Cyberwarfare, le strategie della Russia

Domenico Frascà

UNIVERSITÀ
DEGLI STUDI
FIRENZE

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

Center for Cyber Security and International Relations Studies

Cyberwarfare, le strategie della Russia

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.

Cyberwarfare, le strategie della Russia[1]

Produrre discordia nella società, interrompere il processo decisionale e degradare la libertà di azione senza o con poca distruzione fisica. *L'InfoWar* rappresenta una seria sfida strategica e una minaccia formidabile. Ecco tutte le strategie messe in campo dalla Russia. La guerra moderna – *infowar* o *cyberwarfare*-, 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 avvengono nella psicologia dell'avversario[2].

Cyberwarfare: le parole sono importanti

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[3]. In altre parole, il *cyber* è considerato un meccanismo per consentire allo Stato, o ad attori non statali, di dominare il paesaggio informativo, che è considerato un dominio bellico a sé stante[4]. Generalmente deve essere impiegato come parte di un'intera operazione, insieme ad altre, più tradizionali, armi da

[1] La seguente analisi è apparsa su Agenda Digitale il giorno 15 ottobre 2018 ed è reperibile al seguente link https://www.agendadigitale.eu/cultura-digitale/cyberwarfare-le-strategie-della-russia/.
[2] U. Franke, *War by non-military means. Understanding Russian information warfare*, FOI, Swedish Reserch and Defence Institute, Stockholm, Sweden 2015, pp. 9-10, accessibile: https://dataspace.princeton.edu/jspui/handle/88435/dsp019c67wq22q [ultima consultazione online: 30.06.18]
[3] M. Connell and S. Vogler, *Russia's Approach to Cyber Warfare*, CNA Analysis & Solution, 2017, p. 3.
[4] Ibidem.

guerra dell'informazione, comprese le operazioni di disinformazione, *PsyOps*, guerra elettronica[5].

L'espressione "guerra dell'informazione", qui usata, è stata deliberatamente scelta come una traduzione del concetto russo "*informatsionnaia voina*"[6] (Information Warfare).

Secondo la Dottrina Militare della Federazione Russa (2010), una delle caratteristiche dei moderni conflitti militari è "la precedente attuazione di misure di guerra dell'informazione al fine di raggiungere obiettivi politici senza l'utilizzo della forza militare e, successivamente, nell'interesse di dare una risposta favorevole dalla comunità mondiale all'utilizzo della forza militare"[7].

Le guerre non sono più dichiarate

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" in Nord Africa e nel Medio Oriente, conferma che uno Stato può trasformarsi, in pochi mesi o addirittura giorni, in un'arena di feroce conflitto armato, diventare

[5] 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 [Ultimo accesso online: 01.07.18]

[6] Termini traslitterati da: информационное противоборство & информационная война.

[7] La Dottrina militare della Federazione Russa, approvata con editto presidenziale della FederazioneRussa il 5 febbraio 2010.

vittima di un intervento straniero e sprofondare in una rete di caos, catastrofi umanitarie e guerra civile[8].

Lo sviluppo di Dottrine e strategie in un paese deve essere compreso e collegato a un contesto più ampio, basandosi ad esempio 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 forte" del presidente Vladimir Putin ha influenzato la mentalità; con la fine della Guerra Fredda e la transizione attraverso gli anni di instabilità, la Russia si è orientata verso una società basata su una *leadership* forte[9]. L'esperienza della Russia moderna differisce da quella occidentale e ciò influisce anche sul suo pensiero militare in generale e, più specificamente, sul punto di vista della guerra dell'informazione[10].

Esiste una sovrabbondanza di termini con i quali si tenta di accomunare un certo significato al concetto di guerra dell'informazione, tali come: operazioni di informazione, guerra di comando e controllo, operazioni psicologiche, sicurezza dell'informazione, cyberpotere, operazioni di influenza, guerra elettronica, inganno militare, sicurezza informatica, comunicazione strategica, diplomazia pubblica, spionaggio informatico, *cyberwar* etc.[11] Alcuni di questi termini, per un professionista che studia o applica direttamente tali operazioni, hanno

[8] M. Connell and S. Vogler, *Russia's Approach to Cyber Warfare*, op. cit. p. 4
[9] S. Hanson, "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
[10] Heickero R., *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency (FOI). Stockholm, Sweden, March 2010, pp. 12-14
[11] U. Franke, *War by non-military means*, op.cit., p. 9-10

significati precisi e ben definiti, mentre altri restano vaghi ed ambigui, poiché, per ovvie ragioni, vaga ed ambigua è la materia oggetto di studio; per le persone che, legittimamente hanno deciso di non studiare od inoltrarsi in simili vicissitudini, la difficoltà di comprendere tali concetti aumenta esponenzialmente.

Nell'attuale Dottrina statunitense lo scopo dell'*Information Operation* (IO), è di: influenzare, interrompere, corrompere o usurpare il processo decisionale umano e automatizzato dell'avversario[12].

Per quanto riguarda le minacce alla sua sovranità nazionale, la visione Russa è descritta in Dottrine e documenti strategici come: la Dottrina militare[13] e la Dottrina sulla sicurezza delle informazioni della Federazione Russa[14], entrambe del 2000 (quella militare è stata successivamente rinnovata nel 2010 prima e, poi, nel 2016) e approvate dal Consiglio di sicurezza. 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[15].

Guerra dell'informazione

La guerra dell'informazione è un tipo di minaccia transnazionale, che penetra i confini nazionali e incide sulla stabilità della società e,

[12] U. Franke, *War by non-military means*, op.cit., p.10.
[13] Voyennaia Doktrina Rossiiskoy Federatsii, Utverzhdena Ukazom Prezidenta RF ot 21 aprelya 2000, "The Military Doctrine of the Russian Federation" (traduzione), approvato con decreto del Presidentedella Federazione Russa, 21 aprile 2000.
[14] Doktrina Informatsionnoi Bezopasnosti Rossiiskoi Federatsii, Il documento è tradotto e discusso, adesempio in D. Carman, "Translation and Analysis of the Doctrine of Information Security of theRussian Federation: Mass media and the politics of identity". *Pacific Rim Law & Policy Journal Association*, 2002.
[15] Heickero R., *Emerging Cyber Threats*, op.cit, p. 13.

quindi, dello Stato, mirando ad influenzare la popolazione e sui leader, finanche a manipolare decisioni e azioni[16].

L'ultima pubblicazione del 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 nostri"[17]. Il dizionario identifica inoltre, 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]. l'UE non accetta la guerra dell'informazione come un'unica entità; l'organizzazione europea, considera l'importanza delle attività d'informazione come un fattore di successo e definisce la campagna d'informazione come una serie di attività che supportano gli obiettivi della strategia d'informazione sulle crisi[19]. La visione attuale della guerra dell'informazione è ampiamente estesa tra diverse categorie e aree di competenza[20].

[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 online: http://www.recentscientific.com/sites/default/files/10867-A-2018.pdf
[17] DOD Dictionary of Military and Associated Terms, febbraio 2018, accessibile online: http://www.jcs.mil/Doctrine/DOD-Terminology/
[18] NATO Glossary of Terms and Definitions, AAP – 06 Edition, 2017.
[19] EEAS, *EUMC Glossary of Acronyms and Definitions Revision 2015*, febbraio 2016.
[20] L.B. Monov and M.L. Karev, "Information Warfare Conceptual Framework", op. cit.

Le operazioni della guerra dell'informazione

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 obiettivi nel dominio elettromagnetico.

- 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]. La capacità di Internet di condividere idee e narrazioni porta il conflitto al livello sociale della società, la guerra dell'informazione potrebbe creare false impressioni al fine di costruire o rompere alleanze e simpatie[23]. In altre parole, solleva tensione e attrito su questioni attuali tra diversi gruppi e opinioni, determinando un certo grado di discordia nella società.

[21] *Ibidem*.
[22] C. Downes, "Strategic Blind-spots on cyber threats", *The Cyber Defense Review*, Vectos and Campaigns, 2018, pp. 1-19.
[23] L. Freedman, "The Future of War A Hstory", *PublicAffairs*, New York, 2017.

David Stupples considera l'*Information War* come una combinazione di tre tipi distintivi di guerra per attacco e difesa con uno scopo specifico:

- in primo luogo, include la guerra elettronica che deve distruggere lo spazio elettromagnetico;
- inoltre, individua gli attacchi informatici per influenzare la funzionalità dell'infrastruttura nazionale;
- infine, comprende gli *psy-op* (*Psycological Operation*), che devono degradare i valori e minare le norme morali. La combinazione e l'utilizzo congiunto di questi, potrebbe causare instabilità e caos[24].

Propaganda e disinformazione contro l'Occidente

Helle Dale della Heritage Foundation sostiene che attraverso l'emittente "Today", di proprietà dello Stato russo, Mosca ha condotto una guerra dell'informazione, al fine di diffondere propaganda e disinformazione minando la credibilità degli Stati Uniti e dell'Occidente, mettendo in buona luce l'operato russo[25].

Altresì, se occorre adoperarsi con l'intento di manipolare una determinata situazione informativa interna, lo scopo più importante, è che l'obiettivo agisca contro i propri interessi; per quanto possa sembrare contorto il ragionamento, l'attaccante può usare i media di proprietà statale per diffondere apertamente confusione e distrazione, per far avanzare la sua agenda politica così creando un

[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
[25] L.B. Monov and M.L. Karev, "Information Warfare Conceptual Framework", op. cit.

ambiente artificioso a lui apparentemente sfavorevole, ma fattualmente favorevole[26]. È anche una guerra narrativa che utilizza i *social media* per manipolare i fatti, disperdere la 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[27].

Le tre strade della guerra dell'informazione

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, idee e valori[28];

[26] *Ibidem.*
[27] U. Franke, *War by non-military means*, op.cit., p. 10-20.
[28] 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

- infine, aumenta la portata dei suoi sforzi al fine di reclutare sostenitori e sollecitare risorse[29]. Attraverso una rete di sostenitori, personalità false, *botnet* e *troll*, l'aggressore intensifica il livello delle sue attività per creare un ambiente artificiale di opinioni diverse e per corrompere la credibilità delle informazioni[30].

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

L'*InfoWar* non è una materia che riguarda solo le Forze Armate o il Ministero della Difesa, piuttosto, come ripetutamente sottolineato nei documenti ufficiali, le risorse di molte delle agenzie governative devono riunirsi per condurre un'*InfoWar* di successo. Si può asserire, che nell'area della sicurezza nazionale l'*InfoWar* rappresenta una seria sfida strategica e una minaccia formidabile che ha diverse caratteristiche:

- primo, l'intento generale della guerra dell'informazione è portare avanti obiettivi geopolitici, evitando la competizione e la guerra militare diretta.

- In secondo luogo, la guerra delle informazioni utilizza molteplici canali che includono media regolari come: televisione, testate giornalistiche, radio; media moderni: *social media*, pagine web, blog, reti informatiche, dispositivi elettronici che distribuiscono

[29] L.B. Monov and M.L. Karev, "Information Warfare Conceptual Framework", op. cit.
[30] *Ibidem*.

messaggi e comandi attraverso onde elettromagnetiche ed infrastrutture critiche.

- In terzo luogo, la guerra delle informazioni sfrutta tutte le possibili opportunità e vulnerabilità su diversi punti di vista, spesso controversi, della emarginazione della popolazione, dell'individuo e del gruppo[31].

Uno dei componenti principali del conflitto moderno è il potere di progettare una giusta combinazione tra *softpower* e *hardpower* che diventi un'arma d'influenza sulla popolazione e di controllo sulle decisioni. Tutto questo attraversa i tradizionali confini di difesa e offusca la linea tra scelte e azioni razionali ed irrazionali; con costi e rischi minimi, l'attaccante può pianificare e condurre operazioni offensive segrete e/o palesi che trasformano ed estendono le forme di conflitto tradizionale. Questo approccio proattivo di destabilizzazione strategica aggressiva è una forma di guerra che trae energia dal degrado delle capacità, dall'erosione delle credenze e dalla morale, interrompendo o danneggiando il potere decisionale e generando discordia nella società[32].

[31] L.B. Monov and M.L. Karev, "Information Warfare Conceptual Framework", op. cit
[32] *Ibidem.*

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