russian Way of War", *op.cit.*, p. 60.

militare"[353]. È anche in linea sia con il concetto russo di *informatsionnaya voyna* che con gli scritti del generale Valery Gerasimov[354], sebbene la guerra del 2008 abbia preceduto il suo saggio del 2013, egli affermava che: "le regole della guerra sono cambiate ed il ruolo dei mezzi non militari per raggiungere obiettivi politici e strategici è cresciuto e, in molti casi, hanno superato il potere della forza delle armi convenzionali nella loro efficacia"[355].

Gli effetti intrecciati della guerra d'informazione contro la Georgia, che includono uno strato fisico limitato, uno strato logico degradato e uno strato umano manipolato, sebbene non sufficienti per vincere la guerra, hanno facilitato le operazioni cinetiche a un costo trascurabile per la Russia, ma sostanzialmente più elevato per la Georgia[356]. Mentre si trovava nel bel mezzo di un conflitto cinetico, la Georgia aveva anche il compito di riabilitare la sua immagine globale, il tutto di fronte a una indubbia superiorità militare russa evidente. Per fare ciò, la Georgia ha sfruttato sia le proprie capacità tecniche sia le capacità private degli attori occidentali, principalmente negli Stati Uniti[357]. Dal punto di vista militare convenzionale, gli attacchi informatici del 2008 hanno avuto un limitato beneficio operativo e tattico; gli attacchi non hanno veramente degradato il comando e le funzioni di controllo dell'esercito georgiano, né hanno impedito completamente alla Georgia di comunicare con i suoi cittadini[358].

---

[353] Dottrina militare della Federazione Russa, *op.cit.*
[354] Cfr. § 3.2.10 di questo elaborato.
[355] *Cfr*. il famoso articolo: Герасимов Валерий, Ценность науки в предвидении Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, (trad. Gerasimov Valery, Il valore della scienza in previsione. Le nuove sfide richiedono un ripensamento delle forme e dei metodi di guerra), *Vpk* news, 26 febbraio 2013, disponibile online: https://www.vpk-news.ru/articles/14632 [ultimo accesso: 16.04.22]. *Cfr*. inoltre, la § 3.2.10. di questo elaborato.
[356] L. BEEHENER, et al., Analyzing the Russian Way of War", *op.cit.*, p. 61.
[357] *Ibidem*. I georgiani iniziarono immediatamente a cercare assistenza da attori stranieri, contattando attori statali in Polonia, Estonia e Stati Uniti e attori privati negli Stati Uniti.
[358] *Ibidem*.

Sebbene gli attacchi informatici abbiano avuto scarso effetto sulla guerra convenzionale e non siano stati così decisivi[359] per l'esito del conflitto, hanno comunque offerto lezioni significative sul carattere della guerra moderna, ovvero gli attacchi hanno rafforzato la visione russa dell'*information space* come strumento di manipolazione psicologica, di guerra delle informazioni e di quella informatica[360].

Mentre gli analisti concordano sul fatto che gli hacker russi avessero l'esperienza per creare effetti fisici disastrosi e duraturi sull'infrastruttura georgiana[361], la loro rinuncia a perseguire questo tipo di azione, rafforza l'idea della manipolazione psicologica e del controllo narrativo come uno degli scopi principali della campagna; inoltre, si può affermare che l'attacco informatico ha rispecchiato il pensiero strategico e la pianificazione operativa russa in merito all'approccio generale difensivo sulla guerra dell'informazione. Il comportamento russo nel cyberspazio, in Georgia, deve essere valutato nel contesto dell'orientamento intellettuale della Russia verso il dominio delle informazioni e questo orientamento si manifesta nella "dottrina di sicurezza delle informazioni" che si preoccupa di un senso di vulnerabilità sia fisica che psicologica. Di conseguenza, la prospettiva russa sul ciberspazio considera l'inganno e la manipolazione come strumenti legittimi che, le piattaforme di comunicazione di massa di oggi consentono prontamente ed ampiamente il loro pieno ed efficiente utilizzo.

---

[359] Come lo saranno in Ucraina, questo si vedrà nel paragrafo successivo.
[360] L. BEEHENER, et al., "Analyzing the Russian Way of War", *op.cit.*, p. 70.
[361] *Ivi.*, p. 67. Cfr., K. GILES, *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London, Chatham House, March 2016, p. 9. *Cfr.*, Anche DEIBERT, J. RONALD, R. ROHOZINSKI, E M. CRETE-NISHIHATA, "Cyclones in Cyberspace: Information Denial and Information Shaping in the Russia Georgia War", *Security Dialogue*, vol. 43, n. 1, 2012, pp. 3–24.

Information warfare in Crimea ed Ucraina Sud-orientale nel 2013

Nel novembre 2013, studenti e attivisti ucraini si sono riuniti in una protesta nota come "Euromaidan"[362] per protestare pacificamente contro la decisione, del Presidente filo-russo Viktor Yanukovich, di non firmare l'accordo di associazione con l'Unione Europea[363]. Nel febbraio 2014, quando le tensioni si intensificarono, circa un centinaio di civili furono uccisi dalle forze di sicurezza pubblica, scatenando una serie di eventi che avrebbero portato il Presidente Yanukovich alla fuga dal paese[364]. Poco dopo la Russia inviò i cosiddetti "piccoli uomini verdi" per occupare il parlamento della Crimea, istituire una serie di *checkpoint* e prendere il controllo dell'aeroporto, poco prima di annettere la provincia dopo un referendum ritenuto truccato dagli osservatori[365]. Non diversamente dall'invasione della Georgia da parte della Russia nel 2008, molti analisti ritengono che l'intervento della Russia in Ucraina sia stato sviluppato con largo anticipo; in meno di un mese e senza sparare un solo colpo, la Russia è stata in grado di annettere la Crimea[366]. In altre parole, il Cremlino ha usato la violenza separatista come un conveniente pretesto per intervenire militarmente e annettere territori[367]. In seguito all'annessione della Crimea, le manifestazioni in Ucraina orientale hanno continuato a intensificarsi nelle regioni di Donetsk e Luhansk, dove i militanti sostenuti dalla Russia hanno infine sequestrato edifici governativi e mezzi di informazione[368]; questa volta, tuttavia, l'Ucraina

---

[362] nome della piazza nel centro di Kiev.
[363] Rainews, "Ucraina, cronologia della rivolta", 20 febbraio 2014, disponibile online: http://www.rainews.it/dl/rainews/articoli/ucraina-cronologia-rivolta-guerra-civile-e242cf67-76a7-40e6-bef7-fe711de64eae.html [ultimo accesso: 16.04.22].
[364] *Ibidem*.
[365] A. REID, *Borderland: A Journey through the History of Ukraine*, Basic Books, New York, 2015.
[366] US Department of the Army, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare. Ukraine 2013-2014*, US Army Special Operations Command, 2015, disponibile online: https://www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf [ultimo accesso: 16.04.22].
[367] L BEEHENER., L.COLLINS, S. FERENZI, R. PERSON, A. BRANTLY, *Analyzing the Russian Way of War Evidence from the 2008 Conflict with Georgia*, The Modern War Institute, 2018, pp. 70-71.
[368] *Ibidem*.

ha reagito ed ha effettivamente fermato l'avanzata russa[369]. Prima che la Russia invadesse l'Ucraina nel febbraio 2022, dal febbraio 2015 esisteva un tenue cessate il fuoco grazie agli Accordi di Minsk, ma non rispettati dalle continue violazioni e, scrive l'UNHCR il 4 ottobre del 2019: "il conflitto ha costretto a fuggire circa 1,4 milioni di persone, mentre molte altre sopportano il freddo, la fame, le difficoltà e il rischio di una morte improvvisa nelle loro case. In tutto, 3,4 milioni di persone hanno bisogno di assistenza e protezione umanitaria"[370].

La maggiore durata e intensità del conflitto ucraino riflette i più profondi legami politico-economici tra Russia e Ucraina e la maggiore posta in gioco che la Russia percepisce respingendo l'influenza occidentale sul futuro dell'Ucraina[371]. I leader russi hanno percepito le manifestazioni contro il governo di Viktor Yanukovich come un colpo di stato condotto con la collusione dell'Occidente e come tale, la situazione ha fornito una conferma, da parte del Cremlino, dell'ostilità esistenziale guidata dagli Stati Uniti nei confronti degli interessi russi[372].

Sempre prendendo in esame gli eventi pre-febbraio 2022, Mosca ha creato una notevole operazione d'informazione per modellare il modo in cui gli ucraini, i russi ed il pubblico internazionale potessero percepire gli eventi in corso e, queste operazioni sono state condotte attraverso tutti i media, in particolare quelli basati sul Web[373]. A differenza della Georgia, il *cyberespionage* ha preso di mira i computer e le reti di giornalisti in Ucraina, della NATO, e di funzionari dell'UE; lo sfruttamento di tali obiettivi ha fornito alla Russia uno spaccato delle opposte

---

[369] US Department of the Army, *"Little Green Men"*, *op.cit.*, pp. 55-58.
[370] *Cfr*. "In Ucraina, alcuni esperti rischiano la vita - e gli arti - per trovare e rimuovere le mine", UNHCR, disponibile online: https://www.unhcr.it/news/storie/ucraina-esperti-rischiano-la-vita-gli-arti-trovare-rimuovere-le-mine.html [ultimo accesso: 16.04.22].
[371] S. BLANC, "Cyber War and Information War à la Russe", *op.cit.*, p. 91.
[372] *Ibidem*.
[373] *Ibidem*.

narrazioni giornalistiche nonché una conoscenza di importanti iniziative diplomatiche[374]. La Russia ha utilizzato le trasmissioni televisive in modo tale da generare supporto per le azioni in Crimea e per rafforzare il tema dell'intervento necessario di Mosca al fine di proteggere i madrelingua russi[375]. Inoltre, i media online filo-russi[376] sponsorizzavano contenuti anti-russo e notizie per influenzare l'opinione pubblica, come per esempio: negare la presenza dell'esercito russo in Ucraina o incolpare l'Occidente per aver condotto una vasta guerra informativa contro la Russia[377]. Negando il coinvolgimento degli attacchi fino alle fasi successive del conflitto, la Russia ha continuato a trasmettere il suo desiderio di attenuare la crisi aumentando così la confusione dell'opinione pubblica. Dal momento che gli Stati Uniti, la NATO e l'Unione europea non sono stati in grado di prevedere gli obiettivi della Russia, essa ha potuto sfruttare il *controllo riflessivo* per operare all'interno dei circuiti decisionali occidentali, per ridurre i costi delle sue azioni contro l'Ucraina e per tenere gli Stati Uniti e i loro alleati fuori dal conflitto[378] e, quando Putin ha ammesso la presenza di truppe russe in Ucraina, aveva già annesso la Crimea[379]. Le comunicazioni strategiche della Russia miravano in modo proattivo ai ribelli filo-russi, e alla comunità internazionale al fine di alienare l'Ucraina dai suoi alleati e simpatizzanti, ma in particolare sono due i temi chiave che ha

---

[374] E.J. IASELLO, "Russia's Improved Information Operations: From Georgia to Crimea", *Innovations in Warfare & strategy*, The US Army War College Quarterly Parameters, Vol. 47 n. 2, estate 2017, p. 55.
[375] D. COLIN, "Could Russia Use Cyberwarfare to Further Destabilize Ukraine?", Mashable, 14 aprile 2014, disponibile online: http://mashable.com/2014/04/14/russia-ukraine-cyber-warfare/ [ultimo accesso: 16.04.22].
[376] il sito web Ukrayinska Pravda era una versione pro-russa del popolare sito di notizie ucraino Pravda e le fonti filo-russe avrebbero comunicato false narrazioni su eventi reali.
[377] *Cfr*., "Ukraine, West Wage Information War against Us – Russians", *RT*, 12 novembre 2014, disponibile online: http://www.rt.com/politics/204827-ukraine-west-information-warfare [ultimo accesso: 16.04.22].
[378] E.J. IASELLO, "Russia's Improved Information Operations: From Georgia to Crimea" *op.cit.*, p. 56.
[379] Y. KARMANAU E V. ISACHENKOV, "Vladimir Putin Admits for First Time Russian Troops Took Over Crimea, Refuses to Rule Out Intervention in Donetsk", *National Post*, Toronto, 17 aprile 2014, disponibile online: https://nationalpost.com/news/world/vladimir-putin-admits-for-first-time-russian-troops-took-over-crimea-refuses-to-rule-out-intervention-in-donetsk [ultimo accesso: 16.04.22].

promosso: 1) che il governo ucraino fosse fascista e anti-russo; 2) dichiararono che l'amministrazione russa avrebbe migliorato la qualità della vita della popolazione[380]. I messaggi rivolti ai ribelli li hanno tenuti impegnati nella lotta, mentre i messaggi alla popolazione hanno creato una giustificazione morale per sostenere i ribelli[381].

Indagini d'opinione in Russia indicano l'efficacia di questi sforzi nel modellare le percezioni in Russia[382], ad esempio, un sondaggio del Levada Institute del 2014 ha scoperto che il 69% dei russi riteneva che questi media fornissero un quadro oggettivo della crisi in Ucraina e l'88% degli intervistati riteneva che gli Stati Uniti e l'Occidente stessero conducendo una guerra d'informazione contro la Russia[383].

Mosca aumentò la pressione economica sull'Ucraina e sugli stati dell'Europa occidentale che si affidano alle *pipelines* che attraversano l'Ucraina; ed anche i collegamenti tra lo Stato russo, le imprese e le singole élite ucraine sono stati sfruttati per consolidare sia la presa della Russia sulla Crimea che sugli ucraini filo-russi delle regioni orientali[384].

Il tenente generale e specialista in arte operativa e tattica dell'aeronautica, V. L. Makhnin, ha affermato che le analogie e altre forme di influenza sono introdotte nel processo riflessivo per controllare le percezioni[385]. Ad esempio, le analogie possono essere utilizzate per discutere argomenti che non possono essere osservati e, nell'arte militare, l'analogia è un approccio cognitivo che aiuta a

---

[380] E.J. IASELLO, "Russia's Improved Information Operations: From Georgia to Crimea" *op.cit.*, p. 57.
[381] *Ibidem*.
[382] *Cfr*. D. VOLKOV, "Supporting a War That Isn't: Russian Public Opinion and the Ukraine Conflict", *Carnegie Endowment for International Peace*, Washington DC, 9 settembre 2015, disponibile online: https://carnegie.ru/commentary/61236 [ultimo accesso: 16.04.22].
[383] Intervista, "Information Warfare", *Levada Center*, 12 novembre 2014, disponibile online: http://www.levada.ru/eng/information-warfare [ultimo accesso: 16.04.22].
[384] S. BLANC, "Cyber War and Information War à la Russe", *op.cit.*, p. 91.
[385] V. L. MAKHNIN, "Reflexive Processes in Military Art: The Historico-Gnoseological Aspect", *Military Thought* (versione in inglese), East View publications, n. 2, 2013, p. 40.

sviluppare concetti per ottenere risultati specifici[386]. Si ricorda l'uso dei media russi dell'analogia fascista e nazista in riferimento alle persone che combatterono in piazza Maidan contro il presidente ucraino Viktor Yanukovych; un'analogia disegnata col fine di ottenere il sostegno della popolazione russa, poiché i russi ricordano bene l'assalto nazista nella Seconda guerra mondiale e, quindi, questa analogia tocca un nervo scoperto. Le analogie possono servire riflessivamente come una forte forza unificante, queste sono utilizzate spesso da Putin, ad esempio egli ha affermato in diverse occasioni che l'incursione della Russia in Crimea era diversa dall'incursione della NATO in Kosovo[387].

Andrei Malgin, scrivendo sul Moscow Times[388], ha osservato che, secondo la propaganda di Putin, la Russia doveva salvare la Crimea, ed ora l'Ucraina, dal fascismo e dai seguaci di Stepan Bandera[389].

La narrazione di una realtà affine agli interessi della propria nazione è quindi di estrema importanza per mantenere la lealtà dei cittadini. Mosca fece sembrare che tutti i soggetti coinvolti nella protesta di Maidan fossero fascisti o neonazisti e queste immagini iniziarono a sostituire la realtà oggettiva con l'aiuto di *spin doctor* del Cremlino, tra cui Kiselev, che furono in grado di ricreare nella mente di molti cittadini russi alcuni degli orrori associati a gruppi specifici in Ucraina durante la Seconda Guerra Mondiale[390]. La linea di pensiero era offensiva, incolpando l'Ucraina per la carneficina di Maidan, richiedendo azioni

---

[386] *Ibidem*.
[387] L. CURIKA, "Defence Strategic Communications", *The official journal of the NATO Strategic Communications Centre of Excellence*, NATO Strategic Communications Centre of Excellence, Riga, Lettonia, Vol.1, n. 1, Winter 2015, p. 16.
[388] A. MALGIN, "Russia is Following in Nazi Germany's Footsteps", *The Moscow Times*, 13 marzo 2014, disponibile online: https://www.themoscowtimes.com/2014/03/12/russia-is-following-in-nazi-germanys-footsteps-a32922 [ultimo accesso: 16.04.22].
[389] Stepan Andrijovič Bandera è stato un politico ucraino, leader dell'Organizzazione dei nazionalisti ucraini (OUN), fondatore dell'Esercito Insurrezionale Ucraino (UPA) e aderente all'ideologia fascista, collaborò con la Germania nazista durante la Seconda guerra mondiale per combattere contro l'occupazione sovietica.
[390] *Ivi*, 19-24. Il cast di personaggi che hanno sostenuto questa campagna includeva sia Panrin che Dugin e funzionari chiave del governo, dai vice-ministri al Presidente stesso.

dall'Ucraina per fermare il conflitto[391]. Un metodo chiave usato da Putin per giustificare le attuali conquiste della terra e invocare una nuova realtà è il concetto di autodeterminazione; Putin promette di proteggere i russi residenti al di fuori dei suoi confini e di aiutarli, se necessario, a combattere. Con il sostegno della Russia, questi cittadini sembrano servire da catalizzatori per l'intervento russo "umanitario", se necessario o se appare l'opportunità come con la Crimea[392].

Il Centro di eccellenza cooperativo per la difesa informatica della NATO ha pubblicato un resoconto della guerra cibernetica in Ucraina fino a novembre 2015[393]; questo studio dimostra il verificarsi di attacchi informatici e IW contro la rivoluzione ucraina nel 2013-2014 e durante i conflitti e le indagini hanno rivelato una campagna informatica russa nota come *Operazione Armageddon*, che secondo quanto riferito è iniziata a metà 2013 proprio nel momento in cui sono iniziati i negoziati attivi per un accordo di associazione UE-Ucraina che, la Russia, ha ritenuto pubblicamente una minaccia alla sicurezza nazionale [394]. Secondo una società di sicurezza informatica degli Stati Uniti, gli aggressori hanno utilizzato e-mail di *spear-phishing* con allegati apparentemente ufficiali per attirare i funzionari ucraini ed altri obiettivi di alto livello, il malware ha quindi infettato i computer delle vittime ed è stato utilizzato per identificare le strategie militari ucraine, e su di esse è stata impostata la strategia russa[395].

---

[391] *Ibidem*.
[392] *Ibidem*.
[393] K. GEERS, *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015.
[394] S. BLANC, "Cyber War and Information War à la Russe", *op.cit.*, p. 92.
[395] J.LEWIS, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare", *Looking Glass*, Arlington, 28 aprile 2015, disponibile online: https://www.lookingglasscyber.com/blog/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/ [ultimo accesso: 16.04.22].

Come in Georgia, anche gli hacker nazionalisti, come *CyberBerkut*, hanno intrapreso una varietà di attacchi informatici contro l'Ucraina; questo gruppo ha eseguito attacchi di *distribution denial of service* e *defacement* contro le pagine web del governo ucraino e della NATO, intercettato i documenti di cooperazione militare USA-Ucraina e ha tentato di influenzare le elezioni parlamentari ucraine interrompendo la rete della Commissione elettorale centrale dell'Ucraina[396].

A fine dicembre 2015, tuttavia, i cyber attori filo-russi si sono allontanati da quelli che erano fondamentalmente attacchi di disturbo e hanno perpetrato quello che si ritiene sia il primo attacco informatico ai danni di una rete elettrica di un altro paese. Sofisticati attacchi informatici hanno chiuso tre società regionali di distribuzione di energia elettrica, colpendo circa 225.000 clienti, come registrato da un rapporto investigativo del Dipartimento della Sicurezza Nazionale degli Stati Uniti, questi attacchi sincronizzati e coordinati sono stati condotti da remoto, sfruttando le credenziali di operatori ucraini e dirottando a distanza il funzionamento degli interruttori in più di cinquanta sottostazioni regionali; con molta probabilità, spiega il rapporto, le credenziali sono state ottenute con largo anticipo rispetto all'evento del 23 dicembre 2015[397]. Quasi certamente questo attacco voleva avere principalmente un impatto psicologico e ha voluto sottolineare le conseguenze delle politiche anti-russe di Kiev[398], minando al contempo la fiducia dei cittadini ucraini nel loro governo. Inoltre, si può affermare che l'attacco

[396] Agence France-Presse (AFP), "Hackers Target Ukraine's Election Website", *Security Week*, 25 ottobre 2014, disponibile online: http://www.securityweek.com/hackers-target-ukraines-election-website [ultimo accesso: 16.04.22].
[397] US Department of Homeland Security, *Cyber-Attack against Ukrainian Critical Infrastructure*, 25 febbraio 2016, disponibile online: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01 [ultimo accesso: 16.04.22].
[398] Intorno al periodo dell'attacco, il parlamento ucraino aveva preso in considerazione un disegno di legge per nazionalizzare le compagnie elettriche private in Ucraina, alcune delle quali erano parzialmente possedute da potenti oligarchi russi.

informatico ha rispecchiato il pensiero strategico e la pianificazione operativa russa in merito all'approccio generale difensivo sulla guerra dell'informazione, poiché è stato scatenato dopo che i nazionalisti ucraini e tartari di Crimea hanno disabilitato le linee di trasmissione di elettricità nella Penisola a partire dal 22 novembre 2015[399]. L'interruzione elettrica totale della Crimea è durata due settimane[400], pertanto se l'attacco informatico all'Ucraina, qualora fosse stato prodigato direttamente o indirettamente dalle autorità russe, suggerisce una logica strategica che è stata vista anche in Georgia, dove vi erano le capacità di attaccare l'infrastruttura energetica, ma non sono state attivate, poiché lo Stato georgiano non ha intensificato il conflitto e le potenze occidentali non sono intervenute[401]. In questo caso gli operatori cyber russi non avevano quindi motivo di attaccare il sistema di approvvigionamento energetico della Georgia, al contrario, l'attacco alla fornitura di energia della Crimea è stata, agli occhi russi, un'escalation che ha suscitato una risposta in qualche modo simmetrica[402].

Durante l'incontro formale tenutosi al Cremlino il 18 marzo 2014 in occasione dell'annessione della Crimea alla Federazione Russa, il Presidente Putin ha parlato di "mosse occidentali non professionali e ciniche che destabilizzano la situazione in Ucraina" e la contrappone ad una "pacifica azione intrapresa dalla Russia"[403]. Insieme a membri accuratamente selezionati di entrambe le Camere del Parlamento, gli

---

[399] I. NECHEPURENKO e N. MACFARQUHAR, "As Sabotage Blacks Out Crimea, Tatars Prevent Repairs," *New York Times*, 23 novembre 2015, disponibile online: https://www.nytimes.com/2015/11/24/world/europe/crimea-tatar-power-lines-ukraine.html?searchResultPosition=1 [ultimo accesso: 16.04.22].
[400] I. NECHEPURENKO, "Electricity Restored to Crimea After 2 Weeks of Darkness", *New York Times*, 8 dicembre 2015, disponibile online: https://www.nytimes.com/2015/12/09/world/europe/electricity-restored-to-crimea-after-2-weeks-of-darkness.html?searchResultPosition=1 [ultimo accesso: 16.04.22].
[401] S. BLANC, "Cyber War and Information War à la Russe", *op.cit.*, p. 92.
[402] *Ibidem*.
[403] J. DARCZEWSKA, "The anatomy of Russian information warfare.", *op.cit.*, p. 23.

inviati alla riunione includevano anche i capi dei servizi segreti, i membri del Consiglio di sicurezza, i diplomatici guidati da Sergey Lavrov, i due principali rappresentanti della geopolitica Dugin e Panarin, ed altri, così come Dmitry Kiselev insieme ad alcuni rappresentanti dei media che avevano servito bene il governo, erano altresì presenti tutti i politici e i funzionari che avevano contribuito al successo dell'operazione di Crimea[404]. Questa era una conferma simbolica del fatto che sabotaggi segreti e quelli alla luce del sole: canali diplomatici, tecnologi della comunicazione politica, filosofi, nonché uno stratega mediatico di successo, avevano preso il controllo della Crimea e della sua annessione. Lo stesso giorno, il professor Panarin ha pubblicato una nota intitolata "La tecnologia della vittoria" sul suo gruppo di discussione del portale VKontakte[405], in cui spiegava ai suoi studenti che: a) rispetto all'agosto 2008, la Russia ha adottato molte precauzioni in Crimea per impedire il manifestarsi di uno scenario violento; b) che la Russia ha trovato una ricetta per contrastare le rivoluzioni colorate che assumono la forma di colpi di stato politici; c) che al mondo è stato offerto un percorso alternativo di sviluppo, che si basa su valori spirituali ed etici; d) che le azioni della Russia in tutti i settori della lotta contro l'informazione (diplomatica, finanziaria ed economica, aziendale, ecc.) sono state condotte in stretto coordinamento e dirette personalmente da Vladimir Putin[406].

Panarin classificò l'operazione di Crimea come elemento di una guerra di informazione difensiva ed ha ammesso che si è trattato di un'operazione combinata, pianificata e coordinata, suggerendo indirettamente e metaforicamente che ci dovrebbe essere un

[404] *Ibidem*.
[405] *Ibidem*.
[406] *Ivi*, p. 24.

consolidamento della popolazione di lingua russa dell'Ucraina, sottolineando l'impegno ed il valore di *Berkut* in questa operazione.

I rappresentanti dei media russi e dei servizi segreti hanno rilasciato dichiarazioni in modo simile. Dmitry Kiselev ha annunciato sul canale 1 e sulle stazioni televisive Rossiya-24 che a "Barack Obama gli stanno diventato i capelli grigi dalla paura"[407], ha anche vantato che "la Russia è l'unica potenza in grado di trasformare gli Stati Uniti in polvere radioattiva"[408]. Mentre, il generale Aleksandr Mikhailov, ex capo della direzione per i contatti con il pubblico dell'FSB, ha riassunto l'operazione indicando la data precisa della sconfitta dell'avversario: il 16 marzo, ovvero la data del referendum della Crimea[409]. Ha specificato che la guerra dell'informazione esiste dai tempi che furono, ma gli elementi chiave della guerra dell'informazione condotta in Crimea sono stati principalmente i seguenti: il fattore psicologico, il coinvolgimento personale del Presidente Putin, il ricatto e le sanzioni[410].

Dopo l'annessione della penisola, le forze armate sono state coinvolte in combattimenti nell'Ucraina orientale, questi usi dello strumento militare in concerto con altri mezzi per ottenere l'effetto desiderato sono una buona illustrazione dei principi suggeriti da Saifetdinov e Streltsov. Il centro gravitazionale, per dirla alla Clausewitz, non era il territorio, ma l'impegno dell'Ucraina di resistere e tale volontà è stato deliberatamente diminuito attraverso l'ambiente informativo con l'obiettivo chiave di controllare l'infrastruttura di comunicazione in Crimea. I soldati russi – "i piccoli uomini verdi" senza né mostrine né

---

[407] M. TADEO, "State television presenter warns Russia could turn the US into radioactive dust", *Indipendent*, 17 marzo 2014, disponibile online: https://www.independent.co.uk/news/world/europe/state-television-presenter-warns-russia-could-turn-the-us-into-radioactive-dust-9197433.html [ultimo accesso: 16.04.22].
[408] *Ibidem*.
[409] *Cfr*. Генерал-майор Михайлов об инфовойнах: Собака лает, караван идет, но мы же не верблюды Читайте, (intervista a Mikhailov, *Pravda.ru*, 2014) disponibile online in lingua originale al seguente link: https://www.pravda.ru/news/society/1201182-war/ [ultimo accesso: 16.04.22].
[410] *Ibidem*.

bandiera – hanno assicurato le infrastrutture in mano alla Russia, come stazioni TV e radio, nonché operatori di telefonia mobile. Il movimento Maidan e il nuovo governo di Kiev furono demonizzati, ad esempio con la pubblicazione di e-mail presumibilmente autentiche che dimostravano che i nuovi leader ucraini erano marionette occidentali. Chiunque fosse dietro le pubblicazioni, le storie sono state trattate in modo prominente nei media russi controllati dallo Stato, anche le agenzie governative russe non militari hanno cercato attivamente di controllare l'ambiente dell'informazione, ad es. il social network VKontakte che nel dicembre 2013, l'FSB ha ordinato al CEO e fondatore di VKontakte, Pavel Durov, di fornire informazioni sui gruppi filo-ucraini[411]. Durov afferma di aver rifiutato e successivamente ha pubblicato gli ordini online. In seguito, si è dimesso e ha lasciato la Russia, accusando il governo di un'acquisizione ostile di VKontakte. Tutte queste misure sono in linea con l'idea di uno spazio di informazione russo sovrano che deve essere difeso[412]. Tuttavia, la caratteristica più sorprendente rimane il coordinamento tra le diverse attività, ad esempio: i messaggi inviati dalla leadership politica russa, attraverso canali diplomatici e attraverso media internazionali controllati dallo Stato russo come RT, sono stati supportati da telefonate trapelate che presumibilmente presentavano diplomatici americani[413] ed estoni[414] implicati nella vicenda. Queste azioni corrispondono alle idee sulla guerra dei mass media espresse nel "Concetto per la sicurezza

[411] U. FRANKE, "War by non-military means", *op.cit.*, p. 43.
[412] *Ibidem*.
[413] BBC, *Ukraine crisis: Transcript of leaked Nuland-Pyatt call*, 7 febbraio 2014, online: https://www.bbc.com/news/world-europe-26079957 [ultimo accesso: 16.04.22].
[414] Reuters, *Estonia denies leaked call implicates Ukraine protesters in killings*, 5 marzo 2014, disponible online al seguente link: https://www.reuters.com/article/us-estonia-eu-ukraine/estonia-denies-leaked-call-implicates-ukraine-protesters-in-killings-idUSBREA2423O20140305 [ultimo accesso: 16.04.22].

della società della Federazione Russa" e nella "dottrina della sicurezza delle informazioni" del 2000 e seguente.

L'esercitazione militare[415] su larga scala vicino al confine ucraino è servito da diversivo che ha attirato l'attenzione lontano dalla Crimea e ha reso più difficile capire cosa sarebbe successo[416]. La Russia non ha annesso La Crimea direttamente, ma il parlamento regionale ha eletto un nuovo primo ministro per poi richiedere l'adesione alla Federazione Russa, proiettato l'immagine dell'annessione della Crimea come irreversibile sia militarmente che politicamente. Le forze speciali russe sono riuscite a prendere terreno e obiettivi chiave in Crimea senza, quasi, spargimento di sangue e ciò ha reso molto più difficile per il governo ucraino rispondere con la forza militare[417].

Un altro aspetto interessante da notare è come il ministro degli affari esteri svedese Carl Bildt sia stato oggetto della guerra dell'informazione russa, poiché egli, durante la crisi e la successiva aggressione della Russia contro l'Ucraina dalla fine del 2013 in poi, fu uno schietto sostenitore dell'Ucraina e un critico della Russia fino al termine del suo mandato nel settembre 2014. La campagna diffamatoria contro Bildt è parte della strategia, ovvero si è cercato di intimidire i suoi ascoltatori cercando di raccontare una nuova realtà e deviando l'oggetto della discussione; egli è stato sistematicamente infangato dai media russi controllati dallo Stato, come ad esempio RT[418]. Bildt è stato additato come un agente della CIA e, rimanendo nel contesto svedese, il conduttore televisivo Kiselyov rincara la dose disegnando un'immagine

[415] *Cfr*. Geopoliticalcenter, "L'esercitazione delle forze armate russe al confine con l'Ucraina e non solo", 28 febraio 2014, disponibile online: http://www.geopoliticalcenter.com/attualita/lesercitazione-delle-forze-armate-russe-al-confine-con-lucraina-e-non-solo/ [ultimo accesso: 16.04.22].
[416] U. FRANKE, "War by non-military means", *op.cit.*, p. 43-44.
[417] *Ibidem*.
[418] *Ivi*, p. 44-45.

denigratoria della degenerata educazione dei bambini svedesi[419]. In seguito, Dmitrii Kiselyov, è stato nominato capo della nuova agenzia di stampa internazionale russa *Rossiya Segodnya*[420] ed anche vicedirettore della holding televisiva statale russa VGTRK[421]; il suo spettacolo è stato criticato da altri media occidentali di essere un *soapbox* per promuovere la propaganda pro-Putin, poiché il conduttore televisivo è famoso per le stravaganti asserzioni che demonizzano l'Occidente, stigmatizzano gli omosessuali e ritraendo l'Ucraina come un paese invaso da violenti fascisti[422].

Sulla scia della tragedia del volo MH17 della Malaysian Airlines, Bildt e il ministro degli affari esteri polacco Radek Sikorski sono stati soprannominati i principali responsabili di questa follia, avendo progettato di rompere i legami tra Russia e Ucraina che avevano impiegato secoli per costruire[423].

Il significato della campagna anti-Bildt non deve essere sopravvalutato, ciò che è interessante in questo contesto è il modo in cui la denigrazione di Bildt è strettamente correlata agli aspetti politici della guerra dell'informazione di Streltsov, ed offre un eccellente esempio. Egli, come meglio espresso nel capitolo precedente, sostienine che lo Stato deve mantenere un'immagine positiva dei suoi leader

---

[419] S. ENNIS, "Russia: Children's toilet TV show drawn into Ukraine-EU row", *BBC news*, 4 dicembre 2013 disponibile online: https://www.bbc.com/news/blogs-news-from-elsewhere-25198264 [ultimo accesso: 16.04.22].

[420] formata dalla fusione dell'agenzia di stampa statale *RIA Novosti* e della stazione radio internazionale ufficiale, *Voice of Russia*.

[421] All-Russia State Television and Radio Broadcasting Company (russo: Всероссийская государственная телевизионная и радиовещательная компания, V serossiyskaya G osudarstvennaya T elevizionnaya i R adioveshchatelnaya K ompaniya), quindi VGTRK (in cirillico: ВГТРК) che gestisce trasmissioni televisive e radiofoniche in molte delle lingue, oltre al russo, parlate nelle varie regioni Russia (anche se quella ufficiale rimane il russo). La società è stata fondata nel 1990 e ha sede a Mosca.

[422] S. ENNIS, "Dmitry Kiselyov: Russia's chief spin doctor", *BBC news*, 2 aprile 2014, disponibile online: https://www.bbc.com/news/world-europe-26839216 [ultimo accesso: 16.04.22].

[423] E. LOZANSKY, "Slam dunk journalism" or propaganda warfare?, *RT*, 25 luglio 2014, disponibile online: https://www.rt.com/op-ed/175548-foreign-policy-us-russia-journalism/ [ultimo accesso: 16.04.22]. Cfr., anche B. MACDONALD, "Goodbye to Carl Bildt, out of line and out of time", *RT*, 25 agosto 2014, disponibile online: http://rt.com/op-edge/182600-bildt-swiss-far-right-ukraine/ [ultimo accesso: 16.04.22].

politici, e afferma esplicitamente che la guerra dell'informazione difensiva dovrebbe identificare e fermare la propaganda e la disinformazione dannose, nelle sfere pubbliche nazionali e internazionali. La guerra delle informazioni, ha svolto un ruolo cruciale nel successo dell'operazione di Crimea, sono stati conquistati i nodi della comunicazione, la Crimea è stata tagliata fuori dal resto del mondo e una massiccia campagna è stata diretta verso la comunità internazionale per legittimare l'annessione[424].

Il modello d'azione russo durante l'annessione illegale della Crimea si accosta alle caratterizzazioni ufficiali della guerra dell'informazione, ovvero: l'uso della guerra dell'informazione per raggiungere obiettivi politici senza usare la forza militare e il suo uso per creare una reazione positiva della comunità, internazionale ed interna, all'uso successivo della forza militare[425]; minare i sistemi politici, economici e sociali, destabilizzando una società di uno Stato con una massiccia influenza psicologica e anche esercitare pressioni sui *decision makers* di uno Stato affinché prenda decisioni che siano nell'interesse dell'avversario[426]; l'uso dei mass media stranieri da parte di servizi speciali, per ridurre le capacità di difesa del paese e la sicurezza dello Stato e diffondere disinformazione[427]. Viene rispettata inoltre la visione di Gerasimov sul ruolo dei metodi non militari nei conflitti moderni[428], ovvero egli chiarisce che la deterrenza strategica è una misura militare, ma affinché tali misure siano efficaci devono essere convertite in pressioni politiche

[424] U. FRANKE, "War by non-military means", *op.cit.*, p. 44.
[425] "Dottrina militare della Federazione Russa", 2010, *op.cit.*, § 13, g.
[426] "Opinioni concettuali sulle attività delle forze armate", 2011, *op.cit.*, §1.
[427] "Dottrina sulla sicurezza delle informazioni della Federazione Russa", 2000, *op.cit.*, § 6.
[428] *Cfr*. il famoso articolo: Герасимов Валерий, Ценность науки в предвидении Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, (trad. Gerasimov Valery, Il valore della scienza in previsione. Le nuove sfide richiedono un ripensamento delle forme e dei metodi di guerra), *Vpk* news, 26 febbraio 2013, disponibile online: https://www.vpk-news.ru/articles/14632 [ultimo accesso: 16.04.22]. *Cfr*. inoltre, la § 3.2.10. di questo elaborato.

e diplomatiche ed il modo per farlo è assicurarsi di consegnare il "messaggio" a coloro che devono essere sottoposti a pressioni.

Riassumendo

Il successo della Russia in Crimea è il risultato diretto di ciò che è stato appreso e perfezionato dopo la guerra del 2008[429]. La Federazione Russa ha dimostrato ancora una volta di essere disposta a usare la forza per impedire a un'ex repubblica di aderire alla NATO o all'UE; mentre per quanto riguarda l'annessione della Crimea, questa azione ha un valore strategico specifico, ovvero quello di possedere una base sul Mar Nero. Inoltre, le azioni della Russia nel Donbass si possono leggere come una mossa strategica estremamente sottile ovvero che, per il momento, non bramano l'annessione di ulteriori territori, ma desiderano semplicemente una regione separatista semiautonoma in Ucraina, proprio come in Georgia, così da rendere quasi impossibile l'adesione ad un'organizzazione come la NATO, che richiede ai membri dell'alleanza di avere integrità territoriale[430].

Le dichiarazioni sul sito web del Ministero degli Affari esteri ucraino, che si riportano di seguito, confermano come la Russia segue le linee teoriche sviluppate dai suoi ufficiali militari[431]:

"[a)] la Russia ha pianificato in anticipo un'aggressione militare contro l'Ucraina. La vittoria della rivoluzione della dignità era solo un comodo pretesto. [b)] l'aggressione russa mirava a distruggere l'Ucraina come stato indipendente [questo sostiene la tesi che la Russia non vuole l'Ucraina integra territorialmente così non può entrare a far parte della NATO]. [c)] L'aggressione militare è solo uno degli elementi della guerra russa contro l'Ucraina. Altri elementi comprendono: 1) propaganda basata su bugie e falsificazioni; 2) pressione commerciale ed economica; 3) blocco dell'energia; 4) terrore

[429] L. BEEHENER et. al., "Analyzing the Russian Way of War", *op.cit.*, p. 71.
[430] A. RÁCZ, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, Finnish Institute of International Affairs, Report n. 43, Helsinki, 2015.
[431] *Cfr*. § 2 di questo elaborato.

e intimidazione nei confronti dei cittadini ucraini; 5) attacchi informatici; 6) una forte negazione del fatto stesso della guerra contro l'Ucraina, nonostante un'ampia portata di prove inconfutabili; 7) uso delle forze filo-russe e degli stati satellite nel proprio interesse; 8) incolpare l'altra parte per i propri crimini"[432].

La capacità della Russia di prendere la Crimea senza sparare un colpo è stata brillante, ma non sarebbe potuto accadere senza le basi poste con mesi e anni di anticipo. Oltre alla pianificazione operativa e alla messa in scena delle forze lungo il confine come un forte deterrente, la Russia aveva condotto la sovversione molto prima di introdurre "piccoli uomini verdi"[433]. La Russia ha identificato i punti di vulnerabilità dell'economia, delle forze armate e dell'amministrazione statale e ha usato la corruzione e l'intimidazione per costringere i funzionari locali; inoltre, il Cremlino ha sostenuto e finanziato organizzazioni politiche e culturali fedeli alla Russia ed ha usato i suoi media per creare narrazioni favorevoli a Mosca e contrarie al governo ucraino[434].

Come per la Georgia, la Federazione Russa aveva chiaramente sviluppato piani operativi per un'invasione dell'Ucraina e da quando è diventato uno stato indipendente non è riuscita a sviluppare una seria strategia difensiva, rendendo le cose più facili per la Russia di quanto avrebbero potuto essere[435]. Sempre come la Georgia, osservando gli avvenimenti in Ucraina, occorre mettere in evidenza la capacità della Russia di raggiungere il dominio dell'escalation sulla sua frontiera e di farlo anche con grande velocità se necessario. Dopo aver perso la battaglia di IO in Georgia, la Russia ha continuato a investire in questo campo: ha combinato segretezza, inganno, minacce e accuse nel creare

[432] *Cfr*. Il sito web del Ministero degli Affari Esteri ucraino al seguente link: https://mfa.gov.ua/en/10-facts-you-should-know-about-russian-military-aggression-against-ukraine [ultimo accesso: 16.04.22].
[433] L. BEEHENER et. al., "Analyzing the Russian Way of War", *op.cit.*, pp. 72-73.
[434] A. RÁCZ, "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist", *op.cit.*, pp. 56-60.
[435] L. BEEHENER et. al., "Analyzing the Russian Way of War", *op.cit.*, pp. 72-73.

la narrativa per la comunità internazionale e ha continuamente negato il coinvolgimento russo per promuovere un messaggio coerente[436]. Molti degli obiettivi iniziali per gli agenti russi in Crimea e nel Donbass erano i mezzi di comunicazione, così da poter sostituire le trasmissioni ucraine con quelle russe, stabilendo in tal modo un monopolio dell'informazione[437], questo risulta evidente pensando che in Crimea hanno quasi eliminato tutti i telefoni fissi, Internet e mobili ucraini[438].

La Russia ha diminuito il ruolo delle forze militari palesi, dato sia il costo politico sia quello militare associato al suo impiego[439]. In Crimea, invece di forze militari in uniforme, i russi hanno inviato "piccoli uomini verdi" che hanno continuato a negare di essere agenti russi e nel Donbass, invece di affidarsi principalmente a grandi formazioni, unità più piccole furono inviate attraverso il confine dichiarandosi semplicemente truppe russe in congedo che non agivano per conto dello Stato[440]. Una tecnologia relativamente nuova è stata applicata in Ucraina rispetto al 2008 in Georgia, ovvero l'utilizzo consistente degli UAV, che sono stati usati principalmente per un ruolo di intelligence, sorveglianza e ricognizione[441]. Infine, in Ucraina la Russia ha violato gli accordi di Minsk I e II (2014-2015), che sono stati firmati per eliminare le tensioni nella regione del Donbass così come allo stesso modo in Georgia, la Russia ha violato i termini del cessate il fuoco del 2008 spostando i confini e non smilitarizzando completamente le aree contese[442].

---

[436] US Department of the Army, *"Little Green Men"*, *op.cit.*, p. 48.
[437] A. RÁCZ, "Russia's Hybrid War in Ukraine", *op.cit.*, pp. 62-65.
[438] US Department of the Army, *"Little Green Men"*, *op.cit.*, p. 46.
[439] *Ibidem*.
[440] *Ibidem*.
[441] *Ibidem*.
[442] *Ivi*, p. 76.

Nel loro insieme, gli esempi georgiano e ucraino riflettono una logica di deterrenza con mezzi informatici. Una capacità di arrecare danno è utilizzata per dissuadere gli avversari dall'agire contro gli interessi russi; quando l'avversario non agisce a danno degli interessi russi, l'attacco informatico non viene scatenato, ma nel momento in cui l'avversario offende gli interessi di Mosca, gli attori del Cremlino elargiscono una risposta approssimativamente proporzionata[443].

[443] S. BLANC, "Cyber War and Information War à la Russe", *op.cit.*, p. 92.

Conclusioni

Avendo esplorato le basi intellettuali di alcuni degli accademici e ufficiali militari occidentali, visto ed approfondito i pensieri teorici militari russi e le espressioni di dottrine attraverso i documenti ufficiali *opensource*, nonché esaminando tre casi di studio per comprendere meglio l'uso pratico dell'information warfare russa, adesso si potranno desumere alcune conclusioni.

La guerra dell'informazione russa si è modellata da una storia di scontri con avversari tecnologicamente ed economicamente superiori, la tradizione militare russa ha fatto affidamento sul raggiungimento della vittoria attraverso una superiorità morale qualitativa di carattere quasi spirituale[444]. Questa superiorità morale richiedeva la coltivazione deliberata di un senso di integrità psicologica e culturale abbastanza forte da resistere agli effetti dell'influenza esterna[445]. L'ultima versione della dottrina russa sulla sicurezza delle informazioni ed il quadro concettuale per l'attività russa nel cyberspazio, rivelano la forza di questo impulso, contenendo ferme dichiarazioni di una pressione informativa avversaria che ha l'obiettivo di stemperare lo spirito, il morale ed i valori tradizionali russi; sul conflitto nello spazio delle informazioni quindi si riflette un tono difensivo più interessato all'integrità psicologica, percettiva e culturale che allo stato fisico delle reti[446]. Sia dai documenti strategici analizzati che dalla teoria prodotta

---

[444] D. Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford University Press, 2010, p. introduzione.
[445] *Ibidem*.
[446] L. Beehener et. al., "Analyzing the Russian Way of War", *op.cit.*, p. 66.

dagli ufficiali, si comprende bene come l'approccio russo all'information warfare sia olistico e psicologicamente orientato al cyberspazio come un sottocomponente della guerra dell'informazione.

La campagna di IW Russa funziona in gran parte su tre livelli: la manipolazione di informazioni, spionaggio e attacchi informatici. Quest'ultima è l'unica cosa nuova e di notevole impatto, in quanto consente una maggiore velocità d'azione per le pratiche di vecchio stampo sovietico. La guerra delle informazioni russa è composta da quattro pilastri: in primo luogo, e soprattutto, mira a dare il miglior significato possibile, secondo la visione russa degli eventi, alle notizie ordinarie. In secondo luogo, incita il suo pubblico attraverso informazioni false, a preparare un possibile campo di battaglia. Terzo, usa la disinformazione o crea ambiguità per confondere i soggetti coinvolti sia in attività di comando e controllo che quelli sul campo di battaglia, attraverso un sommo utilizzo del controllo riflessivo. E in quarto luogo, sostiene la falsificazione di notizie oggettivamente veritiere, contribuendo ancor di più a creare ambiguità e caos, per poi rimpiazzare i fatti accaduti con un ambiente favorevole ad una nuova realtà progettata *ad hoc* per assecondare gli obiettivi russi[447]. Questa strategia di informazione ha diversi obiettivi: degradare la fiducia nelle istituzioni; spingere le popolazioni attualmente in conflitto ad accettare semplicemente lo status quo del conflitto e a non chiedere una soluzione; infine, mantenere queste aree in conflitto semi-permanente, per così diminuire le possibilità di questi paesi di aderire alla NATO.

Dal punto di vista geopolitico, la Russia ha incassato ottimi risultati: ha sottratto l'effettiva sovranità georgiana nell'Ossezia meridionale e in Abkhazia rafforzando il controllo dei regimi separatisti filo-Mosca in

[447] *Ivi*, p. 67.

Abkhazia e nell'Ossezia meridionale, negando così il controllo di Tbilisi su questi territori in perpetuo; ha espulso le truppe georgiane e il rimanente della popolazione georgiana dalle due province secessioniste; ha impedito alla Georgia di aderire alla NATO; ha inviato un segnale forte ad altri stati, ex repubbliche sovietiche, facendo intendere che la volontà di adesione alla NATO potrebbe provocare lo smembramento territoriale, quindi perdita di sovranità, subbugli, sovversione e un'invasione militare[448]. Parte degli interessi di Mosca si traducono nella mobilitazione delle minoranze russe all'estero, motivandole ulteriormente a cercare l'autodeterminazione e fare richieste ai governi in cui risiedono. Qualora le richieste non venissero soddisfatte, un *casus belli* viene offerto al Cremlino per aiutare e liberare gli oppressi, e forse occupare il territorio[449].

Mosca ha concesso alla maggior parte degli etnici russi, in Abkhazia ed in Ossezia del Sud, la cittadinanza russa così creando una popolazione "protetta" residente in uno Stato vicino con lo scopo di minare la sua sovranità e, magari, con una probabile intenzione futura di arrivare ad una ridefinizione degli ex confini sovietici. Ma tra gli obiettivi principali di Mosca vi erano: abbattere il presidente Saakashvili e innestare una leadership più filo-russa a Tbilisi, poiché qualora un regime filo-russo si fosse istituito in Georgia, la Russia avrebbe potuto ottenere il controllo strategico dell'oleodotto Baku-Tbilisi-Ceyhan e del Baku-Erzerum; inoltre, fornendo alla Russia il controllo dell'Abkhazia e dell'Ossezia del Sud, compreso il loro spazio aereo Mosca può perseguire obiettivi di difesa più ampi nel Caucaso meridionale[450]. Insomma, tutto questo porta ad asserire che il potere continentale

[448] *Ivi*, pp. 68-69.
[449] L. CURIKA, "Defence Strategic Communications", 2015, *op.cit.*, p. 22-23.
[450] L. BEEHENER et. al., "Analyzing the Russian Way of War", *op.cit.*, p. 67-68.

russo sia in aumento, o comunque fa comprendere che il Cremlino è intenzionato a riappropriarsi del potere perduto nel secolo precedente.

L'annessione della Crimea ha rappresentato un uso deciso, competente e combinato di metodi non lineari, attraverso mezzi militari e non, per modellare lo spazio politico prima del conflitto e dare forma ad una risposta favorevole da parte della comunità nazionale ed internazionale con lo scopo di perseguire ed ottenere obiettivi e vantaggi geopolitici. La Russia è stata in grado di impadronirsi del territorio di uno Stato vicino con velocità e mobilità elevata, schierando una forza agile e professionale, usando la sua superiorità convenzionale come un diversivo. La guerra delle informazioni in Crimea ha senz'altro beneficiato dei numerosi passi falsi della leadership ucraina e del diffuso senso di ansia pubblica dopo l'espulsione di Yanukovich e, approfittando di questi sentimenti in modo predatorio, ha alimentato i timori pubblici facendo ricorso a narrazioni di violenza nazi-fascista. Le operazioni della Russia in Crimea, quindi, hanno anche beneficiato di una serie di circostanze altamente favorevoli - politiche, storiche, geografiche e militari - che limitano questo caso dal servire da modello per operazioni simili in futuro[451]. Mosca ha dimostrato efficacia nell'usare l'inganno e la sorpresa, ma il suo più grande successo è stato quello di capitalizzare la debolezza, i passi sbagliati e il processo decisionale lento o inefficace. L'esperienza nell'Ucraina orientale dà credito all'idea che, quando viene offerta resistenza e quando prevalgono condizioni meno idonee, le operazioni diventano meno efficaci[452].

[451] M. KOFMAN, et. al., "Lessons from Russia's Operations in Crimea and Eastern Ukraine", *op.cit.*, pp. 73-74.
[452] *Ibidem*.

Nell'Ucraina orientale la Russia ha cercato di annullare l'impatto strategico della vittoria di una rivolta filo-occidentale nella capitale e di mantenere l'influenza nelle regioni separatiste impegnandosi in una guerra politica[453]. Mosca sperava che un movimento anti-Maidan, principalmente composto da élite locali, opportunisti e una rete di provocatori, potesse costringere il nuovo governo di Kiev a devolvere il potere alle regioni separatiste. La campagna di informazione di Mosca ha ottenuto un parziale successo nell'evocare una causa storica e giustificabile per il movimento separatista (Novorosya)[454].

Mosca ha continuato ad espandere le sue capacità informatiche e ha effettivamente impiegato CNO a livello tattico; ad esempio, secondo quanto riferito da Reuters: i russi hanno usato dei *malware* installati su dei dispositivi Android per tracciare e colpire le unità di artiglieria ucraina[455] ed inoltre, la Russia ha condotto un attacco informatico per interrompere la rete elettrica dell'Ucraina[456]. Mosca ha ampliato il suo uso della guerra elettronica per danneggiare o distruggere le reti di C2, ostacolare i sistemi radar e falsificare i segnali GPS[457]. I comandanti ucraini hanno ricevuto messaggi di testo dopo una raffica di artiglieria, chiedendo loro se gli fosse piaciuto l'attacco, mentre ai soldati sono stati recapitati messaggi di incoraggiamento alla diserzione tentando di corrompere il morale[458].

---

[453] *Ibidem*.
[454] *Ivi*, p. 75.
[455] D. VOLZ, "Russian Hackers Tracked Ukrainian Artillery Units Using Android Implant: Report", *Reuters*, 21 dicembre 2016, disponibile online: https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU [ultimo accesso: 16.04.22].
[456] P. POTILYUK, "Ukraine Sees Russian Hand in Cyber Attacks against Power Grid", *Reuters*, 12 febbraio 2016, disponibile online: http://www.reuters.com/article/us-ukrainecybersecurity-idUSKCN0VL18E. [ultimo accesso: 16.04.22].
[457] S. SUKHANKIN, "Russian Electron Warfare in Ukraine: Between Real and Imaginable", in *Euraisa Daily Monitor*, The James Town Fondation, n. 71, 24 maggio 2017, disponibile online: https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable [ultimo accesso: 16.04.22].
[458] L. BEEHENER et. al., "Analyzing the Russian Way of War", *op.cit.*, pp. 74-75.

M. Libicki, riferndosi ai Paesi occidentali, afferma che alla luce degli avvenimenti:

> "le percezioni della guerra cibernetica potrebbero dover essere ripensate. Si potrebbe discutere la plausibilità di una determinata campagna di attacco informatico non accompagnata dalla violenza. Tuttavia, è più difficile immaginare una campagna di attacchi informatici non accompagnata da altri elementi della guerra dell'informazione, in gran parte perché quasi tutte le situazioni in cui gli attacchi informatici sono utili sono anche quelle che non offrono buoni motivi per non utilizzare altri elementi di IW. Ma molte caratteristiche di IW - non-letalità, ambiguità e persistenza - suggeriscono di usare la stessa mentalità, gli stessi strumenti e le stesse regole. L'ambiente morale influenza la propensione di un individuo a unirsi a una lotta"[459].

Mosca ha dedicato una quantità crescente di risorse al conflitto, portandolo alla fine a una guerra dagli aspetti convenzionali. Ma senza alcun dubbio, visti gli alti livelli di popolarità e il sostegno pubblico in patria, i leader russi possono ritenere che ne sia valsa la pena, poiché è stata palesata una chiara dimostrazione del potere russo con guadagni tangibili. Anche l'Ucraina, come i casi della Georgia e della Crimea, offre delle lezioni, ma non necessariamente dei modelli. L'articolo del 2013 di Gerasimov ha commentato la natura moderna della guerra, piuttosto che delineare una particolare dottrina o un approccio istituzionale e, comunque anch'egli sottolinea che ogni battaglia ha una sua logica. Non vi sono le basi quindi, per suggerire che la Russia possa adottare simili approcci di guerra contro un membro della NATO[460]. V'è senza alcun dubbio una più ampia applicabilità, di tali approcci, ai danni di altre ex repubbliche sovietiche con popolazioni di lingua russa, come ad esempio la Moldavia. Tuttavia, l'annessione della Crimea e le operazioni in Ucraina orientale potrebbero aver allertato i suoi vicini che, una volta osservato gli avvenimenti, potrebbero aver sviluppato una consapevolezza che renderebbe tali operazioni (russe) meno efficaci[461].

---

[459] M.C. LIBICKI, "The Convergence of Information Warfare", *op.cit.,* p. 62.
[460] M. KOFMAN, et. al., "Lessons from Russia's Operations in Crimea and Eastern Ukraine", *op.cit.*, p. 76.
[461] *Ibidem*.

Contestualizzando il dibattito russo sulla guerra dell'informazione nel più ampio contesto della guerra moderna, si possono trarre ulteriori osservazioni: le misure non militari superano di gran lunga quelle militari, sostiene Gerasimov; Chekinov e Bogdanov temono il mondo globalizzato ed economicamente integrato; è chiaro che v'è un vivace dibattito sulla guerra delle informazioni nel più vasto schema di cose, si attinge sia a teorie classiche come quelle di Liddell Hart sia a quelle più moderne come la guerra nel cyberspace[462]. Un'osservazione ritenuta importante dai più è che la maggior parte dei teorici percepisce la guerra dell'informazione come continua tra periodi di pace e periodi di guerra; l'analisi inoltre indica un'ampia portata dell'utilizzo di RC nel pensiero militare russo. Due aspetti sono importanti da ricordare quando si considera RC: innanzitutto, ci sono vari ambienti – computer, sistemi, spazio, deterrenza, dottrina, ecc. – in cui la Russia impiega tale pratica per ingannare l'avversario e, tale pratica è impiegata costantemente e riflette, più propriamente, il concetto russo di *Maskirovka*; in secondo luogo, è importante sottolineare che la Russia si concentra molto, come riportato da tanti autori, sull'analisi della comprensione del pensiero e sull'elaborazione delle informazioni dell'avversario, poiché senza la logica e il vocabolario del pensiero nemico, gli specialisti di RC russi non saprebbero dove, quando o come inserire le informazioni, appositamente sviluppate, per consentire al consumatore nemico di digerire, elaborare e agire secondo il piano russo[463].

Un'altra conclusione significativa è che la guerra dell'informazione non coinvolge solo le forze armate, ma piuttosto è una questione così

[462] U. FRANKE, "War by non-military means", *op.cit.*, p. 42.
[463] T. THOMAS, "Russian Military Thought", *op.cit.*, pp. 48-49.

complessa che richiede il coordinamento di molte agenzie governative e non governative; l'IW è altamente politicizzata e gli intellettuali russi prendono parte al dibattito sulla teoria militare ed abbracciano una visione della guerra dell'informazione dove la sicurezza del regime è fondamentale. Considerando la complessità dell'IW, risulta essere un'impresa ardua riuscire a separare ed individuare i singoli attori della guerra dell'informazione. Da un lato, è possibile ipotizzare, come suggeriscono alcuni analisti occidentali[464] che, sia Panarin che Dugin, così come altri studiosi che politicamente vocalizzano la narrativa della guerra dell'informazione occidentale contro la Russia, vadano di pari passo con l'establishment politico russo, alimentando l'opinione pubblica russa contro l'Occidente, permettendo così al Cremlino di rafforzare la sua presa sul potere e legittimando le sue azioni e le sue proiezioni di potenza sullo scacchiere internazionale. Sembra giusto supporre che la politicizzazione della guerra dell'informazione della Russia contro l'occidente sia stata diretta da queste scuole di pensiero e adottata di fatto dall'establishment politico[465].

Come dice Dmitri Trenin[466]: "La ricetta principale di Putin per rimanere al potere è rimanere in stretto contatto con la maggior parte delle persone e anticipare le tendenze emergenti"[467]. Secondo uno studio del Levada Center, riportato dal Journal "Defence Strategic Communication", dallo scioglimento dell'Unione Sovietica ai giorni nostri, la stragrande maggioranza della popolazione russa ha lamentato la perdita di potere[468], quasi un terzo della popolazione crede che la

[464] D. TRENIN, "Putin's Biggest Challenge Is Public Support", *Carnegie Moscow Center*, 15 gennaio 2015, disponibile online: https://carnegie.ru/2015/01/15/putin-s-biggest-challenge-is-public-support-pub-57758 [ultimo accesso: 16.04.22].
[465] L. CURIKA, "Defence Strategic Communications", 2017, *op.cit.*, p. 80.
[466] Direttore del Carnegie Moscow Centre ed uno dei critici più espliciti del regime di Putin.
[467] D. TRENIN, "Putin's Biggest Challenge Is Public Support", *op.cit.,*
[468] Il 66% nel 1992, con un picco nel 2000 con il 75% e il 56% nel 2016.

caduta dell'URSS avrebbe potuto essere evitata[469]. In altre parole, questa tristezza per l'orgoglio perduto potrebbe spiegare la sete del pubblico russo per una valida giustificazione della loro sconfitta nella Guerra Fredda contro il nemico tradizionale della Russia: l'Occidente. Forse il Cremlino non fa il lavaggio del cervello al popolo russo, ma segue semplicemente i loro cuori e le loro menti[470]. Forse l'aspetto più significativo del successo conseguito della Russia è stato impedire ai suoi più grandi avversari – gli Stati Uniti e la NATO – di portare dentro l'alleanza militare Nord-Atlantica due delle sue ex repubbliche sovietiche e, mentre l'Occidente rifiuta di riconoscere la secessione della Crimea, la Russia attesta l'annessione della penisola con il "rispetto delle procedure democratiche", un fatto difficile da contestare su una scena internazionale[471].

La guerra delle informazioni è stata definita un'arma asimmetrica e gli incidenti con la Georgia e la Crimea certamente supportano questa categorizzazione. A seguito delle rivoluzioni colorate, che hanno portato a cambiamenti di regime riusciti, sia gli episodi georgiani che quelli di Crimea rafforzano la convinzione che costruire, controllare, e diffondere informazioni in modo efficace, influenza il risultato di eventi politici.

Molti studiosi occidentali hanno classificato le tattiche russe in Ucraina come guerra ibrida: l'uso di tattiche *hard* e *soft* che si basano su deleghe e surrogati per prevenire l'attribuzione, nascondere l'intento e massimizzare la confusione e l'incertezza[472]. Nel 2015, gli ufficiali russi hanno completamente confutato l'uso di "ibrido" per descrivere le loro attività[473]. Tuttavia, il ruolo complementare e di supporto dello scontro

---

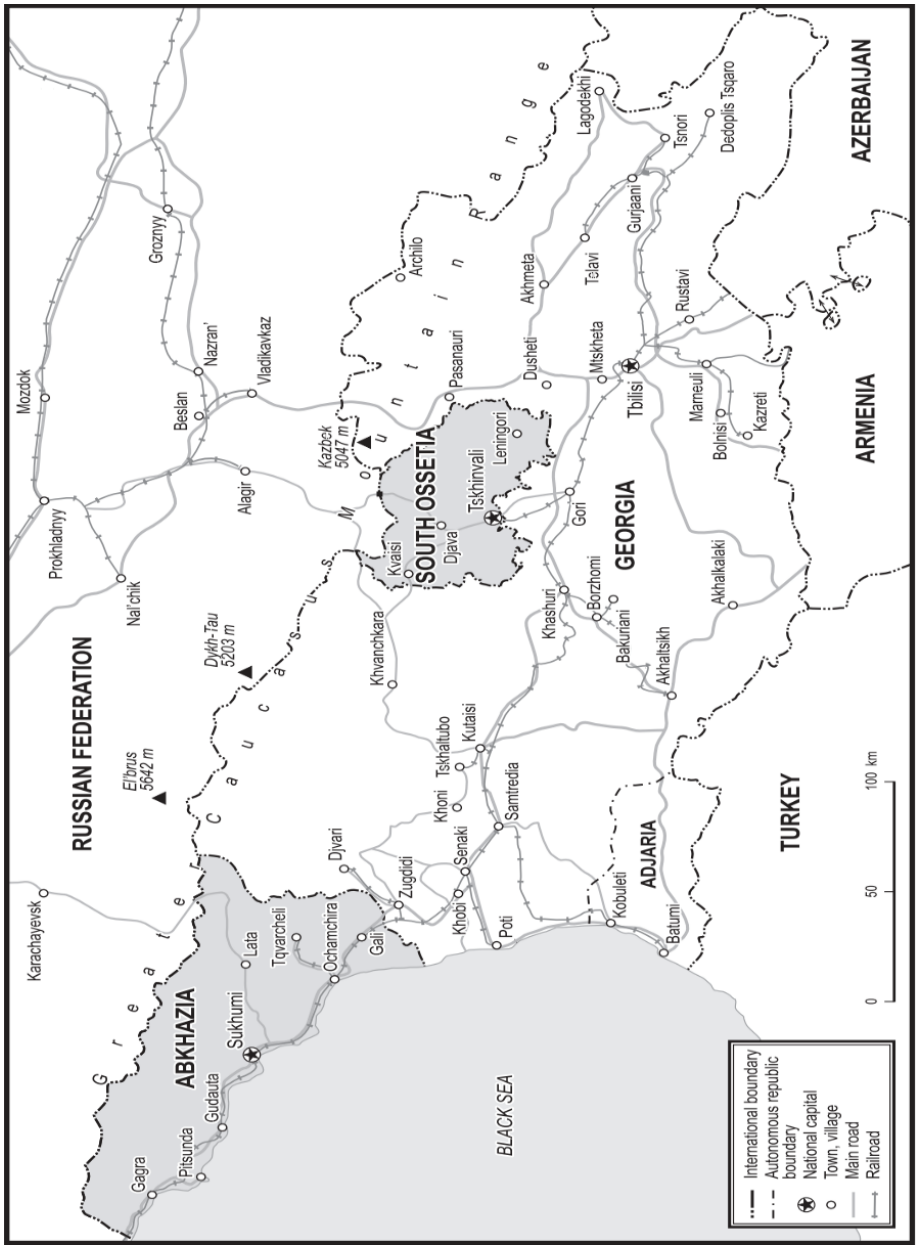
[469] L. CURIKA, "Defence Strategic Communications", 2017, *op.cit.*, p. 80-81.
[470] *Ibidem*.
[471] Sputnik, "US Policy toward Crimea Defies Reality", *Russia Insider*, 16 marzo 2015, disponibile online: http://russia-insider.com/en/2015/03/16/4534 [ultimo accesso: 16.04.22].
[472] A. MONAGHAN, "The War in Russia's Hybrid Warfare", *Parameters45*, n.4, inverno 2015-16, pp. 65–74.
[473] E.J. IASELL., "Russia's Improved Information Operations", *op.cit.,* p. 61.

informativo in Ucraina suggerisce che è meglio implementato in concerto con altre attività convenzionali e non convenzionali per ottenere la massima efficacia in campagne più ampie e non come tattica autonoma[474]. I documenti ufficiali sottolineano apertamente che l'utilizzo dell'*information warfare* è un modo per risolvere i conflitti fra Stati.

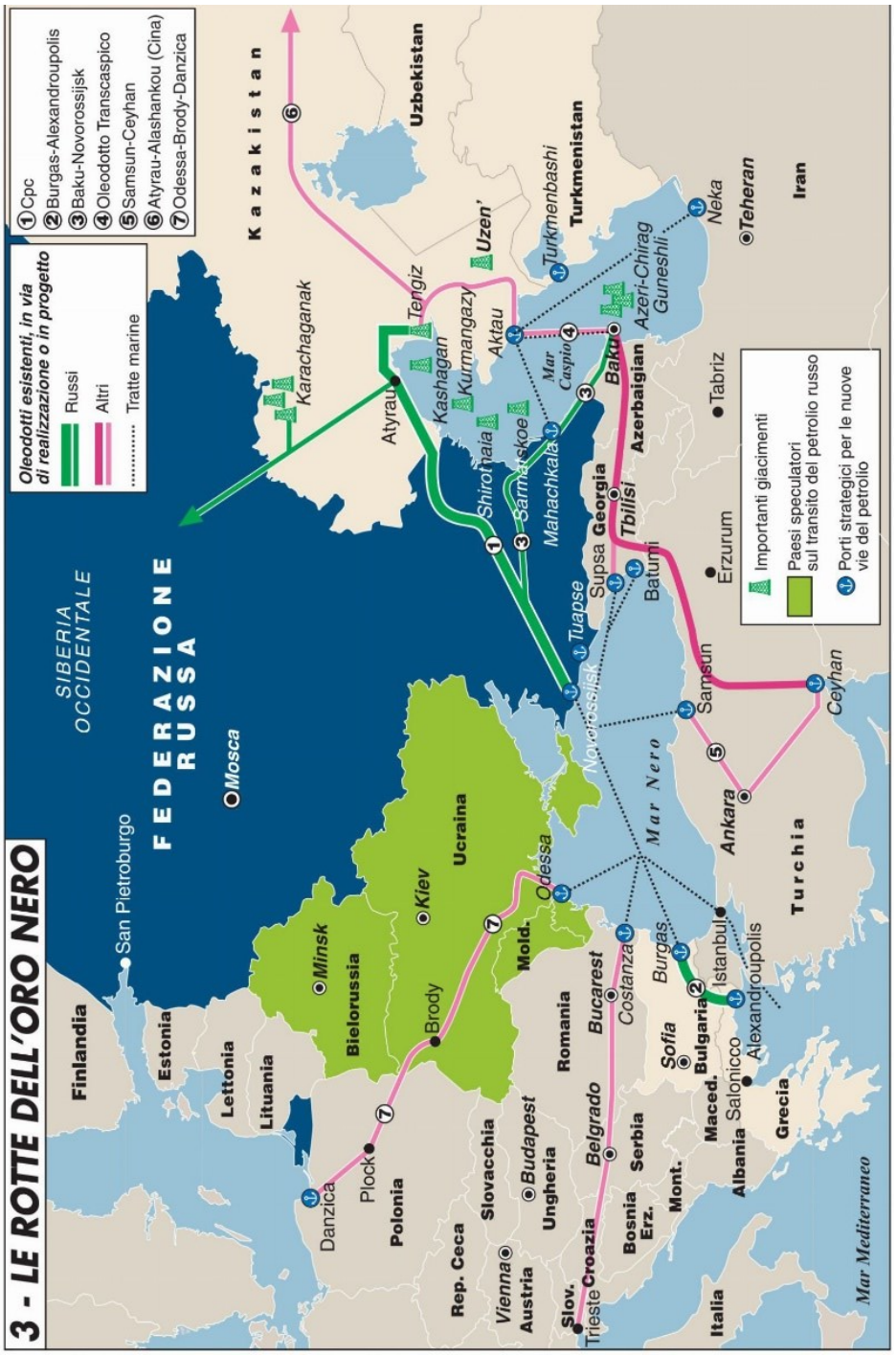
Infine, l'influenza nell'area CSI si sta erodendo, ma la Russia continua a considerare il controllo della Regione un segno distintivo del suo status di grande potenza mondiale, ciò che necessita per riottenere il prestigio perduto. Inoltre, secondo l'esperienza dei casi studio e l'analisi dei documenti si evince chiaramente come la superiorità delle informazioni sia strumentale alle sue future vittorie e, un'attenzione particolare è stata data ai valori ed alla cultura russa che sembrano essere le cose più importanti e di valore da difendere nell'*infowar*, mentre il mondo si muove verso conflitti in cui, come descrive saggiamente il generale Gerasimov: "Le guerre non sono dichiarate ma sono già iniziate".

[474] *Ibidem*.

ALLEGATI

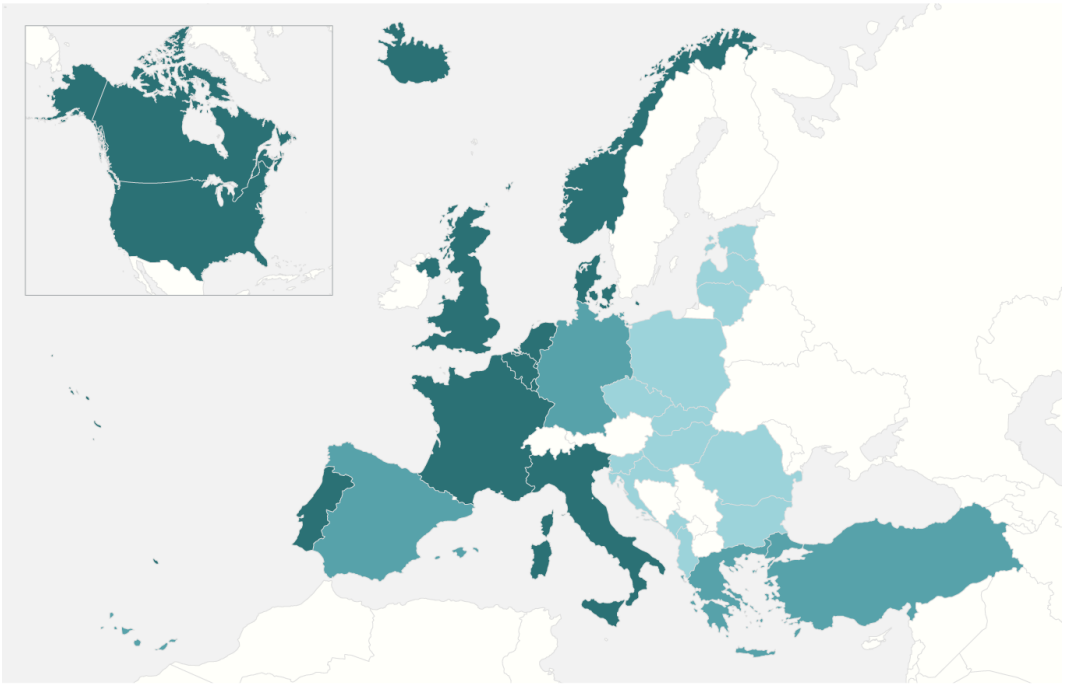


Allegato n.1., fonte: Center for Analysis of Strategies and Technologies, Mosca, 2010.



Allegato n.2, fonte: Limes, rivista italiana di geopolitica.

NATO's Expanding Membership



Founding members

1949 Belgium
Canada
Denmark
France
Iceland
Italy
Luxembourg
Netherlands
Norway
Portugal
United Kingdom
United States

Cold War expansion

1952 Greece
Turkey

1955 Germany

1982 Spain

Post–Cold War expansion

1999 Czech Republic
Hungary
Poland

2004 Bulgaria
Estonia
Latvia
Lithuania
Romania
Slovakia
Slovenia

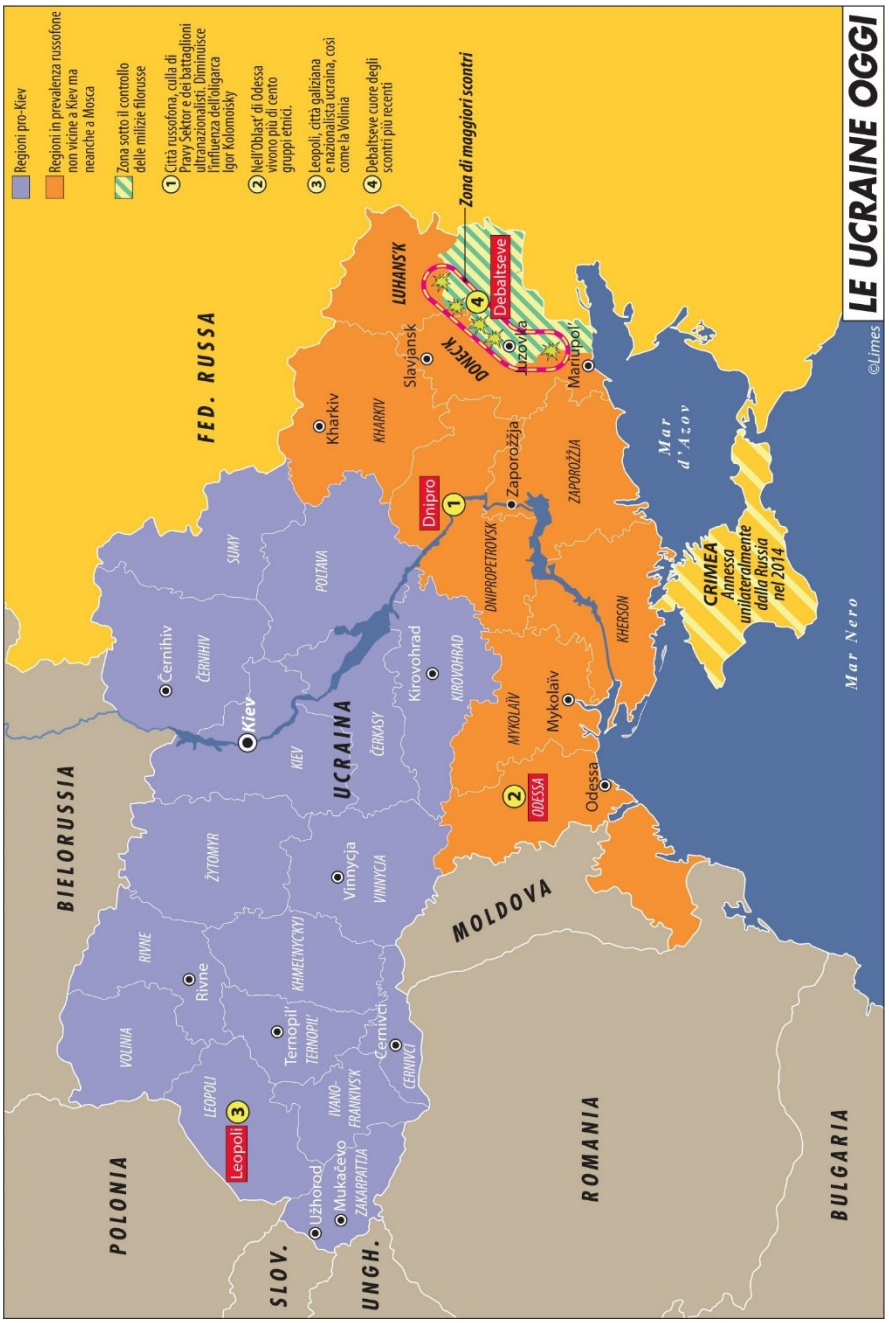
2009 Albania
Croatia

2017 Montenegro

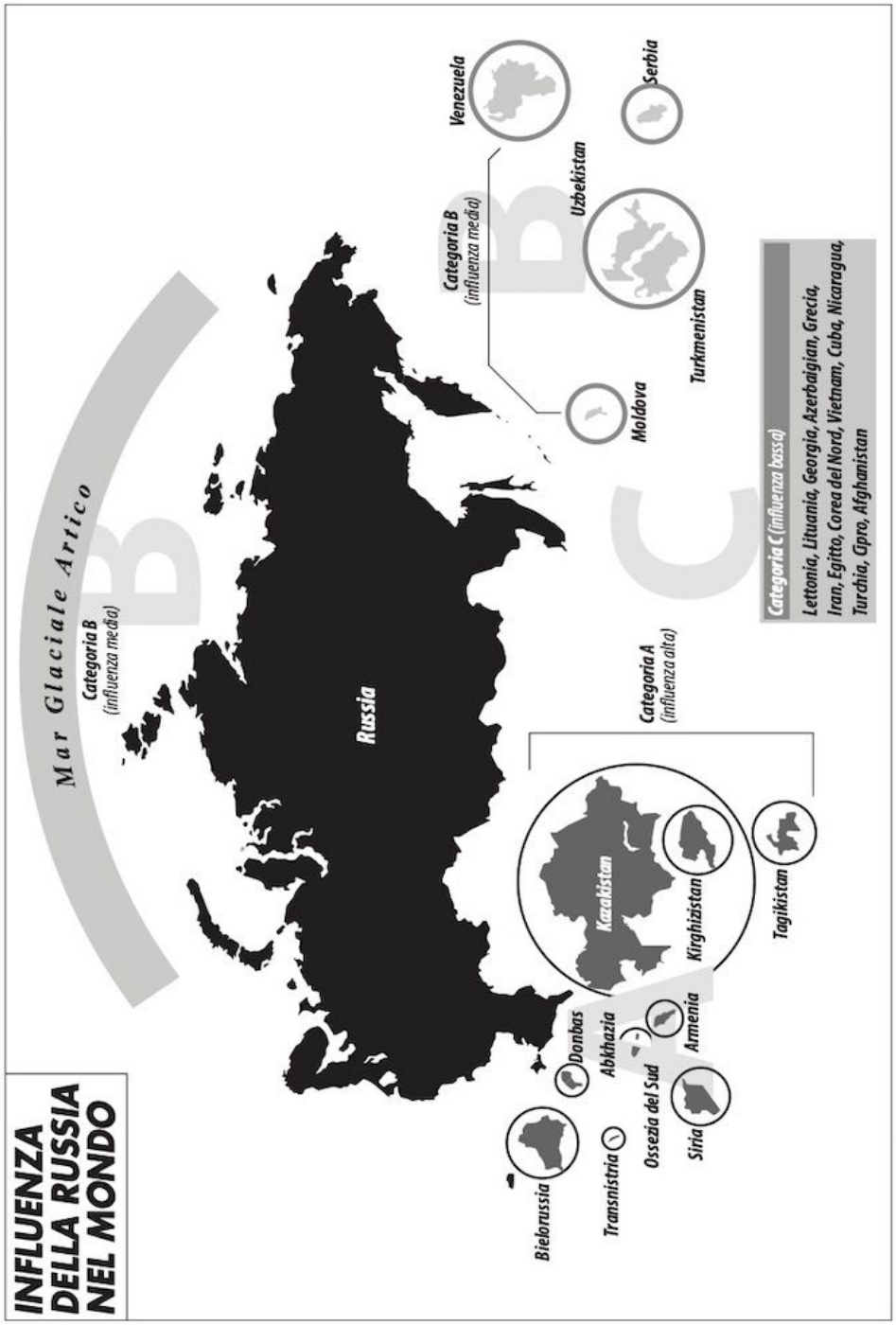
Source: NATO.

COUNCIL on FOREIGN RELATIONS

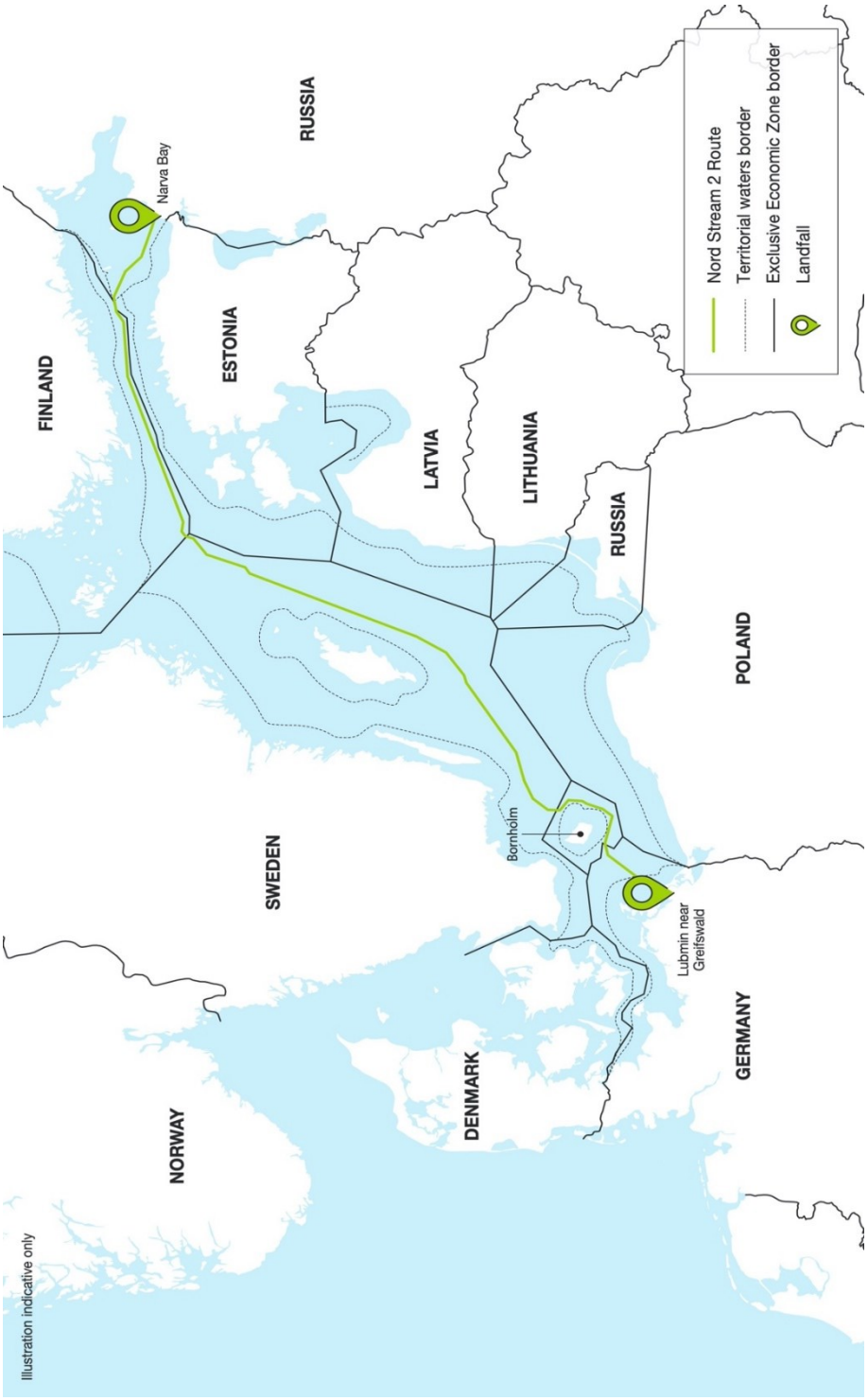
Allegato n. 3, fonte: NATO e Council on Foreign Relations



Allegato n. 4, fonte: Limes, rivista italiana di geopolitica.



Allegato n. 5, fonte: Limes, rivista italiana di geopolitica.



Allegato n. 6, fonte: Nord Stream 2

Bibliografia

Adamsky D., *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford University Press, 2010.

Andrew C., Mitrokhin V., *The Sword AND the Shield: The Mitrokhin Archive AND the Secret History of the KGB*, Basic Books, New York, 1999, disponibile online: https://archive.org/details/TheSwordAndTheShieldTheMitrokhinArchiveAndTheSecretHistoryOfTheKGB/mode/2up [ultimo accesso: 16.04.22].

Antonovich P., "Cyberwarfare: Nature and Content," *Military Thought*, versione in inglese edita da Eastview Publications, n.3, 2011.

Asmus R. D., *The Little War That Shook the World*, Palgrave Macmillian, New York, 2008.

Bacon K.H., e Lynch M., "The Plight of Displaced Persons in the Caucasus", *World Policy Journal*, vol. 19, n 4, 2002.

Barnett R.F., e Lord C. (a cura di), "Afterword-Twelve Steps to Reviving American PSYOP," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, National Defense University Press, Washington, D.C., 1989.

Bazylev S. I., Dylevskii I. N., Komov S. A., e Petrunin A. N., "Activities of the Armed Forces of the Russian Federation in the information space: principles, rules, confidence building measures", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2012.

Beehner L., Collins L., Ferenzi S., Person R., Brantly A., *Analyzing the Russian Way of War Evidence from the 2008 Conflict with Georgia*, The Modern War Institute, 2018.

BIAGINI A. F., "Quanto conta l'Ucraina per la Russia. Quanto conta la Russia per l'Italia", *Istituto Italiano di Studi Politici Internazionali (ISPI)*, 16 aprile 2015, disponibile online: https://www.ispionline.it/en/node/13099 [ultimo accesso: 16.04.22].

BLANK S., "'No Need to Threaten Us, We Are Frightened of Ourselves: Russia's Blueprint for a Police State - the New Strategy," in S. Blank and R. Weitz (a cura di), *The RUSSIAN MILITARY TODAY AND Tomorrow: ESSAYS in Memory of MARY FITZGERALD*, Strategic Studies Institute, US Army War College, 2010.

BLANK S., "Cyber War and Information War à la Russe", From *Understanding Cyber Conflict: Fourteen Analogies*, George Perkovich and Ariel E. Levite, Published by Georgetown University Press, 2017.

BOZZO L., Studi di strategia. Guerra, politica, economia, semiotica, psicoanalisi, matematica, EGEA Editore, Collana Alfaomega, 2012.

BRANGETTO P. and VEENENDAAL M. A., "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in N.Pissanidis et. al. (eds.), *8th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, giugno 2016.

BRZEZINSKI Z., "The Premature Partnership", *Foreign Affairs*, marzo/aprile 1994, disponibile online: https://www.foreignaffairs.com/articles/russian-federation/1994-03-01/premature-partnership [ultimo accesso: 16.04.22].

BURCHIA E., "La conferenza mondiale su Internet è stata un fiasco: a vincere è stato Internet", *Corriere Della Sera*, dicembre, 2012.

CARMAN D., "Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass media and the politics of identity". *Pacific Rim Law & Policy Journal Association*, 2002.

CARR J., *Inside Cyber Warfare*, O'Reilly Media, seconda edizione, dicembre 2011.

CHALMERS M., KORTUNOV A., LAIN S. and SMEKALOVA M., *Defining Dialogue How to Manage Russia–UK Security Relations – Part 2*, Conference Report, Royal United Services Institute for Defence and Security Studies (RUSI) & Russian International Affairs Council (RIAC), marzo 2018.

CHEKINOV e S. A. BOGDANOV, "The Nature and Content of a New-Generation of War", *Military Thought*, East View information services, Vol. 22, n.4, 2013.

CHEKINOV S. G. e BOGDANOV S. A., "Strategic Deterrence and Russia's National Security Today", *Military Thought*, versione in inglese di East View information services, n. 3, 2012.

CHEKINOV S. G. e BOGDANOV S. A., "A Forecast of the Character and Content of a Future War: Problems and Judgements", *Military Thought*, versione in inglese di East View information services n. 10, 2015.

CHEKINOV S.G., e BOGDANOV S.A., "The influence of indirect actions on the character of modern war", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2011.

COHEN A., HAMILTON R. E., *The Russian Military and the Georgia War: Lessons and Implications*, U.S. Army War College, Strategic Studies Institute, Carlisle, giugno 2011.

COLLISON C., *Russia's Information War: Old Strategies, New Tools. How Russia Built an Information Warfare Strategy for the 21st Century and What the West can Learn from the Ukraine Experience*, SL, 2017.

CONNELL M. and VOGLER S., *Russia's Approach to Cyber Warfare*, CNA Analysis & Solution, 2017.

CORKE S. J., "George Kennan and the Inauguration of Political Warfare," *The Journal of Conflict Studies*, Vol. 26, n. 1, estate 2016.

CURIKA L., "Defence Strategic Communications", *The official journal of the NATO Strategic Communications Centre of Excellence,* NATO Strategic Communications Centre of Excellence, Riga, Lettonia, Vol.1 Number 1, Winter 2015.

CURIKA L., *Social media as a tool of Hybrid warfare*, NATO Strategic Communications Centre of Excellence, Riga, Lettonia, 2016.

DANCHEV A., "Liddell Hart and the Indirect Approach", *The Journal of Military History*, Vol. 63, n. 2, aprile 1999.

DARCZEWSKA J., *Russia's Armed Forces on the Information war Front. Strategic Document*, Centre for Eastern Studies, Anna Łabuszewska (Editor), Warsaw 2016.

DARCZEWSKA J., *The Anatomy of Russian Information Warfare. The Crimean operation, a Case Study*, Centre for Eastern Studies, Anna Łabuszewska (Editor), Warsaw 2014.

DARCZEWSKA J., ZOCHOWSKI P., ORTTUNG R.W., LARUELLE M., PÖRZGEN G., "Information Warfare", *Russian Analytical Digest*, No 212, Center for Security Studies ETHzürich, giugno 2018.

DEIBERT, RONALD J., ROHOZINSKI R., E CRETE-NISHIHATA M., "Cyclones in Cyberspace: Information Denial and Information Shaping in the Russia Georgia War", *Security Dialogue*, vol. 43, n. 1, 2012.

DOWNES C., "Strategic Blind-spots on cyber threats", *The Cyber Defense Review*, Vectos and Campaigns, Vol. 3, Army Cyber Institute, 2018.

DUGIN A., *Geopolitika Postmoderna*, 2007. Disponibile online al seguente link: https://it.scribd.com/document/45497425/Aleksandr-Dugin-Geopolitika-Postmoderna [ultimo accesso: 16.04.22].

DUGIN A., *La Quarta Teoria Politica*, Nuova Europa, seconda edizione, 2017.

ERMAK S. e RASKIN A., "Are All Methods Good in Battle? On Some Aspects of Reflexive Control of the Enemy", *Army Journal*, versione in inglese di East View information services, n. 7, 2002.

FACON I., *Russia's National Security Strategy and Military Doctrine and their Implications for the EU*, Directorate General for External Policies - Policy Department - European Paliament, 2017.

FOXALL A., "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain", *Russia Studies Centre Policy Paper*, The Henry Jackson Society, May 2016.

FRANKE U., "On the cyber-reputation of governments", *International Review of Information Ethics*, n.19, 2013.

FRANKE U., *War by non-military means. Understanding Russian information warfare*, Swedish Reserch and Defence Institute (FOI), Stockholm, Sweden 2015.

FREEDMAN L., "The Future of War: A Hstory", *PublicAffairs*, New York, 2017.

FREEDMAN O., "The Russian Perspective on Information Warfare: conceptual roots and politicisation in russian academic, political, and public discourse", *Defence Strategic Communications Journal*, NATO Strategic Communications Centre of Excellence, Lettonia, Vol. 2, 2017.

GAIVORONSKY F. F. e GALKIN M. I., *The Culture of Military Thought*, Mosca, 1991.

GALEOTTI M., *Putin's Hydra: Inside Russia's Intelligence Services*, European Council on Foreign Relations, London 2016.

GALULA D., *Counterinsurgency Warfare: Theory and Practice*, Fredrick Praeger, New York, 1964.

GEERS K., *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015.

GERASIMOV V., "Principal Trends in the Development of Forms and Methods of Employing Armed Forces and Current Tasks of Military Science Regarding their Improvement," Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science), n. 1, 2013.

GILES K. "Information Troops – A Russian Cyber Command?" in *3rd International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2011.

GILES K. e HAGESTAD W. II, *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English*, 5th International Conference on Cyber Conflict, K. Podins, J. Stinissen, M. Maybaum NATO Publications, Tallinn 2013.

GILES K., "Internet Use and Cyber Security in Russia", in *Russia Analytical Digest*, Num. 134, Londra, 30 July 2013.

GILES K., "Russia's public stance on cyberspace issues" in *4Th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2012.

GILES K., "The Military Doctrine of the Russian Federation 2010", *Research Review*, NATO Defense College, Roma, febbraio 2010.

GILES K., *Handbook of Russian Information Warfare*, NATO Defence College, 2016.

GILES K., *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London, Chatham House, March 2016.

GILES K., *Russia's National Scurity Strategy to 2020*, NATO Defence College, 2009.

GOLDSTEIN F.L. (Col. USAF), FINDLEY Benjamin F. Jr. (Col. USAFR), *Psychological Operations. Principles and case studies*, Air University Press, Maxwell Air Force Base, Alabama, September 1996.

GOLTZ T., "The Paradox of Living in Paradise: Georgia's Descent into Chaos", in *The Guns of August 2008: Russia's War in Georgia*, E. Svante, e S. Starr (a cura di), Sharpe, New York, 2008.

GORBENKO A. N., *Informatsionnoe protivoborstvo v politike sovremennykh gosudarstv* (trad. *Guerra dell'informazione nella politica degli stati moderni*), Tesi di dottorato, Università Militare, Mosca, 2009.

GRAU, THOMAS T., "A Russian View of Future War: Theory and direction", *Journal of Slavic Military Studies*, issue 9.3, settembre 1996.

HEICKERO R., *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency (FOI). Stockholm, Sweden, March 2010.

HOLLIS D., "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, vol.7, n. 1, gennaio 2011.

IASELLO E.J., "Russia's Improved Information Operations: From Georgia to Crimea", Innovations in Warfare & strategy, *The US Army War College Quarterly Parameters*, Vol. 47 num. 2, estate 2017.

JACKSON R., SØRENSEN G., *Relazioni Internazionali*, Edizione italiana a cura di L. BOZZO, terza edizione, Egea, 2014.

JAITNER M., MATTSSON P.A., "Russian Information warfare of 2014", in MAYBAUM M., in OSULA A.M., LINDSTRÖM L. (a cura di), *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, NATO CCD COE Publications, Tallinn 2015.

JOPLING, *Countering Russia's Hybrid Threats: an update*, NATO Parliamentary Assembly, Committee on the Civil Dimension of Security, 2018.

KARANKEVICH V. N., "How to Learn to Deceive the Enemy", *Military Thought*, versione in inglese di East View information services, n. 9, 2006.

KASAPOGLU C., *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*, Research Division – NATO Defense College, No. 121, Rome November 2015.

KOFMAN M., MIGACHEVA, NICHIPORUK B., RADIN A., TKACHEVA O., OBERHOLTZER J., *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, RAND Corporation, Santa Monica, 2017, disponibile online al seguente link: https://www.rand.org/pubs/research_reports/RR1498.html. [ultimo accesso: 16.04.22].

KOROTKOV I. A., *The History of Soviet Military Thought*, Mosca, 1980.

KVACHKOV V., Спецназ России (trad. Teoria delle operazioni speciali), Voyennaya Literatura, 2004.

LAIN S., KORTUNOV A., *Defining Dialogue: How to Manage Russia–UK Security Relations*, RUSI–RIAC Russia–UK Track II Bilateral Report, Conference Report, marzo 2017.

LANOSZKA A., "Russian hybrid warfare and extended deterrence in eastern Europe", *International Affairs*, 92: 1, Jan. 2016, pp. 175–95, accessibile online: http://www.alexlanoszka.com/LanoszkaIAHybrid.pdf [ultima consultazione online: 16.04.22].

LAVROV A., "Timeline of Russian-Georgian Hostilities in August 2008." *In the Tanks of August*, Centre for Analysis of Strategies and Technologies, Ruslan Pukhov, Moscow 2010.

LE BON G., *Psicologia delle folle, un'analisi del comportamento delle masse*, TEA Editore, 2004.

LIBICKI M.C., "The Convergence of Information Warfare", *Strategic Studies Quarterly*, spring 2017, p. 49 disponibile online al seguente link: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf [ultimo accesso: 16.04.22].

LIBICKI M.C., *What is Information Warfare?*, Center for Advanced Command Concept and Technology, Institute for National Strategic Studies, National Defence University, Washington DC, Agosto 1995, p. introduzione.

LORD C., "The Psychological Dimension in National Strategy," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, C. LORD and F. R. BARNETT, (a cura di), National Defense University Press, Washington, D.C.,1989.

LUCAS S. e MISTRY K., "Illusions of Coherence: George F. Kennan, U.S. Strategy and Political Warfare in Early Cold War 1946–1950", *Diplomatic History*, Vol. 33, n. 1, gennaio 2009.

MAKHNIN V. L., "Reflexive Processes in Military Art: The Historico-Gnoseological Aspect", *Military Thought* (versione in inglese), East View publications, n. 2, 2013.

MARK M.A.J., BERRY S. P. (British Army), *PSYOP and the Information Age: Assessing US Army Employment of Psychological Operations in the Contemporary Operating Environment*, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, 2008.

MARTEN K., *Warlords: Strong-Arm Brokers in Weak States*, Cornell University Press, New York, 2012.

MCDERMOTT R.N., *Russia's Electronic Warfare Capabilities to 2025. Challenging NATO in the Electromagnetic Spectrum*, International Centre of Defence and Security (ICDS), Ministry of Defence - Republic of Estonia, Tallinn, Estonia 2017.

MEDVEDEV S., *Offense-defense theory analysis of Russian cyber capability*, Calhoun: The NPS Institutional Archive DSpace Repository, Monterey, California: Naval Postgraduate School, 2015.

MONAGHAN A., "The War in Russia's Hybrid Warfare", *Parameters45*, n.4, inverno 2015-16.

MONOV L.B. and KAREV M.L., "Information Warfare Conceptual Framework", *International Journal of Recent Scientific Research*, Vol. 9, Issue, 5(F), maggio 2018.

MOWTHORPE M., "The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views", *University of Hull*, vol. 5, n. 2, estate 2005.

NAGY V., "The geostrategic struggle in cyberspace between the United States, China, and Russia", *Aarms Security*, Vol. 11, num. 1, pp. 13–26, National University of Public Service, Budapest, Hungary 2012.

NORD P., "L'intoxication par un intoxicateur". in V. VOLKOFF, *La désinformation – arme de guerre*, L'age d'homme, Paris 1986.

NYE J., "Soft Power", *Foreign Policy*, n. 80, autunno 1990.

OLIKER O., "Unpacking Russia's New National Security Strategy", *Center for Strategic and International Studies (CSIS)*, January 7, 2016, https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy [ultima consultazione online: 16.04.22].

OVCHINSKY V.S., LARINA E.S., KULIK S.A., *Russia and the Challenges of the Digital Environment*, Working Paper of Russia International Affairs Council (RIAC), Moscow, 2014.

PERSSON G., "Security Policy and Military Strategic Thinking", In J. HEDENSKOG, e C. VENDIL PALLIN (Eds.), *Russian Military Capability in a Ten-Year Perspective*, FOI, the Swedish Defence Research Agency, Stockholm, 2016.

RÁCZ A., *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, Finnish Institute of International Affairs, Report n. 43, Helsinki, 2015.

RASKIN A. V. e PELYAK V. S., "On Network-Centric Warfare", *Military Thought*, versione in inglese di East View information services, n. 3, 2005.

REID A., Borderland: A Journey through the History of Ukraine, Basic Books, New York, 2015.

REID C., "Reflexive Control in Soviet Military Planning", in Brian D. Daily and Patrick J. Parker (a cura di), *Soviet Strategic Deception*, Lexington Books, 1987.

RENZ B. and SMITH H., *Russian and Hybrid Warfare – Going Beyond the Label*, Papers Aleksanteri, Kikimora Publications at the Aleksanteri Institute, University of Helsinki, Finland, 2016.

ROBINSON L., HELMUS T.C., COHEN R.S., NADER A., RADIN A., MAGNUSON M., MIGACHEVA K., *Modern Political Warfare. Current Practices and Possible* Responses, RAND Corporation, Santa Monica, California, 2018.

SAIFETDINOV K.I., "Information warfare in the military realm", *Military Thought*, versione in inglese edita da Eastview Publications, n. 7, 2014.

SAMADASHVILI S., *Muzzling the Bear Strategic Defence for Russia's Undeclared Information War on Europe*, Wilfried Martens Centre for European Studies, Belgium 2015.

SCHELLING T., *The strategy of conflict*, seconda ed., Harvard University Press, Cambridge, 1980.

SEROOKIY Yu., "Psychological-Information Warfare: Lessons of Afghanistan", *Military Thought*, versione in inglese edita da Eastview Publications, vol. 13 n. 1, 2004.

SMITH P.A. Jr., *On Political War*, National Defense University Press, Washington, D.C., 1989.

SOLDATOV A., BOROGAN I., "The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries", *PublicAffairs*, London, 2015.

STEWART V.R., *Russia military power. Building a military to support great power aspirations*, Defence Intelligence Agency, USA, 2017.

STRELTSOV A. A., "The main tasks for government policy in information warfare". *Military Thought*, versione in inglese edita da Eastview Publications, n.5, 2011.

SUN TZU, *L'arte della guerra*, prima ed. Neri Pozza Editore, Vicenza 1999, Nona ed. 2013.

TADDEO M., "Information Warfare: A Philosophical Perspective", *Philosophy and Geography*, Springer-Verlag, June 2011.

TEPERIK D., GRIGORI S., BERTOLIN G., KATERYNA K., ANTON D., *Virtual Russian World in the Baltics, Psycholinguistic Analysis of Online BehavioUr and Ideological Content among Russian-Speaking Social Media Users in the Baltic States*, National Centre of Defence & Security Awareness, NATO Strategic Communications Centre of Excellence, Maggio 2018.

THOMAS T. (Lt. Col., U.S. Army, Retired), "Russia's Forms and Methods of Military Operations. The Implementers of Concepts", *Military Review*, May-June 2018.

THOMAS T. (Lt. Col., U.S. Army, Retired), "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", *The Journal of Slavic Military Studies*, vol. 27, 2014.

THOMAS T. (Lt. Col., U.S. Army, Retired), *Nation-State Cyber Strategies: Examples from China and Russia*, 2012.

THOMAS T. L. "Russian Information Warfare Theory: The Consequences of August 2008," in S. BLANK and R. WEITZ (eds.). *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle, US Army War College Strategic Studies Institute, 2010.

THOMAS T., "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations", *Journal of Slavic Military Studies*, Vol.11, n.1, 1998.

THOMAS T., "Russia's 21st century information war: Working to undermine and destabilize populations", in *Defence Strategic Communications journal*, NATO Strategic Communications Centre of Excellence, vol. 1, n.1, inverno 2015.

THOMAS T., "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking", *Journal of Slavic Military Studies*, Vol. 29, n. 4, 2016.

THOMAS T., *Manipulating the Mass Consciousness: Russian and Chechen "Information War" Tactics in the 2nd Chechen- Russian Conflict,* Foreign Military Studies Office, Fort Leavenworth, 2018.

THOMAS T., *Russian Military Thought: Concepts and Elements*, MITRE Corporation, agosto 2019.

THORNTON R., "The Changing Nature of Modern Warfare", *The RUSI Journal*, 160:4, 40-48, settembre 2015.

TIKK E., KASKA K. E VIHUL L., *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia 2010.

TIMOFEEV I., *Theses on Russia's Foreign Policy and Global Positioning (2017-2024)*, Center for Strategic Research & Russian International Affairs Council (RIAC), Moscow, giugno 2017.

TRINQUIER R., *Modern Warfare: A French View of Counterinsurgency*, Pall Mall Press, London, 1964.

TSELUIKO V., "Georgian Army Reform under Saakashvili Prior to the 2008 Five Day War", in *The Guns of August 2008: Russia's War in Georgia*, Svante E., e Starr S. (a cura di), Sharpe, New York, 2008.

United States Army Special Operations Command, "SOF Support to Political Warfare White Paper", 10 marzo, 2015, Disponibie online: http://orchestratingpower.org/lib/LIC/PW/2015,03,10%20arsoc%20support%20to%20PW.pdf [ultimo accesso: 16.04.22].

US Department of the Army, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare. Ukraine 2013-2014*, US Army Special Operations Command, 2015, disponibile online: https://www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf [ultimo accesso: 16.04.22].

VON CLAUSEWITZ C., *Della guerra*, Mondadori Oscar Classici, II edizione versione integrale, 2017.

VOROBYEV I. N., "The information shock operation", *Military Thought*, versione in inglese edita da Eastview Publications, n. 6, 2007.

VOROBYOV I. N. e KISELEV V. A., "The New Strategy of the Indirect Approach", *Military Thought*, versione in inglese di East View information services, n. 9, 2006.

VOROBYOV I. N. e. KISELEV V. A, "The Evolution of the Principles of Military Art", *Military Thought*, versione in inglese edita da Eastview Publications, n. 3, 2008.

WILSON A., *Virtual Politics: Faking Democracy in The Post-Soviet World*, Yale University Press, 2005.

WIRTZ J.J., "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy", in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications: Tallinn, 2015.

Sussidi

Accademia delle scienze militari, conferenza del 2007, *Cfr.* per una trascrizione del discorso in lingua russa: http://old.redstar.ru/2007/01/23_01/2_04.html [ultimo accesso: 13.03.20], per un commento giornalistico: http://nvo.ng.ru/nvo/20070122/1_enemies.html [ultimo accesso: 16.04.22].

Agence France-Presse (AFP), "Hackers Target Ukraine's Election Website", *Security Week*, 25 ottobre 2014, disponibile online: http://www.securityweek.com/hackers-target-ukraines-election-website [ultimo accesso: 16.04.22].

Allevato M., "Così Putin ha riportato Mosca al centro del Grande Gioco", *AGI*, 26 febbraio 2017, disponibile online al seguente link: https://www.agi.it/estero/cos_putin_ha_riportato_mosca_al_centro_del_grande_gioco-1529516/news/2017-02-26/ [ultimo accesso: 16.04.22].

Askanews, "Putin: chi vuol Georgia, Ucraina nella Nato, non pensa [alle] conseguenze. Irresponsabili, ha detto Putin: Reagiremo proporzionalmente", Giovedì 19 luglio 2018, disponibile online: http://www.askanews.it/esteri/2018/07/19/putin-chi-vuol-georgia-ucraina-nella-nato-non-pensa-conseguenze-pn_20180719_00108/ [ultimo accesso: 16.04.22].

BBC, *Ukraine crisis: Transcript of leaked Nuland-Pyatt call*, 7 febbraio 2014, online: https://www.bbc.com/news/world-europe-26079957 [ultimo accesso: 16.04.22].

BEEHNER L., "U.S.-Russia Interests on Collision Course", *Council on Foreign Relations*, 14 febbraio 2007, disponibile online: https://www.cfr.org/backgrounder/us-russia-interests-collision-course [ultimo accesso: 16.04.22].

BOOT M. and DORAN M., "Political Warfare", *Policy Innovation Memorandum*, Council on Foreign Relations, Washington DC ,n. 33, 2013), https://www.cfr.org/sites/default/files/pdf/2013/06/Policy_Innovation_Memorandum_33_Boot.pdf [ultimo accesso: 16.04.22].

BURCHIA E., "La conferenza mondiale su Internet è stata un fiasco: a vincere è stato Internet", *Corriere Della Sera*, dicembre, 2012, disponibile online: https://www.corriere.it/tecnologia/12_dicembre_15/internet-dubai-conferenza_c00640d0-46c1-11e2-90a4-19087f7b891e.shtml [ultima consultazione online: 16.04.22].

CAPELLI B., "Elezioni parlamentari in Ucraina: volti nuovi e voglia di cambiamento", *Vatican News*, 20 luglio 2019, disponibile online: https://www.vaticannews.va/it/mondo/news/2019-07/ucraina-voto-elezioni-anticipate-europa-russia.html [ultima consultazione: 16.04.22].

CARR J., "Russian Cyber Security Organization", Prezi, 18 July 2014, accessibile online: https://prezi.com/ajo61qec9rwi/russian-cyber-security-organization/ [ultima consultazione online: 16.04.22].

CLAPPER J. R. (US Director of National Intelligence), *Worldwide Threat Assessment of the US Intelligence Community*, Senate Armed Services Committee Statement for the Record, 26 February 2015, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR__SASC_FINAL.pdf [ultimo accesso online: 16.04.22].

CLAPPER J.R. *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*, February 9, 2016. https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf [ultimo accesso online: 16.04.22].

COLIN D., "Could Russia Use Cyberwarfare to Further Destabilize Ukraine?", Mashable, 14 aprile 2014, disponibile online: http://mashable.com/2014/04/14/russia-ukraine-cyber-warfare/ [ultimo accesso: 16.04.22].

Commissione europea e Servizio Europeo per l'Azione Esterna (SEAE), *Strategia di cibersicurezza dell'Unione europea: un ciberspazio aperto, sicuro e protetto.* Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, 2013. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [ultimo accesso: 16.04.22].

Commissione europea e Servizio Europeo per l'Azione Esterna (SEAE), *Strategia di cibersicurezza dell'Unione europea: un ciberspazio aperto, sicuro e protetto.* Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, 2013. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [ultimo accesso online: 16.04.22].

CONANT E., “Come la storia, la geografia aiutano a spiegare la crisi politica dell’Ucraina”, *National Geografic*, 31 gennaio 2014, disponibile online: https://www.nationalgeographic.com/news/2014/1/140129-protests-ukraine-russia-geography-history/ [ultimo accesso: 16.04.22].

Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space del 2011, The NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/library/strategy-and-governance/?search=russian%20 [ultima consultazione online: 16.04.22].

Consiglio Federale russo “Concetto per una strategia di cybersecurity russa”, 2014, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [ultimo accesso: 16.04.22].

Corriere della Sera, “Bush in Georgia: «Medierò con la Russia»”, disponibile online; https://www.corriere.it/Primo_Piano/Esteri/2005/05_Maggio/10/bush.shtml [ultimo sccesso: 16.04.22].

Council of the European Union, “Independent International Fact-Finding Mission on the Conflict in Georgia”, Report, vol. 1, Bruxelles, settembre 2009, disponibile online: https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf [ultimo accesso: 16.04.22].

Decreto del Presidente della Federazione Russa n. 603 “Sull’attuazione di piani (programmi) per la costruzione e lo sviluppo delle Forze armate della Federazione Russa, altre truppe, unità e corpi militari e la modernizzazione del complesso militare-industriale” n. 603, 05.05.2012, *Cfr*. il “Portale Internet ufficiale informazioni legali Sistema statale di informazione” legale per la versione ufficiale in lingua russa: http://publication.pravo.gov.ru/Document/View/0001201205070021 [ultimo accesso: 16.04.22].

DOD Dictionary of Military and Associated Terms, febbraio 2018, accessibile online: http://www.jcs.mil/Doctrine/DOD-Terminology/ [ultima consultazione online: 16.04.22].

Dottrina militare della Federazione Russa del 2000, http://base.garant.ru/181993/#ixzz4qoOtOqe6 [ultima consultazione online: 16.04.22].

Dottrina militare della Federazione Russa del 2014, approvata con decreto n. 2976 del Presidente della Federazione Russa, dicembre 2014. Disponibile online, sul sito dell’ambasciata russa in UK, al seguente link: https://rusemb.org.uk/press/2029 [ultima consultazione online: 16.04.22].

Dottrina militare della Federazione Russa, approvata con decreto del presidente della Federazione Russa, 5 febbraio 2010, accessibile online: https://www.justsecurity.org/7777/russias-2010-military-doctrine/ [ultima consultazione online: 16.04.22].

Dottrina sulla sicurezza delle informazioni della Federazione Russa, 5 dicembre del 2016, disponibile online, *Cfr.* il "Portale Internet ufficiale informazioni legali Sistema statale di informazionelegale", disponibile online al seguente link: http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1 [ultima consultazione online: 16.04.22]. *Cfr*. anche il Ministero degli Affari Esteri della Federazione Russa per una versione in inglese https://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2563163 [ultima consultazione online: 16.04.22].

DUGIN A., "Progetto Euroasiatico e il problema Ucraina", disponibile in lingua russa: http://www.odnako.org/magazine/material/evraziyskiy-proekt-i-ego-ukrainskaya-problema/ [ultimo accesso: 16.04.22].

ENNIS S., "Dmitry Kiselyov: Russia's chief spin doctor", *BBC news*, 2 aprile 2014, disponibile online: https://www.bbc.com/news/world-europe-26839216 [ultimo accesso: 16.04.22].

ENNIS S., "Russia: Children's toilet TV show drawn into Ukraine-EU row", *BBC news*, 4 dicembre 2013 disponibile online: https://www.bbc.com/news/blogs-news-from-elsewhere-25198264 [ultimo accesso: 16.04.22].

EROFEEVA T., "Georgia-Russia War: An Information Control Story", *Prezi*, 6 maggio 2014, disponibile online: https://prezi.com/i4fk4qprev0s/georgia-russia-war-an-information-control-story/ [ultimo accesso: 16.04.22].

European External Action Service (EEAS), European Union Military Commette (EUMC), *EUMC Glossary of Acronyms and Definitions Revision 2015*, febbraio 2016. http://data.consilium.europa.eu/doc/document/ST-6186-2016-INIT/en/pdf [ultima consultazione online: 16.04.22].

FASANI A., *Information warfare, ecco la strategia della Russia per influenzarci online*, Agenda Digitale, maggio 2018, accessibile online: https://www.agendadigitale.eu/sicurezza/information-warfare-ecco-la-strategia-della-russia-per-influenzarci-online/ [ultima consultazione online: 16.04.22].

Geopoliticalcenter, "L'esercitazione delle forze armate russe al confine con l'Ucraina e non solo", 28 febraio 2014, disponibile online: http://www.geopoliticalcenter.com/attualita/lesercitazione-delle-forze-armate-russe-al-confine-con-lucraina-e-non-solo/ [ultimo accesso: 16.04.22].

GERASIMOV V., "Tsennost' Nauki v Vredvidenii", ("Il valore della scienza in anticipo"), Voyenno- Promyshlennyy Kuryer, 27 Febbraio 2013, http://www.vpk-news.ru/articles/14632 [ultima consultazione 16.04.22].

HANSON S., "Putin and the Dilemmas of Russia. Anti-Revolutionary Revolution", *Wilson Center Publications*, 2001, accessibile online:https://www.wilsoncenter.org/publication/the-anti-revolutionary-revolution-russia [ultima consultazione online: 16.04.22].

HOFFMAN F., "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks*, 28 luglio 2014, online: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ [ultima consultazione: 16.04.22].

IGNOTO, “Foreign special services step up online operations targeting Russia - top security official,” RT, 15 giugno 2016, online: https://www.rt.com/russia/346772-foreign-special-services-step-up/ [ultimo accesso: 16.04.22].

IGNOTO, “The Devil has arrived through this mechanism. The Russian authorities weigh in on Pokémon Go Five quotes”, Meduza, 18 July 2016, online: https://meduza.io/en/feature/2016/07/18/the-devil-has-arrived-through-this-mechanism [ultimo accesso: 16.04.22].

Information Security institute, Università statale di Mosca Lomonosov in Russia, http://www.ipib.msu.ru/ [ultimo accesso 16.04.22].

Intervista, “Information Warfare”, *Levada Center*, 12 novembre 2014, disponibile online: http://www.levada.ru/eng/information-warfare [ultimo accesso: 16.04.22].

Joint Development, *Cyberspace Operation*, Joint Pubblication 3-12, June 2018, questo report è accessibile online: https://fas.org/irp/doddir/dod/jp3_12.pdf [ultima consultazione online: 16.04.22].

KARMANAU Y. E ISACHENKOV V., “Vladimir Putin Admits for First Time Russian Troops Took Over Crimea, Refuses to Rule Out Intervention in Donetsk”, *National Post*, Toronto, 17 aprile 2014, disponibile online: https://nationalpost.com/news/world/vladimir-putin-admits-for-first-time-russian-troops-took-over-crimea-refuses-to-rule-out-intervention-in-donetsk [ultimo accesso: 16.04.22].

KENNAN G. F., “The Inauguration of Organized Political Warfare”, Archivio digitale del programma di storia e politiche pubbliche, ottenuto e contribuito da A. Ross Johnson, aprile 1948, disponibile al seguente link: https://digitalarchive.wilsoncenter.org/document/114320 [ultimo accesso: 16.04.22].

KVACHKOV V., Спецназ России (trad. Teoria delle operazioni speciali), Voyennaya Literatura, 2004, http://militera.lib.ru/science/kvachkov_vv/index.html [ultimo accesso online: 16.04.22].

LEVINE Y., "The CNN Effect: Georgia Schools Russia in Information Warfare", *The eXiled Online*, 13 agosto 2008, disponibile online: http://exiledonline.com/the-cnn-effect-georgia-schools-russia-in-information-warfare/ [ultimo accesso: 16.04.22].

LEWIS J., "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare", *Looking Glass*, Arlington, 28 aprile 2015, disponibile online: https://www.lookingglasscyber.com/blog/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/ [ultimo accesso: 16.04.22].

LOZANSKY E., "Slam dunk journalism" or propaganda warfare?, *RT*, 25 luglio 2014, disponibile online: https://www.rt.com/op-ed/175548-foreign-policy-us-russia-journalism/ [ultimo accesso: 16.04.22].

MACDONALD B., "Goodbye to Carl Bildt, out of line and out of time", *RT*, 25 agosto 2014, disponibile online: http://rt.com/op-edge/182600-bildt-swiss-far-right-ukraine/ [ultimo accesso: 16.04.22].

MALDRE P., *The Many Variants of Russian Cyber Espionage*, Atlantic Council, agosto 2015, online: www.atlanticcouncil.org/blogs/natosource/the-many-variants-of-russian-cyber-espionage [ultima visualizzazione online: 16.04.22].

MALDRE P., *The Many Variants of Russian Cyber Espionage*, Atlantic Council, agosto 2015, online: www.atlanticcouncil.org/blogs/natosource/the-many-variants-of-russian-cyber-espionage [ultima visualizzazione online: 16.04.22].

MALGIN A., "Russia is Following in Nazi Germany's Footsteps", *The Moscow Times*, 13 marzo 2014, disponibile online: https://www.themoscowtimes.com/2014/03/12/russia-is-following-in-nazi-germanys-footsteps-a32922 [ultimo accesso: 16.04.22].

MARKOFF J., "Before the Gunfire, Cyberattacks", *NYT Online*, 12 agosto 2008, accessibile online al seguente link: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 [ultimo accesso: 16.04.22].

MASHIRI J., "An Absurd Signal: Pokémon Confirms Russia's War Footing" ("Un segnale assurdo: i Pokémon confermano il piede di guerra della Russia"), 19 luglio 2016, online: https://blogit.apu.fi/somesotilas/an-absurd-signal-pokemon-confirms-russias-war-footing/ [ultimo accesso: 16.04.22].

MASTERS J., "Ukraine: Conflict at the Crossroads of Europe and Russia", *Council on Foreign Relations*, 5 febbraio 2020, disponibile online: https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia [ultimo accesso: 16.04.22].

Ministero degli affari esteri della Federazione Russa, "Convention on international information security (Concept)", 2011. *Cfr*. il sito del Ministero al seguente link: https://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/191666 [ultimo accesso: 16.04.22].

Ministero degli Affari Esteri ucraino al seguente link: https://mfa.gov.ua/en/10-facts-you-should-know-about-russian-military-aggression-against-ukraine [ultimo accesso: 16.04.22].

Ministero della Difesa della Federazione Russa, "opinioni concettuali sulle attività delle forze armate della Federazione Russa nello spazio informazioni", 2011. Documento disponibile online al seguente link: http://www.pircenter.org/media/content/files/9/13480921870.pdf [ultima consultazione online: 16.04.22], *Cfr*. anche il sito del Ministero della Difesa russo al seguente link: http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle [ultima consultazione online: 16.04.22].

NATO Glossary of Terms and Definitions, AAP - 06 Edition, 2017.

NECHEPURENKO I. e MACFARQUHAR N., "As Sabotage Blacks Out Crimea, Tatars Prevent Repairs," *New York Times*, 23 novembre 2015, disponibile online: https://www.nytimes.com/2015/11/24/world/europe/crimea-tatar-power-lines-ukraine.html?searchResultPosition=1 [ultimo accesso: 16.04.22].

NECHEPURENKO I., "Electricity Restored to Crimea After 2 Weeks of Darkness", *New York Times*, 8 dicembre 2015, disponibile online: https://www.nytimes.com/2015/12/09/world/europe/electricity-restored-to-crimea-after-2-weeks-of-darkness.html?searchResultPosition=1 [ultimo accesso: 16.04.22].

PAINE K., "Reputation Redux: Russia Invades Georgia by Land and by Server," *PR News*, 25 agosto 2008, disponibile online: http://www.prnewsonline.com/reputation-redux-russia-invades-georgia-by-land -and-by-server/ [ultimo accesso: 16.04.22].

PANARIN I., "Information War against Russia", RT, 30 dicembre 2011, disponibile: http://rt.com/politics/information-war-russia-panarin-009/ [ultimo accesso: 16.04.22].

PANARIN I., *Informatsionnaya voyna i mir*, Mosca, 2006, p. 165. In cirillico: И. Панарин, Информационная война и геополитика, Поколение, Моська, 2006, п. 165. Disponibile su: https://books.google.it/books [ultimo accesso: 16.04.22].

POTILYUK P., "Ukraine Sees Russian Hand in Cyber Attacks against Power Grid", *Reuters*, 12 febbraio 2016, disponibile online: http://www.reuters.com/article/us-ukrainecybersecurity-idUSKCN0VL18E. [ultimo accesso: 16.04.22].

PUTIN V., "Солдат есть звание высокое и почетное" ("Soldier" is an honourable and respected rank), discorso annuale all'Assemblea federale della Federazione russa, Krasnaya zvezda, 11 maggio 2006. http://en.kremlin.ru/events/president/transcripts/23577 [ultima consultazione online: 16.04.22].

Rainews, "Ucraina, cronologia della rivolta", 20 febbraio 2014, disponibile online: http://www.rainews.it/dl/rainews/articoli/ucraina-cronologia-rivolta-guerra-civile-e242cf67-76a7-40e6-bef7-fe711de64eae.html [ultimo accesso: 16.04.22].

Rapporto del Segretario Generale, A / RES / 65/154, Nazioni Unite, 65a sess. 2010, pp. 2-5.

Rapporto del Segretario Generale, A / RES / 69/112, Nazioni Unite, 69a sess. 2014, pp. 9-10.

Reuters, *Estonia denies leaked call implicates Ukraine protesters in killings*, 5 marzo 2014, disponible online al seguente link: https://www.reuters.com/article/us-estonia-eu-ukraine/estonia-denies-leaked-call-implicates-ukraine-protesters-in-killings-idUSBREA2423O20140305 [ultimo accesso: 16.04.22].

RT, “Ukraine, West Wage Information War against Us – Russians”, 12 novembre 2014, disponibile online: http://www.rt.com/politics/204827-ukraine-west-information-warfare [ultimo accesso: 16.04.22].

Russkiy Mir Foundation: https://russkiymir.ru/it/ [ultimo accesso 16.04.22].

Servizio di intelligence estero di Estonia, report sulla Russia 2018, questo report è accessibile online: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf [ultima consultazione online: 16.04.22].

SINELSCHIKOVA E., “Perché dopo il crollo dell’Urss tutte le armi nucleari sono rimaste solo alla Russia?”, *Russia Beyond*,19 giugno 2019, disponibile online: https://it.rbth.com/scienza-e-tech/82917-perché-dopo-il-crollo-dellurss [ultimo accesso: 16.04.22].

Sito web dedicato al *Nord Stream 2*, disponibile al seguente link: https://www.nord-stream2.com/en/pdf/document/124/ [ultimo accesso: 16.04.22].

Sputnik, “US Policy toward Crimea Defies Reality”, *Russia Insider*, 16 marzo 2015, disponibile online: http://russia-insider.com/en/2015/03/16/4534 [ultimo accesso: 16.04.22].

Strategia per la Sicurezza Nazionale della Federazione Russa fino al 2020, 12 maggio del 2009. *Cfr*. sito internet del “NATO Cooperative Cyber Defence Centre of Excellence”, documento disponibile in versione inglese al seguente link: https://ccdcoe.org/library/strategy-and-governance/?search=russia [ultima consultazione online: 16.04.22].

Strategia di Sicurezza Nazionale, approvata con decreto del Presidente della Federazione Russa n. 400, 2 luglio 2021. Accessibile online: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1 [ultima consultazione online: 16.04.22].

STRETCH C., Hearing Before the United States Senate Commiteeon the Judiciary Subcommittee on Crime and Terrorism, ottobre 2017. https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf [ultima consultazione online: 16.04.22].

STUPPLES D., *The next war will be an information war, and we're not ready for it*, novembre 2015, accessibile online: http://theconversation.com/the- next-war-will-be-an-information-war-and-were-not- ready-for-it-51218 [ultima consultazione online: 16.04.22].

SUKHANKIN S., "Russian Electron Warfare in Ukraine: Between Real and Imaginable", in *Euraisa Daily Monitor*, The James Town Fondation, n. 71, 24 maggio 2017, disponibile online: https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable [ultimo accesso: 16.04.22].

TADEO M., "State television presenter warns Russia could turn the US into radioactive dust", *Indipendent*, 17 marzo 2014, disponibile online: https://www.independent.co.uk/news/world/europe/state-television-presenter-warns-russia-could-turn-the-us-into-radioactive-dust-9197433.html [ultimo accesso: 16.04.22].

TRENIN D., *Information is a potent weapon in the new cold*, 17 settembre 2016, online: https://www.theguardian.com/commentisfree/2016/sep/17/hacking-politics-us-russia [ultimo accesso: 16.04.22].

TRENIN D., "Putin's Biggest Challenge Is Public Support", *Carnegie Moscow Center*, 15 gennaio 2015, disponibile online: https://carnegie.ru/2015/01/15/putin-s-biggest-challenge-is-public-support-pub-57758 [ultimo accesso: 16.04.22].

TSYGANOK A., "Informational Warfare - a Geopolitical Reality", rivista online della *Strategic Culture Foundation*, 5 novembre 2008, disponibile online al seguente link: https://www.rbth.com/articles/2008/11/05/051108_strategic.html [ultimo accesso: 16.04.22].

UNHCR, "In Ucraina, alcuni esperti rischiano la vita - e gli arti - per trovare e rimuovere le mine", disponibile online: https://www.unhcr.it/news/storie/ucraina-esperti-rischiano-la-vita-gli-arti-trovare-rimuovere-le-mine.html [ultimo accesso: 16.04.22].

UNITED NATIONS, "Developments in the field of information and telecommunications in the context of international security", RESOLUTION ADOPTED BY THE GENERAL ASSEMBLY [on the report of the First Committee (A/53/576)], 1999, https://undocs.org/en/A/RES/53/70 [ultima consultazione online: 16.04.22].

United Nations, GA, "Developments in the field of information and telecommunications in the context of international security", risoluzione adottata dall'Assemblea Generale delle Nazioni Unite [sulla relazione del primo comitato (A / 53/576)], 1999. Disponibile online sul sito delle Nazioni Unite nella sezione "documenti" al seguente link: https://undocs.org/en/A/RES/53/70 [ultima consultazione online: 16.04.22].

Università militare del Ministero della Difesa della Federazione Russa: https://vumo.mil.ru/ [ultimo accesso 16.04.22].

US Department of Homeland Security, *Cyber-Attack against Ukrainian Critical Infrastructure*, 25 febbraio 2016, disponibile online: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01 [ultimo accesso: 16.04.22].

VOLKOV D., "Supporting a War That Isn't: Russian Public Opinion and the Ukraine Conflict", *Carnegie Endowment for International Peace*, Washington DC, 9 settembre 2015, disponibile online: https://carnegie.ru/commentary/61236 [ultimo accesso: 16.04.22].

VOLZ D., "Russian Hackers Tracked Ukrainian Artillery Units Using Android Implant: Report", *Reuters*, 21 dicembre 2016, disponibile online: https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU [ultimo accesso: 16.04.22].

WILBY P., "Georgia Has Won the PR War", *The Guardian*, 17 agosto 2008, disponibile online: https://www.theguardian.com/media/2008/aug/18/pressandpublishing.georgia [ultimo accesso: 16.04.22];

Генерал-майор Михайлов об инфовойнах: Собака лает, караван идет, но мы же не верблюды Читайте, (intervista a Mikhailov, *Pravda.ru*, 2014) disponibile online in lingua originale al seguente link: https://www.pravda.ru/news/society/1201182-war/ [ultimo accesso: 16.04.22].

Герасимов, В. *Мир на гранях войны*, 2017. Gerasimov V., *Mondo sull'orlo della guerra*, 13 marzo 2017. Online: https://vpk-news.ru/articles/35591 [ultimo accesso: 16.04.22].

КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ (Trad. Concetto della Strategia di Sicurezza Cyber della Federazione Russa), 2014 http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [ultima consultazione online: 16.04.22].

Мединский обвинил власти США в попытке «залезть в каждый телевизор» через Netflix ("Medinsky accusa le autorità statunitensi di aver tentato di infiltrarsi in ogni televisione tramite Netflix"), RNS, 22 giugno 2016, online: https://www.dp.ru/a/2016/06/22/Medinskij_obvinil_SSHA_v_p/ [ultimo accesso: 16.04.22].

Первый канал, *Владимир Путин провел заседание Совбеза, на котором обсуждалась информационная безопасность страны*, 2017. "Il primo canale" (media russo), *Vladimir Putin ha presieduto una riunione del Consiglio di sicurezza per discutere della sicurezza delle informazioni del paese*, 26 ottobre 2017. Online: https://www.1tv.ru/news/2017-10-26/335150-vladimir_putin_provel_zasedanie_sovbeza_na_kotorom_obsuzhdalas_informatsionnaya_bezopasnost_strany [ultimo accesso: 16.04.22].

Словарь терминов и определений в области информационной безопасности, Voyennaya Akademiya (trad. Dizionario dei termini e delle definizioni sulla sicurezza delle informazioni), General'nogo Shtaba, 2nd Edition, Moscow Voyeninform, 2008.

Щеголев: цензуры Интернета в России не допустят (Shchegolev: la censura di Internet non verrà consentita in Russia), Interfax, 20 gennaio 2012, accessibile in lingua russa online: http://www.interfax.ru/print.asp?sec=1448&id=226823 [ultimo accesso: 16.04.22].

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies