L'information Warfare della Russia, i fondamenti

Domenico Frascà

Research Analysis

Ottobre 2018

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 della Russia, i fondamenti

Domenico Frascà

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Ottobre 2018

Riguardo all'autore

Domenico Frascà Si è laureato in Scienze Politiche indirizzo Relazioni Internazionali presso la Facoltà di Scienze Politiche "Cesare Alfieri" in Firenze, con una tesi sulla Social Media Intelligence. Durante gli studi ha seguito un corso di formazione sui processi e tecniche di negoziazione delle Nazioni Unite presso *Consules*, partecipando successivamente alle simulazioni "Consules Model United Nations" a Roma, e "National Model United Nations", svoltosi a New York. Ha frequentato il corso intensivo Summer School 2015 "Il negoziato nelle crisi umanitarie" presso l'Istituto per gli Studi di Politica Internazionale (ISPI) in Milano. Attualmente sta frequentando il corso di Laurea magistrale in Relazioni Internazionali e Studi Europei presso la Facoltà "Cesare Alfieri". Si interessa principalmente di studi strategici e cyber intelligence.

L'information Warfare della Russia, i fondamenti[1]

Nella visione russa, la guerra dell'informazione è una forma di potere politico e uno strumento geopolitico che consente un alto livello di manipolazione e influenza. Un'attività sempre in corso di natura olistica e onnicomprensiva. Un'analisi delle varie declinazioni dell'Infowar e le differenze con l'approccio occidentale

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[2]. All'interno dello spazio dell'informazione, il pensiero russo giunge a separare il *Computer Network Operation* (CNO) dalle altre attività[3]; i due principali filoni della guerra dell'informazione nel pensiero russo sono:

- *guerra psicologica*, per colpire il personale delle forze armate e della popolazione. Questa viene condotta in condizioni di competizione naturale, cioè permanentemente;
- *guerra tecnologica dell'informazione*, per incidere sui sistemi tecnici che ricevono, raccolgono, elaborano e trasmettono informazioni, condotta durante guerre e conflitti armati[4].

[1] La seguente analisi è apparsa su Agenda Digitale il giorno 09 ottobre 2018 ed è reperibile al seguente link https://www.agendadigitale.eu/sicurezza/linformation-warfare-della-russia-i-fondamenti/

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

[3] T. L. Thomas. "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.

[4] V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, 2004, http://militera.lib.ru/science/kvachkov_vv/index.html [ultimo accesso online: 06.07.18] 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.

La dottrina sulla sicurezza delle informazioni (2000)

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[5]; la manovra rivelatrice è stata l'adozione da parte dello Stato, della "Dottrina" della sicurezza informatica nel 2000. Una delle componenti principali della Dottrina, è di garantire la protezione delle informazioni strategicamente importanti da attività straniere dirette contro gli interessi della Federazione nella sfera dell'informazione; la Dottrina è una sintesi della posizione ufficiale della politica statale per il mantenimento della sicurezza delle informazioni[6]. Tratta un'ampia varietà di questioni, non solo la necessità di proteggere reti e informazioni, ma anche come rafforzare l'identità nazionale e preservare il patrimonio culturale al fine di garantire che le giovani generazioni sviluppino valori morali costruttivi, patriottismo e responsabilità civile per il destino del paese[7]; questo ricco documento espone senza mezzi termini l'obiettivo del governo russo di rendere sicura l'*Information space*[8].

Giles, *Handbook of Russian Information Warfare*, op.cit., p.9)

[5] 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, 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

[6] 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.

[7] *Ibidem*

[8] 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.

La dottrina militare (2010)

Dall'analisi di questo documento si evince che il governo russo degli anni 2000 ha avuto la percezione di essere in una posizione vulnerabile sia a livello globale che interno, in termini sia delle sue capacità militari convenzionali che della crescente sfera dell'informazione digitale[9]. Come il documento del 2000, la Dottrina militare russa del 2010, identifica una serie di "strumenti" per proteggere gli interessi nazionali della Russia, ma questa volta indica specificamente che la NATO ha il desiderio di spostare l'infrastruttura militare dei paesi membri più vicina ai confini della Federazione Russa e di espandere l'influenza dell'Alleanza, tentando di destabilizzare lo status quo nei singoli stati e regioni legati alla Federazione russa, così minando la stabilità strategica della Russia[10].

Già questi documenti, sia la Dottrina sulla sicurezza delle informazioni del 2000 che la Dottrina militare del 2010, precisano che le operazioni d'informazione sono delle operazioni da mettere in atto durante il tempo di pace e come preludio alla guerra, piuttosto che solo una componente della guerra stessa[11].

La dottrina della sicurezza informatica 2010

Infine, a dicembre 2016 il Presidente Putin firma l'ultima Dottrina della sicurezza informatica della Russia, quest'ultima si basa sulle precedenti Dottrine della sicurezza militare e dell'informazione, sostenendo la necessità di equilibrare il bisogno dei russi di ottenere informazioni e le esigenze di sicurezza delle informazioni nazionali, enfatizzando ulteriormente la politica dello Stato di mettere la sicurezza davanti alle libertà civili; inoltre, il documento denunzia che

[9] C. Collison, Russia's Information War, op. cit.
[10] *Ibidem.*
[11] R. Heickero, Emerging Cyber Threats, op.cit., pp. 18-21.

i media russi sono soggetti a una clamorosa discriminazione all'estero ed evidenzia l'obbligatorietà di ritrarre intenzionalmente un'immagine positiva della Russia[12].

Il campo di applicazione del termine Information Warfare

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 performance in pubblico eseguita da un *influencer*[13].

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[14]. Ma anche all'interno del CNO, un'arma dell'informazione non deve necessariamente avere un effetto distruttivo del mondo reale nello stile di *Stuxnet*[15]; in linea con gli obiettivi di *Information Warfare*, in generale, la distruzione fisica delle strutture del tuo avversario non è necessaria per influenzare il trasferimento e l'archiviazione dei dati[16].

[12] C. Collison, Russia's Information War, op. cit.
[13] K. Giles, *Handbook of Russian Information Warfare*, op. cit., pp. 10.
[14] K. Giles e H. William II, *Divided by a Common Language*, op. cit.
[15] Un virus informatico creato con lo scopo di sabotaggio la centrale nucleare iraniana di Natanz.
[16] K. Giles, *Handbook of Russian Information Warfare*, op. cit., pp. 13.

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[17]. 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[18].

Secondo Stephen Blank, data l'ampia concezione di *Information Warfare* nella teoria russa, l'attenzione delle operazioni cibernetiche tende a essere di natura strategica, piuttosto che operativa o tattica[19] (ciò non preclude che non venga 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[20].

L'InfoWar per obiettivi politici

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 colleghi occidentali, concentrandosi sulla teoria e sulla pratica[21].

Il punto di vista russo sull'Information Warfare è stato influenzato dal dibattito sulla *Revolution in Military Affair* (RMA) durante gli anni '80

[17] T. Thomas (Lt. Col., U.S. Army, Retired), *Nation-State Cyber Strategies*, op. cit. 266.
[18] M. Connell and S. Vogler, *Russia's Approach to Cyber Warfare*, op. citp. 2-6.
[19] 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.
[20] M. Connell and S. Vogler, *Russia's Approach to Cyber Warfare*, op. cit. p. 6.
[21] R. Heickero, *Emerging Cyber Threats*, op. cit, pp. 12-17.

e '90, così come dalla costruzione del concetto di *Network – Centric War* (NCW). Gli elementi del RMA possono essere riassunti come:

- attacchi di precisione,
- concetti di guerra guidata dalle informazioni,
- guerra di comando e controllo,
- dominio dell'informazione sul campo di battaglia[22].

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 eserciti di massa in operazioni guidate dalla tecnologia, soppiantato poi, dall'uso di RMA da parte dei funzionari del Pentagono[23].

Tecnologie dell'informazione, armi del XXI secolo

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[24]. Dichiararono la Guerra del Golfo del 1990-91 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[25].

[22] M. Mowthorpe, "The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views", University of Hull, vol. 5, no. 2 (Summer), 2005.
[23] *Ibidem.*
[24] Heickero R., *Emerging Cyber Threats*, op. cit, pp. 12-17.
[25] *Ibidem*

La guerra in Afghanistan del 1979-89 e la guerra in Cecenia 1994-96 e quella del '99 hanno influenzato la mentalità russa e hanno portato conoscenze pratiche e approfondimenti sull'approccio russo all'Information Warfare[26]. Da un punto di vista psicologico della guerra la Russia ha sofferto gravi problemi in Afghanistan e non è riuscito a influenzare i suoi avversari[27]. Entrambe le guerre in Cecenia hanno mostrato come in alcune aree, anche un avversario piccolo e relativamente povero, poteva ottenere il dominio dell'informazione su un avversario potente, usando i mass media ed Internet efficientemente, al fine di trasmettere la loro opinione ed ottenere influenza positiva sull'opinione pubblica.

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[28]. Al fine di contrastare questa strategia, i *policy maker* 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[29].

[26] 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

[27] Yu. Serookiy, "Psychological-Information Warfare: Lessons of Afghanistan", Military FOI-R–2970–SE Thought, vol. 13 no 1, 2004.

[28] .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

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

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

La fusione e il coordinamento tra i 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[30].

La natura olistica dell'InfoWar

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[31]. 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[32]. Come descritto dal presidente Vladimir Putin, *"Dobbiamo tenere conto dei 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"*[33].

[30] P. Brangetto and 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.
[31] *Ivi*, pp. 3-5.
[32] *Ibidem.*
[33] V. Putin, "Солдат есть звание высокое и почетное" ("Soldier" is an honourable

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[34]. Non è nemmeno limitato alla fase iniziale delle ostilità, dove generalmente, include la preparazione d'informazioni utili in merito al campo di battaglia[35]. Invece, viene considerata un'attività costantemente in corso, a prescindere dallo stato delle relazioni con l'avversario[36].

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[37].

L'Information Warfare può coprire una vasta gamma di diverse attività e processi che cercano di rubare, piantare, interdire, manipolare, distorcere o distruggere le informazioni ed i canali e i metodi disponibili per farlo coprono una gamma altrettanto ampia, inclusi computer, smartphone, dichiarazioni di leader o celebrità, campagne online di troll o messaggi di testo, fino ad arrivare a trasmettere video su YouTube rivolti ad una pluralità di individui o approcci diretti a singoli obiettivi[38].

and respected rank), excerpts from annual Address to the Federal Assembly of the Russian Federation, Krasnaya zvezda, 11 maggio 2006.
[34] K. Giles, *Handbook of Russian Information Warfare*, op.cit., pp. 3-5.
[35] P. Antonovich, "Cyberwarfare: Nature and Content," *Military Thought*, No.3, Vol.20, 2011, pp. 35-43.
[36] Heickero R., *Emerging Cyber Threats*, op.cit, p. 20.
[37] ловарь терминов и определений в области информационной безопасности, Voyennaya Akademiya General'nogo Shtaba, 2nd Edition, Moscow Voyeninform, 2008.
[38] K. Giles, *Handbook of Russian Information Warfare*, op.cit., pp. 3-5.

Le armi informatiche sono una forma di moltiplicatore di forza che cambia il paradigma della stabilità strategica[39].

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[40].

La guerra dell'informazione russa rappresenta una forma di potere politico e uno strumento geopolitico che consente un alto livello di manipolazione e influenza, con una bassa probabilità di confronto militare.

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[41]. 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)[42].

Maskirovka: metodi per l'inganno

La Russia ha una lunga tradizione nel condurre campagne d'inganno e, con il termine "*Maskirovka*" (letteralmente, "metodi per l'inganno"),

[39] Per un approfondimento su studi di strategia *Cfr*. L. Bozzo, Studi di strategia. Guerra, politica, economia, semiotica, psicoanalisi, matematica, EGEA Editore, Collana Alfaomega, 2012.
[40] 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
[41] V. Ovchinsky, S. Larina, & Kulik, Russia and the Challenges of the Digital Environment, *Russian International Affairs Council (RIAC)*, Moscow, 2015.
[42] *Ibidem.*

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[43]. Da un punto di vista russo, *Maskirovka* è una componente cruciale della guerra dell'informazione[44], misure organizzative e interconnesse, operative-tattiche e ingegneristiche condotte per ingannare l'avversario e proteggere i sistemi di comando e controllo[45]. Nello specifico, mira a ingannare i servizi d'intelligence stranieri; inganna i centri di comando e controllo con lo scopo di indurre, e quindi influenzare, un avversario a prendere decisioni a beneficio delle forze russe[46].

Gli Stati Uniti usano il termine *Military Deception* (MILDEC) come una capacità fondamentale di IO per ingannare i decisori 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[47].

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'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

[43] Heickero R., *Emerging Cyber Threats*, op.cit, p. 20.
[44] T. Thomas, *Manipulating the Mass Consciousness*, op. cit. p. 12.
[45] Heickero R., *Emerging Cyber Threats*, op.cit, p. 21.
[46] *Ivi*, p. 22.
[47] *Ivi*, p. 23-26.

Cremlino dà la priorità a una strategia multiforme che enfatizza l'informazione come mezzo per promuovere obiettivi politici.

Guerra per approccio indiretto

È curioso considerare come la guerra dell'informazione possa essere collocata in un contesto ancora più ampio. Il colonnello in pensione Sergei Chekinov e il tenente generale in pensione Sergei Bogdanov si occupano dell'*InfoWar* nel contesto della guerra con mezzi non militari (*nevoennye sredstva*) e guerra per approccio indiretto (*nepriamye deistviia*)[48].

Chekinov e Bogdanov, sostengono che l'approccio indiretto stia diventando sempre più importante nel mondo moderno, infatti dai loro studi emerge che: mentre l'approccio indiretto è stato storicamente al secondo posto rispetto a quello diretto, nel mondo attuale, esso, sta diventando sempre più il primo e principale strumento del maestro stratega[49]. L'approccio indiretto nella guerra può essere approssimativamente descritto come segue: non attaccare il nemico dove è più forte, ma dove è più debole, farlo di sorpresa con manovre rapide e cercando continuamente opportunità inattese per l'attacco; Chekinov e Bogdanov descrivono l'idea riferendosi a Sun Tzu e Napoleone, ma in primo luogo citano il generale britannico Liddell Hart, a cui viene generalmente attribuita l'idea moderna dell'approccio indiretto[50]. Mentre Liddell Hart indaga sull'azione indiretta principalmente nel contesto militare tradizionale, Chekinov e Bogdanov esplorano così il suo uso nel più ampio contesto delle relazioni internazionali in senso più ampio e, facendo eco alla

[48] Alla loro analisi dovrebbe essere dato un peso considerevole quando si tenta di comprendere la prospettiva russa sulla guerra dell'informazione poiché, gli autori, sono entrambi affiliati al Centro per gli studi strategici militari dello stato maggiore.
[49] U. Franke, *War by non-military means*, op.cit., 38-48.
[50] *Ibidem*

formulazione dei documenti ufficiali, essi sostengono l'importanza della guerra dell'informazione: l'esperienza delle guerre locali e dei conflitti armati degli ultimi decenni dimostra che la guerra strategica dell'informazione (*strategicheskoe informatsionnoe protivoborstvo*) svolge un ruolo importante nello smantellare la *leadership* militare e governativa, sabotare i sistemi di difesa aerea e spaziale, ingannare il nemico formando opinioni pubbliche desiderabili e altre misure per ridurre la volontà dell'avversario di resistere[51].

Il capo dello Stato maggiore, Valerii Gerasimov, in un discorso all'Accademia militare russa nel gennaio 2013, ha discusso il ruolo dei metodi non militari nei conflitti moderni, osservando che il loro ruolo è aumentato e che ora possono essere molto più efficaci delle armi tradizionali[52].

Secondo il modello di Gerasimov, i mezzi militari non sono che una piccola parte della guerra, la parte più importante è di gran lunga utilizzata da mezzi non militari.

[51] *Ibidem*
[52] *Ivi*, p. 38-42.

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