RESEARCH ANALYSIS
2015

UNIVERSITÀ DEGLI STUDI FIRENZE

# CYBERWAR, LO STRUMENTO BELLICO DEL FUTURO?

## IL CASO RUSSO-GEORGIANO

NICCOLÒ TADDEI

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

# CYBERWAR, LO STRUMENTO BELLICO DEL FUTURO?

# IL CASO RUSSO-GEORGIANO

Niccolò Taddei

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

2017

# RIGUARDO ALL'AUTORE

Dopo un periodo di studio presso il Center for International Relations dell'Università di Varsavia ed un tirocinio a Bruxelles, durante il quale si è occupato di comunicazione e advocacy per Human Rights Watch, si è laureato con 110 e lode alla Cesare Alfieri di Firenze con una tesi di laurea sul ruolo della deterrenza nel cyberspace. Ha svolto il Master in Studi diplomatici alla "SIOI – UNA Italy" di Roma e attualmente lavora per Deloitte come analista di cybersecurity. È membro del Center for Cyber Security and International Relations Studies fin dalla sua nascita e per lo stesso ha pubblicato un paper dal titolo "Cyber War: lo strumento bellico del futuro? Il caso Russo-Georgiano". Si occupa delle relazioni esterne del Center.

# CYBERWAR, LO STRUMENTO BELLICO DEL FUTURO? IL CASO RUSSO-GEORGIANO

## Introduzione

Questo lavoro si propone di studiare un elemento sempre più rilevante nelle dinamiche della politica internazionale, un fattore in particolare molto incisivo nel panorama della conflittualità contemporanea e – con ogni probabilità – futura.

La *cyberwar* è la nuova frontiera della guerra. Il *cyberspace* – accanto a terra, aria, mare e spazio extra-atmosferico, i domini bellici tradizionali – rappresenta oggi "la quinta dimensione della conflittualità", utilizzando la brillante definizione di Luigi Martino[1].

Fatta questa premessa e sottolineata l'importanza della dimensione *cyber* nel panorama bellico contemporaneo, è opportuno smorzare e ridimensionare le previsioni catastrofiche – oggi sempre più frequenti – di una guerra cibernetica *tout court*. Parafrasando Clausewitz: "mai il mezzo può essere concepito senza lo scopo"[2]. La *cyberwar* è uno strumento tra i tanti utilizzabili nell'ampia categoria della guerra, da mettere al servizio degli obiettivi strategici della politica. Uno strumento che sta acquisendo sempre maggiore rilevanza e che – come vedremo – ha già avuto modo di dimostrare la sua efficacia, ma pur sempre uno strumento.

*Cyberspace* è anche sinonimo di accesso diffuso. Uno dei punti cardine nello studio di questa disciplina è infatti il problema dell'accesso ad informazioni sensibili da parte di soggetti non statali, o comunque un tempo vincolati al controllo ed alla sorveglianza dall'alto. Questa forma di diffusione del potere a favore di attori (un tempo) deboli è senza dubbio foriera di nuove sfide e minacce che gli Stati ed i *policymakers* dovranno affrontare e dagli esiti non certo scontati. Nonostante ciò, in questo lavoro non ci si soffermerà – per motivi di spazio e d'interesse - sull'aspetto della diffusione del potere *cyber* ad attori cosiddetti

[1] Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII*, febbraio 2014.
[2] Von Clausewitz, Carl, *Della guerra*, Milano, Mondadori, 1997.

"minori", ma piuttosto si manterrà al centro dell'analisi l'utilizzo dello strumento *cyberwar* nella dimensione "tradizionale" della guerra tra Stati, andando anche a vedere un caso specifico e ben esemplificativo come quello del conflitto russo-georgiano dell'agosto 2008.

Prima di passare all'osservazione del caso citato – nel paragrafo iniziale - si cercherà di fornire una definizione più completa ed approfondita di *cyberwar* e si studieranno le possibili applicazioni di questa risorsa al teatro bellico.

Nel paragrafo successivo si andranno a vedere alcuni precedenti di utilizzo dello spazio cibernetico nella conduzione di operazioni militari, o comunque in situazioni di conflittualità a livello statale.

Infine, il paragrafo finale sarà dedicato al caso di studio su cui è incentrata la ricerca. I fatti georgiani – paradigmatici per il futuro - sono il primo vero esempio di utilizzo intensivo (e decisivo) della dimensione cibernetica nel corso di un conflitto tra Stati.

## Un nuovo strumento di guerra

Lo spazio cibernetico non va più pensato limitatamente al suo primario - in apparenza - ruolo civile, ma va riconsiderato come concreta e potenziale fonte di minacce per la sicurezza nazionale. Il *cyberspace* si è ormai affermato a tutti gli effetti come un nuovo "ambiente strategico"[3] e come tale è necessario che sia trattato da analisti e *policymakers* che vogliano sfruttare le potenzialità di questo nuovo dominio, ma che soprattutto mirino a tutelarsi dalle potenziali minacce e ad ottenere una difesa efficace. Questa considerazione – e ciò che ne consegue – risulterà meno scontata se si riflette sul fatto che il *cyberspace* – a differenza di tutti gli altri domini tradizionali – rappresenta qualcosa di intangibile per natura, dotato dunque di una forte volatilità intrinseca[4]. Luigi Martino lo definisce come un ambiente "*placelessness*"[5], mentre nella *National Military Strategy for Cyberspace Operations* possiamo

[3] Cfr. Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII*, febbraio 2014

[4] Cfr. Libicki, Martin C., "Cyberdeterrence and Cyberwarfare", Santa Monica CA, RAND, 2009.

[5] Cfr. Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII*, febbraio 2014.

trovare l'acronimo *VUCA: Volatility, Uncertainity, Complexity, Ambiguity*[6]; il cyberspace è caratterizzato da velocità di propagazione ed abbattimento dei confini, le operazioni (nel nostro caso militari) che ne scaturiscono sono istantanee ed insensibili a qualsiasi tipo di attrito ambientale. Nonostante ciò, non si può affermare che con l'avvento della dimensione cibernetica si giunge al superamento del fattore territoriale – o, se vogliamo, della geopolitica in senso stretto – in quanto le azioni condotte tramite l'ambiente cibernetico, pur sviluppandosi a livello virtuale, producono effetti "concreti" nel mondo reale[7]; si tratta dunque di "una minaccia che, sebbene riferita al mondo intangibile del *cyberspace*, presenta ormai tratti di estrema concretezza"[8] . Rendersi conto della potenziale valenza del *cyberspace* come nuova arena della conflittualità[9], dovrebbe portare alla trattazione di questo ambiente secondo le consuete dinamiche e regole delle relazioni internazionali[10].

I primi a muoversi in direzione di un riconoscimento "ufficiale" della valenza dello spazio cibernetico nella politica internazionale – al solito "ansiosi" nel (vano?) tentativo di mantenere una qualche forma di controllo in un mondo sempre più multipolare e sempre meno controllabile – sono stati gli Stati Uniti; nel 2001 un documento ufficiale del Dipartimento per la Difesa definiva il dominio cibernetico come "un potenziale moltiplicatore delle minacce per la sicurezza e gli interessi americani"[11]. Questa linea guida verrà poi confermata dalla *National Strategy to Secure Cyberspace* del 2003, nella quale lo spazio cibernetico – che garantisce il controllo del Paese – viene paragonato ad un sistema nervoso il cui funzionamento è di vitale importanza sia dal punto di vista dell'economia che della sicurezza nazionale"[12]. Il riconoscimento definitivo è poi da far risalire al marzo 2005, quando nella *National Defense Strategy* si afferma senza mezzi termini "*cyberspace is a new theater of operations*"[13].

---

[6] NMS CO, novembre 2006: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber 023.pdf.
[7] Cfr. Jean, Carlo e Tremonti, Giulio, *Guerre stellari: società ed economia nel cyberspazio*, Milano, FrancoAngeli editore, 2000.
[8] Relazione sulla politica dell informazione per la sicurezza 2010: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp content/uploads/2011/02/relazione 2010.pdf.
[9] Cfr. Choucri, Nazli, *Cyberpolitics in International Relations*, Massachussetts, MIT Press Cambridge, 2012.
[10] Cfr. Jean, Carlo, *Geopolitica del XXI secolo*, Roma Bari, GLF editori Laterza, 2004.
[11] 2001 Quadriennial Defense Review Report: http://www.comw.org/qdr/qdr2001.pdf.
[12] The National Strategy to Secure Cyberspace: https://www.us cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[13] The National Defense Strategy of the United States of America, marzo 2005: http://www.globalsecurity.org/military/library/policy/dod/nds usa_mar2005.htm.

Libicki sostiene che il concetto di guerra cibernetica è un derivato di quello – più generico ed onnicomprensivo – di *Information Warfare*[14]. Ciò che interessa ai fini di questa ricerca è l'utilizzo delle scoperte tecnologiche in campo elettronico, informatico e satellitare con l'obiettivo di compiere atti bellici[15], in particolare "al fine di negare all'avversario l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati"[16]; o anche le "attività militari svolte dalle Forze Armate nel e tramite il cyberspazio, in tempo di guerra o di crisi, allo scopo di garantire e sfruttare il cyberspazio ai propri fini e, contemporaneamente, negando tale capacità all'avversario"[17].

La parola chiave nello studio degli usi che si possono fare dello spazio cibernetico nel teatro bellico – ed in particolare quelli che qui saranno analizzati - è dunque negare (*to deny*); utilizzare e sfruttare uno status di superiorità nelle capacità di accesso e comando per estromettere un altro attore, negando quindi in sostanza all'avversario la possibilità di accesso alla risorsa[18].

Nella conduzione di un conflitto armato la possibilità (e la capacità) di utilizzo del dominio cibernetico consente l'introduzione di diverse novità, a partire dalla trasmissione in tempo reale di informazioni, fino allo svolgimento di operazioni militari coordinate, istantanee, economiche (e - se necessario - "globali"), basate su di un sistema di comando e controllo automatico ed autonomo. Attraverso lo spazio cibernetico si possono raggiungere obiettivi militari e strategici senza bisogno di ricorrere ad un'azione armata, con tutto ciò che ne consegue; non è più possibile separare il concetto di guerra cibernetica da quello più generale di *warfare*, del quale rappresenta anzi ed a pieno titolo una nuova componente. Emerge dunque con forza la sempre maggiore "rilevanza strategica" che lo spazio cibernetico va assumendo all'interno

[14] Cfr. Libicki, Martin C., *What is Information Warfare?*, Center for Advanced Command Concept and Technology, Institute for National Strategic Studies, National Defense University, Washington DC, agosto 1995.

[15] Per quanto non tutte le operazioni illecite condotte tramite il cyberspace – anche condotte tramite obiettivi statali – possano essere considerate atti di cyberwar.

[16] Dipartimento delle Informazioni per la Sicurezza, *Il linguaggio degli organismi informativi. Glossariodi intelligence*, in "Gnosis. Rivista Italiana di Intelligence. Quaderni di Intelligence", Roma, De Luca Editori, 2012.

[17] Scotto di Castelbianco, Paolo, "La cyber minaccia: attori, mutamenti e sfide al sistema Paese. Il ruolo della cyber intelligence", in Gori, Umberto e Germani, Luigi Sergio a cura di , *Information Warfare2011. La sfida della cyber intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano, FrancoAngeli editore, 2012.

[18] Cfr. Posen, Barry R., "Command of the Common. The Military Foundation of U.S. Hegemony", International *Security*, estate 2003.

dell'arena internazionale e delle dinamiche che la compongono e regolano[19].

Per poter parlare di guerra cibernetica nell'ottica che interessa ai fini di questa ricerca – senza dunque deviare verso alcune declinazioni "minori" del concetto, ma anche non scandendo nel generico – è necessario specificare alcuni punti. Il concetto generale di *Information Warfare* – come abbiamo visto precedentemente – ricopre uno spettro ampio di fenomeni; tra questi possiamo ad esempio trovare gli atti di *Economic Information Warfare* o di *Hacker Warfare*[20], molto diffusi e condotti con finalità di natura strettamente economica. Inoltre, molte di queste azioni sono spesso effettuate da attori minori, non statali e relativamente deboli, facenti leva sullo sproporzionato potere derivatogli dall'avvento del dominio cibernetico nella determinazione dei rapporti di forza del sistema internazionale[21]. Qui ci concentriamo però esclusivamente sulle azioni condotte da uno Stato contro un altro Stato, con finalità bellica.

Il termine "guerra", anche nella dimensione *cyber*, abbisogna di elementi coercitivi e finalità distruttiva; più precisamente, la guerra cibernetica consisterebbe in "un'azione da parte di uno Stato atta a penetrare i sistemi informatici o le reti di un altro Stato con la finalità di causare danni o distruzione"[22]. Non bisogna confondere tra guerra cibernetica e attacco informatico "fine a sé stesso"; la guerra ha finalità più ampie e lo spazio cibernetico è utilizzato come strumento, *medium*, con l'obiettivo reale di causare danni alle infrastrutture del nemico[23]. In questo senso va letta anche l'interessante considerazione di Luigi Marino, secondo cui per la guerra cibernetica si può parlare di un modello di *Indirect Approach*: attraverso la *cyberwar*, si punta all'annientamento strategico dell'avversario, piuttosto che a quello tattico[24].

---

[19] Cfr. Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII*, febbraio 2014.

[20] Vedi nota 14.

[21] Cfr. Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII*, febbraio 2014.

[22] Clarke, Richard A., Knake, Robert K., *Cyber War. The Next Threat to National Security and What to do About It*, New York, Harper Collins Publishers, 2010.

[23] Borg, Scott, "Logica della guerra cibernetica", in *Limes, Quaderno Speciale*, aprile 2012.

[24] Cfr. Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII,* febbraio 2014.

Secondo Umberto Gori, per la definizione e lo studio di un atto di *cyberwar*, è importante la valutazione del contesto – e soprattutto, conseguentemente, dell'obiettivo finale – in cui l'atto stesso viene posto in essere; è necessaria una certa dose di letalità, almeno tale da produrre una qualche influenza – e conseguenze reali, concrete - sulle scelte di chi subisce l'attacco[25]. Dietro alla messa in atto di un'offensiva cibernetica vi è la ben precisa intenzione di colpire il nemico arrecandogli dei danni concreti, nel perseguimento di obiettivi politico-strategici più ampi; lo strumento cibernetico è utilizzato per costringere chi subisce l'attacco a piegarsi alla volontà di chi lo attua ed un tale potenziale coercitivo – a partire dal punto di vista economico/organizzativo – può possederlo soltanto uno Stato[26] (che poi questo effettui l'attacco cibernetico "direttamente" o, come spesso accade, preferisca delegare – in particolare nel tentativo di sottrarsi ad eventuali responsabilità davanti alla comunità internazionale – è un altro discorso).

## Alcuni precedenti

Il caso georgiano – sul quale è incentrato questo studio e che sarà approfondito nel prossimo paragrafo – non è stato il primo esempio di attacco cibernetico. Allo stesso tempo però, non sono molti gli episodi in cui si è potuto assistere ad offensive della dimensione qui analizzata, ovvero con un utilizzo consistente e diffuso del dominio cibernetico, che diventasse dunque strategicamente rilevante – se non decisivo – ai fini degli obiettivi perseguiti; altra componente necessaria – come anticipato – è il coinvolgimento di attori statali, sia questo diretto (e dimostrabile) o meno.

Tra i casi più celebri di *infowar*[27] vi è sicuramente l'attacco russo all'Estonia – Paese rinomato per essere fortemente interconnesso ad internet - risalente alla fine del mese di aprile del 2007. Il movente

[25] Gori, Umberto, "Cyberspazio e relazioni internazionali: implicazioni geopolitiche e geostrategiche", in Gori, Umberto e Lisi, Serena a cura di , *Information Warfare 2012. Armi cibernetiche e processo decisionale*, Milano, FrancoAngeli editore, 2013.

[26] Cfr. Von Clausewitz, Carl, *Della guerra*, Milano, Mondadori, 1997, citato in Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII* , febbraio 2014.

[27] Cfr. Gori, Umberto, "Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici", in Gori, Umberto e Germani, Luigi Sergio a cura di , *Information Warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Milano, FrancoAngeli editore, 2011.

dell'offensiva sarebbe da ricercare nella decisione del Governo estone di spostare (o meglio, rimuovere) dalla piazza centrale di Tallinn la statua del "Soldato di Bronzo", memoriale eretto a suo tempo in onore dei liberatori sovietici. Come conseguenza di questa mossa politica, l'intero sistema informatico estone – a partire da siti di banche, giornali, ministeri, fino anche al sito ufficiale del Parlamento – viene intasato e reso inutilizzabile da gruppi di *hacker* russi, attraverso una serie di attacchi *DDoS* che immobilizzarono di fatto il Paese per diverse ore.

Ciò che è accaduto in Estonia nell'aprile del 2007, è rilevante ai fini di questo studio per diversi aspetti. Innanzitutto i fatti estoni hanno reso evidente agli occhi della comunità internazionale quanto una società fortemente interconnessa alla rete – come lo sono quelle in cui viviamo – sia fortemente vulnerabile dinnanzi ad un attacco informatico anche non dotato di un livello di sofisticazione troppo elevato.

Secondariamente di poi, l'attacco subito dal Paese baltico, rappresenta probabilmente il primo esempio di *cyberwarfare* "politicamente motivato" ed in cui è evidente una responsabilità ed un coinvolgimento – anche se, in questo caso, soltanto a livello di appoggio logistico ed organizzativo – statale (per la precisione, la prima volta che si è parlato di azioni offensive cibernetiche "sponsorizzate" a livello statale, fu in occasione delle operazioni poi definite "*Titan Rain*", una serie di attacchi subiti dai computer di agenzie - governative e non – americane e provenienti dalla Cina[28]; in questo caso però, è più corretto parlare di *cyber espionage*, non rientrando dunque questa situazione nell'accezione di *cyberwarfare* adottata in questa ricerca). A questo proposito, basti pensare che il Governo estone – nonostante le ripetute smentite di rito da parte del Cremlino su un suo coinvolgimento – arrivò ad invocare l'applicazione dell'articolo V del Trattato della NATO, chiedendo dunque l'intervento militare degli alleati in difesa di un membro che, di fatto, stava subendo un attacco[29]. Ciò ovviamente non

[28] Cfr. Surhone, Lambert M., Timpledon, Miriam T., Marseken, Susan F. a cura di , *Titan Rain: Titan Rain, U.S. government, Corporate Espionage, Hacker computer security , SANS Institute, Lockheed Martin*, Betascript Publishing, 2010.

[29] Così recita l'articolo V del Trattato di Washington: "Le parti convengono che un attacco armato contro una o più di esse in Europa o nell'America settentrionale sarà considerato come un attacco diretto contro tutte le parti, e di conseguenza convengono che se un tale attacco si producesse, ciascuna di esse, nell'esercizio del diritto di legittima difesa, individuale o collettiva, riconosciuto dall'ari. 51 dello Statuto delle Nazioni Unite, assisterà la parte o le parti così attaccate intraprendendo immediatamente, individualmente e di concerto con le altre parti, l'azione che giudicherà necessaria, ivi compreso l'uso della forza armata, per ristabilire e mantenere la sicurezza nella regione dell'Atlantico settentrionale. Ogni attacco armato di questo genere e tutte le misure prese in conseguenza di esso saranno immediatamente portate a conoscenza del Consiglio di

avvenne, a causa della doppia difficoltà a dimostrare un coinvolgimento diretto della Russia (tanto più che da un'analisi approfondita del traffico "malevolo" di dati verso l'Estonia, risultava che gli attacchi provenivano dalla Russia come dal Canada, Brasile, Vietnam e persino Stati Uniti) e a giustificare un'eventuale azione dell'Alleanza Atlantica in risposta a qualcosa di così poco tangibile (e in parte anche sconosciuto all'opinione pubblica) come un attacco informatico; l'unica risposta da parte della NATO fu l'istituzione – proprio a Tallinn – del *Cooperative Cyber Defense Centre of Excellence (CCDCOE)*[30]. Risulterà evidente come la comunità internazionale "faccia fatica" a considerare questo tipo di attacchi come atti di guerra nel senso tradizionale del termine, stimolando in questo modo ulteriormente gli attori – statali e non – a privilegiare lo strumento cibernetico nel conseguimento di obiettivi che, se perseguiti con mezzi tradizionali, porterebbero ad una sicura condanna da parte della comunità internazionale stessa[31].

C'è poi un terzo elemento, di primaria importanza, che rende interessante l'osservazione dei fatti estoni, alla luce di quanto succederà poco più di un anno dopo in Georgia: la dinamica e le modalità dell'attacco. Come anticipato, si è trattato di attacchi *DDoS*, acronimo per *Distributed Denial of Service* (negazione diffusa di servizio). Gli attacchi *DDoS* sono tra i più difficili da contrastare, poiché sfruttando una debolezza intrinseca nel modo in cui funziona ed è strutturata la rete, in sostanza non c'è possibilità di evitarli. Un attacco *DoS* (togliendo dunque la D iniziale) è un attacco inviato da un singolo computer verso un *server* con lo scopo di sovraccaricarlo e negare quindi l'accesso agli utenti; per fare ciò è sufficiente bombardare il server con chiamate simili a quelle dei normali utenti, fino a rallentarlo od a bloccarlo completamente. Un esempio utile per comprendere questo meccanismo può essere quello del casello autostradale: è come se qualcuno inviasse deliberatamente al casello una flotta di automobili, creando una situazione di traffico mille volte superiore al normale; si formerebbero delle lunghe code, nelle quali – insieme alle automobili dell'attacco – verrebbero

Sicurezza. Queste misure termineranno allorché il Consiglio di Sicurezza avrà preso le misure necessarie per ristabilire e mantenere la pace e la sicurezza internazionali".

[30] Il sito del CCDCOE: https://ccdcoe.org

[31] Cfr. Lombardi, Francesco, "Cyber Warfare, quali regole…?", *Informazioni della Difesa* 5/2010, citato in, Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali (CSSII)*, febbraio 2014.

intrappolate anche quelle dei normali utenti[32]. Quando è in corso un attacco *DoS*, si riscontra una grande lentezza del sito, proprio perché il *server* sta cercando di rispondere a tutte le richieste che gli sono giunte. Ci sono però delle soluzioni per mettersi al riparo da questo tipo di attacco, ad esempio si può aumentare il numero dei *server* o – meglio ancora – utilizzare dei *software* che permettano di capire quando stiano arrivando troppe richieste sospette da un determinato indirizzo IP, consentendo di ignorarle. Le cose si fanno ben più complesse – e pressoché impossibili da gestire – quando si aggiunge la D iniziale e l'attacco diventa dunque *DDoS*, ovvero distribuito, diffuso.

Il principio è lo stesso del *DoS*, con la differenza che l'attacco viene lanciato contemporaneamente da un gran numero di computer; molti dei quali partecipano inconsapevolmente all'attacco, essendo stati infettati in passato e rispondendo ad una sorta di controllo remoto inserito dall'*hacker* a suo tempo (la rete mondiale che *l'hacker* si crea è definita *botnet* e ciò spiegherebbe come mai gli attacchi subiti dall'Estonia provenissero da computer di tutto il mondo e non soltanto dalla Russia). Aumentare il numero dei *server* diventa inutile viste le dimensioni dell'attacco e anche le tecniche di filtraggio precedentemente illustrate sono vane, proprio perché è impossibile distinguere quali siano gli indirizzi da bloccare od ignorare, provenendo le richieste da migliaia di computer sparsi per il mondo. Un attacco *DDoS* crea un'ondata di traffico di enorme intensità e per questo quasi impossibile da contrastare, gli attacchi all'Estonia lo avevano dimostrato e in Russia avrebbero saputo ricordarsene.

L'esempio estone – nonostante sia particolarmente rilevante ai fini di questo studio, per i motivi sopra elencati – è difficile da catalogare come un vero e proprio atto di guerra ed è forse più corretto parlare di attacco cibernetico versione *soft*, non fosse altro che per la sua temporaneità, per la modalità con cui è stato implementato e, soprattutto, per le sue conseguenze[33]. Non certo la stessa cosa si può dire per quello che Umberto Gori definisce il primo vero caso di *cyberwar* (non a caso per i

[32] Ho trovato questa esaustiva descrizione qui: http://www.mondoxbox.com/news/47983/attacchi_ddos_cosa_sono_e_perche_e_cosi_difficile_contrastarli.html.

[33] Cfr. Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali CSSII,* febbraio 2014.

fatti estoni si era parlato di *infowar*[34]), l'attacco cibernetico sferrato agli impianti nucleari iraniani con il virus *Stuxnet*[35].

Assecondando la volontà di Gerusalemme – che stava percependo come una minaccia sempre più diretta i continui progressi nucleari iraniani – a partire dal 2006 l'amministrazione Bush dà vita ad una serie di progetti mirati a bloccare o ritardare le conquiste scientifiche di Teheran. Il primo passo consiste nello sviluppo e nell'invio di un virus che raccolga informazioni sull'impianto nucleare iraniano di Natanz, per poi – nella seconda fase – crearne una fedele riproduzione. Nel 2008 un secondo virus – creato sulla base delle informazioni acquisite - viene testato nei laboratori americani, i risultati sono positivi e Bush decide quindi di autorizzare l'attacco; il virus viene introdotto nei sistemi di gestione informatici dei siti nucleari iraniani di Natanz e Busher attraverso una penna *USB*, provocando la distruzione di gran parte delle centrifughe[36].

Tornando al pensiero di Gori, ci sono una serie di fattori che nel caso di questo attacco ci permetterebbero di parlare di *cyberwar* in senso stretto. Il fatto che l'obiettivo dell'operazione fosse la distruzione di centrifughe nucleari in un (anzi due) sito nemico è già di per sé piuttosto rilevante; inoltre, essendo l'attacco andato a buon fine, il risultato è consistito in effetti e danni reali, concreti. Le difficoltà per l'organizzazione e la messa in atto di una tale operazione – oltre al grande dispendio economico ed al ruolo centrale giocato dai servizi di *intelligence* – parrebbero poi rendere manifesto il coinvolgimento dell'entità statale, questa volta in modo diretto[37].

Un caso abbastanza simile a quello appena osservato – anche solo per l'obiettivo perseguito – è l'operazione *Orchard* del settembre 2007. Per riuscire a bombardare un impianto nucleare in Siria senza essere intercettato e soprattutto senza lasciare prove evidenti di un suo coinvolgimento, l'esercito israeliano ha inviato – prima di procedere al bombardamento – un aereo senza pilota dotato di uno strumento informatico che permettesse di disturbare, emettere falsi segnali ed

[34] Vedi nota 27.

[35] Cfr. Gori, Umberto, "Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici", in Gori, Umberto e Germani, Luigi Sergio (a cura di), *Information Warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Milano, FrancoAngeli editore, 2011.

[36] Cfr. Martino, Luigi, "Implicazioni strategiche della guerra cibernetica", academia.edu.

[37] Cfr. Gori, Umberto, "Cyberspazio e relazioni internazionali: implicazioni geopolitiche e geostrategiche", in Gori, Umberto e Lisi, Serena (a cura di), *Information Warfare 2012. Armi cibernetiche e processo decisionale*, Milano, FrancoAngeli editore, 2013.

inserire false informazioni nella rete di difesa aerea siriana, facendo credere agli operatori del comando e controllo che non ci fossero penetrazioni nello spazio aereo siriano. In questo modo i caccia israeliani sono riusciti a penetrare indisturbati in territorio nemico, radendo poi al suolo l'intero impianto nucleare siriano[38].

Ciò che è accaduto in Georgia nell'agosto del 2008 – e che vedremo nel prossimo paragrafo - si potrebbe dire in qualche modo che riassume e dimostra tutto ciò di cui si è parlato finora, sia a livello teorico che di esempi concreti.

## Georgia, agosto 2008. "Before the Gunfire, Cyberattacks"[39]

Studiando il caso georgiano si osserva la dinamica "strettamente" *cyber* degli attacchi, sviluppata ed attuata in modo analogo a quanto accaduto in Estonia (prevalenza di attacchi *DDoS*), parallelamente ad una dimensione più concreta e mirante al raggiungimento di obiettivi reali, come nel caso degli altri esempi precedentemente osservati. Allo stesso modo, sarà interessante notare come nel contesto del conflitto russo-georgiano la dimensione cibernetica è stata utilizzata nel perseguimento di obiettivi strategici – come da tradizione per la *cyberwar*[40] - così come a livello tattico e per conseguire risultati durante le operazioni sul campo. Volendo osservare il ruolo della dimensione cibernetica ed i suoi risvolti nel quadro del conflitto, non ci si soffermerà troppo sulle dinamiche strettamente belliche e ancora meno sulle (lunghe) premesse della vigilia.

Brevemente, si può dire che già all'inizio dell'estate 2008, le avvisaglie di un conflitto imminente parevano lampanti. Mosca – come da tradizione – aveva iniziato a svolgere una serie di esercitazioni militari in diversi punti lungo il confine georgiano; basti pensare che a partire dalla metà di luglio vi erano stati trasferiti circa 8000 soldati che – non certo a caso – furono mantenuti anche una volta concluse le esercitazioni[41]. Una di queste esercitazioni prevedeva addirittura la simulazione di un attacco contro Ossezia del Sud ed Abkhazia (evidentemente da parte della

[38] Cfr. Martino, Luigi, "Implicazioni strategiche della guerra cibernetica", academia.edu.
[39] Markoff, John, "Before the Gunfire, Cyberattacks", *New York Times*, 12 agosto 2008.
[40] Vedi nota 24.
[41] Cfr. Berryman, John, "Russia, NATO Enlargemen, and "Regions of Privileged Interests"", in Kanet, Roger E. (a cura di), *Russian Foreign Policy in the XXI Century*, New York, Palgrave Macmillan, 2011.

Georgia), cui le forze russe avrebbero dovuto saper rispondere, proteggendo gli interessi di Mosca in quell'area (abitata quasi esclusivamente da russi). Nel corso di questa esercitazione, le forze russe ricevettero precise indicazioni circa la composizione ed i punti di forza e debolezza dell'esercito georgiano[42], altro segnale di non poco conto. Dunque - dopo settimane di tensione crescente e provocazioni reciproche – la sera del 7 agosto 2008 le truppe georgiane iniziano l'invasione della regione separatista dell'Ossezia del Sud – che era, come detto, la ragione del contendere insieme all'altra regione separatista, l'Abkhazia; entrambe erano spalleggiate da Mosca – culminata in un intenso bombardamento sulla capitale, Tskhinvali. La risposta russa non si fece ovviamente attendere e la soverchiante forza militare – in particolare a confronto del poco attrezzato esercito georgiano – mise fine alle ostilità in poche settimane. Era inoltre la prima volta che Mosca inviava le sue forze militari fuori confine dopo l'Afghanistan[43].

Il conflitto dunque non durò molto, non coinvolse un gran numero di forze militari e – all'apparenza – potrebbe sembrare uno dei numerosi micro-conflitti combattuti lungo le frontiere del *near abroad* russo, nello spazio post-sovietico. Ma se si osservano i fatti in modo più approfondito – in particolare alla luce dell'aspetto che qui ci interessa – si può certamente affermare che il conflitto russo-georgiano rappresenta un precedente storico di non poca rilevanza[44].

Si tratta infatti del primo caso di conflitto in cui un attacco (o più) condotto attraverso il dominio cibernetico è stato sincronizzato e coordinato con azioni belliche nei domini tradizionali (in questo caso, invasione via terra, blocco navale e bombardamento aereo). Si può dunque sostenere che la Russia ha condotto la sua invasione attraverso quattro fronti – tre tradizionali – il quarto dei quali è rappresentato dal *cyberspace*; ed è abbastanza improbabile pensare che il parallelo attacco attraverso il dominio cibernetico sia stato una coincidenza. Mentre carri armati e truppe varcavano il confine e mentre iniziavano i bombardamenti, i cittadini georgiani erano impossibilitati a consultare i

[42] Cfr. Cornell, Svante e Starr, Frederick, *The Guns of August 2008: Russia's War in Georgia*, New York, Central Asia Caucasus Institute, 2009.
[43] Cfr. Ziegler, Charles E., "Russia, Central Asia and the Caucasus after the Georgia Conflict", in Kanet, Roger E. (a cura di), *Russian Foreign Policy in the XXI Century*, New York, Palgrave Macmillan, 2011.
[44] Cfr. Hollis, David, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, Small Wars Foundation, gennaio 2011.

siti *web* che avrebbero potuto fornire informazioni ed istruzioni sulla condotta da tenere.

Come anticipato – contrariamente a quanto avvenuto durante il precedente estone – l'attacco cibernetico russo nei confronti della Georgia è stato realizzato parallelamente allo scontro "fisico", nei domini tradizionali, tra le forze militari russe e quelle georgiane. Ed anzi – più precisamente – si è potuto notare come tutte le numerose operazioni offensive cibernetiche russe fossero una sorta di indicatore di ciò che – a breve termine – sarebbe accaduto via terra (o aria).

Il fatto che questo sia stato il primo caso di attacco cibernetico coinciso con una "*shooting war*"[45], ci porta ad un'altra riflessione; un'operazione così complessa, richiede una preparazione strategica lunga, sicuramente antecedente al luglio 2008. Inoltre, il fatto stesso che – appunto – gli obiettivi colpiti dagli attacchi cibernetici fossero sempre coincidenti con gli obiettivi strategici del Governo e delle forze militari russe, deve far riflettere. E lo stesso discorso vale anche da un punto di vista strettamente geografico; siti e località ben precise venivano prese di mira e "bombardate ciberneticamente" subito prima che – nello stesso luogo – iniziassero le operazioni militari vere e proprie. Emblematico in questo senso è il caso di una della città più duramente colpite durante questo conflitto, Gori. Qualsiasi sito "ufficiale" in qualche modo connesso con la città, così come tutti i maggiori canali di informazione *online* della zona, vennero messi fuori uso poco prima che i bombardamenti e l'azione militare russa colpissero la città. Ma come è possibile che chi ha condotto gli attacchi attraverso il *cyberspace* sapesse che proprio in quella fase del conflitto ci si sarebbe concentrati su di una cittadina come Gori e non piuttosto – e volendo anche più logicamente – sulla capitale Tbilisi[46]?

È chiaro – per quanto allo stesso tempo pressoché indimostrabile – che non si tratta di coincidenze e che dietro a queste azioni di *cyberwar* non possono esserci semplicemente quelli che sono gli esecutori materiali degli attacchi, ovvero degli anonimi *hacker* russi. Ed è proprio l'ombra lunga dell'esercito, dell'*intelligence* e dunque del Cremlino stesso che ci permette di classificare gli eventi georgiani – molto più che quelli estoni - come un vero e proprio caso di *warfare tout court*, oltre al fatto che agli attacchi cibernetici si siano accompagnate operazioni militari "reali".

[45] Cfr. Markoff, John, "Before the Gunfire, Cyberattacks", *New York Times*, 12 agosto 2008.
[46] Cfr. Menn, Joseph, "Expert: CyberRattacks on Georgia websites tied to mob, Russian government", *Los Angeles Times*, 13 agosto 2008.

Anche riutilizzando la classificazione di Libicki[47], possiamo osservare come l'utilizzo del dominio cibernetico nel contesto del conflitto russo-georgiano, rappresenti perfettamente una delle sette forme in cui l'esperto studioso di guerra cibernetica divide la *Information Warfare*, ovvero quella che lui stesso definisce "*Command-and-Control Warfare*" (*C2W*): "è la strategia militare che mette in atto la *Information Warfare* sul campo di battaglia ed integra la distruzione fisica. L'obiettivo è decapitare la struttura di comando nemica, isolando il corpo delle forze armate"[48]. Il fine principale degli attacchi cibernetici russi non era infatti soltanto quello di rendere inutilizzabili ed inconsultabili i principali siti governativi e di informazione georgiani per generare una situazione di panico tra la popolazione, ma anche di creare delle problematiche (praticamente irrisolvibili) alla catena di comando e controllo – ed in generale ai sistemi di comunicazione – del nemico. Mettere in crisi in questo modo i sistemi di comunicazione georgiani doveva avere una doppia volenza, interna ed esterna. Dal punto di vista interno – oltre a creare un po' di sempre utile panico tra la popolazione civile – si rendevano difficoltose le comunicazioni anche a livello governativo e soprattutto militare, con i vertici che spesso si ritrovarono impossibilitati a comunicare gli ordini da mettere in atto sul campo. Ma c'è anche una rilevanza – all'apparenza meno evidente – dal punto di vista esterno e più precisamente nei confronti della comunità internazionale; gestendo il traffico internet dei principali siti e canali di comunicazione georgiani, agli *hacker* russi fu in qualche modo possibile manipolare – per un certo periodo di tempo - la rappresentazione del conflitto agli occhi della comunità internazionale, impedendo parallelamente alla Georgia di mostrare la "sua" versione dei fatti e/o invocare aiuto[49]. A questa situazione si riuscì ad ovviare (parzialmente) soltanto dopo alcuni giorni e – soprattutto – grazie ad un "variegato" supporto proveniente dall'estero. Furono inviati esperti di *cyber security* dall'Estonia stessa – dove si era fatto tesoro dell'esperienza del 2007 – per provare ad imbastire una qualche forma di difesa cibernetica, ma il fatto che gli attacchi fossero già partiti e pienamente in corso di svolgimento rese questa contromisura abbastanza vana. Ebbe invece miglior fortuna il tentativo di traferire – con l'intento di rendere almeno parzialmente di

[47] Vedi nota 14.
[48] Libicki, Martin C., *What is Information Warfare?*, Center for Advanced Command Concept and Technology, Institute for National Strategic Studies, National Defense University, Washington DC, agosto 1995.
[49] Cfr. Melikishvili, Alexander, "The Cyber Dimension of Russia's Attack on Georgia", *The Jamestown Foundation*, 12 settembre 2008.

nuovo fruibili ed operativi i principali canali di informazione – determinati siti internet a *server* situati in altri Paesi, nello specifico Stati Uniti, Estonia e Polonia[50]. In particolare, il sito ufficiale del Presidente georgiano Saakashvili fu ospitato da *server* di *Google* in California, il sito del Ministero della Difesa da una compagnia privata ad Atlanta, il sito del Ministero degli Esteri da *server* estoni, mentre il Presidente polacco mise a disposizione una finestra sul suo sito ufficiale da utilizzare per la diramazione degli annunci da parte del Governo georgiano[51].

Bisogna aggiungere che gli attacchi di tipo *DDoS* – per quanto prevalenti – non furono gli unici messi in atto. Furono anche utilizzate tecniche come "*SQL injection*" e "*cross-site scripting*" (XSS), che fondamentalmente perseguono lo stesso obiettivo di negare l'accesso ai siti presi di mira. In particolare la "*SQL injection*" è un metodo particolarmente sofisticato, che permette di conseguire il medesimo risultato di un attacco *DDoS*, ma senza la necessità di avere un gran numero di computer al servizio dell'*hacker*, consentendo dunque un'azione più diretta ed immediata[52]. Alcuni siti georgiani subirono addirittura il cosiddetto "*defacing*" – letteralmente, "deturpazione" – ovvero una vera e propria modifica di aspetto e contenuti del sito stesso. Diversi siti di informazione e governativi georgiani furono tempestati di propaganda filo-russa; particolarmente gettonata era un'immagine ritraente il Presidente georgiano Saakashvili che assumeva le sembianze di Hitler[53].

Vi sono molti elementi che rendono il coinvolgimento del Governo russo sempre meno "presunto" ed indiretto. Innanzitutto, studi approfonditi sul traffico internet durante i giorni più caldi del conflitto hanno dimostrato che diversi tra i principali attacchi cibernetici provenivano da *server* collegati ad alcune tra le più importanti compagnie russe nel ramo delle telecomunicazioni[54]; ciò renderebbe improbabile il solo coinvolgimento di semplici *hacker* autonomi e disorganizzati. Al contrario, l'azione degli *hacker* è parsa fin da subito fortemente coordinata e – potremmo dire – strutturata in modo gerarchico, quasi si trattasse di un ramo vero e proprio delle forze armate. Un ex *hacker*

[50] Cfr. Nazario, Jose, "Politically Motivated Denial of Service Attacks", *NATO Cooperative Cyber Defense Center of Excellence*, 2009.
[51] Cfr. Clarke, Richard A., Knake, Robert K., *Cyber War. The Next Threat to National Security and What to do About It*, New York, Harper Collins Publishers, 2010.
[52] Cfr. Krebs, Brian, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks", *The Washington Post*, 16 ottobre 2008.
[53] Cfr. Danchev, Dancho, "Coordinated Russia vs Georgia cyber attack in progress", *ZD Net*, 11 agosto 2008.
[54] Cfr. Markoff, John, "Before the Gunfire, Cyberattacks", *New York Times*, 12 agosto 2008.

russo avrebbe persino dichiarato che nel suo Paese - molto spesso – a chi viene accusato di *cyber crimes*, viene offerta la possibilità di evitare il carcere andando a lavorare per l'*intelligence* e – dunque – per il Cremlino[55]; *hacker* di questo tipo, sotto il controllo del Governo, sarebbero a quel punto liberi di "istruire" e guidare qualsiasi tipo di operazione, per esempio semplicemente intervenendo – sempre anonimamente – nei tanti forum di *hacker* e simili presenti in rete. In questo modo si creerebbe una sorta di *cyber* milizia – gli stessi protagonisti degli attacchi sia contro l'Estonia che contro la Georgia si sono definiti così[56] - composta da *hacker* e nazionalisti vari (o meglio ancora da *hacker* nazionalisti) all'occorrenza molto utile per il Governo, che dovrebbe soltanto limitarsi al fornimento di obiettivi ed istruzioni, mantenendosi inoltre al riparo da qualsiasi responsabilità – cosa avvenuta per i fatti estoni come per quelli georgiani – per quanto riguarda gli attacchi cibernetici. Internet è sinonimo di anonimato; la vera origine di un attacco cibernetico è difficile da determinare e soprattutto da dimostrare. Inoltre – come abbiamo visto – per un *hacker* sufficientemente esperto non è difficile reindirizzare il traffico internet a suo piacimento, magari verso *server* locati in Paesi del tutto estranei alla vicenda[57].

Tra gli attori principalmente coinvolti negli attacchi cibernetici contro la Georgia c'è una *cyber-gang* criminale con sede a San Pietroburgo, conosciuta come "*Russian Business Network*" (*RBN*)[58] e che già in passato si era resa protagonista di crimini "tipici" della rete come furti d'identità, pedopornografia ed estorsioni[59]. Soprattutto su internet si parla moltissimo di questa compagnia criminale, che però pare non abbia alcuna identità legale; è noto che la *RNB* vende i suoi servizi a terze parti ed il fatto che le autorità russe non siano mai concretamente intervenute per contrastare questa organizzazione, lascerebbe nuovamente pensare che il Governo russo possa avere "qualche collegamento" con questa *cyber-mafia*[60]. Il sito "*Stopgeorgia.ru*" – anche questo pesantemente coinvolto negli attacchi – si era reso protagonista di crimini quali la falsificazione di passaporti e carte di credito, ma anche

[55] Cfr. Krebs, Brian, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks", *The Washington Post*, 16 ottobre 2008.
[56] Cfr. Keizer, Gregg, "Russian hacker "militia" mobilizes to attack Georgia", *Computerworld*, 13 agosto 2008
[57] Cfr. Espiner, Tom, "Georgia accuses Russia of coordinated cyberattck", *C Net*, 11 agosto 2008.
[58] Cfr. Markoff, John, "Before the Gunfire, Cyberattacks", *New York Times*, 12 agosto 2008.
[59] Cfr. Krebs, Brian, "Shadowy Russian Firm Seen as Conduit for Cybercrime", *The Washington Post*, 13 ottobre 2007.
[60] Cfr. Wentworth, Travis, "You've Got Malice", *Newsweek. The Daily Beast*, 22 agosto 2008.

in questo caso le autorità si sono sempre dimostrate poco propense a condurre indagini serie. Inoltre queste organizzazioni hanno sempre mostrato una strana attitudine a concentrarsi su obiettivi non nazionali nella conduzione dei loro crimini informatici[61]. Tutti questi elementi – quali la mancanza di identità, il fatto di non essere perseguiti nonostante i numerosi crimini commessi e la volontà di non colpire obiettivi nazionali – non possono essere trascurati quando si cerca di indagare su di un possibile coinvolgimento russo a livello governativo. A partire dal crollo dell'Unione Sovietica – e con la ristrutturazione del vecchio *KGB* – ci sono diverse prove che dimostrerebbero un legame sempre più stretto tra il Governo russo ed organizzazioni criminali di varia natura; queste sarebbero una sorta di "estensione" del potere politico, da utilizzare in quelle aree ed in quei casi in cui il Governo non può agire "ufficialmente"[62].

Gli attacchi cibernetici perpetrati durante il conflitto russo-georgiano nell'agosto del 2008, oltre a destare sospetti per la precisione con cui sono avvenuti – intesa come precisione sia tempistica che in senso geografico – dovrebbero farlo anche se si osservano con attenzione le modalità – da un punto di vista strategico e militare – con cui sono stati condotti. Al momento di lanciare i primi attacchi, non ci si limitò infatti a colpire le principali linee di comunicazione nemiche ed altri obiettivi sensibili, ma ci si preoccupò parallelamente di rendere inefficace qualsiasi potenziale *cyber* risposta difensiva, bersagliando fin da subito – ad esempio – tutti i forum di *hacker* georgiani. Strategie come questa di attacco preventivo o come la dottrina del "Dominio Rapido" – "imporre un livello travolgente di *shock and awe* contro il nemico in un tempo sufficientemente ridotto per paralizzare la sua volontà di andare avanti, [...] per prendere il controllo della zona e bloccare o sovraccaricare la percezione e la comprensione degli eventi in modo tale che il nemico sarà incapace di resistere a livello tattico e strategico"[63] – sono state chiaramente utilizzate dai russi nel conflitto – in particolare quest'ultima, scegliendo di colpire inizialmente ed in modo consistente il nemico attraverso tutti i domini, compreso quello cibernetico e ad eccezione dello spazio extra-atmosferico – ed apparirà evidente come dietro la conduzione di operazioni di questo tipo non

[61] Cfr. Krebs, Brian, "Shadowy Russian Firm Seen as Conduit for Cybercrime", *The Washington Post*, 13 ottobre 2007.
[62] Cfr. Harding, Luke, "WikiLeaks cables: Russian government 'using mafia for its dirty work", *The Guardian*, 1 dicembre 2010.
[63] Ullman, Harlan K. e Wade, James P., *Shock and Awe: Achieving Rapid Dominance*, Institute for National Strategic Studies, National Defense University, Washington DC, 1996.

può che esserci l'esercito vero e proprio e non una semplice e patriottica "*cyber* milizia".

Precedentemente si è sostenuto che attraverso la *cyberwar* si punta a colpire il nemico prevalentemente a livello strategico, più che tattico[64]. Anche alla luce di quanto emerso da questo studio, tale affermazione si può considerare generalmente valida; allo stesso tempo però – avendo analizzato il caso georgiano – si è osservato quella che potremmo definire una commistione di operazioni cibernetiche, a livello strategico come anche a livello tattico. Se operazioni come quelle volte all'oscuramento dei siti governativi, a mettere in crisi la catena di comando e controllo, ad ostacolare il regolare flusso delle comunicazioni (sia interne che esterne) sono attacchi veri e propri al centro di gravità – in senso clausewitziano – del nemico[65], durante il conflitto russo-georgiano si è potuto assistere anche ad attacchi cibernetici mirati a conseguire vantaggi tattici nelle operazioni militari condotte attraverso i domini tradizionali[66].

[64] Vedi note 23 e 24.

[65] Cfr. Von Clausewitz, Carl, *Della guerra*, Milano, Mondadori, 1997.

[66] Cfr. Hollis, David, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, Small Wars Foundation, gennaio 2011.

## Conclusioni

Una potenza che voglia assicurarsi un ruolo di primo piano – o che voglia mantenerlo, preservando lo *status quo*, come nel caso degli Stati Uniti – nell'arena internazionale, dovrà concentrare tutti i suoi sforzi – a partire dal piano diplomatico, fino a quello militare – per ottenere il monopolio dell'accesso ai cosiddetti *global commons*[67], un aspetto strategicamente fondamentale. Il dominio cibernetico è uno di questi, per quanto a causa delle sue caratteristiche peculiari, non sia del tutto assimilabile ai *commons* tradizionali.

La rilevanza strategica del *cyberspace* è strettamente connessa al fatto che la maggior parte delle cosiddette "infrastrutture critiche" del sistema Paese – come dighe, centrali elettriche ed atomiche, gasdotti ed acquedotti, sistemi aerei, radar, ecc. – si basano su questo sistema di comando e controllo informatico, con tutti i rischi a ciò connessi. Un incidente – o un attacco – al *cyberspace*, potrebbe trasformarsi in un evento distruttivo capace di mettere in ginocchio uno Stato intero (o anche di più), a maggior ragione visto il livello di interdipendenza ed interconnessione raggiunta a livello globale grazie ai sistemi informatici. Maggiore interdipendenza, da un lato significa costante miglioramento dei servizi ed in particolare rapidità straordinaria di comunicazione, dall'altro porta però ad un aumento della vulnerabilità dinnanzi ad attacchi cibernetici, con inoltre possibilità di facile diffusione e conseguente effetto domino[68].

È senza dubbio necessario raggiungere un grado di maggiore regolamentazione delle dinamiche – anche a livello di conflitti - che regolano il *cyberspace*. Continua a non essere chiara – i casi estone e georgiano lo hanno dimostrato – la distinzione tra *cybercrime* e *cyberwar*; ma c'è una bella differenza tra un attacco cibernetico di origine criminale – avente però scopi esclusivamente lucrativi – ed uno

[67] Cfr. Denmark, Abrham M. e James Mulvenon, "Contested Commons: The Future of American Power in a Multipolar World", Center for a New American Security, Washington, DC, gennaio 2010, citato in Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali (CSSII)*, febbraio 2014.

[68] Cfr. Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali (CSSII)*, febbraio 2014.

che coinvolga in modo chiaro i vertici politici e militari di un Paese, rientrando dunque appieno nella categoria di *warfare*.

Se non si dovesse raggiungere una qualche forma di accordo su regole comuni, la stessa neutralità di attori potenzialmente estranei sarebbe messa a rischio. Il proprietario della *Tulip System* di Atlanta ha offerto il suo sostegno al Governo georgiano ospitando alcuni dei siti internet attaccati, ma lo ha fatto senza ricevere alcuna autorizzazione da parte del Governo degli Stati Uniti[69]. Se gli *hacker* russi avessero deciso di prendere di mira i *server* ospitanti, questa avrebbe potuto essere vissuta dagli Stati Uniti – così come dall'Estonia o dalla Polonia – come una minaccia alla propria sicurezza nazionale, mettendo appunto in dubbio la neutralità del Paese – di fatto estraneo a qualsiasi situazione tra Russia e Georgia – nel conflitto in corso.

Il caso georgiano ha ben dimostrato quanto potrà (e può, già oggi) essere rilevante lo strumento della *cyberwar* all'interno delle dinamiche belliche e come è destinato a perire sul campo di battaglia chi si farà trovare impreparato da questo punto di vista. Questa è una delle lezioni che gli Stati possono trarre dal conflitto qui analizzato, ma ce ne sono altre. L'utilizzo dello strumento cibernetico durante un conflitto ha dimostrato di essere molto più efficace se coordinato e sincronizzato con gli attacchi condotti attraverso gli altri domini, in una sorta di unione tra dimensione virtuale e fisica. Anche lo sviluppo di quella che si potrebbe definire un'*intelligence* "cibernetica" dovrebbe essere preso in considerazione dagli Stati che vogliano tutelarsi da questo punto di vista; monitorare i forum di *hacker* russi si sarebbe di certo rivelata una mossa utile alla causa georgiana, come ancora di più lo sarebbe stata la consapevolezza che le operazioni di terra ed aree sarebbero avvenute precisamente nelle località appena colpite dagli attacchi cibernetici.

E bisogna precisare che il conflitto russo-georgiano non è stata certo una dimostrazione completa delle potenzialità raggiungibili dallo strumento cibernetico durante un conflitto; le stesse capacità militari non sono state dispiegate appieno, limitandosi prevalentemente ad un utilizzo a livello di strategia. La *cyberwar* è diventata uno strumento necessario nella conduzione di un conflitto contemporaneo ed il ruolo avuto dalla "non ufficiale" *cyber* milizia russa lo ha dimostrato alla comunità internazionale. Bisogna riflettere su quanta altra rilevanza

[69] Cfr. Nazario, Jose, "Politically Motivated Denial of Service Attacks", *NATO Cooperative Cyber Defense Center of Excellence*, 2009.

potrà essere ancora acquisita dal *cyberspace* in futuro, quando presumibilmente si arriverà ad un utilizzo sempre crescente dello strumento, raggiungendo allo stesso tempo una ben maggiore sofisticazione.

## Bibliografia

### Monografie:


Berryman, John, "Russia, NATO Enlargemen, and "Regions of Privileged Interests"", in Kanet, Roger E. (a cura di), *Russian Foreign Policy in the XXI Century*, New York, Palgrave Macmillan, 2011.

Choucri, Nazli, *Cyberpolitics in International Relations*, Massachussetts, MIT Press Cambridge, 2012.

Clarke, Richard A., Knake, Robert K., *Cyber War. The Next Threat to National Security and What to do About It*, New York, Harper Collins Publishers, 2010.

Falgenhauer, Pavel, "After August 7: The Escalation of the Russia-Georgia War", in Cornell, Svante e Starr, Frederick, *The Guns of August 2008: Russia's War in Georgia*, New York, Central Asia-Caucasus Institute, 2009.

Goble, Paul A., "Defining Victory and Defeat: The Information War Between Russia and Georgia", in Cornell, Svante e Starr, Frederick, *The Guns of August 2008: Russia's War in Georgia*, New York, Central Asia-Caucasus Institute, 2009.

Gori, Umberto, "Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici", in Gori, Umberto e Germani, Luigi Sergio (a cura di), *Information Warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Milano, FrancoAngeli editore, 2011.

Gori, Umberto, "Cyberspazio e relazioni internazionali: implicazioni geopolitiche e geostrategiche", in Gori, Umberto e Lisi, Serena (a cura di), *Information Warfare 2012. Armi cibernetiche e processo decisionale*, Milano, FrancoAngeli editore, 2013.

Illarionov, Andrei, "The Russian Leadership's Preparation for War, 1999-2008", in Cornell, Svante e Starr, Frederick, *The Guns of August 2008: Russia's War in Georgia*, New York, Central Asia-Caucasus Institute, 2009.

Jean, Carlo e Tremonti, Giulio, *Guerre stellari: società ed economia nel cyberspazio*, Milano, FrancoAngeli editore, 2000. Jean, Carlo, *Geopolitica del XXI secolo*, Roma-Bari, GLF editori Laterza, 2004.

Libicki, Martin C., *What is Information Warfare?*, Center for Advanced Command Concept and Technology, Institute for National Strategic Studies, National Defense University, Washington DC, agosto 1995.

Nye, Joseph S., *The future of power*, New York, Public Affairs, 2011.

Posen, Barry R., "Command of the Common. The Military Foundation of U.S. Hegemony", *International Security*, estate 2003.

Scotto di Castelbianco, Paolo, "La cyber minaccia: attori, mutamenti e sfide al sistema Paese. Il ruolo della cyber intelligence", in Gori, Umberto e Germani, Luigi Sergio (a cura di), *Information Warfare 2011. La sfida della cyber intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano, FrancoAngeli editore, 2012.

Sherr, James, "The Implications of the Russia-Georgia War for European Security", in Cornell, Svante e Starr, Frederick, *The Guns of August 2008: Russia's War in Georgia*, New York, Central Asia-Caucasus Institute, 2009.

Skak, Mette, "Russia's New "Monroe Doctrine", in Kanet, Roger E. (a cura di), *Russian Foreign Policy in the XXI Century*, New York, Palgrave Macmillan, 2011.

Smith, David J., "The Saakashvili Administration's Reaction to Russian Policies Before the 2008 War", in Cornell, Svante e Starr, Frederick, *The Guns of August 2008: Russia's War in Georgia*, New York, Central Asia-Caucasus Institute, 2009.

Ullman, Harlan K. e Wade, James P., *Shock and Awe: Achieving Rapid Dominance*, Institute for National Strategic Studies, National Defense University, Washington DC, 1996.

Von Clausewitz, Carl, *Della guerra*, Milano, Mondadori, 1997.

Ziegler, Charles E., "Russia, Central Asia and the Caucasus after the Georgia Conflict", in Kanet, Roger E. (a cura di), *Russian Foreign Policy in the XXI Century*, New York, Palgrave Macmillan, 2011.

**Articoli:**

Borg, Scott, "Logica della guerra cibernetica", *Limes, Quaderno Speciale*, aprile 2012.

Danchev, Dancho, "Georgia President's web site under DDoS attack from Russian hackers", *ZD Net*, 22 luglio 2008.

Danchev, Dancho, "Coordinated Russia vs Georgia cyber attack in progress", *ZD Net*, 11 agosto 2008.

Espiner, Tom, "Georgia accuses Russia of coordinated cyberattck", *C-Net*, 11 agosto 2008.

Goodwin, Dan, "Georgian cyber attacks launched by Russian crime gangs", *The Register*, 18 agosto 2009.

Haddick, Robert, "This Week at War: Lessons from Cyberwar", *Foreign Policy*, 28 gennaio 2011.

Harding, Luke, "WikiLeaks cables: Russian government 'using mafia for its dirty work", *The Guardian*, 1 dicembre 2010.

Hollis, David, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, Small Wars Foundation, gennaio 2011.

Keizer, Gregg, "Russian hacker "militia" mobilizes to attack Georgia", *Computerworld*, 13 agosto 2008.

Kirk, Jeremy, "Estonia recovers from massive DDoS attack", *Computerworld*, 17 maggio 2007.

Krebs, Brian, "Shadowy Russian Firm Seen as Conduit for Cybercrime", *The Washington Post*, 13 ottobre 2007.

Krebs, Brian, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks", *The Washington Post*, 16 ottobre 2008.

Libicki, Martin C., "Cyberdeterrence and Cyberwarfare", Santa Monica (CA), RAND, 2009.

Markoff, John, "Before the Gunfire, Cyberattacks", *New York Times*, 12 agosto 2008.

Martino, Luigi, "La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", *Centro di Studi Strategici, Internazionali e Imprenditoriali (CSSII)*, febbraio 2014.

Melikishvili, Alexander, "The Cyber Dimension of Russia's Attack on Georgia", *The Jamestown Foundation*, 12 settembre 2008.

Menn, Joseph, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government", *Los Angeles Times*, 13 agosto 2008.

Nazario, Jose, "Politically Motivated Denial of Service Attacks", *NATO Cooperative Cyber Defense Center of Excellence*, 2009.

Swaine, Jon, “Georgia: Russia 'conducting cyber war'”, *The Telegraph*, 11 agosto 2008.

Wentworth, Travis, “You’ve Got Malice”, Newsweek. *The Daily Beast*, 22 agosto 2008.

## Sitografia

NMS-CO, novembre 2006: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

Relazione sulla politica dell’informazione per la sicurezza 2010: http://www.sicurezzanazionale.gov.it/sisr.nsf/wpcontent/uploads/2011/02/relazione-2010.pdf.

2001 Quadriennial Defense Review Report: http://www.comw.org/qdr/qdr2001.pdf.

The National Strategy to Secure Cyberspace: https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

The National Defense Strategy of the United States of America, marzo 2005: http://www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm.

Il testo del Trattato di Washington, istitutivo della NATO: http://www.nato.int/cps/en/natohq/official_texts_17120.htm.

Il sito del CCDCOE: https://ccdcoe.org.

Descrizione degli attacchi DDoS: http://www.mondoxbox.com/news/47983/attacchi-ddos-cosa-sono-e-perche-e-cosidifficile-contrastarli.html.

Martino, Luigi, “Implicazioni strategiche della guerra cibernetica”, academia.edu: https://www.academia.edu/6530095/Implicazioni_strategiche_della_guerra_cibernetica.

# 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