#03

ICT Security MAGAZINE

CYBER WARFARE

PREFAZIONE DI

LUIGI F. DE LEVERANO

Generale di Corpo d'Armata, già Consigliere Militare del Presidente del Consiglio dei Ministri

2023

QUADERNI DI CYBER INTELLIGENCE

WWW.ICTSECURITYMAGAZINE.COM

WWW.SOCINIT.ORG

CYBER CRIME CONFERENCE

11-12 MAGGIO 2023

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
11ª Edizione della Cyber Crime Conference

ICT Security MAGAZINE

ICT SECURITY MAGAZINE

1° rivista italiana di sicurezza informatica, attiva da oltre 20 anni, dedicata in forma esclusiva alla cyber security e alla business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, aziende e istituzioni pubbliche, per la diffusione degli elementi conoscitivi legati a tutti gli aspetti della information security.

SOCIETÀ ITALIANA DI INTELLIGENCE

SOCINT è un'associazione scientifica senza fini di lucro, il cui obiettivo è quello di promuovere la cultura e lo studio dell'intelligence in Italia.

QUADERNI DI CYBER INTELLIGENCE

La presente collana, frutto della collaborazione tra ICT Security Magazine e la Società Italiana di Intelligence (SOCINT), inaugura una serie di contenuti volti ad arricchire e approfondire il dibattito scientifico sulla *Cyber Intelligence*.

Indice

PREFAZIONE

Mentre ampie parti della società si interrogavano sul fenomeno Covid-19 e sulle conseguenze scaturite dalla pandemia, esplodeva il conflitto tra Russia e Ucraina. Al momento il primo e più esteso confronto militare dell'era "cyber", sviluppato sia con metodologie tradizionali che moderne e con il corollario evidente di un'incrementata intensità, mai registrata prima, di operazioni in tale nuovo dominio operativo.

L'emergenza sanitaria ci ha proiettato in un mondo ove l'ambiente cibernetico e le risorse digitali sono divenute spesso fulcro della sopravvivenza di Enti/aziende/imprese e fattore di continuità di azione per le istituzioni pubbliche. Se da un lato si è scoperto di poter fruire di servizi che in precedenza erano riservati solo a pochi, dall'altro sono emerse nuove possibilità sulle quali si è polarizzato anche il mondo del crimine informatico. Evidenze tutte che sottolineano come la digitalizzazione e la pervasività dell'ambiente cibernetico ci espongano a nuove tipologie di minaccia.

Con tecniche simili a quelle impiegate dal crimine informatico, nei mesi antecedenti l'inizio delle ostilità tra Russia e Ucraina, gruppi cyber "*State sponsored*" riconducibili (con molta probabilità) alla Fede-

razione Russa hanno creato le condizioni tese all'avvio della cosiddetta Operazione militare speciale, attraverso l'impiego di *malware* distruttivi e attacchi *Distributed Denial of Service* (DDoS) contro obiettivi governativi, ICT e infrastrutture critiche.

Il 24 febbraio 2022, allo scoppio delle ostilità, le azioni nel dominio cibernetico e le operazioni in quelli convenzionali da parte della Federazione Russa hanno perseguito per alcune settimane i medesimi obiettivi, evidenziando la necessità di precise misure di coordinamento. Successivamente tale coordinamento è andato decrescendo, lasciando in larga misura campo all'azione dei collettivi "*hacktivisti*", che hanno agito quale "forza ausiliaria"dei reparti regolari, svolgendo principalmente azioni di DDoS e di "*Hack&Leak*", il cui impatto è stato sostanzialmente reputazionale. Contestualmente è stato dato corso ad azioni di "*information warfare*" volte ad alterare la percezione oggettiva del conflitto. Per non parlare della strategia comunicativa che ha manipolato le menti. L'Ucraina, dal canto suo, ha beneficiato di un rinnovato ecosistema digitale resiliente, nonché di un supporto senza precedenti da parte delle aziende e dei Governi con le capacità cyber più avanzate del mondo. Il risultato finale, tuttavia, è che fino ad ora il temuto "*cyber-doom*" non si è verificato: gli attacchi perpetrati nel dominio cibernetico non hanno avuto effetti in grado di stabilire l'esito del conflitto e le ragioni di ciò sono ancora oggetto di analisi tra gli esperti di settore. Questa guerra ha confermato la trasversalità delle operazioni cyber in un contesto multi-dominio, condotte da gruppi "*State-sponsored*" e dalla comunità informatica globalizzata, i cui attacchi sono stati indirizzati verso infrastrutture critiche, taluni sistemi ad uso militare, impianti e apparati di telecomunicazione e, in particolare, verso tutto ciò che in qualche modo è riconducibile all'apparato governativo nemico.

In tale quadro e sulla base di quanto osservato sino ad oggi, emerge come sia necessario che la Difesa assicuri la libertà di manovra del proprio strumento militare nell'ambito del dominio cyber e concorra, con le Organizzazioni nazionali e internazionali, alla prevenzione e al contrasto delle sempre più insidiose minacce cibernetiche. Ciò potrà essere conseguito con l'incremento delle attuali capacità di condurre "*Cyber Operations*" e attraverso la disponibilità di sistemi tecnologicamente evoluti, dando peso a un pragmatico dialo-

go con il mondo accademico e industriale, al fine di stimolare sinergie e azioni condivise.

Se l'elemento tecnologico sarà quindi l'elemento caratterizzante in tali scenari, e le cosiddette "*Disruptive Technologies*" avranno il ruolo di moltiplicatori di potenza, appare altresì essenziale preservare un approccio che persegua la centralità dell'uomo evoluto nel campo e che sia orientato a una sempre più spiccata valorizzazione del capitale umano posseduto.

Gen. C.A. **Luigi Francesco De Leverano**, *già Consigliere Militare del Presidente del Consiglio dei Ministri*

BIOGRAFIA

Luigi Francesco De Leverano

Il Generale di Corpo d'Armata Luigi Francesco De Leverano, nato a Lecce il 25 maggio 1958, si è arruolato nell'Esercito nel 1976 frequentando il 158° corso presso l'Accademia Militare di Modena e la Scuola di Applicazione di Torino (1976-1980).

Al termine del ciclo di studi (1980) è stato trasferito presso il Battaglione "Leonessa" di Civitavecchia ove ha svolto, nel grado di Tenente, le funzioni di Comandante di plotone, nel grado di Capitano quelle di Comandante di compagnia e nel grado di Tenente Colonnello quelle di Comandante di battaglione.

Ha svolto incarichi di staff presso l'Ispettorato delle Trasmissioni, quale Ufficiale Addetto e Capo della Sezione Ordinamento e Regolamenti; presso lo Stato Maggiore dell'Esercito di Addetto alla 1a Sezione e Capo della 1a Sezione dell'Ufficio RESTAV; Capo Sezione dell'Ufficio Affari Giuridici; Capo Ufficio Reclutamento, Stato e Avanzamento e quello di Capo Ufficio Reclutamento (SME-RAGEP).
Nel grado di Colonnello, ha espletato l'incarico di Comandante del 235° RAV "Piceno", Ente scolastico che per primo ha accolto le Volontarie in ferma breve.
Nel grado di Generale di Brigata, dopo aver espletato l'incarico di Vice Comandante del Contingente Italiano in Iraq, ha ricoperto l'incarico di Comandante della Brigata meccanizzata "Sassari".

Ha svolto l'incarico di Vice Capo di Gabinetto del Ministro della Difesa e Capo di Gabinetto in s.v.; nel grado di Generale di Divisione ha espletato l'incarico di Capo Ufficio Generale del Capo di Stato Maggiore della Difesa.

Nel grado di Generale di Corpo d'Armata è stato Comandante del 2° Comando delle Forze Operative di Difesa in San Giorgio a Cremano, di Comandante delle Forze di Difesa Interregionale Sud in Napoli, di Comandante del Comando Forze Operative Sud, di Comandante Logistico dell'Esercito e di Sottocapo di Stato Maggiore della Difesa.

Dal 27 aprile 2021 al 30 novembre 2022 ha rivestito l'incarico di Consigliere Militare del Presidente del Consiglio dei Ministri e, in tale

veste, ha svolto anche l'incarico di Segretario del Comitato interministeriale per le politiche relative allo spazio e all'aerospazio.

Durante l'espletamento del servizio ha svolto anche altri incarichi, in qualità di: Membro del Collegio decisionale per la valutazione del personale da inserire nelle Forze di Completamento - Riserva Selezionata; Tutor per il dottorato di ricerca in Scienze strategiche presso l'Università di Torino; Membro della Commissione di verifica amministrativo-contabile costituita presso il Comitato Centrale della C.R.I.; Membro del Tavolo Tecnico per il raccordo e il coordinamento per l'attuazione delle disposizioni in materia di vittime del dovere a causa di azioni criminose, nonché dei loro familiari superstiti istituito con DCPM n.22/2008; Membro del Gruppo di Lavoro per la revisione delle leggi penali militari di pace e di guerra; Membro della Commissione governativa per l'attuazione delle disposizioni dell'Accordo tra Italia e Santa Sede 18 febbraio 1984, ratificato con la legge 25 marzo 1985, n.121; Ufficiale di progetto per la razionalizzazione/armonizzazione/implementazione degli spazi disponibili nella "piazza" di Napoli (con particolare riferimento a "Palazzo Salerno" e al comprensorio costituito dalle Caserme "Calò", "Minucci", "Marselli" e Stadio "Albricci".

Ha svolto docenze presso l'Università degli Studi di Firenze riguardanti le donne nelle F.A.; l'Università degli Studi "Tor Vergata" riguardanti "Organizzazione e compiti delle Forze Armate" nell'ambito del Corso di Specializzazione Universitaria in "Giornalismo per inviati in aree di crisi" e la Libera Università Maria SS. Assunta riguardanti "Le missioni internazionali delle Forze Armate – inserimento del personale femminile: i primi dieci anni".

Ha collaborato con la rivista "Specchio Economico" e pubblicato articoli sulla Rivista Militare: "Il Riallineamento è una realtà", "... La chiamano mini naja", "Ha dieci anni e non li dimostra"; Informazioni Difesa: "La specificità della condizione militare", "La formula del giuramento", "3P: Professionalità, Professionalizzazione, Professionisti" e "Specificità: vantaggio o svantaggio?", "In nome del Comitato dei Capi".

Ha svolto i seguenti Corsi: Sessione informativa per Ufficiali di guerra elettronica; 23° Corso per Ufficiali "I' di btg/gr.; 8° Corso di lingua inglese per corrispondenza; 115° Corso di Stato Maggiore; 115° Corso Superiore di Stato Maggiore; NATO Joint Service Course for EW Planning and Analysis in Exercise; XXXVI^ Sessione della Scuola Italiana Orga-

nismi Internazionali; Master in Studi Europei presso l'Istituto "Alcide De Gasperi"; Corso di perfezionamento in giornalismo per inviati in aree di crisi "M. Cutuli".

Ha conseguito la Laurea in Scienze strategiche, con relativo Master, presso l'Università degli Studi di Torino nonché in Scienze politiche presso l'Università degli Studi di Trieste.

Ha ricevuto la Cittadinanza Onoraria dall'Amministrazione Comunale di San Giorgio a Cremano.

Parla inglese e spagnolo e conosce il francese.

Il Generale di Corpo d'Armata De Leverano è insignito delle seguenti decorazioni:

- Grande Ufficiale dell'Ordine al Merito della Repubblica;
- Medaglia Mauriziana al merito di dieci lustri di carriera militare;
- Medaglia d'Oro al merito della Croce Rossa Italiana;
- Medaglia di Bronzo al merito della Croce Rossa Italiana;
- Medaglia d'Oro al merito di lungo comando;
- Croce d'Oro con stelletta per anzianità di servizio;
- Croce commemorativa per le missioni di mantenimento della pace;
- Croce commemorativa per soccorso umanitario a popolazioni al di fuori del territorio nazionale (Antica Babilonia/X in Iraq);
- Medaglia di Bronzo commemorativa per le operazioni di soccorso alle popolazioni colpite dal sisma del 1980 (Campania - Basilicata);
- Croce Commemorativa per le operazioni di salvaguardia e delle libere istituzioni e di mantenimento dell'ordine pubblico "Strade Sicure";
- Medaglia commemorativa Nato – Bosnia Herzegovina;
- Decorazione d'Onore Interforze dello Stato Maggiore della Difesa;
- Croce di Grande Ufficiale con Spade al Merito Melitense del Sovrano Militare Ordine di Malta;
- Cavaliere dell'Ordine di San Silvestro Papa;
- Cavaliere di Gran Croce di Merito del Sacro Militare Ordine Costantiniano di San Giorgio;
- Ufficiale dell'Ordine Nazionale al Merito della Repubblica Francese;
- Distintivo d'Onore della Federazione Italiana Scherma.

Il Generale De Leverano è coniugato con la Signora Flavia Bottioni ed ha un figlio di nome Adriano. Riveste l'attuale grado dal 1° luglio 2015.

White Paper

LA DIGITAL FORENSICS NEL PROCESSO PENALE

Download gratuito su www.ictsecuritymagazine.com

INTRODUZIONE

Siamo ormai giunti alla terza edizione del nostro quaderno tematico.

Questa volta la Commissione *Cyber Threat Intelligence* e *Cyber Warfare* (di seguito Commissione), parte integrante della SOCINT (Società Italiana di Intelligence), ha voluto affrontare il tema relativo all'utilizzo delle tecnologie di *cyber intelligence* nel contesto della guerra Russia-Ucraina, oggetto di grande interesse pubblico a livello sia nazionale sia internazionale.

L'approccio utilizzato mantiene una natura multidisciplinare, cercando di affrontare il tema nella sua complessità da tutti i punti di vista: giuridico, geopolitico, tecnico – con l'utilizzo dell'OSINT e della *Cyber Threat intelligence* – e infine tecnologico, con l'utilizzo di tecnologie cyber utili alla gestione/prevenzione del conflitto. Il tutto sempre con l'obiettivo di comprendere le dinamiche, le sfide, i rischi e le conseguenze dell'uso di alcuni strumenti e metodologie cyber in caso di *Cyber War*.

Prima di intraprendere una lettura più approfondita del quaderno, vale forse la pena analizzare come il dominio cyber abbia contribuito a modificare gli andamenti dell'attuale conflitto in termini di "costi/benefici".

Albert Einstein diceva: «Y*ou cannot simultaneously prevent and prepare for war. The very prevention of war requires more faith, courage, and resolution than are needed to prepare for war. We must all do our share, that we may be equal to the task of peace*».

Einstein sosteneva che prevenire una guerra richieda più fede e coraggio che prepararla, perché è sicuramente più complesso cercare di capire cosa sta accadendo nello scenario globale e come le informazioni devono essere raccolte, analizzate e condivise al fine di dare la giusta indicazione al decisore politico.

Nell'era moderna – e in particolare negli ultimi 30 anni – possiamo sostenere che la nostra capacità di "*information intelligence*" sia aumentata a dismisura; ma contemporaneamente è aumentata anche la difficoltà di comprendere quali tra queste informazioni siano corrette o false.

Il tema si è quindi spostato sulla complessità da gestire: ai primi quattro domini (terrestre, marittimo, aereo, spaziale) si è unito il quinto dominio (cyber), creando un'ulteriore difficoltà a livello tattico/operativo al comparto militare e di *Intelligence*.

Possiamo scomporre le difficoltà a livello tattico/operativo in due variabili principali che influenzano l'utilità delle tecnologie informatiche in guerra: la **tempistica** e la **complessità operativa** delle operazioni informatiche.

La **tempistica** si riferisce a domande su quando e per quanto tempo occorre impegnarsi in operazioni informatiche per massimizzarne gli effetti, mentre la **complessità operativa** è la disponibilità dell'*intelligence* necessaria per ottenere l'accesso a qualsiasi obiettivo difficile da colpire, in particolare quelli militari[1].

Metcalf e **Barber** (2014) sostenevano che la componente cyber è di fatto una componente essenziale a livello tattico in caso di *Cyber War*. «*Cyber activities on the tactical level take place - in the context of a traditional kinetic battlefield, where authorization, deconfliction, and control for the specific operation is at battalion level or lower*».

[1] Matthias Schulze, Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations - 2020 12th International Conference on Cyber Conflict

La storia, inoltre, ci insegna che in caso di mancanza di informazioni affidabili sugli obiettivi le operazioni informatiche diventano sempre più rischiose e meno fattibili. La raccolta di informazioni e la ricognizione della rete comportano un processo spesso dispendioso in termini di tempo, soprattutto se i target sono obiettivi altamente sicuri e isolati, dove in alcuni casi è richiesta l'intelligenza umana. Anche le grandi forze informatiche non possono prepararsi contro qualsiasi avversario immaginabile, soprattutto considerando attori non statali e criminali informatici sui quali spesso esiste poca "*intelligence*".

In conclusione, possiamo affermare che l'elemento tecnologico, inteso come *Cyber Intelligence* in un contesto di *Cyber War*, ha di certo aiutato i comparti della Difesa e dell'*Intelligence* nella previsione e prevenzione del conflitto; ma non è stato un elemento decisivo nella creazione e definizione di un modello di pace mondiale, aspetto che rimane soltanto all'uomo risolvere.

Albert Einstein: «*Science in itself could have no direct influence in building the international organization that was necessary if world chaos were to be avoided; man's determination alone could solve that problem* ".

Mattia Siciliano, *Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare*

BIOGRAFIA

Mattia Siciliano

L'ing. Siciliano ha oltre 15 anni di esperienza in *Cyber Security* e *Cyber Intelligence*. Attualmente è *Business Director* per una società internazionale con sede negli Emirati Arabi Uniti e docente presso le Università "Luiss Guido Carli" di Roma e "Federico II" di Napoli. In precedenza, partner e co-fondatore di DeepCyber, una società boutique focalizzata sulla *Cyber Threat Intelligence* e manager in diverse società di consulenza come EY e KPMG. Docente all'Università degli Studi di Napoli Federico II. Consulente per Ministero della Difesa (Innova Difesa), agenzie di *intelligence* e forze dell'ordine. Presidente della Commissione di Studio in *Cyber Threat Intelligence e Cyber Warfare* della Società Italiana di Intelligence.

Russia-Ucraina: il contributo del dominio cyber al conflitto.

La guerra in Ucraina si protrae dal 24 febbraio 2022: quasi un anno di conflitto in seno all'Europa che molti, in quest'epoca moderna, non credevano possibile.
Proprio il contesto moderno ha fatto subito associare allo scontro la possibilità di vedere utilizzate minacce che negli anni recenti hanno preso sempre più piede, quelle legate al mondo cyber.

Le tensioni presenti tra Mosca e Kiev si erano concretizzate già in passato anche in alcune operazioni cibernetiche, come l'attacco alla rete elettrica ucraina del 2015[1], contribuendo a creare l'idea di una guerra combattuta sul piano tanto militare quanto digitale.
La realtà, però, è stata ben diversa dalle aspettative: il temuto *cyber-doom* non si è verificato e gli attacchi perpetrati non hanno avuto effetti in grado di stabilire l'esito dello scontro.

Nelle settimane precedenti lo scoppio ufficiale del conflitto si sono verificati diversi episodi di attacchi: Microsoft ha individuato il 13 gennaio un malware chiamato WhisperGate[2], che aveva come target diverse organizzazioni governative, no-profit e IT ucraine. Si trattava di un malware distruttivo, che appariva come un *ransomware* chiedendo un riscatto ma che in realtà aveva l'obiettivo di rendere inutilizzabile il sistema-vittima.
Whispergate e la sua successiva versione perfezionata, HermeticWiper, erano gli attacchi con più potenziale distruttivo tra quelli identificati ma che - per quanto noto - non hanno avuto un impatto davvero significativo per le sorti dello scontro. Se fossero stati gli attacchi con cui la parte russa puntava a incapacitare le infrastrutture ucraine, si sono allora rivelati poco efficaci e hanno avuto una concentrazione nei primi step dell'invasione, per poi lasciare il passo al contesto cinetico.

La maggioranza degli attacchi rilevati prima dell'invasione e nelle settimane subito successive sono stati invece di tipo DDoS, *defacement* e furto di informazioni, quest'ultimo volto principalmente all'ottenimento di informazioni su cui elaborare *fake news* e propaganda o come supporto alle attività di *intelligence*. Sul piano dell'*intelligence* vale la pena menzionare le intercettazioni, come quelle effettuate verso i soldati russi[3]. Queste sono poi state utilizzate a fine propagandistico visti i contenuti, almeno in parte e per quanto noto, ma fanno intuire come l'*intelligence* sia in campo e ci siano sicuramente attività meno palesi, come potenziali intercettazioni di personalità di spicco, ma di indubbia utilità.
Questo tipo di operazioni sono state *non-disruptive* perché non hanno causato impedimenti permanenti o di lungo periodo e hanno principalmen-

[1] https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

[2] www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations.

[3] nytimes.com/interactive/2022/09/28/world/europe/russian-soldiers-phone-calls-ukraine.html.

te avuto invece lo scopo di manipolare l'opinione pubblica e generare in essa timore, contribuendo ai tentativi russi di influenzare le decisioni occidentali a proprio vantaggio.

Un altro fattore che ha portato la minaccia cyber sul piano propagandistico è stata la presa di posizione di gruppi legati al *cybercrime*, come Conti, che si sono schierati a favore di Mosca[4], minacciando ritorsioni verso le aziende degli Stati occidentali che avessero compiuto qualsiasi tipo di attacco verso zone del mondo a lingua russa.

Sebbene l'uso della tecnologia abbia certamente giocato un ruolo all'interno della guerra, non si può dire che ne sia stato l'elemento centrale. Si è vista una presenza della componente cyber principalmente all'inizio del conflitto; e con una declinazione più che altro psicologica. Lo scontro è poi proseguito sul piano militare tradizionale, senza che si siano verificati sabotaggi su vasta scala o attacchi verso infrastrutture critiche (come acquedotti, centrali elettriche, reti satellitari) con impatti considerevoli per l'andamento della guerra.
In questo specifico caso quindi non si può dire che sia in atto un vero e proprio scenario di *cyber warfare*, ma forse un più generico *information warfare*. La differenza sostanziale è che con *cyber warfare* si indicano forme di conflitto i cui attacchi sono rivolti a computer, *software* e/o sistemi di controllo, mentre con *information warfare* si intende l'utilizzo e la gestione dell'informazione per ottenere un vantaggio. Quindi le attività comprese possono andare dall'ottenimento di informazioni alla propaganda, diffusione di *fake news* e manipolazione. Vale la pena però provare a chiedersi se ci sarebbero potuti essere veri e propri cyber attacchi che avrebbero potuto dare un vantaggio concreto e più incisivo, soprattutto dal punto di vista dell'invasore.

Gli attacchi informatici sono abbastanza lontani dalla narrativa cinematografica che a volte li rappresenta. Necessitano di preparazione, partendo dalla raccolta informativa riguardante i sistemi bersaglio, continuando con l'individuazione di possibili punti di ingresso ed eventualmente con lo sviluppo *ad hoc* di *malware*. Prendendo come esempio forse il più famoso *malware* a scopo di sabotaggio, Stuxnet, che aveva lo scopo di fermare le attività iraniane di arricchimento di uranio, si può notare come alcune evidenze portino a supporre che il *malware*, individuato a inizio 2010, possa essere stato scritto a cominciare dal 2005[5].

L'assenza di un attacco altamente impattante potrebbe quindi essere dovuta a una mancata preparazione, causata dalla relativa rapidità della decisione di invadere - che quindi avrebbe reso impossibile il processo descritto sopra - o, comunque, dall'impossibilità di trovare una soluzione tecnica nel tempo concesso.

A questo proposito, una interessante ricerca che ha preso in oggetto proprio le tensioni russo-ucraine dal 2014 pone queste difficoltà sotto la luce di quello che viene chiamato "*subvertive trilemma*[6]" . Un *cyber attack* potenzialmente importante

[4] https://www.cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure.

[5] https://docs.broadcom.com/doc/stuxnet-missing-link-13-en.

[6] https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall.

per un conflitto si basa su segretezza ed *exploiting* di un sistema, in quanto sono le due condizioni che consentono di ottenere un risultato significativo. Inoltre, l'attacco è visto in funzione di tre variabili - velocità, intensità e controllo - le quali sono correlate negativamente: un guadagno in una di esse corrisponde a una perdita sulle altre due. Un attacco ad alto impatto, per esempio, non potrà quindi essere molto veloce, od ottenere un grande controllo sui sistemi e sugli effetti generati tramite essi. Esaminando le operazioni cyber sotto questa lente, è facile intuire che le immagini evocate di attacchi fulminei che devastano una infrastruttura critica difficilmente possono concretizzarsi nella realtà.

Una terza ipotesi per l'assenza di attacchi cyber decisivi per lo scontro può essere la mancata capacità di coordinamento tra corpi militari e unità informatiche. Un'azione concertata tra i due avrebbe potuto portare idealmente, per esempio, a una invasione coordinata con lo *shutdown* delle infrastrutture di comunicazione nemiche.
I motivi per cui questa sincronizzazione non si è verificata possono essere solo supposizioni, che vanno dall'errore umano al voler cambiare i piani a seguito delle segnalazioni dell'*intelligence* americana riguardo i cyber attacchi russi, rendendo così le loro previsioni non reali, ma pagando in termini di efficacia.

Per i motivi e le ipotesi appena visti è difficile immaginare una guerra, intesa in senso tradizionale, che che venga fortemente condizionata dal piano cyber.
Il cyber ha comunque un grande potenziale, che può esprimersi al meglio nel giusto contesto. Ipotizziamo di togliere una delle tre variabili richiamate in precedenza: velocità, intensità e controllo. Togliendo nello specifico la velocità, si ha uno scenario in cui il *cyber attack* non deve svolgere il suo compito in concomitanza di qualche altro evento limitato nel tempo, o in un orizzonte temporale molto limitato. In questa casistica il threat actor ha il tempo per studiare un attacco che punti su una delle altre due variabili, che sia quindi molto intenso o su cui avere un ottimo controllo.
Un contesto diverso da una guerra e più adeguato alle caratteristiche dello strumento. Una zona grigia in cui due entità non sono in guerra dichiarata ma hanno motivazioni e scopi che portano a utilizzare attacchi cyber per logorare la resistenza dell'altra parte, per minarne la salute economica e il normale funzionamento delle infrastrutture, in una sorta di nuova guerra permanente a bassa intensità.

In conclusione, sicuramente in questo conflitto il cyber ha comunque avuto un ruolo forte; ma soprattutto sul fronte mediatico, e con una funzione di pressione psicologica. Il campo di battaglia di una tradizionale guerra militare in corso, però, non è forse l'ecosistema che meglio si sposa con le caratteristiche delle operazioni cyber, che rendono invece al meglio senza una finestra temporale ristretta e quindi con la possibilità di infliggere continui colpi alla salute del nemico, in un logoramento strategico sul lungo periodo. Questa riflessione vuole portare verso un disaccoppiamento tra guerra e *cyber warfare*, al fine di inquadrare quest'ultimo nel giusto contesto.

Andrea Leoni, *Cyber Security Manager, Segretario Commissione Studi Cyber Threat Intelligence & Cyber Warfare di SOCINT*

BIOGRAFIA

Andrea Leoni

Cyber security manager presso una società multinazionale nel settore del *credit and business information*, è specializzato in governance e ambito GRC, con esperienza pluriennale di *security advisory* verso realtà nazionali e internazionali. Già ricercatore di *intelligence* presso il Laboratorio di Intelligence dell'Università della Calabria, presso cui ha conseguito un Master di II livello in *Intelligence*, si è occupato anche di politica e geopolitica e del loro rapporto col dominio cyber.

Attualmente, presso la Società Italiana di Intelligence, è Segretario della Commissione Studi *Cyber Threat Intelligence & Cyber Warfare*.

Gli effetti dell'embargo tecnologico sulle aziende occidentali con uffici e stabilimenti in Russia.

Come ben noto a tutti, prima della guerra russo-ucraina la Russia era considerata una nazione molto redditizia e promettente per molte aziende occidentali. Solo l'Italia aveva ben 480 aziende con stabilimenti e rappresentanze in territorio russo; e ad aprile 2022 quasi il 70% di esse ha deciso di rimanere nonostante l'*escalation* del conflitto[1].

Oltre alle questioni di natura etica, i primi problemi emersi sono stati quelli logistici, in quanto tutte le merci di provenienza e con destinazione la Russia sono state fermate dai governi che hanno aderito alle sanzioni, bloccando in buona sostanza ogni possibilità di generare denaro con i beni prodotti e sviluppati in loco.

Sebbene questo problema possa sembrare uno dei più impattanti, non è il solo che ha dato un grande scossone alle nostre aziende. L'integrità di un'azienda si realizza anche mediante la conservazione dei propri processi, che oggi sono al 99% informatizzati, ovvero transitano sui sistemi informatici normalmente ospitati presso *data center* dei paesi di origine; questi possono essere in spazi cloud privati o pubblici, ma sempre e comunque di proprietà di aziende del comparto occidentale.

Come noto, la quasi totalità delle tecnologie per la sicurezza informatica e cibernetica sono di produzione statunitense, mentre poche altre di produzione israeliana, francese e di qualche altro paese aderente alla NATO.

La Casa Bianca ha dato ordine all'US Commerce Department di introdurre il divieto di esportazione di tecnologie (comprese quelle informatiche e di *Cyber Security*) alla Russia in data 24 febbraio 2022, iniziando a causare molti disagi a tutte le aziende occidentali che hanno acquistato regolarmente le licenze di utilizzo dei propri software di sicurezza informatica ma che si sono trovate, involontariamente o meno, a violare le nuove restrizione di *export* per i propri uffici e stabilimenti in territorio russo.

Contestualmente, in Italia, il governo - tramite l'Agenzia per la Cybersicurezza Nazionale diretta dal prof. Baldoni, insieme alle agenzie per la *Cyber Security* francese (ANSSI) e tedesca (BSI) - hanno deciso di mettere al bando le tecnologie di sicurezza informatica sviluppate in Russia; in particolare è noto il caso di Kaspersky che, nonostante sia conosciuto sul mercato per il valore dei propri prodotti, vende tecnologia completamente sviluppata e controllata in territorio russo, oltre ai software delle aziende Group IB e Positive Technology. La raccomandazione interna dell'Agenzia per la Cybersicurezza Nazionale (ACN) del 15 marzo,

[1]-https://www.today.it/attualita/russia-imprese-italiane-che-restano.html.

seguita dalla circolare del 21 aprile 2022, pubblicata in Gazzetta Ufficiale il 26 aprile, ha disposto la rimozione di queste tecnologie dalla Pubblica Amministrazione e da tutte le aziende strategiche inserite nel "Perimetro di Sicurezza Cibernetica" in quanto sostanzialmente considerate una minaccia alla sicurezza nazionale[2].

Detto tutto ciò, se il problema, per quanto serio, fosse solo di natura legale, tutto sarebbe "facile o quasi". Proprio per questo, le tutte le *software house* sviluppatrici di questa tipologia di software e prodotti del comparto occidentale non si sono limitate ad applicare le disposizioni governative da un punto di vista formale, ma hanno anche implementato meccanismi di blocco sulle proprie *server farm*, facendo sì che, nel caso in cui i propri software tentino di collegarsi ai server di aggiornamento e/o gestione da zone di internet classificate come russe, vengano automaticamente bloccati, rendendo in buona sostanza inservibili tutti gli strumenti di protezione cyber.

L'identificazione degli apparati che concorrono al funzionamento di internet è molto precisa oggi: in particolare, l'autorità competente per l'assegnazione degli indirizzi IP pubblici (ovvero quegli indirizzi di rete che permettono il funzionamento di internet) è il Réseaux IP Européens Network Coordination Centre per Europa e Russia, con sede ad Amsterdam (Olanda).

Questa situazione ha creato enormi difficoltà a tutti gli IT Manager, CTO e CISO delle aziende occidentali, che erogavano i propri servizi ICT alle sedi sul territorio russo, complicando in particolare l'accesso ai sistemi ERP (o Gestionali) con i quali venivano gestita la produzione e la logistica, oltre a permettere operazioni semplici come l'accesso ai file aziendali residenti sui *File Server* delle aziende. La difficoltà di non poter più proteggere efficacemente questi sistemi come si proteggono normalmente in qualsiasi altra zona del mondo, ha fatto sì che i *Board of Directors* delle aziende prendessero delle decisioni difficili, alcune chiaramente in contrasto alle disposizioni governative pur di garantire l'integrità della totalità dei propri asset informatici ricompresi nei territori oggi considerati ostili.

Una soluzione percorsa da alcuni, particolarmente onerosa e spesso anche poco efficace, è stata quella di aggiornare i sistemi di protezione manualmente, ovvero caricando gli aggiornamenti, quando questo sia possibile, direttamente su tutti i sistemi interessanti. Come si può facilmente immaginare, questo ha generato un carico di lavoro per gli operatori di settore difficilmente sostenibile nel medio periodo.

La soluzione alternativa, anche questa chiaramente in contrasto con i disposti governativi, è stata creare presso i data center di paesi non soggetti a questo genere di sanzioni dei veri e propri concentratori di traffico ("*VPN Concentrator*") ospitati presso data center locali in paesi come gli Emirati Arabi, l'India o la Cina, in cui dirottare tutto il traffico internet delle aziende occidentali presenti in Russia.

Ma se qualcuno si domandasse se questa soluzione è stata la panacea di tutti i mali, la risposta

[2]-https://www.wired.it/article/kaspersky-russia-italia-circolare-acn-group-ib-positive-technologies-governo-sicurezza-informatica.

Gli effetti dell'embargo tecnologico sulle aziende occidentali con uffici e stabilimenti in Russia.

è "solo parzialmente". Ha sicuramente permesso che i problemi più pressanti riguardanti gli aggiornamenti di tutti quei software controllati direttamente dalle *software house* occidentali riprendessero a funzionare almeno parzialmente, lasciando comunque un rischio residuo importante. Quale?

Il rischio legale per il personale locale in territorio russo. Infatti, il 1° novembre del 2017, il Cremlino ha emesso una legge che vieta l'uso dei collegamenti crittografati tra soggetti, comunemente dette "*Virtual Private Networks*", oltre a mettere fuori legge tutti i siti in grado nascondere l'identità di chi vi accede ("*anonymizers*"). Sebbene fosse stato dichiarato all'inizio che le *Virtual Private Network* (o VPN) aziendali erano escluse da questo provvedimento, come molti esperti hanno dichiarato, non c'è modo di distinguere chi è il tipo di utilizzatore, se un soggetto privato o una persona fisica. L'autorità preposta a questo genere di controllo è il Servizio Federale per la supervisione delle comunicazioni o Roskomnadzor, che misteriosamente ha dichiarato di non aver mai ricevuto richieste di censimento di servizi VPN e "*Anonymizer*", nonostante la legge le obbligasse a censirsi per il governo. Gli articoli della stampa specializzata hanno riportato come la volontà del governo fosse quella di bloccare l'utilizzo di questi strumenti, piuttosto che inseguire gli utilizzatori e perseguirli.

Sebbene ci siano tecnologie occidentali che hanno ottenuto la certificazione FSTEK russa, ovvero un titolo emesso dall'omonima agenzia "Federal Service for Technical and Export Control of Russia", non è ancora chiaro come il governo russo si vorrà muovere circa l'uso di sistemi crittografici per i collegamenti internet e che potrebbero essere utilizzati anche per scopi militari.

Sul versante dei paesi NATO, verrebbe da domandarsi se le aziende costruttrici di tecnologia per la *Cyber Security* abbiano offerto collaborazione alle agenzie di *Intelligence* per identificare l'abuso dei propri strumenti commercializzati e prevenire la violazione di queste disposizione governative, oggi ritenute particolarmente strategiche per l'interesse collettivo. È lecito domandarsi se quelle "*backdoor* o accessi occulti ai sistemi" della National Security Agency (NSA) sui prodotti delle statunitensi Fortinet e Juniper, svelate sui giornali di settore già nel 2016, possano essere utili a mitigare in qualche forma l'abuso di queste tecnologie o quantomeno a identificare chi viola palesemente i disposti governativi. È certo che, mai più di oggi, la collaborazione tra governi e operatori del settore che sviluppano tecnologia per la sicurezza è diventata così importante e strategica[3].

Per concludere, la difesa degli interessi economici delle aziende occidentali che hanno fatti investimenti importanti in periodo pre-guerra sul territorio russo, la protezione dei collaboratori locali che ci sono trovati nel mezzo di una crisi internazionale senza precedenti e che si trovano a dover utilizzare strumenti potenzialmente vietati dal governo, la necessità di proteggere gli asset informatici e tecnologici che sono sul territorio russo ma di fatto protetti da tecnologie USA o filo occidentali, l'embargo tecnologico hanno creato una situazione veramente difficile da gestire, in

[3]-https://www.techeconomy2030.it/2016/01/15/juniper-fortinet-perche-quelle-backdoor.

cui qualsiasi azione venga intrapresa comporta significativi rischi di errore, perché viola sicuramente almeno le norme di una delle due parti, se non di entrambe insieme e contemporaneamente.

Gabriele Minniti, *esperto di Sicurezza Informatica e Sicurezza delle informazioni*

BIOGRAFIA

Gabriele Minniti

È un informatico specialista in Sicurezza Informatica e Sicurezza delle informazioni con oltre 15 anni di esperienza. Ha conseguito molteplici certificazioni internazionali in ambito tecnologico ed ha lavorato in Germania ed Inghilterra per importanti aziende costruttrici di tecnologie per la Sicurezza Informatica. Nel corso della sua carriera è stato chiamato sia come consulente che come docente per entità afferenti al comparto della Difesa. Fondatore di WhySecurity srl, oggi si occupa di supporto ad indagini difensive collaborando con investigatori privati, svolge analisi di rischio economico connesso al rischio informatico e offre servizi SOC a favore dei propri clienti.

FORUM ICT SECURITY

25-26 OTTOBRE 2023

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
11ª Edizione della Cyber Crime Conference

La guerra d'informazione in Ucraina e le misure di contrasto proposte in seno alla NATO e all'Unione europea.

L'attuale ampio ricorso alla guerra d'informazione (*information warfare*), offline e online, da parte della Federazione russa contro l'Ucraina (e non solo) ne evidenzia la crescente rilevanza strategica e solleva una serie di problematiche relative alla sua natura, nonché alle caratteristiche e alle strategie di contrasto e difensive.

La guerra d'informazione si sovrappone al conflitto cinetico in atto e si caratterizza anche per un'imponente attività di interferenza condotta dal Governo russo nei confronti di Kiev e degli Stati occidentali già a partire dal 2014[1]. L'intento delle autorità russe è la promozione di una nuova dimensione della conflittualità fornendo una propria versione degli eventi, spingendo verso la resa dell'avversario e rompendo il fronte comune dei Paesi alleati[2].
Tale tipologia di guerra si realizza:

- con la diffusione di informazioni errate, anche se non fabbricate o trasmesse intenzionalmente (la c.d. misinformazione);
- con la creazione, manipolazione intenzionale e diffusione coordinata e sistematica di false informazioni nello specifico intento di manipolare l'ecosistema informativo (la c.d. disinformazione).

Il suo obiettivo è ottenere un deciso **vantaggio strategico politico e militare** nel corso del conflitto armato (anche verso Stati non belligeranti) attraverso l'alterazione della percezione della realtà - che è alla base di ogni azione umana - per modificare in modo significativo le decisioni politiche del governo nemico e la conduzione delle ostilità[3].
In proposito, se da un lato è innegabile che la guerra di informazione esiste da tempi antichi, sotto forma di propaganda, dall'altro è evidente che oggi essa influenza le dinamiche della politica internazionale grazie a strumenti innovativi e sofisticati di comunicazione, quali le piattaforme digitali, tra cui i social media[4].
È noto, infatti, che la diffusione della disinformazione online avviene in modo pervasivo, senza limiti

[1]-Professore aggregato di Diritto internazionale, Università degli studi di Bari Aldo Moro, *Cyber security Specialist*. A. Cole, H. Le Guyader, *Cognitive: a 6th Domain of Operations*, in NATO ACT Edition, Innovation Hub, Norfolk, 2020; B. Fiore-Silfvast, *User-Generated Warfare: A Case of Converging Wartime Information Networks and Coproductive Regulation on YouTube*, in I*nternational Journal of Communication*, 6 2012, p. 1965–1988; D. Hollis, *The Influence of War; the War For Influence, in Temple Int'l & Comp. L.J.*, 2018, p. 31 ss., in https://sites.temple.edu; D. Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, ABC-CLIO, Westport, 2016.

[2]-V. la Risoluzione del Parlamento europeo del 1º marzo 2022 sull'aggressione russa contro l'Ucraina (2022/2564(RSP)) (2022/C 125/01), Aggressione russa contro l'Ucraina, par. 31. T. Thomas, *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?*, in *The Journal of Slavic Military Studies,* 1, 2014, p. 101 ss; R. Thornton, *The Changing Nature of Modern Warfare. Responding to Russian Information Warfare*, in *The RUSI Journal,* 2015, p. 40 ss.

[3]-P. Ottewell, Defining the Cognitive Domain, 2020, https://overthehorizonmdos.wpcomstaging.com.

geografici, in tempi rapidissimi e verso un numero indefinito di destinatari. Viepiù, essa è realizzata con l'ausilio di strumenti quali l'intelligenza artificiale e il *Machine Learning* che consentono la creazione, alterazione e manipolazione dei contenuti digitali (testi, audio, foto e video) secondo modalità difficilmente individuabili dagli esseri umani[5;6].
Un esempio è la diffusione massiccia da parte del Governo russo di audio, video, testi e immagini *fake* e *deep-fake*: si pensi, ad esempio, al video su YouTube in cui il Presidente ucraino Zelensky dichiara pubblicamente la resa alle forze russe (insieme a molti altri presenti in Rete)[7;8].
Per svolgere tali attività gli Stati impiegano o funzionari delle forze di sicurezza, o individui e società (*proxies*) che agiscono per loro conto o con il loro consenso, in modo da non essere indicati quali responsabili evitando in tal modo di essere oggetto di contromisure, sebbene occorra non escludere la mano occulta della criminalità organizzata e dei gruppi terroristici (si pensi all'ISIS)[9].
Su queste strategie si sono cimentati con particolare interesse anche militari cinesi secondo cui la mente umana rappresenta un "campo di battaglia" e le ostilità devono essere condotte attraverso i tre domini concorrenti: il dominio fisico, quello informativo e quello cognitivo[10].
Ciò ha portato allo sviluppo di un **nuovo concetto e metodo di combattimento** - il "*brain war combat style*" - grazie alla "*Military Brain Science*"[11] , che si basa sul presupposto che la "*psychological disruption*", da un punto di vista strategico, sia importante quanto la distruzione fisica[12].
L'attuale panorama impone, quindi, di prendere

[4]-NATO, Johns Hopkins University, Imperial College London, *Countering Cognitive Warfare: Awareness and Resilience*, https://www.nato.int; Chema Suárez Serrano, *From Bullets to Fake News: Disinformation as a Weapon of Mass Distraction. What Solutions Does International Law Provide?*, in *The Spanish J. of Intl. Law*, 2020, p. 129 ss.; Commissione europea, Independent High-level Group on fake news and online disinformation, *A Multi-Dimensional Approach to Disinformation*, Luxembourg, 2018, p. 5.

[5]-S. Hill, N. Marsan, *Artificial Intelligence and Accountability: A Multinational Legal Perspective" in Big Data and Artificial Intelligence for Military Decision Making, in Meeting proceedings STO-MP-IST-160, NATO*, 2018.
[6]-L. Bilyana, *Russian Information Warfare*, 2022, Naval Institute Press, Annapolis, p. 22.

[7]-*Depfake Zelensky surrender video is the 'first intentionally used' in Ukraine war*, 2022, https://www.euronews.com; H. Nasu, *Deepfake Technology in the Age of Information Warfare*, https://lieber.westpoint.edu/deepfake-technology-age-information-warfare, 2022.
[8]-International Committee of the Red Cross, *Artificial intelligence and machine learning in armed conflict: A human-centred approach*, https://www.icrc.org, p. 5; J. Aro, *The Cyberspace War: Propaganda and Trolling as Warfare Tools, in European View*, 2016, p. 121 ss.; B. Claverie, F. du Cluzel, *Cognitive Warfare: The Future of Cognitive Dominance, in NATO Collaboration Support Office*, 2022, p. 7, https://hal.archives-ouvertes.fr.

[9]-M.N. Schmitt, L. Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution, in The Fletcher Security Review*, 2014, p. 55 ss., in https://ccdcoe.org/uploads/2018/10/c28a64_2fdf4e7945e9455cb8f8548c9d328ebe.pdf.

[10]-K. Takagi, *The Future of China's Cognitive Warfare: Lessons from the War in Ukraine*, 2022, https://warontherocks.com, che espone anche lo sviluppo della Cina nel settore della "*intelligentized warfare*" con l'impiego dell'intelligenza artificiale nel dominio cognitivo elaborato nel 2019 dal People's Liberation Army. V. anche D. Cheng, *Winning Without Fighting. The Chinese Psychological Warfare Challenge,* 2021, in https://www.heritage.org; L. Naiguo, *New Theories of Information War,* Academy of Military Science Press, Beijing, 2004, p. 154; Y. Wenxian, *The Science of Military Information*, National Defense University Press, Beijing, 2008, p. 77 ss.

[11]-*Depfake Zelensky surrender video is the 'first intentionally used' in Ukraine war*, 2022, https://www.euronews.com; H. Nasu, *Deepfake Technology in the Age of Information Warfare*, https://lieber.westpoint.edu/deepfake-technology-age-information-warfare, 2022.

[12]-J. Arquilla, D.F. Ronfeldt, *The Advent of Netwar, i*n J. Arquilla, D. F. Ronfeldt (eds.), *Networks And Netwars: The Future of Terror, Crime, And Militancy,* Santa Monica, Rand, 2001, p. 1 ss.

atto di un significativo ampliamento del campo di battaglia, divenuto ibrido, in cui si impiegano mezzi **non convenzionali**[13]; e, conseguentemente, di cercare di contrastare il fenomeno della disinformazione.

Sul punto, a livello statale e nel contesto europeo e internazionale, la cooperazione internazionale rappresenta lo strumento essenziale per prevenire, individuare e rispondere in modo efficace, nel rispetto dei principi democratici, alla guerra d'informazione.

Con riguardo alla guerra d'informazione, una delle prime reazioni è stata quella dell'Unione europea che, per voce del Parlamento europeo, nel 2019 e con riferimento alle interferenze provenienti dall'estero durante le elezioni politiche europee, ha dichiarato che la disinformazione è una crescente, diretta e consistente minaccia all'ordine pubblico e alla sicurezza dell'Unione europea e degli Stati membri, e in particolar modo per le scelte politiche, il settore economico, la pubblica amministrazione e i cittadini[14].

All'indomani dell'aggressione russa contro l'Ucraina, poi, sempre il Parlamento europeo ha condannato "*il ricorso alla guerra dell'informazione da parte delle autorità russe, dei media statali e dei mandatari per creare divisioni con contenuti denigranti e false narrazioni sull'UE, la NATO e l'Ucraina, con l'obiettivo di creare negazioni plausibili riguardo alle atrocità russe*". Peraltro, il Parlamento europeo ha invitato "*tutti gli Stati membri a sospendere immediatamente la concessione di licenze di trasmissione per tutti i canali mediatici statali russi, compresa la loro ritrasmissione*". Successivamente, esso ha chiesto alla Commissione europea e al Servizio europeo per l'azione esterna di "*migliorare le informazioni alternative e online in lingua russa in merito agli sviluppi in atto per contrastare la disinformazione, a garantire che le dichiarazioni pubbliche dell'UE siano tradotte in russo e a rivolgersi anche al pubblico e alle piattaforme russofoni*". Altresì, è stato ribadito l'invito a "*Google e YouTube di vietare gli account di propaganda di guerra*" [15].

Viepiù, nella sentenza del 27 luglio 2022 (causa RT c. *Consiglio*) il Tribunale dell'Unione europea per la prima volta ha definito la disinformazione "*un'arma del moderno arsenale di uno Stato*" e ha disposto il blocco delle trasmissioni televisive da parte di network televisivi finanziati dal Governo russo con sede in Francia e altri Stati europei, che trasmettevano propaganda e *fake news*[16].

Anche l'Agenzia europea per la *cybersecurity* (ENISA) ha dichiarato che la disinformazione

[13]-G. Siboni, *The First Cognitive War*, in A. Kurz, S. Brom (eds.), Strategic Survey for Israel 2016/2017, Institute for National Strategic Studies, Tel Aviv, 2016, p. 215 ss.

[14]-Parlamento europeo, Risoluzione del 10 ottobre 2019 sulle interferenze elettorali e la disinformazione nei processi democratici nazionali ed europei, 2019/2810(RSP).

[15]-Parlamento europeo, Risoluzione del 1° marzo 2022 sull'aggressione russa contro l'Ucraina (2022/2564(RSP)) (2022/C 125/01), par. 31. T. Thomas, *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?*, in *The Journal of Slavic Military Studies*, 1, 2014, p. 101 ss; R. Thornton, *The Changing Nature of Modern Warfare. Responding to Russian Information Warfare*, in *The RUSI Journal*, 2015, p. 40 ss.

[16]-Agenzia europea per la *cybersecurity* (ENISA), Servizio europeo per l'azione esterna (SEAE), *Foreign Information Manipulation And Interference (Fimi) And Cybersecurity – Threat Landscape*, dicembre 2022, p. 6; sentenza del Tribunale dell'Unione europea, Grande Sezione, RT c. Consiglio, causa T-125/22, del 27 luglio 2022, testo rettificato con ordinanza del 14 ottobre 2022.

costituisce una minaccia alla democrazia e alla sicurezza europea ed è parte integrale dei conflitti moderni[17]. Per il Servizio europeo per l'azione esterna dell'UE (SEAE) ciò implica che la manipolazione e l'interferenza di informazioni, provenienti dall'estero, deve essere gestita sia nel contesto del "Piano europeo di azione per la democrazia" sia dello *Strategic Compass for Security and Defence* del 2022.

Secondo il Servizio europeo per l'azione esterna, la "*Foreign Information Manipulation and Interference*" (FIMI) consta prevalentemente di comportamenti non illeciti che minacciano o che hanno il potenziale per avere un impatto negativo su valori e processi democratici e politici[18]. In proposito, quindi, riteniamo preferibile inserire la guerra d'informazione nel più ampio *genus* delle operazioni di influenza ("*influence operation*"), che sono definite come "*azioni coordinate, integrate e sincronizzate di misure diplomatiche, informative, militari ed economiche in tempo di pace, di crisi, di conflitti, o nella fase post-conflittuale, decise da uno Stato per modellare, su propri interessi e obiettivi nazionali, atteggiamenti, comportamenti o decisioni di decisori o di opinioni pubbliche di Stati terzi*"[19].

Infatti, ad oggi nella Comunità internazionale non vi è consenso unanime circa la responsabilità internazionale dello Stato a cui siano imputabili tali comportamenti, neanche alla luce della Dichiarazione di principi dell'Assemblea generale dell'Organizzazione delle Nazioni Unite del 24 ottobre 1970 concernente le relazioni amichevoli e la cooperazione fra gli Stati, contenuta nella risoluzione 2625(XXV)[20].

Sulla base delle tipologie di operazioni testé rilevate, la NATO e l'UE hanno identificato alcuni strumenti di contrasto funzionali a una strategia difensiva[21].

La soluzione proposta della NATO è la creazione di un sistema di monitoraggio e di allerta della guerra cognitiva[22] per identificare e gestire in tempo reale le azioni e individuare la *kill chain* e le tattiche, tecniche e procedure (TTPs) da caricare su una *dashboard*. Ciò consentirebbe la realizzazione di mappe geografiche interattive per mostrare, con l'ausilio della intelligenza artificiale, lo sviluppo di operazioni di influenza sospette.

In ambito europeo, la soluzione proposta per contrastare le campagne di disinformazione verte

[17] Agenzia europea per la cybersecurity (ENISA), Servizio europeo per l'azione esterna (SEAE), *Foreign Information Manipulation And Interference (Fimi) And Cybersecurity – Threat Landscape*, dicembre 2022, p. 6.

[18] Ibidem, p. 6.

[19] E. Larson, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*, 2, 2009, in https://www.rand.org; T. Nagasako, *Global Disinformation Campaigns and Legal Challenges, in Int. Cybersecur. Law Rev.*, 2020, vol. 1, p. 125 ss., in https://doi.org.

[20] S.P. Kanuck, *Recent Development, Information Warfare: New Challenges for Public International Law*, in Harv. Int'l. L.J., 1996, p. 72 ss.

[21] B.C. Lewis, *Information Warfare*, https://irp.fas.org.

[22] https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html; NATO, *Media – (Dis)Information – Security,* 2020, https://www.nato.int; International Committee of the Red Cross, *Artificial intelligence and machine learning in armed conflict: A human-centred approach,* https://www.icrc.org.

sull'assoluta importanza della *situational awareness* e del coordinamento tra i servizi di *intelligence* nazionali e il Centro di *intelligence* e analisi dell'UE (UE IntCen) per migliorare la previsione strategica e l'autonomia strategica dell'Unione[23].

In conclusione, occorre riflettere sulla circostanza che in futuro Stati ed enti non statuali ricorreranno sempre più di frequente alle operazioni d'influenza, che se svolte per un tempo prolungato online, esprimono un importante potenziale capace di incidere sulla sicurezza nazionale e di causare danni non meno gravi di quelli fisici tipicamente associati ai conflitti armati[24]. Occorre quindi realizzare una strategia difensiva della dimensione cognitiva a livello nazionale: ben sapendo che essa richiede investimenti significativi sia in tecnologia, per realizzare solide capacità di rilevamento della provenienza e di contrasto delle disinformazioni digitali, sia nello sviluppo delle capacità di *intelligence* in sinergia con la dimensione europea e con i Paesi alleati e *like-minded*.

Annita Larissa Sciacovelli, *Prof. aggr. di Diritto internazionale e dell'Unione europea, Univ. degli studi di Bari Aldo Moro, Cybersecurity specialist*

[23] Risoluzione del Parlamento europeo del 17 febbraio 2022, par. 37.

[24] D.B. Hollis, *Why States Need an International Law for Information Operations,* in *Lewis & Clark L. Rev.*, 2007, p. 11.

BIOGRAFIA

Annita Larissa Sciacovelli

Annita Sciacovelli è Professore aggregato di Diritto internazionale presso il Dipartimento di giurisprudenza dell'Università degli studi di Bari Aldo Moro e *Cyber Security Specialist*. È *Cyber Research Fellow* presso il *Jerusalem Institute of National Security and Strategy* (Israele) e Componente del Direttivo del *Seminario Permanente di Studi internazionali*. Insegna Diritto internazionale presso l'Università degli studi internazionali di Roma (UNINT) ed è coordinatrice delle attività del Polo delle scienze giuridiche internazionalistiche e delle nuove tecnologie dell'Università di Cassino e del Lazio Meridionale. È Componente del Team INNOV@DIFESA, Ufficio Generale Innovazione della Difesa (UGID) presso il Capo di Stato maggiore, e membro del Comitato scientifico della rivista '*Giustizia militare*' e delle riviste elettroniche '*Sicurezza e Intelligence*' e '*Antiriciclaggio & Compliance*'. È anche membro dell'*Advisory Board* dell'*International Institute for Peace* di Vienna (Austria), membro della Commissione *Cyber Security Cyber Warfare* della SOCINT, e dell'Istituto di Diritto Internazionale Umanitario di Sanremo e della Società italiana di Diritto Internazionale. Febbraio 2023.

Teorie cospirative e disinformazione nel conflitto russo-ucraino. Il caso dei laboratori di armi chimiche[1].

«In a world of lies the lie is not removed from the world by means of its opposite, but only by means of a world of truth»

Franz Kafka, Eight Octavo Notebooks, February 4

INTRODUZIONE

Nella battaglia silente e senza fine per il dominio dello spazio informazionale (*information operations* - IO), i paesi occidentali sembrano scontare importanti ritardi. A solo titolo esemplificativo, nella testimonianza resa al Congresso US dagli esperti di *intelligence* e delle operazioni speciali statunitensi, nel marzo dello scorso anno (117° Congresso, Subcommittee on Intelligence and Special Operations, 2021), si affermava esplicitamente che paesi quali la Repubblica Popolare Cinese e la Federazione Russa avevano superato, di gran lunga, gli Stati Uniti nella corsa per plasmare l'opinione pubblica nazionale e internazionale. Nella testimonianza resa da James Sullivan, Defense Intelligence Officer for Cyber, disponibile su YouTube[2], è dato ascoltare la seguente dichiarazione pubblica relativa alle attività russe. «*We are increasingly seeing the integrated use of cyber-enabled psychological actions, distributed denial-of-service attacks, propaganda disseminated through social media and bots, strategic deception and disinformation, and electromagnetic warfare to achieve strategic goals*». Riguardo alle operazioni informazionali cinesi lo stesso Sullivan si esprimeva nei termini seguenti. «*The People's Liberation Army has developed the concept of "Three Warfares" - which is to say, public opinion, legal, and psychological warfare - as key components of its psychological-cognitive warfare efforts. These efforts are designed to demoralize adversaries and to influence foreign and domestic public opinion*». Sulla rilevanza di tale tematica, basti qui riportare anche quanto evidenziato nel corso del Vertice NATO del 14 giugno 2021: «*We are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies. Rapid advances in the space domain are affecting our security*[3]» .

[1] Achille Pierre Paliotta, ricercatore INAPP, a.paliotta@inapp.org.

[2] https://www.youtube.com/watch?v=N-RCBwyamdY&t=323s.

[3] https://www.nato.int/cps/en/natohq/news_185000.htm.

Nel caso citato da Sullivan, delle "*Three Warfares*" di stampo cinese, sia in tempo di pace che in tempo di guerra l'applicazione di tale politica ha lo scopo esplicito di controllare la narrazione prevalente e di influenzare le percezioni in un modo che promuova gli interessi della Repubblica Popolare Cinese, compromettendo al contempo la capacità di risposta degli oppositori (Walton, 2012).

La Federazione Russa è invece conosciuta, nell'ambito della comunità dell'*intelligence*, come la depositaria di un'ultradecennale attività disinformativa che data dai tempi della Ochrana zarista, della sovietica Čeka di Feliks Ėdmundovič Dzeržinskij [1877-1926] e poi delle varie diramazioni recenti (GPU, NKVD, KGB, FSB) la quale prende il nome generale di reflexive control (Thomas 2004, 2011; Giles et al. 2018).

Sia nel costrutto cinese delle "tre guerre" che nel "controllo riflessivo" russo, vi è l'esplicita consapevolezza che molteplici strumenti debbano essere utilizzati al fine di ottenere gli obiettivi politici prefissati. In questo senso non vi è dubbio alcuno che, nell'ampia panoplia delle tecniche e degli strumenti ancillari a disposizione dei vertici politici, vi siano anche le teorie cospirative o del complotto. Queste ultime hanno l'obiettivo esplicito di creare uno stato di diffusa frammentazione e discordia all'interno del corpo sociale del paese preso di mira.

Le teorie cospirative, difatti, hanno implicazioni potenzialmente dannose per la fiducia nelle istituzioni pubbliche, nella stessa scienza "ufficiale" - come si è visto nel caso della crisi pandemica - e nella vita democratica, nel caso delle elezioni politiche. In termini più generali, questo processo è legato alle trasformazioni socioculturali che hanno portato a crescenti intersezioni tra competenze degli esperti e conoscenze dei singoli cittadini, i quali sono maggiormente attivi nel divulgare le loro posizioni sui social media favorendo una partecipazione non esperta nei processi di dibattito pubblico. Lo sviluppo delle tecnologie digitali e la pervasività dei media personali hanno rafforzato questo processo, mettendo in discussione il ruolo dei governi, degli addetti ai lavori e delle istituzioni. In molti paesi le informazioni digitali ingannevoli sono collegate all'intensificarsi del conflitto politico, all'accrescersi delle tensioni etniche e hanno provocato crisi, indebolendo la fiducia nelle istituzioni democratiche e nei risultati elettorali. A ciò hanno contribuito anche la diffusione di movimenti populisti anti-elitisti (Mancosu, Vassallo & Vezzoni, 2017) e gli effetti delle *echo-chambers* sui social media (Sunstein, 2002). Ciò mostra assai bene come la propaganda, la mis/dis-informazione, il sabotaggio, le teorie cospirative e altre tattiche non cinetiche si stiano diffondendo sempre di più, anche nel campo occidentale (Graphika & Stanford Internet Observatory, 2022). Del resto, la tecnologia attuale consente di raggiungere comunità sia più ampie sia più granulari a cui applicare metodi di guerra ibridi. Tutte queste attività hanno due obiettivi distinti, ma complementari: destabilizzare e influenzare. Sebbene entrambi gli obiettivi possano essere raggiunti separatamente per militarizzare (*weaponize*) con successo l'opinione pubblica, possono anche essere raggiunti congiuntamente utilizzando l'uno come mezzo dell'altro. Gli obiettivi degli attacchi di guerra cognitiva possono spaziare da intere popolazioni a singoli leader della politica, dei social network (*influencer*), dell'economia, della cultura, della religione, del mondo accademico e dell'ecosistema mediatico. A questo riguardo, può essere sottolineato che anche il ruolo di altri leader sociali meno conosciuti non deve essere trascurato. I cosiddetti

"connettori" - esperti, addetti ai lavori, blogger e comunicatori a vario titolo - possono essere determinanti nelle operazioni di guerra narrativa.
In questo contesto, la fiducia può essere considerata un obiettivo cruciale e vulnerabile nell'ambito delle attività di guerra ibrida in quanto essa mira a ottenere un vantaggio sugli avversari, o a provocare un cambiamento nella politica del gruppo bersaglio, attraverso il processo narrativo. Non si può trascurare il fatto, pertanto, che gli esseri umani costituiscono l'obiettivo primario di tali operazioni.
La tesi che qui si sostiene è, dunque, che le teorie cospirative possano rientrare all'interno delle più generali attività di guerra ibrida: e questo sembra proprio il caso di specie che verrà preso in esame nelle prossime pagine, vale a dire quello relativo alla presenza di laboratori di armi chimiche e batteriologiche in territorio ucraino.

LE TEORIE COSPIRATIVE: BREVE ESAME DELLA LETTERATURA

In generale, le teorie cospirative o del complotto spaziano dalla scienza, alla salute, all'ambiente, all'immigrazione, al razzismo, al terrorismo, alla politica e alle relazioni internazionali. La diffusione di teorie cospirative è aumentata notevolmente negli ultimi anni, con picchi durante le elezioni presidenziali statunitensi e la pandemia di COVID-19. Lo stesso concetto di "*post-truth*" ha ricevuto un'ampia risonanza pubblica, tanto da essere stata considerata la parola dell'anno dall'Oxford English Dictionary nel 2016. La definizione scelta dal dizionario è stata la seguente: «*relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief*» (Oxford English Dictionary 2016).
Come esempio di tale situazione, vale qui menzionare che durante la recente crisi sanitaria il 20% dell'opinione pubblica globale credeva che Bill Gates stesse pianificando di usare il COVID-19 per implementare un programma di vaccini obbligatori con microchip di tracciamento (Nightingale & Farid, 2020). Nello stesso periodo, la teoria complottistica QAnon (Holoyda, 2022) si diffondeva sui social network, sostenendo che «*a group of Satan-worshipping elites who run a child sex ring are trying to control our politics and media*» e che tali gruppi stessero attivamente complottando contro il Presidente Donald Trump. Un sondaggio rivelava che il 37% dei rispondenti non era sicuro che l'affermazione sopra riportata fosse vera o falsa, mentre il 17% la riteneva vera[4].
Come riportato da Jovan Byford (2011) le teorie del complotto, diversi decenni orsono, venivano considerate una caratteristica precipua di opinioni politiche estreme, correlate a un'ideologia che «*remains just beyond the mainstream of everyday thinking*» (Billig, 1988:201). A tutt'oggi, invece, come si può evincere dai numeri dei sondaggi di opinione, la mentalità cospirativa non è più considerata una prerogativa di una frangia di "estremisti", quanto piuttosto una forma di narrazione sociale quotidiana nonché un modo sempre più comune di spiegare alcune delle principali sfide politiche e, secondo alcuni, esistenziali dell'epoca moderna: la segretezza della politica, l'aumento della sorveglianza e delle minacce alla privacy, l'incremento del potere degli organismi societari transnazionali

[4] https://www.ipsos.com/en-us/news-polls/npr-misinformation-123020.

e la loro diminuita responsabilità nei confronti dei comuni cittadini, il diffuso senso di indebolimento dell'*agency* personale e così via (Knight 2000; Fenster 2008). In altri termini, le teorie del complotto sono migrate dai margini al centro della politica e, come messo in evidenza costantemente dai sondaggi, è possibile rinvenire tali opinioni, in maniera diffusa, tra la popolazione generale, spesso in percentuali piuttosto significative.

Dal punto di vista etimologico la cospirazione, dal latino *conspirare* - "respirare insieme" - suggerisce lo sforzo intrapreso da un determinato gruppo al fine di ottenere un risultato condiviso (Byford, 2011:20). In questi casi, il ricorso al segreto ricopre un aspetto centrale perché si vogliono promuovere degli interessi personali o di gruppo, causando di conseguenza un danno alla comunità. Una definizione generale di cospirazione mette in luce proprio questo aspetto, ovvero che essa è un «*secret arrangement between a small group of actors to usurp political or economic power, violate established rights, hide vital secrets or illicitly cause widespread harm*» (Uscinski et al., 2016: 58).

Come chiosava lo scrittore Elias Canetti [1905-1994] «*secrecy lies at the very core of power*» (Canetti, 1978:290). Il detentore del segreto è colui che conosce ma non palesa ciò che conosce; è colui che ha il potere del silenzio poiché non può rispondere alle domande che gli vengono poste; è colui che seleziona cosa dire e cosa tacere. «*It is assumed that only a single individual, or a very small group of his creatures, is capable of keeping a secret and that deliberation is thus best confined to quite small groups, formed with secrecy in view and with very heavy penalties attached to indiscretion. The decision, it is said, should lie with one person; even he cannot know it before he has taken it and, once taken, it is quickly carried out as a command*» (ibid:295).

Tutto ciò racchiude, in maniera perspicua, il carattere selettivo ed elitario del segreto. A partire da tale assunto di base, le teorie cospirative concentrano la loro attenzione sull'idea di una lotta manichea tra il popolo - necessariamente puro - e l'élite, inevitabilmente corrotta, sia che quest'ultima sia costituita da un gruppo politico oppure da uno economico o culturale. A questo riguardo, il segreto rimanda necessariamente al potere e alla manipolazione dello spazio informazionale (IO). Pertanto, una teoria del complotto è prima di tutto una teoria del potere e i teorici del complotto desiderano invertire la dinamica del potere che opprime la società risvegliando (*red-pilling*)[5] i loro concittadini. In questo contesto si situano anche il "*Great awakening*" e il "*The Storm is Coming*" dei gruppi QAnon, inteso come il momento storico in cui i segreti della Cabala globale verranno finalmente resi pubblici, da parte di Trump.

In definitiva, «*the epithet "conspiracy theory" tends to be reserved for conspiracy-based explanations which deal with large scale, dramatic social and political events (such as the AIDS epidemic,*

[5] Il *topos* della pillola rossa proviene dal popolare e influente film di fantascienza del 1999 *The Matrix*. In esso è presente una scena, all'inizio del film, in cui al personaggio principale - Neo - vengono offerte due pillole: una rossa e una blu. La pillola rossa lo porterebbe a un brusco risveglio, difficile e doloroso, ma grazie al quale prenderà atto della dura realtà vigente nel mondo. La pillola blu rappresenta, invece, il voler continuare a vedere il mondo così come lo si è sempre visto, senza porsi ulteriori domande su quali siano i veri rapporti di potere. Il concetto ha un precedente nel film di fantascienza del 1990 ***Total Recall.*** In quel film, un personaggio offre a un altro una pillola rossa, che si dice sia un simbolo del suo desiderio di tornare alla realtà. Tuttavia, in questo caso, non viene presentata alcuna pillola blu. Guadagnando crescente importanza, durante le elezioni presidenziali di Donald Trump del 2016, anche i gruppi dell'*alt-right* hanno adottato la pillola rossa come emblema del "Grande risveglio" nei confronti delle minacce apportate agli uomini bianchi da alcuni fenomeni sociali quali il socialismo, il femminismo, l'immigrazione, la giustizia sociale e altri aspetti associati alle politiche progressiste.

the assassination of John F. Kennedy or 9/11); for explanations that do not just describe or explain an alleged conspiracy, but also uncover it and in doing so expose some remarkable and hitherto unknown 'truth' about the world (such as that the Illuminati orchestrated the French Revolution or that the Bush administration had a hand in 9/11); and for accounts that allege the existence of a plot with nefarious and threatening aims (to destroy Christianity, establish the New World Order, take a country to war or eliminate a racial group)» (Byford, 2011:21).

Come si può vedere da quanto sin qui argomentato, le teorie cospirative - assimilabili a una "*stigmatised knowledge*" (Barkun, 2016) - si distinguono dalle mere cospirazioni, in quanto queste ultime sono accordi segreti in vista del raggiungimento di determinati fini; le teorie complottistiche sono, invece, un tipico costrutto intellettuale mediante il quale si cerca di fornire un ordine logico e sequenziale agli eventi del mondo. «*They are modes of thinking, templates imposed upon the world to give the appearance of order to events. In their simplest form, conspiracy theories sometimes seek only to explain a single event, for example, a plane crash or an assassination. However, many conspiracy theories are far more ambitious and seek to impose order on a wide range of phenomena that may encompass entire countries, whole regions, or decades of history*» (Barkun, 2016:114).

A questo punto ci si può chiedere in che relazione si pongano le teorie cospirative rispetto ad altre tecniche e tattiche della disinformazione e a un più generale contesto di operazioni IO svolte nello spazio informazionale. La figura 1 mostra un *framework* generale, ripreso da Backes e Swab (2019:8), in cui gli autori trattano delle attività IO messe in atto dalla Federazione Russa nei confronti dei Paesi Baltici mettendo in risalto i seguenti elementi. Esse possono essere inserite, pertanto, tra le *Operations*.

Fig. 1

Foreign policy: «*Restore Russia to great power status. Maintain influence in countries previously occupied by the Soviet Union*»;

Grand strategy: «*Promote a multipolar world order. Use the Baltic States to discredit Western institutions such as the EU and NATO*»;

Strategy: «*Cognitive warfare, a strategy to influence the mindset of the population, without resorting to kinetic military action*»;

Operations: «*Information operations during elections to emphasize historical memory, failure of Baltic governments and influence Russian minority*»;

Tactics: «*Russian language broadcast news, fake social media accounts, manipulation of truths*».

UN CASO DI TEORIE COSPIRATIVE E DISINFORMAZIONE: I LABORATORI DI ARMI CHIMICHE IN UCRAINA

L'8 marzo 2022, durante la sua testimonianza davanti alla Commissione per le relazioni estere del Senato sull'invasione russa dell'Ucraina, il sottosegretario di Stato USA per gli Affari politici Victoria Nuland aveva risposto a una domanda del senatore repubblicano della Florida, Marco Rubio, sul fatto se l'Ucraina disponesse o meno di armi chimiche o biologiche. La sua risposta era stata la seguente: «*Ukraine has biological research facilities which, in fact, we are now quite concerned Russian troops, Russian forces, may be seeking to gain control of. So we are working with the Ukrainians on how they can prevent any of those research materials from falling into the hands of Russian forces should they approach*». Alla replica di Rubio «*I'm sure you're aware that the Russian propaganda groups are already putting out there all kinds of information about how they've uncovered a plot by the Ukrainians to release biological weapons in the country and with Nato's coordination. If there's a biological or chemical weapon incident or attack inside of Ukraine, is there any doubt in your mind that 100% it would be the Russian that would be behind it?*» il sottosegretario replicava: «*There is no doubt in my mind, Senator, and it is classic Russian technique to blame on the other guy what they're planning to do themselves*»[6].

A seguito di tali eventi Donald Trump Jr., figlio dell'ex presidente, il 9 marzo aveva postato il seguente messaggio sulla piattaforma Twitter: «*Well that went from conspiracy theory to senate testimony in about 6 days… It used to take six months to go from conspiracy theory to fact*»[7]. Sempre lo stesso giorno, qualche ora prima, il rappresentante repubblicano del Kentucky Thomas Massie postava questo messaggio: «*There's so much propaganda on both sides that I didn't take the concern over Ukrainian biological labs seriously… until now. This is a serious admission, under oath, from a person who would know*»[8].

Tucker Carlson, il conduttore di Fox News, citava in modo fuorviante osservazioni di funzionari statunitensi come prova che i laboratori stessero producendo o conducendo ricerche su armi biologiche. «*Out of nowhere, the Biden official in charge of Ukraine confirmed the story. Victoria Nuland, the under secretary of state, casually mentioned in a Senate hearing on Tuesday that actually, yes, the Biden administration does fund a series of biolabs in Ukraine*». Tale affermazione veniva sostenuta da Carlson durante il suo programma televisivo in cui segnalava anche un'intervista con Robert Pope, direttore del Cooperative Threat Reduction Program del Pentagono, programma che aiuta i paesi dell'ex Unione Sovietica a proteggere o eliminare le armi nucleari e chimiche. Carlson sottolineava che «*as Pope put it, scientists are scientists, they don't want to destroy all the bioweapons. Instead, they're using them to conduct new bioweapons research*»[9].

[6] https://www.c-span.org/video/?c5005520/senator-rubio-questions-undersecretary-nuland-biolabs-ukraine.

[7] https://twitter.com/DonaldJTrumpJr/status/1501336793941258240.

[8] https://twitter.com/RepThomasMassie/status/1501637637668548613.

[9] https://nyti.ms/3Vd0hAf.

Teorie cospirative e disinformazione nel conflitto russo-ucraino. Il caso dei laboratori di armi chimiche.

Il Dipartimento di Stato, il 9 marzo, emetteva un comunicato stampa in cui rigettava le operazioni di guerra cognitiva messe in atto dal Cremlino e citava espressamente le teorie cospirative e il fatto che esse erano state abbondantemente confutate. «*The Kremlin is intentionally spreading outright lies that the United States and Ukraine are conducting chemical and biological weapons activities in Ukraine. We have also seen PRC officials echo these conspiracy theories. This Russian disinformation is total nonsense and not the first time Russia has invented such false claims against another country. Also, these claims have been debunked conclusively and repeatedly over many years*»[10].

Come si può vedere da questa breve sintesi, gli effetti di tale notizia sull'ecosistema politico e mass mediatico statunitense non sono stati indifferenti e vale la pena provare a risalire al corso degli eventi, vale a dire nel momento in cui è stata diffusa la notizia, facendo uso delle informazioni disponibili sul sito della Arms Control Association, un'organizzazione apartitica fondata nel 1971 dedita a promuovere la comprensione e il sostegno pubblico per il controllo degli armamenti[11]. Sul sito è possibile avere contezza di tutta la timeline che qui viene riportata, per brevità, solo fino al 9 marzo.

- 21 dicembre 2021: il ministro della Difesa russo, Sergei Shoigu, aveva affermato che delle società private militari statunitensi stessero segretamente contrabbandando in Ucraina «*tanks filled with unidentified chemical components for the purpose of carrying out acts of provocation*».
- 17 febbraio 2022: il segretario di Stato americano Antony Blinken affermava, davanti al Consiglio di sicurezza delle Nazioni Unite, che la Federazione Russa avrebbe potuto inscenare una "*false flag*" come pretesto per un'invasione, compreso un attacco con armi chimiche.
- 27 febbraio 2022: l'Ucraina presentava alla Organization for the Prohibition of Chemical Weapons (OPCW) la nota verbale n. 61219/30-196/50-3 in cui veniva ipotizzato che le forze armate russe potessero preparare una "*false flag*" utilizzando sostanze chimiche, come far esplodere serbatoi industriali pieni di prodotti chimici.
- 8 marzo 2022: durante la 99a sessione del Consiglio esecutivo della OPCW la delegazione ucraina condannava le operazioni di disinformazione russa e ribadiva il rispetto e il sostegno dell'Ucraina alla Chemical Weapons Convention (CWC). L'ambasciatore ucraino, Maksym Kononenko, dichiarava che, in caso di incidente chimico in Ucraina, il suo paese avrebbe invocato l'articolo X della CWC, la quale prevede la fornitura di "Assistenza e protezione contro le armi chimiche" da parte di altri Stati membri della CWC. In seguito, quarantanove nazioni presentavano una dichiarazione congiunta alla OPCW condannando la campagna di disinformazione di Mosca, in particolare le dichiarazioni del 21 dicembre del ministro della Difesa russo Shoigu.
- 9 marzo 2022: la portavoce del Ministero degli Esteri russo, Maria Zakharova, affermava che

[10] https://www.state.gov/the-kremlins-allegations-of-chemical-and-biological-weapons-laboratories-in-ukraine.

[11] https://www.armscontrol.org/factsheets/timeline-chemical-biological-weapons-developments-during-russias-2022-invasion-ukraine.

il suo paese aveva a disposizione "*documents showing evidence that the US had supported a bioweapons program in Ukraine*" e che i nazionalisti ucraini stavano preparando una provocazione basata sull'impiego di armi chimiche.

Il punto di intersezione tra le attività di disinformazione e le teorie cospirative è il presunto legame tra il figlio del Presidente Biden, Hunter, e il finanziamento dei laboratori ucraini. Ciò permette agli agenti di influenza stranieri di collegare l'attività di disinformazione alla tradizionale attività politica, in questo caso al duro confronto politico instauratosi tra i politici repubblicani e i sostenitori di Trump (la variegata componente dell'*alt-right* e dei gruppi QAnon) con i democratici e i sostenitori dei diritti civili. In questo modo gli attori malevoli cercano di accentuare le fratture socio-politiche (*cleavages*) degli Stati Uniti al fine di minarne la coesione interna.

Una conferma di tale strategia è possibile coglierla dall'articolo seguente, pubblicato dal sito di news *Chinadaily.com.cn* il 29 marzo 2022, in un'edizione globale pubblicata in inglese, arabo e spagnolo, così come è dato vedere dal sito stesso: «"*An investment fund run by […] Hunter Biden funded research and the implementation of the United States' military biological program. It is obvious that Joe Biden, as his father and the head of state, was aware of that activity" Russian State Duma speaker Vyacheslav Volodin said, according to Russian media. Volodin called for a US congressional investigation and a White House explanation*»[12].

L'articolo illustra in dettaglio gli investimenti effettuati dalla società del figlio di Biden. «*Russia's new claim, however, that Hunter Biden's investment fund was involved in raising money for biolab projects in Ukraine is accurate, according to emails first obtained by the New York Post and initially reported by the Daily Mail of London on March 25. Rosemont Seneca Technology Partners invested $500,000 in Metabiota, a pathogen-research company headquartered in San Francisco, and raised millions more through firms that included Goldman Sachs, according to emails found on the computer, which was abandoned at a Wilmington, Delaware, repair shop in April 2019. Rosemont Seneca is an investment firm based in Washington DC. It was founded in 2009 by Hunter Biden, Christopher Heinz and Devon Archer*».

Un'ultima notazione di carattere storico può essere qui brevemente svolta e riguarda la datata campagna di Mosca relativa alle false accuse sullo sviluppo e l'utilizzo di armi biologiche (BW) da parte degli statunitensi. Un recente articolo, del 2021, di Milton Leitenberg mette in luce come la campagna sovietica di false accuse possa essere fatta risalire fino al 1949 e sia stata promossa fino al 1988, a volte sostenuta dalla Repubblica di Cuba, dalla Repubblica Democratica Tedesca (Germania dell'Est), dalla Repubblica Popolare Cinese o dalla Repubblica Popolare Democratica di Corea. Dopo una pausa tra il 1988 e il 1995, l'attività disinformativa russa è ripresa. Leitenberg sottolinea come uno dei motivi per cui il Cremlino conduce campagne di disinformazione di BW è «*to end US support for and US research presence in all the CTR [Cooperative Threat Reduction] facilities in the CIS [Commonwealth of Independent States] states on Russia's periphery*» (Leitenberg, 2021:16).

[12] https://global.chinadaily.com.cn/a/202203/29/WS62426127a310fd2b29e53d95.html.

CONCLUSIONI

La natura fondamentale della guerra non è cambiata neppure durante l'attuale invasione dell'Ucraina da parte della Federazione Russa. Essa continua a basarsi sempre su sanguinose operazioni cinetiche, guerriglia urbana, attacchi di droni alla popolazione civile, bombardamenti a tappeto di intere città, finanche minacce di utilizzo dell'Armageddon nucleare.

Allo stesso tempo, è anche vero che la guerra evolve continuamente tanto da divenire sempre più onnipervasiva, non risparmiando nessuna delle dimensioni spaziali sin qui individuate: terra, acqua, mare, spazio, cyberspazio. Questa continua evoluzione, infine, non può che essere strettamente intrecciata con la tecnologia e i suoi ultimi ritrovati, che anzi costituiscono un campo di sperimentazione precipuo durante tutte le guerre portando a decisi avanzamenti tecnologici. Del resto è sempre stato così, fin dai primordi della comparsa dell'uomo su questo pianeta. Fino ad arrivare alla dittatura informazionale delle piattaforme dei social media, le quali costituiscono una landa di non poco conto dell'infosfera (Floridi, 2020) attuale, con aspetti non ancora esplorati sino in fondo, soprattutto dal lato della cybersicurezza.

È proprio questa dimensione dello spazio informazionale (IO) ad aver palesato aspetti di forte centralità e innovatività nell'attuale conflitto russo-ucraino. Tra tutte le lezioni del conflitto in corso, difatti, non si può sottacere l'importanza di raggiungere la supremazia nel dominio dell'informazione: fin dai primi giorni di guerra, ambedue i contendenti hanno utilizzato le informazioni per modellare a proprio vantaggio il corso del conflitto.

Ciò è dovuto alla mera costatazione che la qualità delle notizie e delle informazioni che le persone incontrano online riveste un aspetto assolutamente centrale. È oramai ben documentato che le piattaforme digitali facilitano la scoperta di contenuti e notizie di varia qualità, che vanno dalle testate giornalistiche affidabili a quelle che promuovono la disinformazione o la propaganda a titolo definitivo.

Ed è proprio riguardo ad alcune brevi esemplificazioni di attività messe in essere da entità riconducibili alla Federazione Russa, poco prima e durante l'inizio dell'invasione dell'Ucraina, che si è trattato in questo articolo. Vale a dire di come queste entità hanno cercato di sfruttare la presunta produzione di armi biologiche a livello di disinformazione prima e di collegarle, successivamente, a un più ampio network di teorie cospirative le quali hanno trovato terreno fertile in una vasta area culturale statunitense che si può definire prettamente pre-politica e fa riferimento ai gruppi dell'*alt-right* e di QAnon. In questo modo, è stato possibile avere un riscontro degli effetti e della pericolosità che gli attori malevoli stranieri possono ottenere nel fomentare discordie all'interno delle nazioni concorrenti, fatte oggetto di operazioni IO e di attività di guerra ibrida. In questo caso di specie, una narrativa che può essere fatta addirittura risalire al periodo sovietico viene ripresa da alcuni media *mainstream* e da diversi politici di primo piano, all'interno dell'arena pubblica statunitense, e fatta oggetto di duro scontro politico.

In conclusione si tratta di situazioni che, pur avvenendo nel cyberspazio informazionale, devono essere attentamente monitorate ai fini della sicurezza nazionale, poiché ne possono derivare

forti fratture nel corpo sociale, le quali possono persino sfociare in episodi drammatici: una classica esemplificazione di questa tipologia può essere considerato l'assalto al Capitol Building del 6 gennaio 2021.

Achille Pierre Paliotta, *Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL).*

BIOGRAFIA

Achille Pierre Paliotta

Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL). Laurea in Sociologia all'Università di Roma "La Sapienza", Master in Data Science (DS) all'Università di Roma "Tor Vergata" nel 2015 e Master in Cybersecurity (SIIS) all'Università di Roma "La Sapienza" nel 2021. Svolge studi e ricerche sull'innovazione tecnologica, sulla *cyber intelligence*, sulla cybersicurezza, sulle professioni, sull'incrocio tra domanda ed offerta di lavoro, sulla formazione continua, sull'invecchiamento attivo, sulla contrattazione collettiva e, in generale, su tematiche di sociologia economica. Sta attualmente svolgendo il I Dottorato nazionale in Cybersecurity presso IMT Lucca e IIT CNR.

Quaderno di Cyber Intelligence #2

CYBER CRIME

White paper gratuito su www.ictsecuritymagazine.com

Threat Actor russi operanti nel confitto russo-ucraino.

La guerra in Ucraina rappresenta senza dubbio il più grande conflitto militare dell'era cibernetica e il primo a unire significativi ed eterogenei livelli di operazioni informatiche. Allo stato attuale, il quadro complessivo degli impatti sui target derivanti dagli attacchi cyber è difficilmente valutabile perché - a differenza di quelli cinetici - non si ha una piena conoscenza e comprensione dei risultati ottenuti dalle *Cyberattacks & Operation* né di tutti gli attori che li stanno attuando.

Sebbene molti aspetti della *cyberwarfare*[1] siano oggetto di approfondimento da parte degli analisti di *intelligence*, diversi aspetti interessanti sono già evidenti e riguardano sia le strategie ad approccio tecnologico ibrido, utilizzate dalla Federazione Russa, sia le conseguenze viste in termini di comprensione delle strategie di attacco nella determinazione di contromisure da parte della repubblica ucraina e di tutti gli eventuali target (governativi e privati) potenzialmente impattati dai cyber attacchi.

Un aspetto interessante riguarda la frequenza degli attacchi informatici eseguiti dai russi durante il conflitto. La Russia, in periodo di pace, esegue attacchi cyber basati su tecniche notevolmente simili a quelle utilizzate durante i conflitti, con la differenza di diventare più frequenti e di avere come obiettivi la disabilitazione/distruzione di infrastrutture critiche. Questo *modus-operandi* di guerra ibrida è in linea con la dottrina militare russa, che comprende fondamentalmente qualsiasi tipo di azione intenzionalmente pensata e progettata per indebolire un avversario anche attraverso l'uso di leve politiche-economiche, culturali o ambientali.

Il modello russo di guerra ibrida è facilmente riconoscibile e la sua efficacia è fondata su alcuni strumenti militari, come la concentrazione ingiustificata delle truppe alle frontiere, gli esercizi di scansione su larga scala basati su scenari offensivi, l'uso di manovre provocatorie nello spazio aereo internazionale e in mare; ma anche attacchi informatici, campagne mediatiche aggressive e altre attività.

L'obiettivo ultimo dell'attuazione del modello ibrido è generare ambiguità, sia nella popolazione colpita che in quella attaccante e in generale nella più grande comunità internazionale, sostenendo che non siano state adottate alcune azioni. La flessibilità e l'adattabilità sono due altri elementi chiave del modello ibrido di guerra russa.

All'origine della guerra ibrida del Cremlino vi è la dottrina di Yuri Andropov, ex Segretario generale del Partito Comunista dell'Unione Sovietica, basata sull'infiltrazione in Occidente allo scopo di minarlo dall'interno. La declinazione di questa dottrina in termini attuali è stata realizzata dal generale Capo di Stato Maggiore dell'esercito russo Valery Gerasimov[2], che vede la guerra ibrida come composta da sei stadi (Fig. 1).

[1] Bilyana Lilly, *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*, Naval Institute Press (2019) e *Russian Cyber Warfare: The History of Russia's State-Sponsored Attacks across the World*, Charles River Editors (2022).

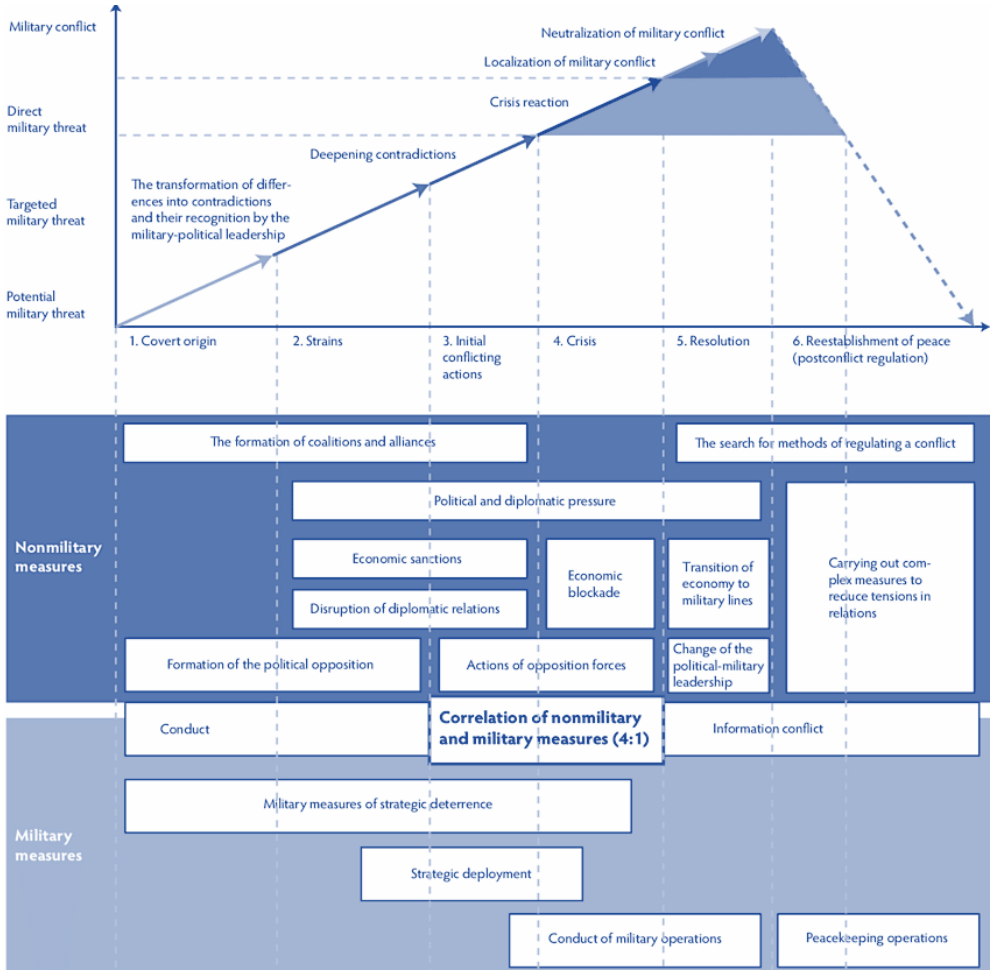

Fig. 1 - Misure non militari e militari considerate nella dottrina Gerasimov (fonte: Wikipedia)

Gerasimov teorizza che la nuova guerra asimmetrica si gioca (e si vince) soprattutto attraverso un nuovo tipo di difesa, basata su fattori scientifici ed economici, e sulla partecipazione di parti non militari come aziende private o identità civili di vario tipo che si muovono in ambito politico, economico e persino umanitario.

L'essenza di una guerra ibrida è spesso descritta come *controlled chaos*[3]: pertanto, gli analisti russi spesso lo descrivono come una sorta di "caos pulsante" che può essere utilizzato per regolare il livello di disordine inflitto a uno Stato bersaglio (o qualsiasi altra entità, solitamente definita geograficamente).

[2] Valerij Vasil'evič Gerasimov, *Cennost' nauki v predvidenii* (traducibile come "Il valore della scienza nella previsione") ; Charles K. Bartles, *Getting Gerasimov Right,* Military Review - Vol. 96 (2016) .

[3] Mark Galeotti, *Controlling Chaos: how Russia manages its political war in Europe*, Information&Security - Vol. 53 (2017); Eli Cohen & Elizabeth Boyd, *The KGB and anti-Israel propaganda operations*, Informing Science: the International Journal of an Emerging Transdiscipline - Vol. 22 (2019).

Lo scopo è causare e alimentare l'instabilità, per indebolire il tessuto sociale all'interno di una società e complicare o minare il processo decisionale (Fig. 2).

Lo Stato bersaglio dovrebbe, idealmente, essere indebolito lungo le due dimensioni complessive di legittimità (orizzontale e verticale)[4] che servono a definire la sua posizione su un *continuum* di Stati forti e Stati deboli.

Sintetizzando, la dottrina impiegata nelle guerre ibride considera l'uso della politica, della diplomazia, dell'economia e di altre misure non militari in

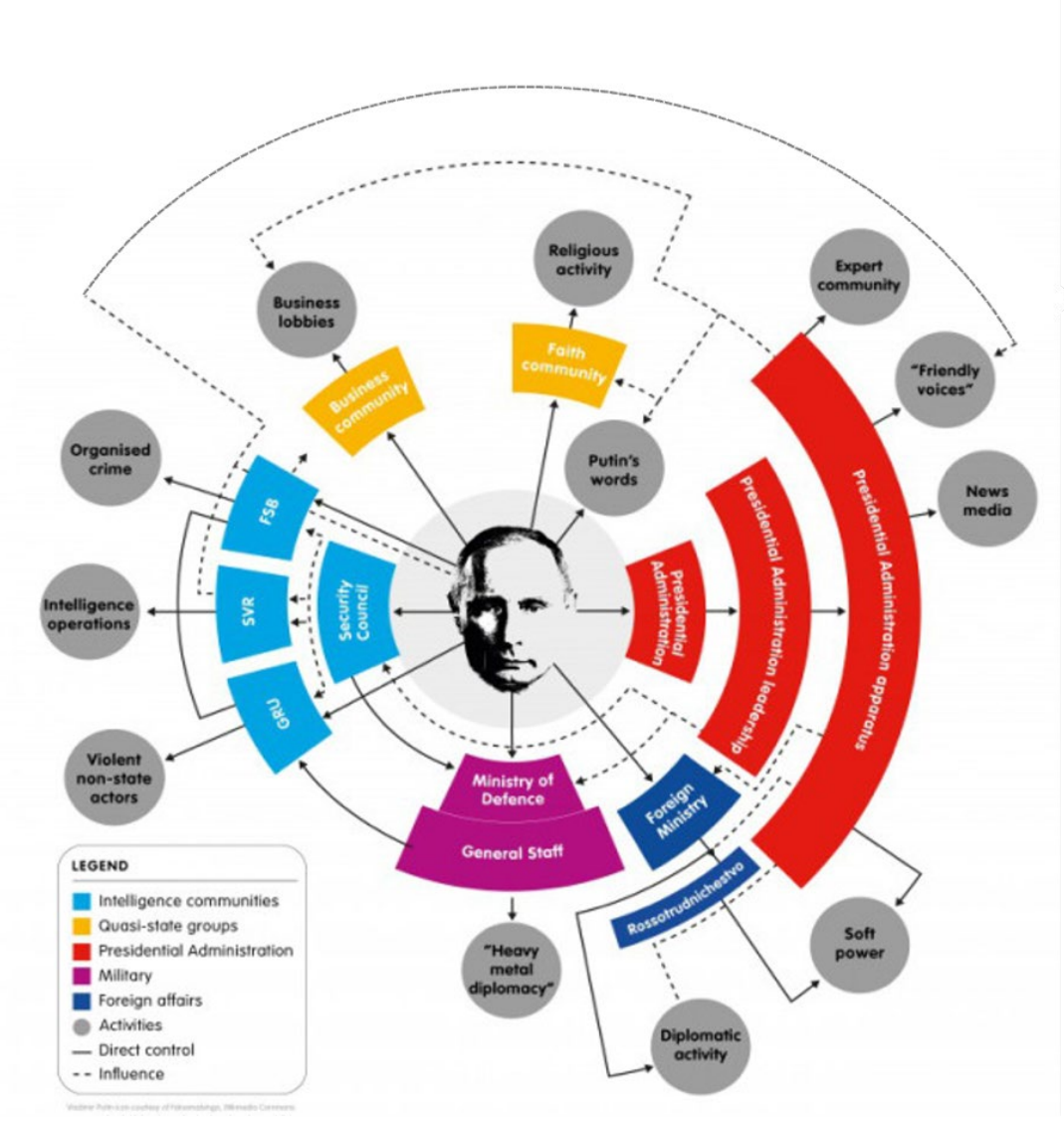

Fig. 2 - How Putin Coordinates Russia's Active Measures. (fonte: M. Galeotti, 2017)

[4] Il concetto di legittimità è distinto in orizzontale, come misura in cui la popolazione di uno Stato accetta di essere inclusa in questo, e verticale, come misura in cui la popolazione di uno Stato accetta il diritto di governare di coloro che sono al potere.

combinazione con l'uso di forze militari.
La si può riportare nei seguenti punti:

- invio di unità di linea[5] in tempo di pace;
- collocazioni di operazioni *noncontact combatt*[6] attraverso unità di linea di diversi settori;
- impoverimento del potenziale economico-militare di uno Stato attraverso la veloce distruzione di strutture di fondamentale importanza, del suo esercito e delle infrastrutture civili;
- uso massiccio di armi ad alta precisione, impiego su larga scala di forze operative speciali, nonché di sistemi robotici e partecipazione di una componente civile-militare alle operazioni di combattimento;
- azioni simultanee delle unità di linea contro le strutture nemiche presenti nel territorio e nell'*information space*[7]
- utilizzo di operazioni asimmetriche e indirette.

L'aspetto da evidenziare consiste nel fatto che mentre l'Occidente considera le misure non militari (come ad esempio le sanzioni economiche, l'interruzione dei rapporti diplomatici, le pressioni politiche e diplomatiche, etc.) come modi per evitare la guerra, la Russia considera queste misure come tattiche di guerra. Per quello che maggiormente ci interessa, Gerasimov evidenzia che una caratteristica determinante dell'*information warfare* è che essa può essere impiegata sia in tempo di pace che di guerra. Se in tempo di pace le operazioni informatiche possono essere utilizzate in parallelo o in combinazione con altre misure non militari, in tempo di guerra vengono invece utilizzate per catturare e mantenere la superiorità dell'informazione accanto alla forza militare e mirano ad amplificarne l'efficacia. L'impiego complessivo di questa gamma di misure militari e non militari porterà – secondo questa dottrina - alla vittoria.

Come precedentemente esposto, la guerra ibrida combattuta dalla Federazione Russa prevede - insieme all'impiego dei gruppi APT - l'utilizzo effettivo di gruppi di *threat actor* (cosiddetti *Cyber Proxy*) affiliati all'*intelligence* russa e di tecniche di disinformazione e propaganda. Molti settori industriali dei partecipanti al conflitto (direttamente o indirettamente) sono stati oggetto di attacchi, anche se gli impatti principali sono stati subiti dallo Stato ucraino.

Nella figura 3 sono mostrati tutti gli Stati oggetto degli attacchi cyber.

Sebbene quasi tutti i settori industriali siano stati oggetto di attacchi e di *Cyber Operation*, di seguito verranno approfonditi soltanto le ripercussioni sui settori *Energy, Financial, ICT, Transportation, Public Administration* e Media:

- ***Energy*** (elettricità, gas, vapore e fornitura di aria condizionata): il settore energetico fornisce servizi essenziali in tutti i paesi e gli attacchi informatici contro questo settore possono causare interruzioni o carenze di energia, con ripercussioni anche sulla capacità di funzio-

[5] Le unità di linea (line unit) sono qualsiasi unità in una squadra di combattimento di brigata.

[6] I mezzi non militari consistono principalmente nelle tecniche per influenzare le menti dell'avversario.

[7] Il concetto russo di Information Space è equivalente al concetto di Cyberspace adottato negli Stati Uniti.

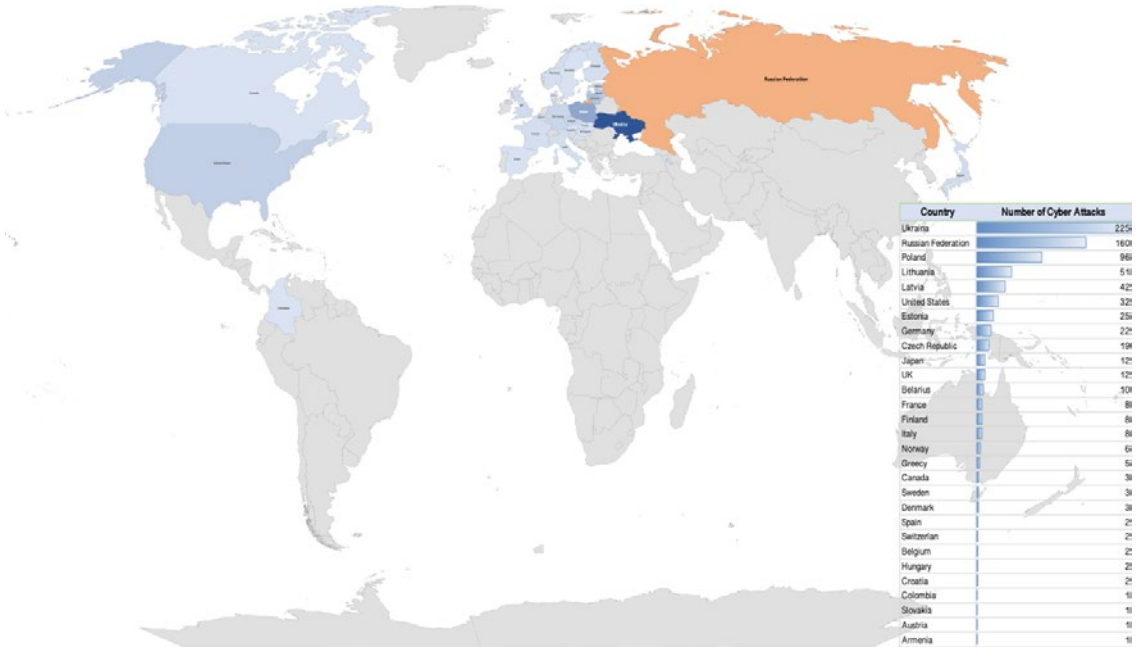

Fig. 3

namento di altri settori. L'impatto di attacchi cyber di tipo *destruction* e *disruption* sul settore energetico si fa sentire in tutta la società: se un attacco porta al *downtime* di infrastrutture critiche, ciò può comportare l'interruzione dell'accesso all'elettricità e al gas per migliaia di famiglie, servizi pubblici (ad es. sanità, trasporti, istruzione e servizi di emergenza), organizzazioni e imprese.

- ***Financial*** (*Financial and insurance activities*): il settore dei servizi finanziari è vitale per il funzionamento della società (Fig. 4). Le sanzioni hanno comportato l'esclusione di diverse organizzazioni russe e bielorusse dal sistema globale di messaggistica per i pagamenti Swift. Durante il conflitto sono stati segnalati attacchi DDoS contro istituti finanziari in Ucraina, oltre ad una serie di attacchi di *hacking* e *data leak* che hanno sollevato preoccupazioni relative a problemi di protezione dei dati pubblicati online che possono comportare l'esposizione a rischi di attacchi digitali o fisici. Gli attacchi informatici alle banche

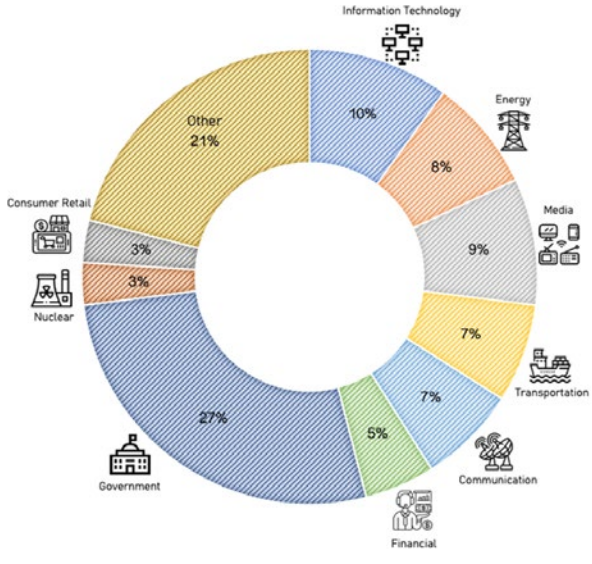

Fig. 4

di tipo *disruptive* possono limitare l'accesso della popolazione civile al denaro necessario per acquistare provviste e proteggere se stessi e le proprie comunità dai pericoli.

- **ICT** (*Information & Communication*): la deliberata distruzione delle infrastrutture di trasmissione televisiva e radiofonica e dei fornitori di telecomunicazioni in Ucraina sono utilizzati come mezzo per interrompere l'accesso a informazioni affidabili relative agli sviluppi della guerra e alla situazione in Ucraina, ma - ancor più grave - impediscono alla popolazione civile di cercare assistenza medica, accedere ai servizi online, coordinare gli sforzi di soccorso e molto altro.
- ***Transportation*** (*Transportation and storage*): gli attacchi informatici al settore dei trasporti possono interrompere o arrestare interi sistemi e/o servizi, compromettere la sicurezza del personale e dei passeggeri e avere un impatto sulle catene di approvvigionamento in tutti i settori. Durante il conflitto sono stati documentati attacchi DDoS a fornitori di servizi di trasporto in diversi paesi. Oltre a questo, i cosiddetti collettivi di *hacktivist* prendono di mira anche i fornitori di trasporti legati all'industria mineraria/petrolifera, compromettendo i loro sistemi, estraendo dati e pubblicandoli online.
- ***Public Administration* & Defence:** gli attacchi informatici al settore della pubblica amministrazione minacciano le attività di *e-government*, la protezione dei dati sensibili governativi e personali, nonché il funzionamento dei servizi. A causa del collegamento diretto del settore con entità governative, l'Amministra-

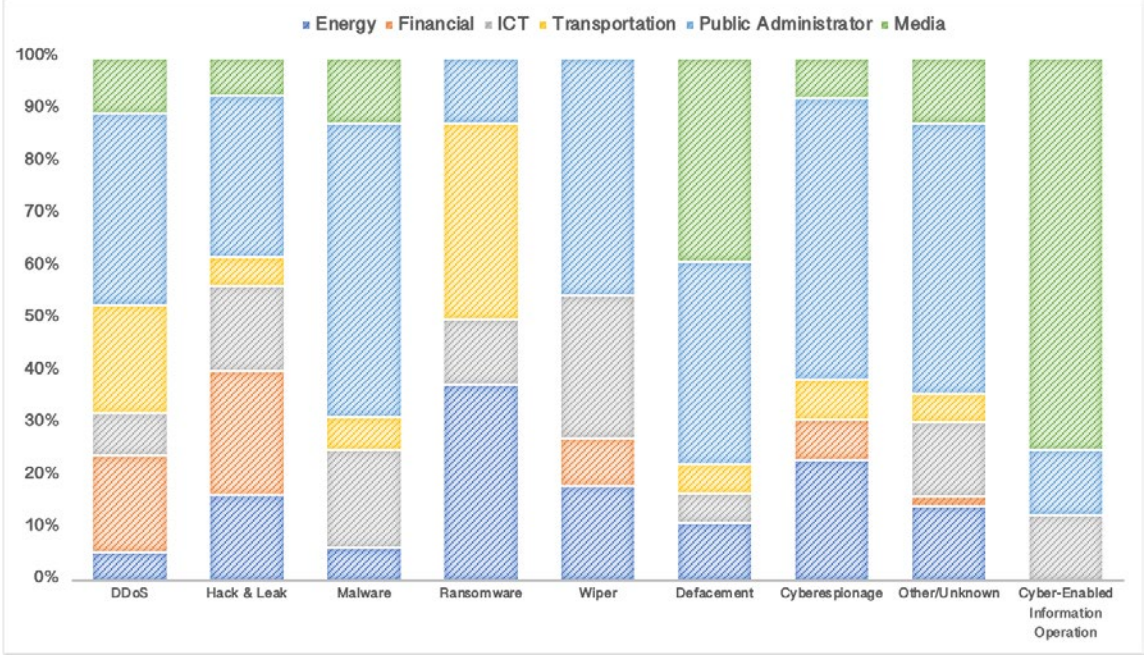

Fig. 5 - Tipologia di attacchi cyber sui diversi settori industriali

zione Pubblica è stata un obiettivo specifico di attacchi di tipo *disruptive* in Ucraina sia prima dell'invasione sia nel corso nel conflitto attuale. D'altra parte, anche le istituzioni governative in Russia sono state oggetto di vari tipi di attacchi. Il conflitto ha visto anche attacchi che hanno colpito la pubblica amministrazione e i siti web governativi di paesi che hanno dimostrato sostegno all'Ucraina.

- **Media** (*Media & Content)*: il settore dei media svolge un ruolo fondamentale nell'informazione, oltre che nel formare e informare l'opinione pubblica. L'uso di *botnet* (o *botfarm*) per diffondere account e messaggi falsi su larga scala al pubblico, attraverso attacchi per deturpare i siti Web, circolazione di disinformazione e propaganda in questo conflitto viene condotta online con impatti dannosi offline. Gli attacchi al settore dei media sono stati implacabili nel loro tentativo di interrompere e/o influenzare lo spazio dell'informazione attraverso la diffusione di disinformazione e disabilitando o interrompendo i servizi per limitare l'accesso a informazioni tempestive, affidabili e ufficiali alle popolazioni sia in Ucraina che nella Federazione Russa. Risulta del tutto evidente che la diffusione di *misinformation* (informazioni errate o fuorvianti) e *disinformation* (informazioni volutamente ingannevoli) può causare danni a persone e organizzazioni.

La figura 5 mostra la distribuzione della tipologia di attacchi cyber sui settori industriali sopra discussi.

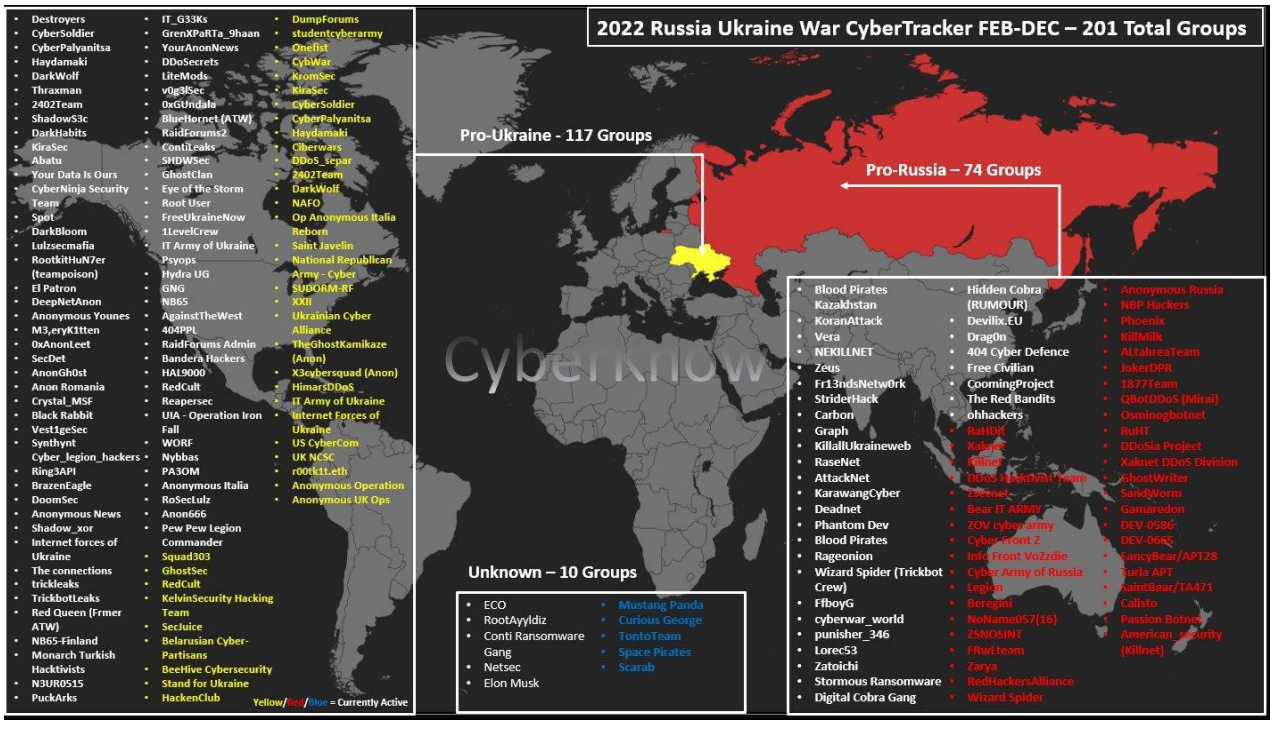

Fig. 6 - Lista a febbraio 2022 dei gruppi pro-Russia e pro-Ucraina realizzata da Cyberknow

La galassia degli attaccanti polarizzati verso la Russia o l'Ucraina è davvero molto ampia e - solo a titolo di esempio - si riporta una mappa pubblicata da Cyberknow (Fig. 6), che fotografava la presenza di 201 gruppi totali a febbraio 2022.

Volendo considerare solo i *threat actor* russi coinvolti in *cyber Attack & Operation*[8] documentati (vedasi Tabbella n.1) si è realizzata la seguente classificazione:

- *State actor* conosciuti - sono i gruppi *Nation-State* conosciuti e legati ai tre rami dell'*intelligence russa* (SRV, GRU e FSB):
  - Il gruppo APT29 è un gruppo di spionaggio informatico attribuito all'SVR. Gli obiettivi del gruppo includono governi e organizzazioni occidentali. Più di recente, nel 2019, il gruppo ha condotto una campagna di phishing in diversi settori negli Stati Uniti (militare, *imagery*, trasporti, farmaceutica, governo nazionale e *defense contracting*).
  - Il Gruppo Turla, attribuito all'FSB, è noto per aver condotto campagne di furto di informazioni e spionaggio in 45 diversi paesi. Gli obiettivi di questo gruppo vanno dal governo, alle ambasciate, all'esercito, all'istruzione, alla ricerca fino alle aziende farmaceutiche.
  - Il gruppo Sandworm, attribuito all'Unità 74455 del GRU, ha preso di mira obiettivi di alto profilo all'interno dei settori ucraini. Sandworm presenta somiglianze con altri gruppi come Iron Viking e Voodoo Bear. Il gruppo è presumibilmente responsabile degli attacchi basati su *ransomware* (NotPetya) o basati sulla supply-chain. Il gruppo ha eseguito attacchi informatici contro vari sistemi informatici in Ucraina; compromettere le infrastrutture critiche e altre attività della nazione.
  - Il gruppo APT28 è stato attribuito all'Unità 26165 e all'Unità 74455 del GRU. Al momento, si dice che l'APT 28 raccolga informazioni sui governi dell'Europa orientale dando al governo russo la possibilità di influenzare l'opinione pubblica in questi paesi.
  - Il gruppo Gamaredon è attribuito alla 16-ma sezione dell'FSB ed è specializzato in furto di informazioni e spionaggio. Per tutto il 2019 il gruppo ha preso di mira funzionari diplomatici, governativi e militari ucraini. Gli ultimi attacchi registrati risalgono a marzo e aprile 2020, utilizzando i contenuti Covid19 come esca nelle campagne di *phishing*.

Questi gruppi (insieme agli *State actor* sconosciuti) stanno impiegando durante il conflitto strumenti nuovi e sofisticati strumenti sia per realizzare attività di *information gathering* & *cyber-espionage* e sia di tipo *destructive*[9] (AcidRain, WhisperGate, WhisperKill, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero e Industroyer2)

[8] I La lista delle *Cyber Attack & Operation* che sono stati ottenuti dal Cyber Peace Institute (cyberconflicts.cyberpeaceinstitute.org), dettagli tecnici e TTP dei principali *Nation-State Threat Actor* sono forniti dalla CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

[9] https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets.

- *Private actor* conosciuti - sono *cyber-proxy* legati direttamente all'*intelligence* russa. In particolare, gli analisti di Mandiant valutano le Cyber Operation svolte dai gruppi XakNet Team, CyberArmyofRussia_Reborn e Infoccentr come coordinate dall'APT28 del GRU[10].
- *Hacktivist* conosciuti - sono gruppi di attivisti pro-Russia. I principali collettivi (molti dei quali si sono organizzati - o pubblicano i loro manifesti - sui loro canali Telegram) dei quali si ha un'evidenza certa degli attacchi e della loro rivendicazione sono Killnet, NoName057(16), DDOS_Service, Nemez1da, From Russia with Love (@frwl_team), People's Cyberarmy, Zarya (@ddos_channel_rus), ICC_H@ckTeam e Mirai. Questi gruppi, a vario titolo sono in relazione (o coordinati) dal gruppo XakNet Team. Da un punto di vista operativo, gli attacchi eseguiti da questi gruppi sono generalmente di tipo DDoS, *Hacks&Leaks* e *Web Defacement*. Cyble Research and Intelligence Labs[11] ha collegato KillNet con una versione modificata di Chaos Ransomware. Sicuramente, tra i collettivi conosciuti, KillNet rappresenta il prototipo dei nuovi gruppi di *hacktivist* in quanto usa un proprio canale Telegram seguito da molte migliaia di iscritti, si basa su una struttura fortemente gerarchizzata e un'organizzazione basata su alleanze con altri gruppi secondari e distaccamenti. Attorno ai gruppi secondari ruotano un numero imprecisato di gruppi minori che garantiscono al collettivo una elevata resilienza. Altro aspetto fondamentale di questo nuovo fenomeno è il reclutamento su base volontaria di nuovi collettivi che devono, però, avere una serie di prerequisiti minimi in termini di capacità tecniche, in assenza dei quali potranno essere impiegati per l'esecuzione di attività di basso profilo come gli attacchi DDoS. Altri gruppi, come per esempio NoName057(16)[12], offrono persino un programma strutturato di *training*. Lo stesso gruppo ha lanciato nel luglio del 2022 un *crowdsourced botnet project* chiamato DDOSIA[13]. L'obiettivo di questo progetto è sfruttare gli *hacktivist* pro-Russia disposti a scaricare e installare un bot sui propri computer per lanciare attacchi DDoS in cui sono forniti incentivi finanziari ai principali contributori.

L'ecosistema degli *hacktivist* pro-Russia risulta essere estremamente variabile. Solo a titolo di esempio, nella figura 7 si riporta un *cluster* di gruppi secondari coordinati dal KillNet attraverso il gruppo Legion. Sono mostrati dei gruppi secondari coordinati, attraverso Legion, da KillNet che è stato creato e gestito dal KillMilk fino a luglio del 2022 per poi lasciare il comando a BlackSide, che risulta avere una profonda competenza nello sviluppo di *ransomware*[14].

[10] https://www.mandiant.com/resources/blog/gru-rise-telegram-minions.

[11] https://blog.cyble.com/2022/11/08/pro-russian-hacktivists-targeting-adversaries-with-killnet-ransomware.

[12] https://press.avast.com/en-us/noname05716-pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks.

[13] https://www.radware.com/security/threat-advisories-and-attack-reports/project-ddosia-russias-answer-to-disbalancer.

[14] https://www.groupsense.io/resources/killnet-founder-leaves-hactivist-group.

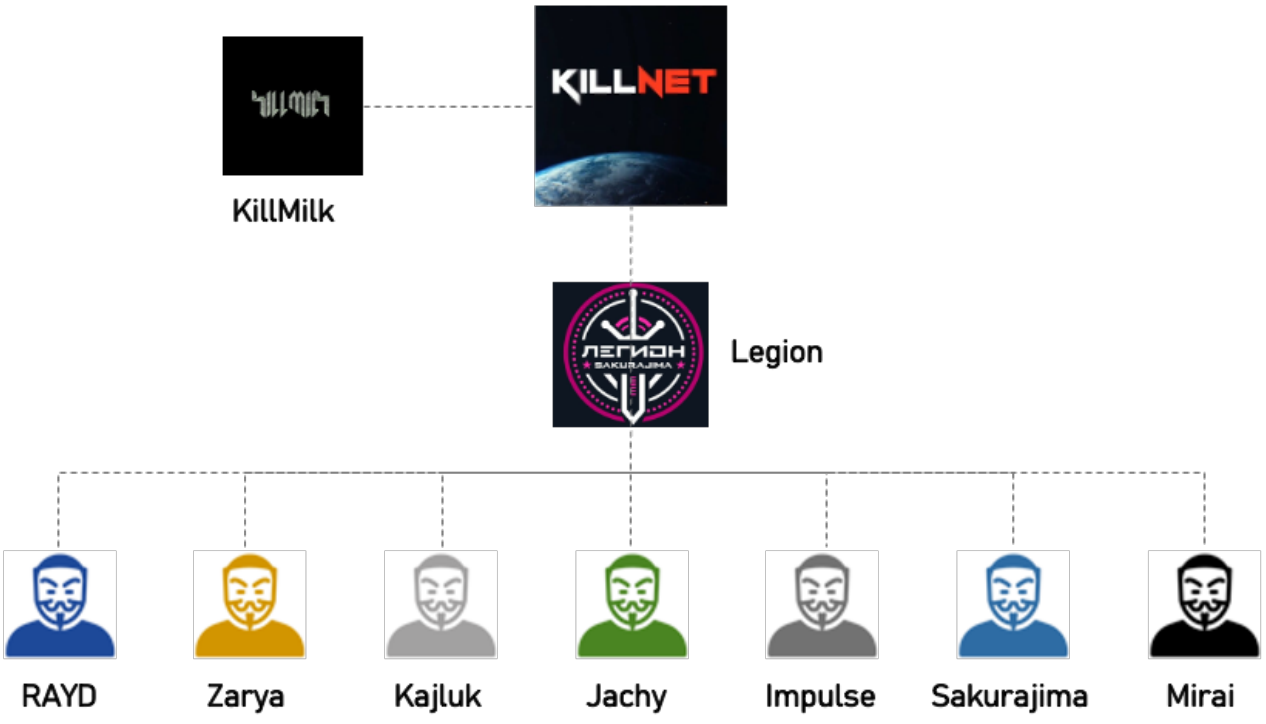

Fig. 7 - KillNet Order of Battle (ORBAT)

- *Non-State* o *Private actor* conosciuti - sono gruppi che hanno realizzato attacchi a favore della federazione russa, ma non sono strutturati o direttamente coordinati dall'*Intelligence* russa. I gruppi di questo tipo che hanno rivendicato cyber attacchi (generalmente DDoS e Hack&Leak) sono Phoenix, Russian Hackers Team, Anonymous Russia, Clowns, Red Hackers Alliance, RaHDIt e theMx0nday.
- *State actor* sconosciuti (o in via di attribuzione) - sono gruppi che sulla base della complessità delle tecniche impiegate negli attacchi è ragionevole ipotizzare siano *Nation-State*, ma la cui *attribution* (e in generale l'analisi delle TTP utilizzate) è ancora in corso. I gruppi che sono stati individuati sono UNC4166, C-0100, C-0041, C-0088, C-0094, C-0098, C-0132, C-0133, DEV-0586, InvisiMole, Vermin e Cloud Atlas.

Nella figura 8 vengono riportati, sulla base della precedente classificazione, gli attori sopra individuati.

In conclusione occorre riferire l'opinione della maggior parte degli osservatori occidentali, secondo i quali - nonostante il largo dispiegamento di gruppi di cyber attaccanti a favore della Russia - le operazioni informatiche russe non hanno avuto un grande impatto strategico in Ucraina; ma c'è meno consenso sulle motivazioni di questo fallimento.

Threat Actor russi operanti nel confitto russo-ucraino.

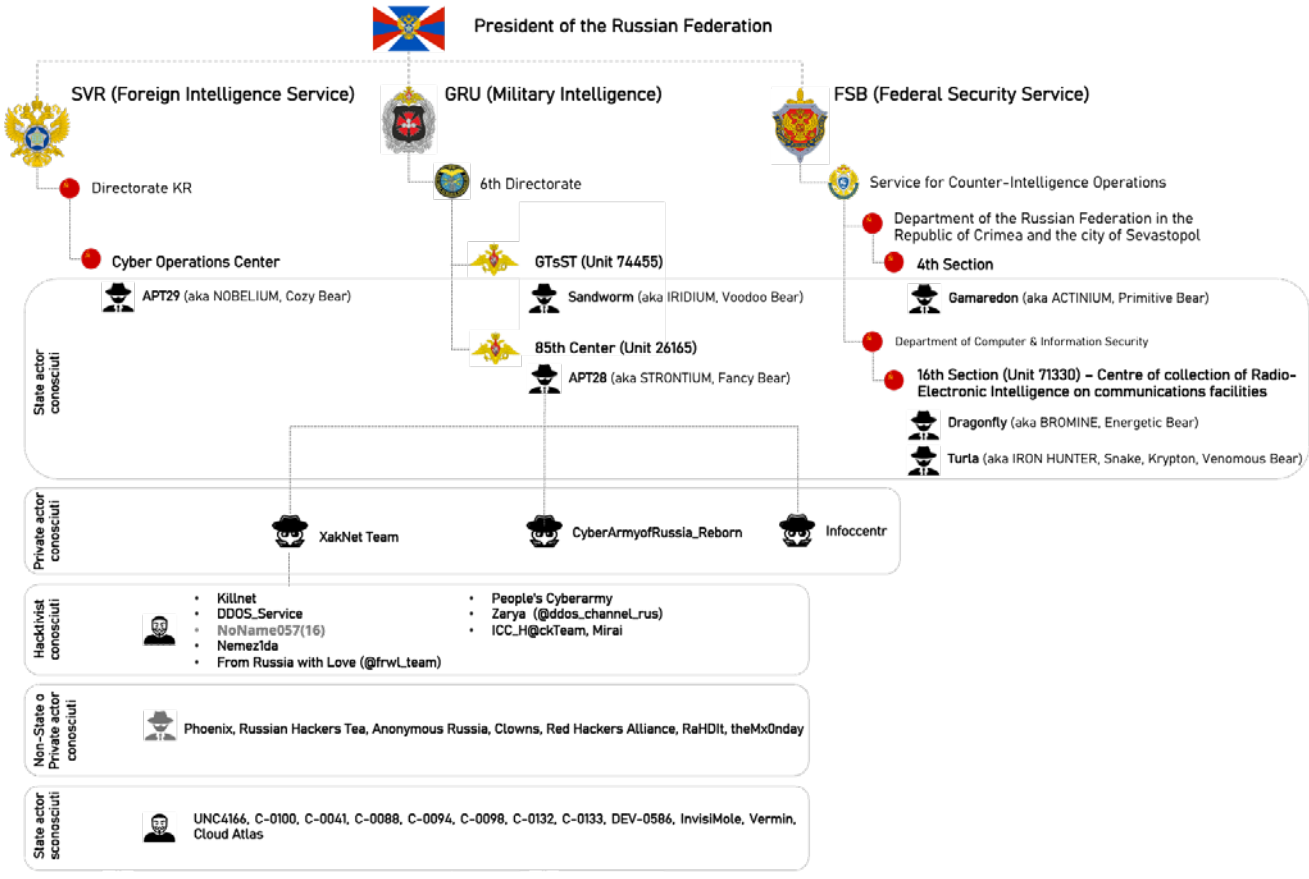

Fig. 8 - Principali Threat Actor coinvolti nei Cyber Attack & Operation

Alcuni analisti basano questa opinione sull'incapacità della Russia di sostenere nel tempo le frequenze degli attacchi informatici sferrati nelle prime settimane del conflitto. Inoltre occorre considerare che, anche durante il conflitto, la Russia ha continuato a svolgere attività di spionaggio informatico su larga scala e altre penetrazioni di rete su scala globale, lasciando quasi esclusivamente al GRU la guida delle azioni di *cyber offensive* contro l'Ucraina.

Naturalmente gli analisti, in aggiunta alle motivazioni appena fornite, sottolineano gli sforzi difensivi dell'Ucraina e dei suoi alleati.

Francesco Schifilliti, *Consulente in Cyber Security & Threat Intelligence*

BIOGRAFIA

Francesco Schifilliti

Esperto in sicurezza delle informazioni, *digital forensic* e *cyber threat intelligence* per grandi aziende. È stato il *Practice Manager* di F*orensic Technology & Discovery Services* (FTDS) in Fraud Investigation & Dispute Services (EY). Ricercatore nel campo di *Malware* e *Memory Analysis*, *Structured Analytic Procedures* (SAT), OSINT, *Intelligence Investigation Techniques, Incident Responding Techniques* e *Cyber Threat Intelligence*. Laureato in Informatica presso l'Università degli Studi di Catania, è docente in corsi e master in *digital forensics* e *malware forensics*.

Successi e fallimenti dell'intelligence nella guerra in Ucraina.

«Intelligence not only has to train new recruits but also to educate its customers. This is a formidable task... They have to be convinced of what intelligence can, and what it cannot achieve: they must learn that an overload of requests will result in diminishing returns; that intelligence should be taken into the confidence of policy-makers if these wish to obtain relevant information».

Walter Ze'ev Laqueur, 1986:34

L'OPINIONE PUBBLICA E L'INTELLIGENCE

L'*intelligence* non gode sempre di buona stampa, né di buona fama. A volte il discredito è dovuto a tecniche poche ortodosse impiegate nelle operazioni coperte o nei metodi di interrogatorio, di cui viene a conoscenza l'opinione pubblica; altre volte il discredito deriva dal fallimento delle operazioni stesse o della capacità di prevedere rischi o minacce future. I limiti delle capacità predittive dei sistemi di *intelligence* sono fisiologici, essendo impossibile prevedere esattamente e con certezza assoluta il comportamento futuro di persone dotate di autonome capacità decisionali e di libero arbitrio. Tuttavia persiste nell'opinione pubblica la convinzione ingenua che le agenzie di *intelligence* dovrebbero essere dotate del potere magico di anticipare con precisione assoluta l'opzione che sceglierà, tra le diverse alternative possibili che gli si presentano, un decisore politico. Spesso i giudizi ingenerosi sono causati proprio da aspettative irrealistiche e irraggiungibili della stampa e dell'opinione pubblica. È molto diffusa, ad esempio, la bizzarra convinzione che le conseguenze della frettolosa e maldestra ritirata del contingente NATO dall'Afghanistan sia dovuta a un "fallimento dell'*intelligence*", piuttosto che a un "fallimento della politica"[1]. In realtà l'*intelligence* non fornisce mai indicazioni predittive certe, ma ipotesi di sviluppo degli eventi che possono essere più o meno probabili. Il caso storico più citato (spesso a sproposito) a titolo di esempio è quello dei missile sovietici a Cuba, perché allora le agenzie governative americane (*«professional intelligence bureaucracies»*) avevano ritenuto molto improbabile ciò che invece accadde realmente (*«it would be incompatible with Soviet*

[1] *«Leading U.S. intelligence agencies failed to predict the rapid Taliban takeover of Afghanistan prior to the final withdrawal of American troops and instead offered scattershot assessments of the staying power of the Afghan military and government». Vivian Salama, Warren P. Strobel, Four U.S. Intelligence Agencies Produced Extensive Reports on Afghanistan, but All Failed to Predict Kabul's Rapid Collapse, wsj.com, October 28, 2021,* https://on.wsj.com/3IhZeeH.

policy to introduce strategic missiles into Cuba», come riporta il Rapporto Stennis [John Cornelius, 1901-1995] citato in Knorr)[2].

LA POLITICA E I "FALLIMENTI DELL'INTELLIGENCE"

D'altronde è abbastanza naturale e fisiologico che i fallimenti previsionali ci siano - e che non siano rari - in un campo caratterizzato da aleatorietà e incertezza. Nella storia dell'*intelligence* del secolo scorso i sovietici furono "sorpresi" dall'attacco tedesco nel 1941 (perché Stalin non volle credere alle informazioni corrette inviate da Richard Sorge, che era infiltrato nell'ambasciata tedesca di Tokyo) e i tedeschi furono sorpresi dallo sbarco alleato in Normandia (perché furono tratti in inganno da numerose ed efficaci operazioni alleate di disinformazione). Pearl Harbor è considerato un classico caso di scuola di "fallimento" dell'*intelligence* e di come i decisori politici furono colti di "sorpresa" dagli eventi[3]. Nel secondo dopoguerra, gli americani furono "sorpresi" anche dallo scoppio della guerra di Corea e poi dall'intervento cinese. E ancora più "sorprendenti" possono essere considerati gli attacchi al World Trade Center e al Pentagono del 9/11/2001[4]. Un altro celebre "fallimento dell'*intelligence*" è considerato il mancato ritrovamento delle armi di distruzione di massa nel caso della guerra all'Iraq di Saddam Hussein [1937-2006] dichiarata da George Walker Bush (Betts, 2007-08). Non ci si chiede però quanta pressione la Casa Bianca avesse esercitato sulle agenzie di *intelligence*, per ottenere qualche indizio che avvalorasse la tesi della presenza di queste armi e giustificasse l'intervento militare. Quando le cose non sono andate per il verso giusto, di solito sono le agenzie governative di *intelligence* ad essere criticate e a venir accusate di inefficacia o inefficienza. Di solito i primi che cercano di reindirizzare la responsabilità di un loro insuccesso verso le «burocrazie professionalizzate» dell'*intelligence* sono proprio i politici, che pensano di ottenere così dall'opinione pubblica l'assoluzione per gli errori che hanno commesso[5]. Scaricare tutte

[2] Del resto, come già scriveva Klaus Knorr sull'installazione dei missili sovietici a Cuba che minacciavano gli Stati Uniti, «*why did the intelligence community fail to warn the government earlier that such a Soviet move was distinctly possible, if not probable, instead of estimating that it was improbable, though not impossible?*» (Knorr, 1964:456).

[3] «*Pearl Harbor drove the idea of surprise attack so deeply into the American psyche that "Pearl Harbor" became almost a generic term for any sneak attack. The United States became surprise-attack conscious, and rightly so. After World War II, it was generally agreed that any future attack almost certainly would be in the nature of a surprise*» (Prange et alii, 1986:605). Infatti Pearl Harbor ebbe come conseguenza il rovesciamento del sentimento prevalente nell'opinione pubblica statunitense, che sino ad allora era rimasta ostile alla possibilità di un intervento militare diretto nella Seconda Guerra Mondiale. Solamente l'affondamento di una gran parte della flotta navale USA nel Pacifico convinse gli americani della necessità di entrare in guerra.

[4] Questa vicenda viene giustamente paragonata a una Pearl Harbor, persino più terribile della precedente, nell'immaginario collettivo d'oltreoceano.

[5] Il politologo Betts spiegava proprio così il processo decisionale di un evento che aveva colto tutto il sistema politico di "sorpresa", evidenziando l'immancabilmente spiegazione pubblica successiva, regolarmente imperniata sul "fallimento dell'*intelligence*". Le evidenze empiriche insegnano che «*in the best-known cases of intelligence failure, the most crucial mistakes have seldom been made by collectors of raw information, occasionally by professionals who produce finished analyses, but most often by the decision makers who consume the products of intelligence services. Policy premises constrict perception, and administrative workloads constrain reflection. Intelligence failure is political and psychological more often than organizational*» (Betts, 1978:61).

le responsabilità su di un "capro espiatorio" è la soluzione più semplice per eludere un problema. Lo ha fatto ad esempio il Presidente francese Macron, quando ha licenziato il capo dell'*intelligence* militare francese, Eric Vidaud, colpevole di non aver previsto l'invasione russa dell'Ucraina.

"FALLIMENTI DELL'INTELLIGENCE" IN UCRAINA

Il più delle volte questo rimpallo delle responsabilità assume anche una dimensione pubblica, tra i produttori di *intelligence* e i decisori politici, committenti e fruitori delle informazioni. Un esempio interessante riguarda proprio il teatro ucraino e le operazioni speciali condotte dal Cremlino nel corso del 2014, che produssero l'occupazione della Crimea. In un'udienza al Senato del 6 marzo 2014[6], il senatore John McCain [John Sidney III, 1936-2018) accusava il Segretario alla Difesa Chuck Timothy Hagel di una *«massive failure»* dell'*intelligence*[7] militare statunitense e dei funzionari dell'Amministrazione Obama, e di un *«total misreading of the intentions of (Russian President) Vladimir Putin»* nei giorni precedenti l'invasione della regione ucraina. A queste accuse Todd Ebitz, il portavoce della Central Intelligence Agency, ribatteva di aver fornito tutti gli *alert* possibili e necessari[8]. In realtà la strategia che permise alla Federazione Russa di annettere la Crimea, senza sparare un colpo, è considerata anche dagli esperti di studi strategici americani una delle più brillanti e "sorprendenti" operazioni di guerra asimmetrica che si siano mai viste. L'annessione della Crimea sarebbe da considerare un'operazione da manuale, oltre che un successo strategico della Federazione Russa, piuttosto che un fallimento dell'*intelligence*. Tutte le agenzie di *intelligence* occidentali erano consapevoli dell'intenzione di Vladimir Putin di riconquistare l'influenza sull'Ucraina, persa dopo i fatti di piazza Maidan e la destituzione del Presidente filorusso Viktor Janukovyč: ma nessuno immaginava che un'azione tempestiva e sinergica di *cyber warfare* e *info warfare*, l'impiego di agenti provocatori, quinte colonne, milizie irregolari e mercenari, potesse portare ad un'annessione di fatto dell'intera penisola di Crimea. Invece l'operazione fu un successo completo, e all'Occidente non rimase altro che la condanna dell'accaduto e l'adozione di un blando regime sanzionatorio.

INTELLIGENCE SHARING E INVASIONE DELL'UCRAINA

La diffusione pubblica, attraverso i mass media, delle informazioni relative ai piani russi di invasione militare dell'Ucraina è una novità assoluta, che merita una riflessione. Forse questa vicenda specifica

[6] Courtney Kube, U.S. *Spy Agencies Deny Failure on Crimea Seizure*, *nbcnews.com*, March 6, 2014, https://nbcnews.to/3ImkG1Y.

[7] *Intelligence* è un termine ampio riferito alle informazioni che le agenzie governative raccolgono, analizzano e distribuiscono in risposta alle domande e ai requisiti dei capi di governo: «*Collection, analysis, and production of sensitive information to support national security leaders, including policymakers, military commanders, and members of Congress. Safeguarding these processes and this information through counterintelligence activities. Execution of covert operations approved by the president*» (Rosenbach & Peritz 2009:10).

[8] «*Since the beginning of the political unrest in Ukraine, the CIA has regularly updated policymakers to ensure they have an accurate and timely picture of the unfolding crisis. […] These updates have included warnings of possible scenarios for a Russian military intervention in Ukraine. Any suggestion otherwise is flat wrong*».

inaugura anche un capitolo completamente nuovo nell'uso politico e diplomatico dell'*intelligence* negli affari internazionali, perché potrebbe essere il primo caso di impiego diretto di materiale informativo segreto nella costruzione di una strategia di consolidamento della propria alleanza internazionale e di isolamento dell'avversario. Riducendo ai termini essenziali la questione, potremmo sintetizzare dicendo che le informazioni di *intelligence* diffuse dalle agenzie statunitensi e britanniche hanno smascherato in anticipo, davanti all'opinione pubblica internazionale, ciò che la dirigenza russa ha cercato inutilmente di tenere segreto, cioè l'intenzione di condurre un'operazione militare cinetica su larga scala, che prevedeva l'invasione dei confini dello Stato ucraino, l'occupazione di una parte di esso, il rovesciamento del Governo legittimo e la sua sostituzione con un nuovo Governo fantoccio guidato da Mosca. Una cosa molto diversa da quanto accadde nel 2014 con l'occupazione della Crimea, che come si diceva è da considerare un'operazione perfettamente riuscita di guerra ibrida. L'occupazione della Crimea fu un successo pieno perché colse alla sprovvista l'Occidente, che non era preparato a reagire a un'iniziativa di questo tipo e di questa portata. Ma l'effetto sorpresa funziona solamente la prima volta.

LA "GUERRA NELLE ZONE GRIGIE"

La caratteristica principale della "guerra nelle zone grigie", come viene definita dalla cosiddetta "dottrina Gerasimov", è la sua ambiguità, che la rende difficilmente comprensibile e attribuibile grazie all'impiego prevalente - se non esclusivo - di mezzi non militari: attacchi cyber, disinformazione, *PsyOp*[9] nell'ambito della guerra dell'informazione, uso di milizie locali impiegate come *proxy* e sostenute esclusivamente da mercenari, o da "omini verdi" senza insegne sulla divisa. La preferenza strategica per questa nuova forma di conflitto, dimostratasi vincente, poteva trarre in inganno l'*intelligence* occidentale, facendo pensare che la dirigenza russa avrebbe escluso l'impiego di attività militari cinetiche con mezzi convenzionali, a favore di una strategia di lungo periodo volta alla destabilizzazione interna dell'Ucraina. Il successo in Crimea aveva infatti portato la Federazione Russa a proseguire nell'impiego della medesima strategia, allargando il contagio alle aree Est dello Stato ucraino, più densamente abitati da russi. Ma senza il vantaggio dell'effetto sorpresa l'impiego della tattica basata sull'interazione tra mezzi militari asimmetrici e mezzi non militari, adottata con pieno successo in Crimea, non ha portato a ottenere gli stessi risultati nel Donbass, che è rimasto per ben otto anni in una condizione di stallo e guerriglia tra l'esercito regolare ucraino e le milizie indipendentiste filorusse.

PERCHÉ PUTIN HA INVASO L'UCRAINA?

Si può presumere che il motivo per cui Vladimir Putin abbia scelto di invadere l'Ucraina, impiegando mezzi militari convenzionali e soldati di leva, sia proprio

[9] PSYOP sta per *PSYchological OPerations* e può essere definito come l'insieme delle operazioni pianificate allo scopo di trasmettere specifiche informazioni e indicazioni a destinatari di altra nazione per influenzare le loro emozioni, motivazioni, ragionamenti e, in ultima analisi, per manovrare il comportamento di governi stranieri, organizzazioni, gruppi di persone o individui, in modo strumentale alle necessità del committente delle operazioni.

l'insoddisfacente paralisi di quella iniziativa. Era ormai chiaro che ripetere il successo ottenuto in Crimea nelle altre aree del territorio ucraino fosse impossibile, e che lo stallo consolidato stesse producendo il fallimento di fatto dell'iniziativa russa, rimasta ormai senza sbocco. A quel punto forse Putin avrà pensato che la mossa che poteva cogliere più impreparati gli avversari poteva essere proprio quella più ovvia, cioè il ritorno alle forme della guerra novecentesca e quindi l'invasione del territorio nemico, con una distruzione preventiva dei centri di comando e controllo, delle difese aeree e la successiva occupazione del territorio con la fanteria e i mezzi corazzati.

Naturalmente preparare questa operazione comportava la necessità di portare lungo i confini ucraini molte più truppe di terra e carri armati di quanto qualsiasi esercitazione avrebbe potuto giustificare. Putin sapeva benissimo che l'*intelligence* militare occidentale avrebbe evidenziato questa presenza, perché è impossibile nascondere più di 80 mila uomini in assetto di guerra con tanto di mezzi corazzati e la catena logistica necessaria a rifornire un'invasione, grazie all'osservazione dei satelliti e dei droni *global hawks*, o di aeroplani tradizionali, dotati della più avanzata tecnologia di intercettazione di segnali elettronici.

Tuttavia la scommessa di Putin confidava proprio su questo: gli Occidentali sanno della minaccia di invasione ma penseranno che sia soltanto una minaccia, finalizzata a esercitare una pressione psicologica sul Governo ucraino, per costringerlo a una trattativa diplomatica in posizione di debolezza. La simulazione di un bluff che potremmo sintetizzare così: *"Tu sai che io so che tu sai"*.

"TU SAI CHE IO SO CHE TU SAI"

Questo avrebbe dovuto portare alla condivisione riservata delle informazioni di *intelligence* tra le potenze occidentali e il Governo ucraino, e alla condivisione della serietà e pericolosità della minaccia russa. Questa condivisione avrebbe portato tutti i Governi dell'Occidente a credere che l'intenzione reale dei russi potesse essere l'irragionevole impiego di questi mezzi militari per occupare il territorio ucraino?

Putin, forse ricordando la celebre espressione del suo predecessore Vladimir Lenin, il quale sosteneva che *"i capitalisti ci venderanno la corda con cui li impiccheremo"*, confidava che gli alleati europei degli Stati Uniti, soprattutto quelli più legati alla Federazione Russa per i propri approvvigionamenti energetici, avrebbero fatto di tutto per scongiurare il rischio di subire le conseguenze economiche disastrose di un possibile conflitto, al quale non avrebbero voluto credere.

Questo avrebbe permesso alla Russia di trarre nuovamente vantaggio dalla paralisi delle capacità di reazione occidentale, di fronte a un'iniziativa militare poco ragionevole e con modeste possibilità di successo. Per la Russia la guerra in Ucraina è irragionevole, fin dall'inizio. Ma proprio perché irragionevole gli analisti l'avrebbero giudicata improbabile; e questo avrebbe consentito di avere nuovamente il vantaggio della sorpresa. In altre parole, era ragionevole confidare in un errore di valutazione, un "fallimento dell'*intelligence*" e della politica dell'Occidente.

IL PIANO DI PUTIN

Il piano era, dunque, la *Blitzkrieg* (guerra lampo) per conquistare l'Ucraina e annetterla alla Russia? Non credo. Il territorio ucraino è troppo ampio per essere annesso e controllato senza l'impiego permanente e prolungato di almeno centomila uomini: uno sforzo militare ed economico difficilmente sostenibile per un Paese cha ha un PIL inferiore a quello della Spagna. Ma il 20% della popolazione ucraina è russofona, di origine russa, filorussa. Per ragioni storiche non potevano non esserci legami tra gli ufficiali delle forze armate ucraine e di quelle russe; perché fino a tre decenni fa appartenevano entrambe al Patto di Varsavia, si formavano e si addestravano insieme, parlavano la stessa lingua, studiavano la stessa dottrina militare, usavano gli stessi sistemi d'arma. Se questa antica affinità aveva permesso a ufficiali del Mali, addestrati a Mosca, di prendere il potere e insediare una giunta militare in quel Paese con un colpo di Stato, perché questo non poteva funzionare anche in Ucraina?

Se dopo qualche giorno di guerra con la superpotenza nucleare russa un colpo di Stato interno alle forze armate ucraine avesse deposto il Presidente Zelensky, per sostituirlo con un burattino di Mosca, sarebbe stato molto difficile per l'Occidente intervenire per evitare che l'Ucraina tornasse nell'orbita di influenza russa. Un'Ucraina subalterna, come la Bielorussia, sarebbe stata molto più gestibile di un territorio occupato militarmente.

LA GUERRA NON VA MAI SECONDO I PIANI

Però il piano di "tovarish Platov" è fallito. Compagno Platov era il nome in codice di Vladimir Putin quando era un tenente colonnello del KGB nella DDR, a Dresda. Allora leggeva Clausewitz e sapeva bene che nella guerra le cose non vanno mai secondo i piani.
Infatti tre cose sono andate diversamente da quanto ci si sarebbe potuti aspettare (anche questo è un fallimento dell'*intelligence* e della politica russa).

1. L'Occidente non si è diviso. La dipendenza di molte economie europee dalle forniture energetiche russe e le importanti opportunità che il mercato di sbocco russo offre per le aziende europee in settori come la moda, il turismo o l'*automotive* non hanno prodotto una frattura politica all'interno della Nato, come Putin si aspettava. Tutti i Paesi occidentali hanno condannato l'invasione, adottato sanzioni contro la Federazione Russa e fornito aiuti militari all'Ucraina;
2. questo ha consentito al Governo Zelensky di organizzare una resistenza efficace, che ha messo a dura prova le capacità militari russe, sopravvalutate dal Cremlino stesso. Le forze armate ucraine erano state preparate e addestrate da tempo in vista di una minaccia di questo tipo, che l'*intelligence* occidentale (soprattutto USA e GBR) aveva previsto come possibile. Le capacità acquisite e gli aiuti militari occidentali hanno prodotto sul campo una condizione di equilibrio difficilmente immaginabile all'inizio;

3. complessivamente questa situazione ha vanificato la speranza di Putin nel rovesciamento interno del regime, che probabilmente avrebbe avuto successo se vi fosse stato un governo allo sbando, con Zelensky in fuga per salvarsi la vita. Se nelle forze armate ucraine si nascondevano traditori, che avevano preso preventivamente accordi con i russi, non sono mai emersi, o sono stati individuati ed eliminati precocemente. La politica filorussa in Ucraina è sostanzialmente scomparsa dalla scena, perché l'invasione del territorio l'ha eliminata. È l'eterogenesi dei fini, si potrebbe concludere.

INTELLIGENCE TRA SEGRETEZZA E CONDIVISIONE

Ma che importanza ha avuto nel determinare gli eventi accaduti lo *sharing* diffuso all'opinione pubblica delle informazioni di *intelligence*?

Il valore dell'*intelligence* è sempre stato legato alla sua segretezza. Le agenzie di *intelligence* concepiscono il loro lavoro sapendo che un'informazione ha tanto più valore quanto meno è conosciuta. Se l'avversario non immagina che conosciamo alcune informazioni sul suo conto, non potrà adottare misure conseguenti: per questo le dobbiamo tenere segrete. Durante la Seconda Guerra Mondiale, quando Alan Turing riuscì a decifrare il codice Enigma con il quale la Germania nazista comunicava ai sommergibili U-boat la posizione dei convogli navali che rifornivano la Gran Bretagna da oltreoceano, gli Alleati rinunciarono a salvare tutte le navi perché i tedeschi non capissero che le loro comunicazioni non erano più segrete. In caso contrario avrebbero cambiato i codici e privato, quindi, gli Alleati del vantaggio competitivo di poter comprendere le trasmissioni che riuscivano a intercettare. Questo non significa che le agenzie di *intelligence*, come gli Stati, non si scambino informazioni riservate. In genere però lo fanno salvaguardandone la segretezza. Per la prima volta l'opinione pubblica mondiale invece è stata informata direttamente, attraverso i mezzi di comunicazione di massa, dell'intenzione russa di invadere l'Ucraina. La scelta di pubblicizzare l'*intelligence* non può essere casuale.

CONDIVISIONE DI INTELLIGENCE E GUERRA DELL'INFORMAZIONE

Non abbiamo la controprova e quindi non possiamo sapere che orientamento avrebbe tenuto il governo di quei Paesi europei che più avevano da perdere dalla rottura dei rapporti di scambio economico con Russia. Non possiamo sapere se la riservatezza delle informazioni di *intelligence* avrebbe favorito un atteggiamento più prudente e attendista o meno. Tuttavia, appare evidente che la diffusione di alcune informazioni relative al posizionamento delle truppe russe lungo i confini ucraini e il fatto che questo preludesse all'invasione, è parte di una guerra dell'informazione che ha messo in difficoltà l'espertissimo e abile Ministro degli Esteri Russo, Sergej Lavrov e la sua portavoce Maria Zakharova. Al tempo stesso, appare abbastanza evidente che nella complessità del conflitto ucraino si assiste all'impiego di risorse del massimo livello nell'*infowarfare.*

INFOWARFARE

Peter Pomerantsev (autore di *Niente è vero, tutto è possibile* e di *Questa non è propaganda*) e numerosi altri autori hanno studiato ed evidenziato la potenza e l'efficacia, a livello globale, della potente macchina della propaganda russa. Secondo Paul Gallagher dell'Independent *"centinaia di lavoratori sono pagati circa 500 sterline al mese e sono obbligati a scrivere almeno 135 commenti al giorno, oppure subire il licenziamento immediato"*[10]. Secondo altre fonti, il governo russo ha fatto largo uso non solo dei forum ma anche dei social network, ad esempio a supporto della propria posizione nella crisi ucraina, in quel caso proprio per cercare di influenzare la popolazione ucraina screditando il governo di Kiev[11]. L'Occidente però ha contrapposto un'iniziativa altrettanto efficace, coinvolgendo le migliori agenzie di pubbliche relazioni occidentali. In questo contesto, la trasparenza pubblica delle operazioni di divulgazione pubblica di alcuni prodotti dell'*intelligence* non ha solamente reso possibile rivelare, contestare e mettere in guardia la popolazione civile dai preparativi e dalle intenzioni bellicose della Federazione Russa nelle settimane immediatamente precedenti l'invasione, ma ha soprattutto permesso di contrastare le sue operazioni psicologiche e strategie di *infowarfare*. Nelle *PsyOp* entrambi gli schieramenti integrano *intelligence* e guerra dell'informazione, perché le informazioni di *intelligence* forniscono le basi necessarie a calibrare la strategia informativa e manipolativa, e sono anche materiale oggetto di divulgazione. Il target di queste operazioni è direttamente l'opinione pubblica globale, quindi non solamente quella avversa ma anche quella interna e dei Paesi alleati. Produrre *sentiment* nell'opinione pubblica significa condizionare le decisioni dei Governi nazionali e creare le condizioni migliori per ottenere gli obiettivi strategici pianificati. Non farlo significherebbe assumere il rischio che le iniziative informative avversarie abbiano successo e producano gli effetti desiderati di confusione, destabilizzazione, disorientamento dell'opinione pubblica stessa. Questo potrebbe persino compromettere la solidità di un'alleanza politica e militare e condizionare il destino del conflitto.

NON TUTTA L'INTELLIGENCE È STATA RESA PUBBLICA

Ovviamente, se la diffusione dell'*intelligence* è funzionale a condizionare l'opinione pubblica ed è quindi uno strumento di guerra dell'informazione, vengono diffuse e condivise soltanto le informazioni utili e funzionali a questo scopo. Le altre rimangono segrete. Ma nel conflitto ucraino l'attività di *intelligence* è molto più intensa

[10] Sempre secondo Gallagher *"la struttura è semplice. Una volta che una vicenda viene pubblicata su un forum di informazione locale l'esercito dei troll va a al lavoro dividendosi in squadre composte da tre elementi: uno gioca il ruolo del 'cattivo' criticando le autorità mentre gli altri due discutono con esso e forniscono supporto agli ufficiali del governo. Uno dei troll pro-Kremlino deve fornire un'immagine o una foto a suffragio della propria ipotesi e l'altro compagno di squadra inserisce un link a qualche contenuto che supporti i suoi argomenti"*. https://www.independent.co.uk/news/world/europe/revealed-putins-army-of-pro-kremlin-bloggers-10138893.html.

[11] https://www.abc.net.au/news/2015-08-12/inside-russias-troll-factory-internet-forums-social-media/6692318.

di quanto è stato divulgato e ha plasmato il conflitto, perché la collaborazione con i servizi segreti occidentali ha permesso a quelli ucraini di disporre delle informazioni necessarie a tenere a bada l'orso russo, benché fosse molto più dotato di armamenti e risorse. L'*intelligence* russa è storicamente molto presente in Ucraina, ha studiato il terreno e avviato le operazioni di penetrazione; ma anche l'*intelligence* occidentale era attenta e impegnata da tempo a sostegno di quella ucraina. Ha monitorato l'addensamento delle truppe russe al confine, come ha reso pubblico la stessa Amministrazione Biden che si è irritata per la diffusione di altre notizie relative al contributo dello spionaggio statunitense. Secondo quanto recentemente rivelato dal NYT, ad esempio, l'uccisione di una quindicina di generali russi non sarebbe stata possibile senza la loro geolocalizzazione, ottenuta dall'*intelligence* americana attraverso il traffico telefonico. Anche per il fallimento dello sbarco russo a Hostoml e dell'operazione degli incursori paracadutisti russi che avrebbero dovuto uccidere Zelensky è stato determinante l'intervento dell'*intelligence* occidentale. Lo stesso si può dire per l'attacco ucraino del 12 agosto, che portò alla distruzione del comando del Wagner Group.

IL CONTRIBUTO DELLE AZIENDE DEL SETTORE ICT, DELLE SOCIETÀ PRIVATE DI INTELLIGENCE E DELLE PRIVATE SECURITY COMPANY

Analizzare il contributo delle attività di *intelligence* isolandolo dall'insieme delle operazioni militari e non militari che caratterizzano il contesto bellico ucraino è insensato e impossibile. La componente cinetica della guerra è stata orientata e guidata da *intelligence* prodotta da agenzie di molti Paesi, alcune delle quali a sostegno della Russia e altre dell'Ucraina. Altrettanto importante però, se non di più, è il contributo che queste hanno fornito e forniscono alle componenti non cinetiche della guerra. Basti pensare all'importanza della collaborazione tra le agenzie governative americane e compagnie private, come Facebook o Twitter, per la cancellazione di migliaia di account che diffondevano in rete la propaganda filorussa. Infatti, come l'*intelligence* russa è impegnata nel controspionaggio e nella disiniformazione, così lo sono anche quella ucraina, quella occidentale e persino le società di *intelligence* private. È trapelata la notizia, ad esempio, che la società di *intelligence* privata Anomaly 6, che attraverso la compagnia Prevail Partners collabora con l'esercito britannico, avrebbe fornito informazioni ottenute per mezzo di un suo software di tracciamento e sorveglianza, che sarebbe incorporato nelle applicazioni più diffuse, per analizzare dati e ricostruire informazioni sensibili sul proprietario

[12] L'uso massiccio di telefoni cellulari, nonostante il divieto, è la ragione principale delle perdite subite d'esercito russo a Makiivka. Lo ha affermato il primo vice capo della Direzione principale politico-militare delle forze armate della Federazione Russa, il tenente generale Sergei Sevryukov: "*Questo fattore ha permesso al nemico di localizzare e determinare le coordinate della posizione del personale militare per lanciare un attacco missilistico [...] Sono state prese le misure necessarie per prevenire tali tragici incidenti in futuro*". Secondo le sue dichiarazioni, dopo le indagini i funzionari colpevoli saranno puniti. In precedenza, il Ministero della Difesa ha chiarito che il numero dei militari morti era salito a 89.

di un dispositivo connesso alla rete. Monitorando in questo modo lo smartphone di ogni possibile target sarebbe stato possibile fornire una miniera di informazioni utili alle organizzazioni clandestine ucraine, che per conto dell'*intelligence* di Kiev avrebbero pianificato offensive militari[12], attacchi di artiglieria, omicidi mirati, reclutamento di risorse e azioni di sabotaggio, come l'attentato al ponte di Kerch.

Alberto Pagani, *Docente all'Università di Bologna e advisor nel settore della sicurezza*

RIFERIMENTI

1. *Analysis, War, and Decision. Why Intelligence Failures Are inevitable, World Politics*„ v. 31, n. 1, October, pp. 61-89, Betts Richard Kevin (1978).

2. *Two Faces of Intelligence Failure. September 11 and Iraq's Missing WMD, Political Science Quarterly*, v. 122, n. 4, Winter, pp. 585-606, Betts Richard Kevin (2007-08).

3. *The Craft of Intelligence,* New York (NY), Harper and Row, Dulles Allen W. (1963).

4. *Failures in National Intelligence Estimates. The Case of the Cuban Missiles, World Politics,* v. 16, n. 3, April, pp. 455-467, Knorr Klaus (1964).

5. *Spying and Democracy. The Future of Intelligence, Current*, March/April, n.281, pp. 25-34, Laqueur Ze'ev Walter [1921-2018] (1986).

6. *Pearl Harbor, The Verdict of History,* New York (NY), McGraw-Hill, Prange Gordon W., Donald M. Goldstein, Katherine V. Dillon (1986).

7. *Confrontation or Collaboration? Congress and the Intelligence Community,* Belfer Center for Science and International Affairs, Harvard Kennedy School, June 12, p. 116, Rosenbach Eric, Aki J. Peritz (2009)

BIOGRAFIA

Alberto Pagani

Docente all'Università di Bologna e *advisor* nel settore della sicurezza; è stato parlamentare dal 2013 al 2022, prima in Commissione trasporti e telecomunicazioni, poi capogruppo PD in Commissione Difesa e delegato nell'Assemblea Parlamentare della NATO. Laureato in Scienze politiche all'Università di Bologna, 70° corso IASD del Centro di Alti Studi della Difesa, Master di II livello in "Strategia globale e sicurezza" della SUISS di Torino, Corso di perfezionamento in "Intelligence e sicurezza nazionale" dell'Università di Firenze in convenzione con il DIS. È stato amministratore pubblico e dirigente politico, ha insegnato nella facoltà di Sociologia dell'Università di Urbino.

“Intelligence does not have to be secret to be valuable”.
Sì, ma solo fino a un certo punto

Sono ormai diversi anni che si parla della rilevanza dell’*Open Source Intelligence* (OSINT) anche al di fuori degli ambiti istituzionali in cui questa branca dell’*Intelligence* ha avuto origine.

Oggi, come è noto, la disciplina è utilizzata da un’ampia gamma di professionisti e aziende, oltre ad associazioni e collettivi con finalità sociali che svolgono investigazioni digitali finalizzate, ad esempio, a contrastare il traffico di essere umani, la violazione dei diritti umani e la disinformazione digitale, o ancora ad accertare la condotta di crimini contro l’umanità o a monitorare aree di conflitto.

Nonostante l’ampio utilizzo in molteplici settori, non esiste una definizione ufficiale e condivisa di OSINT. Tra le svariate definizioni disponibili è però possibile identificare quattro elementi caratterizzanti:

- la creazione di conoscenza “*actionable*”, tipica di ogni attività di *Intelligence*, ovvero una conoscenza non fine a sé stessa, utile a innescare un processo decisionale che non è solo attribuibile al *customer* bensì a tutta la “filiera produttiva” dell’*Intelligence*. Infatti assume molte decisioni, implicitamente, anche chi ricerca o analizza le informazioni, ad esempio in merito al valore da attribuire alle fonti ovvero alle informazioni stesse;
- l’assenza di segretezza, perché le informazioni che vengono acquisite (seppur con diverse tipologie di accesso) devono essere pubblicamente disponibili;
- la liceità delle informazioni acquisite, che quindi non devono essere state ottenute attraverso metodologie illegali;
- la possibilità di creare conoscenza attraverso l’acquisizione di informazioni relative a ogni luogo, individuo e organizzazione, anche distanti migliaia di chilometri, con costi relativamente contenuti.

Per quanto invece attiene gli aspetti più “procedurali”, al pari di qualsiasi attività di *Intelligence*, l’OSINT si sviluppa attraverso un classico processo di *problem solving* - attivabile in presenza di un’esigenza informativa da soddisfare attraverso la ricerca di informazioni - che si esplica in 4 passaggi essenziali: la selezione delle fonti, la valutazione delle informazioni, un aggiornamento costante che consenta di poter sfruttare sempre i *tool* più aggiornati e, infine, la capacità di riuscire a pensare “*out of the box*”.

È evidente che, in un mondo caratterizzato da un sovraccarico informativo senza precedenti, ciascuno di questi passaggi presenta importanti livelli di complessità che non possono essere ignorati. **Infatti, un conto è saper utilizzare strumenti**

che ci consentano di ricercare e acquisire dati; altro è analizzare le informazioni trasformandole in *Intelligence*, soprattutto in una prospettiva previsionale. Parliamo, in estrema sintesi, non solo di competenze ma anche di attitudini differenti. Quindi, a titolo esemplificativo, un conto è verificare attraverso strumenti *open source* se una notizia è *fake*, altro è comprendere le ragioni per cui la stessa notizia sia stata inserita all'interno di un circuito informativo. Pertanto, parlare di *open source* in una prospettiva di *Intelligence* significa prima di tutto saper governare un processo metodologico che ci consenta di comprendere:

- se le informazioni acquisite sono rilevanti rispetto alle nostre specifiche esigenze informative;
- se tali informazioni sono accurate e quanto, in mancanza di accuratezza, si corre il rischio di colmare le lacune informative con ipotesi pregresse non verificate, spesso accompagnate da *bias* cognitivi, culturali e organizzativi;
- se ci si possa trovare all'interno di un contesto di disinformazione e inganno.

A valle di questa doverosa premessa il ruolo assunto dall'OSINT, specie nell'ambito del conflitto ucraino, rimane comunque indiscutibile.

Come ricorda Eliot Higgins, fondatore di Bellingcat[1], è dal conflitto siriano che abbiamo assistito ad un utilizzo sempre più estensivo dell'OSINT: "*everything that happened in Syria, as well as what happened in Ukraine between 2014 and 2017, really laid the groundwork for what is happening today […] It was basically in Syria where we learned all the processes we are now using with Ukraine*"[2].

È indubbio che la guerra in Ucraina ha visto un utilizzo senza precedenti di immagini, filmati e informazioni che, acquisite e pubblicate in tempo reale, continuano ad influenzare il conflitto in corso.

In questo senso, a una prima lettura superficiale potrebbe apparire corretta e premonitrice la frase "*Intelligence does not have to be secret to be valuable*", apparsa per la prima volta in un articolo[3] a firma di Vee Herrington, finalizzata a esaltare la rilevanza che l'OSINT riveste nell'ambito delle attività informative.

In realtà, pur riconoscendo l'evidente valore che riveste la capacità di ricercare informazioni pubblicamente disponibili con strumenti *open source*, bisogna fare attenzione e non commettere l'errore di credere che l'OSINT possa sostituire l'*Intelligence* tradizionale, soprattutto quando questa è svolta dagli apparati istituzionali. Sarebbe solo un'illusione, perché ciò che contraddistingue l'*Intelligence* è cercare di comprendere le intenzioni dei nemici, dei *competitor* o dei gruppi terroristici e/o criminali che si è chiamati di volta in volta a fronteggiare.

[1] L'uso Collettivo internazionale indipendente di ricercatori, investigatori e cittadini che utilizza l'*open source* e le indagini sui social media per indagare su una varietà di argomenti: dai signori della droga messicani e i crimini contro l'umanità, al monitoraggio dell'uso di armi chimiche e dei conflitti in tutto il mondo.

[2] https://www.dw.com/en/open-source-investigators-syria-ukraine/a-61236760.

[3] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj7kdLkxYH9AhXG_KQKHQ9B2kQFnoECAoQAQ&url=https%3A%2F%2Ffas.org%2Firp%2Fagency%2Farmy%2Fmipb%2F2005_04.pdf&usg=AOvVaw3TPCe4Y_Hv5S0JaxCDGtXq

“Intelligence does not have to be secret to be valuable”.

Intenzioni che per loro stessa natura sono “intangibili”, quindi difficilmente anticipabili e prevedibili con strumenti *open source* che risultano essere invece molto efficaci per osservare le capacità[4] delle realtà oggetto di interesse. Per comprendere con maggiore chiarezza questo concetto può essere utile ripercorrere la cronologia di alcuni “passaggi informativi” che hanno preceduto l’attacco russo. Tra la fine di marzo e gli inizi di aprile 2021, quindi ben prima dell’invasione (iniziata il 24 febbraio 2022), il giornalista del New York Times Christian Triebert[5] ha pubblicato sul suo profilo Twitter[6] (figura 1) alcune immagini satellitari della Maxar Technologies Inc[7]. Nello specifico, le immagini sembravano indicare la presenza di veicoli militari russi nella regione di Voronezh, circa 250 km dal

Fig. 1

territorio ucraino. Contestualmente, gli analisti del Conflict Intelligence Team (CIT)[8] hanno analizzato video e foto provenienti dai *social media* e, avvalendosi anche del *database* russo Gdevagon, sono riusciti a tracciare i percorsi dei vagoni utilizzati per movimentare i mezzi militari grazie ai numeri identificativi univoci scritti sulle carrozze[9]. Come riportato dagli stessi analisti del CIT sulle pagine di The Insider[10], i movimenti registrati in quei giorni, pur definiti come "senza precedenti dal 2015", non sono stati sufficienti a dimostrare l'intenzione della Russia di invadere l'Ucraina. Si sarebbe potuto trattare, infatti, di attività esercitative o ancora di una dimostrazione di forza finalizzata a mettere pressione alla comunità internazionale in merito al "presunto" allargamento della NATO ad est o ancora, aggiungiamo, a movimenti logistici.

Nello stesso periodo, gli analisti di JANES in un loro *assessment*[11] hanno evidenziato che "*While **Russia's intentions are still unclear**, this movement stands out as possibly the largest unannounced movement of troops since Russia's invasion of Crimea and eastern Ukraine in 2015. Video footage shows trains carrying Russian troops are still heading to the area of operations, with some according to the freight tracking service GdeVagon not scheduled to arrive in Crimea until mid-April. **Current indicators suggest it is unlikely the forces deployed to the border are in an offensive posture.**"*

In questo caso, in una modalità che si ritiene assolutamente corretta, gli analisti si sono limitati a valutare ciò che potevano osservare, esprimendo quindi come poco probabile una postura offensiva delle unità russe schierate lungo il confine.

Come ben noto, la situazione ha subito un'accelerazione importante a partire dai primi giorni

[4] Capacità e intenzione sono i due fattori che, contestualmente alla conoscenza del contesto di riferimento e alla valutazione delle fonti e delle informazioni disponibili, ci consentono di esprimere una valutazione della minaccia.

[5] Già appartenente al gruppo Bellingcat, considerato tra i più importanti gruppi di giornalisti investigativi, specializzato in *fact-checking* e *Open Source Intelligence*.

[6] https://twitter.com/trbrtc/status/1380069652584230914?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwtem%5E1380069652584230914%7Ctwgr%5Ea44b666f199d8d4df36486e4c60f1edc9413c4c3%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fciteam.org%2Fru-military-camp-near-ukraine.html.

[7] Azienda impegnata nella fornitura di immagini terrestri ad alta risoluzione, applicazioni informative geospaziali avanzate, infrastrutture spaziali, robotica, sottosistemi e soluzioni informative agli operatori satellitari e agenzie governative, tra cui il Governo Civile, la Difesa, l'*Intelligence* degli Stati Uniti e numerose altre realtà statali e commerciali a livello internazionale.

[8] Organizzazione investigativa indipendente, originaria della Russia, che conduce indagini open source sugli eventi che si verificano durante i conflitti armati, in particolare sulle azioni delle truppe russe in Ucraina, Siria, Libia e Repubblica Centrafricana. Insieme a Bellingcat e InformNapalm, è uno dei maggiori gruppi di questo tipo emersi durante la guerra russo-ucraina. Il gruppo collabora con i principali media mondiali che pubblicano le sue indagini, tra cui BBC, Reuters, Sky News e Der Spiegel (fonte: https://en.wikipedia.org/wiki/Conflict_Intelligence_Team).

[9] https://citeam.org/ru-military-camp-near-ukraine.html.

[10] https://theins.ru/en/politics/240830.

[11] https://www.janes.com/defence-news/news-detail/russian-ground-troop-units-and-iskander-ballistic-missiles-identified-at-ukrainian-border-by-janes.

“Intelligence does not have to be secret to be valuable”.

di dicembre 2021, quando sono emerse ulteriori informazioni relative ad afflussi sempre più consistenti di unità russe al confine con l’Ucraina. Talmente consistenti che il 3 dicembre del 2021, alle 1:54 P.M. EST, Jen Psaki - all’epoca portavoce della Casa Bianca - è arrivata a esprimere la preoccupazione degli Stati Uniti circa l’intenzione di Putin di invadere l’Ucraina: *“And we want to make sure that we are prepared. We know what President Putin has done in the past. We see that he is putting in place the capacity to take action in short order. And should he decide to invade, that is why we want to be prepared and — in an area we have expressed serious concern about.”* E ha proseguito *“we can’t predict from here what President Putin’s calculus is or what the Russians’ calculus is.”*[12] Ancora una volta ritroviamo il fattore “intenzione” come dichiaratamente non prevedibile, seguito da un altro elemento che possiamo definire concorrente ma non determinante nell’ambito della valutazione della minaccia: i precedenti. *“We saw what they did in 2014. We’ve seen what they’re doing on the border. And we’re going to consult with our allies and partners and Congress here to be prepared for a range of options.”*

Lo stesso giorno, alle 7:00 P.M. EST, dopo appena 5 ore dalla conferenza alla Casa Bianca, il Washington Post ha titolato sul proprio sito *“Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns”*[13], pubblicando un documento non classificato indicato come proveniente dall’*Intelligence* USA (figu-

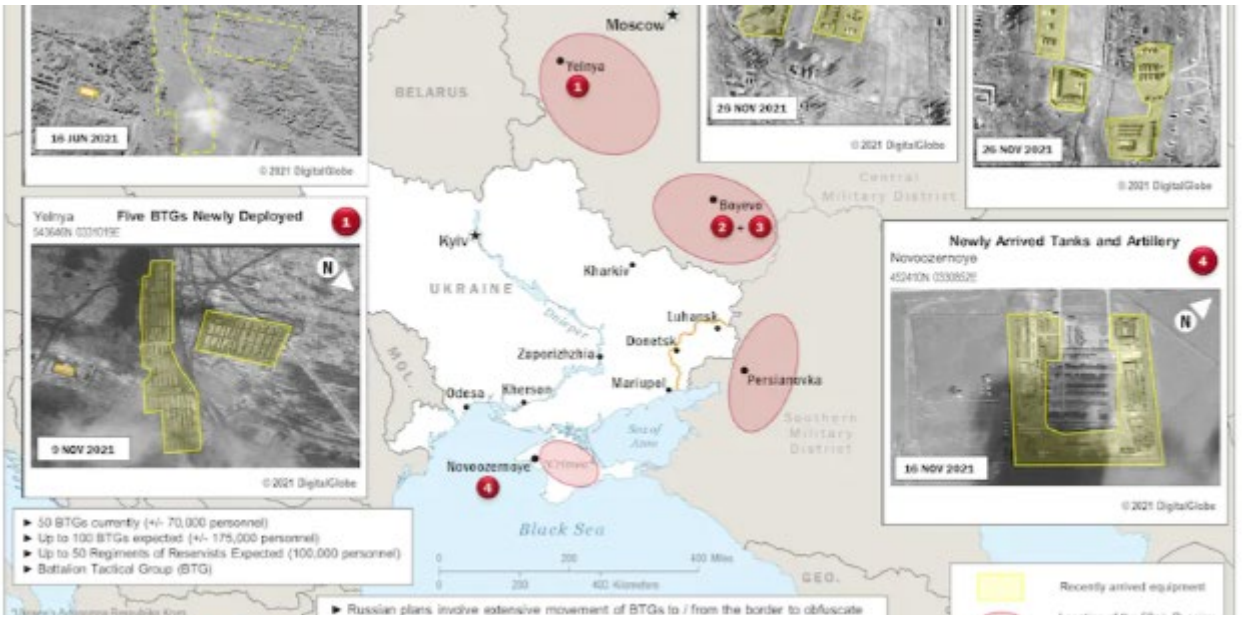

Fig. 2 - An unclassified U.S. intelligence document on Russian military movement. (Obtained by The Washington Post)

[12] https://www.whitehouse.gov/briefing-room/press-briefings/2021/12/03/press-briefing-by-press-secretary-jen-psaki-deceber-3-2021.

[13] https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html

ra 2). Di fatto, è da questo momento che sono iniziati ad aumentare in maniera consistente i contributi non solo delle principali testate internazionali, ma anche di singoli e gruppi di attivisti, organizzazioni private e non governative. Tanto che un mese dopo, il 4 gennaio 2022, il Wall Street Journal ha pubblicato un articolo dal titolo significativo: *"Russia's Military Buildup Near Ukraine Is an Open Secret"*[14]. Denso di spunti di particolare interesse il documento sottolineava come, ritagliandosi un ruolo in passato appannaggio dell'*Intelligence* istituzionale, ora vi siano investigatori non professionisti e intere organizzazioni non statali impegnate ad analizzare immagini dei satelliti commerciali, post su *social media*, strumenti di messaggistica istantanea, forum e dati di tracciamento dei voli che consentono di delineare un quadro situazionale definito come straordinariamente preciso.

Tuttavia, nonostante l'elevata quantità di dati disponibili a pochi giorni dall'attacco, vi erano ancora opinioni molto contrastanti sulle effettive intenzioni della Russia. Da un lato Washington e Londra convinte che Putin avrebbe attaccato, dall'altro i Paesi europei, in ordine sparso, che nutrivano molti più dubbi. Addirittura lo stesso Presidente Zelensky, durante una conferenza stampa, a chi gli ha fatto notare che lungo il confine la Russia aveva schierato circa 175.000 uomini, ha risposto in questo modo: *"If you look only at the satellites, you will see the increase of troops. You can't assess whether this is a threat, attack or simple rotation."*[15]

In effetti, le considerazioni espresse dal Presidente ucraino appaiono ancora oggi condivisibili perché attraverso l'acquisizione di informazioni *open source* è stato possibile documentare l'aumento delle truppe russe lungo il confine, ma non comprenderne chiaramente le motivazioni fino al momento in cui si è concretizzato l'attacco.

Ed è proprio qui che si evidenziano i limiti dell'OSINT; a fronte della capacità di intercettare alterazioni e variazioni all'interno del contesto di riferimento, nel caso in questione un consistente e inusuale movimento di uomini e mezzi, vi è poi la necessità di disporre di ulteriori strumenti, ad esempio di natura SIGINT (disciplina che si occupa della raccolta di informazioni mediante l'intercettazione e analisi di segnali) o HUMINT (*Intelligence* acquisita da fonti umane), che forniscano indicazioni circa le intenzioni delle entità che si stanno osservando. Strumenti che, almeno nel caso della SIGINT, si auspica restino - per ovvie ragioni appannaggio esclusivo degli Stati. In questo senso, è verosimile ritenere che gli Stati Uniti si siano potuti spingere a prevedere il momento "quasi esatto" dell'attacco anche in funzione della disponibilità di informazioni non pubblicamente disponibili.

Ecco spiegato, a carattere generale e senza la presunzione di ritenerlo un paradigma incontrovertibile, perché l'OSINT - pur rappresentando un fondamentale strumento di monitoraggio utile a intercettare tempestivamente qualunque tipologia di cambiamento - non può sostituire *tout court*

[14] https://www.wsj.com/articles/russias-military-buildup-near-ukraine-is-an-open-secret-11641292202

[15] https://www.washingtonpost.com/national-security/2022/01/29/us-allies-debate-intelligence-how-quickly-putin-will-order-an-invasion-ukraine-or-whether-he-will-all/

“Intelligence does not have to be secret to be valuable”.

l’*Intelligence* cosiddetta *all sources.* Quest’ultima, infatti, si avvale di molteplici branche che convergono in un processo complesso che vede coinvolti svariati *stakeholders*, con interessi peraltro non sempre convergenti.

Fatta salva questa doverosa precisazione, come già evidenziato, la rilevanza dell’OSINT, in particolare per quanto attiene le attività di *monitoring* a livello tattico/operativo e per investigare eventi già accaduti, è indiscutibile.

Del resto, se agli albori dell’OSINT le fonti principali erano rappresentate dalla stampa, dalla radio e dalla letteratura scientifica e accademica (tutti ricordano il film *“I tre giorni del Condor”*, in cui Robert Redford ricerca informazioni di interesse attraverso la lettura e lo studio di giornali e libri provenienti da ogni parte del mondo), oggi l’evoluzione della tecnologia, con la diffusione di Internet e degli smartphone, ha reso ogni singolo individuo un potenziale sensore e/o fonte di informazione. Gli smartphone in particolare, oltre a diffondere informazioni personali sui loro possessori, consentono anche di documentare e geo-localizzare qualsiasi tipo di evento. Prendiamo ad esempio Telegram, che rappresenta uno strumento ibrido a metà strada tra una piattaforma di messaggistica istantanea e un *social network*: questa piattaforma ha visto proliferare al proprio interno una quantità smisurata di canali e gruppi dedicati al contesto ucraino utilizzati per informare, disinformare e monitorare ogni tipologia di attività militare; basti pensare che, ad appena una settimana dall’inizio della guerra, il 1° marzo 2022, il collettivo SMAT ha pubblicato sul proprio blog[16] un file contenente un elenco di circa 150 canali Telegram collegati al conflitto.

Su questo argomento, è possibile ricavare interessanti spunti di riflessione dalla lettura dell’articolo *“How Telegram Became the Digital Battlefield in the Russia-Ukraine War”*[17], pubblicato il 21 marzo 2022 sulle pagine del Times, nel quale la giornalista Vera Bergengruen arriva ad affermare che *“è difficile immaginare come sarebbe la guerra della Russia in Ucraina senza Telegram”*; quest’ultimo definito dall’ex agente dell’FBI Clint Watts, oggi collaboratore del Foreign Policy Research Institute ed esperto di disinformazione estera, come *“l’ultimo ponte sui social media che collega il mondo occidentale a quello russo… dove si può vedere cosa sta succedendo e come si sta svolgendo la battaglia. Chiunque riesca a sostenere le proprie campagne di informazione su Telegram ha le migliori possibilità di plasmare le opinioni del mondo su ciò che sta accadendo in Ucraina”*. Quindi Telegram, ma non solo, diventa il campo di battaglia ideale per le attività di *info-warfare* e propaganda. Non a caso Bergengruen evidenzia anche che *“la potenza e la pericolosità di Telegram”* derivano principalmente dalla mancanza di sorveglianza che, fin dalla sua nascita, ha reso questa piattaforma uno strumento di comunicazione importante per molteplici realtà estremiste. Non ultimo il sedicente Stato Islamico oltre a *“groups like Covid-19 and QAnon conspiracy theorists and white nationalists, but also Black Lives Matter organizers, pro-democracy groups from South Korea to Cuba and Iran, and Russia’s own opposition groups.”*

[16] https://blog.smat-app.com/p/kremlin-hunting.

[17] https://time.com/6158437/telegram-russia-ukraine-information-war/

Del resto, questa piattaforma sembra essere lo strumento perfetto per amplificare ogni tipo di narrativa, specie attraverso i canali che consentono di disattivare i commenti degli utenti, lasciando così ai creatori di ogni singolo canale la possibilità di diffondere qualsiasi tipo di informazione. Un eccezionale strumento di comunicazione di massa in grado di raggiungere chiunque, anche grazie alla preziosa funzione di traduzione dei messaggi che contiene al proprio interno.

Telegram è stato fin dall'inizio del conflitto anche un importante strumento di difesa per il Governo ucraino, che aveva già utilizzato la piattaforma durante la campagna presidenziale ucraina del 2019. L'applicazione si è trasformata quindi nel fronte principale della guerra dell'informazione, consentendo anche ai normali cittadini di inviare alle autorità ucraine, in tempo reale, informazioni sui movimenti delle truppe e dei veicoli corazzati. Oltre a Telegram e alle immagini satellitari commerciali, sono molteplici gli strumenti attraverso cui è possibile seguire in tempo reale il conflitto. Ad esempio, la mappa interattiva[18] realizzata dall'Institute for the Study of War (ISW), alimentata unicamente con informazioni non classificate, citata da Amy Zegart nel suo recente contributo *"Open Secrets Ukraine and the Next Intelligence Revolution"*[19] pubblicato sull'ultimo numero di Foreign Affairs. A quella dell'ISW si affiancano la piattaforma liveuamap, che monitora tutte le aree di crisi nel mondo, e la mappa *Eyes on Russia*[20], realizzata dal Centre for Information Resilience (CIR). Ognuna di queste mappe è costantemente alimentata dalle notizie pubblicate in rete, in particolare attraverso Twitter che si conferma, anche in questa occasione, uno strumento di aggiornamento rapido ed efficace; purché - tenendo conto che a luglio del 2022 sono stati gli stessi dirigenti di Twitter a dichiarare che ogni giorno vengono rimossi dalla piattaforma circa 1 milione di account *bot*[21] - si abbiano gli strumenti per compiere un'attenta valutazione degli account che si decide di consultare.

Peraltro quest'ultima considerazione, valida per ogni strumento, piattaforma od organizzazione che si intende seguire e/o monitorare, rimanda necessariamente al processo metodologico richiamato in precedenza e in assenza del quale sarà difficile, se non impossibile, produrre un'*Intelligence* efficace e fruibile. ***Intelligence* che, non dimentichiamolo mai, non sarà mai esclusivamente *open source*, ma sempre frutto di un processo *all sources* in cui le informazioni segrete, acquisite mediante le altre discipline dell'*Intelligence*, continueranno a rivestire un ruolo determinante**.

Mirko Lapi, *Presidente di Osintitalia, Consulente in ambito di Intelligence e Sicurezza delle Informazioni.*

[18] https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375

[19] https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart.

[20] https://eyesonrussia.org.

[21] Un *bot* è un programma autonomo che sulle piattaforme social simula un comportamento umano, interagendo in maniera automatica con gli altri utenti.

“Intelligence does not have to be secret to be valuable”.

SITOGRAFIA

https://www.dw.com/en/open-source-investigators-syria-ukraine/a-61236760

https://twitter.com/trbrtc/status/1380069652584230914?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetebed%7Ctwterm%5E1380069652584230914%7Ctwgr%5Ea44b666f199d8d4df36486e4c60f1edc9413c4c3%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fciteam.org%2Fru-military-camp-near-ukraine.html

https://fas.org/irp/agency/army/mipb/2005_04.pdf

https://citeam.org/ru-military-camp-near-ukraine.html

https://theins.ru/en/politics/240830

https://www.janes.com/defence-news/news-detail/russian-ground-troop-units-and-iskander-ballistic-missiles-identified-at-ukrainian-border-by-janes

https://www.whitehouse.gov/briefing-room/press-briefings/2021/12/03/press-briefing-by-press-secretary-jen-psaki-december-3-2021/

https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html

https://www.wsj.com/articles/russias-military-buildup-near-ukraine-is-an-open-secret-11641292202

https://www.washingtonpost.com/national-security/2022/01/29/us-allies-debate-intelligence-how-quickly-putin-will-order-an-invasion-ukraine-or-whether-he-will-all/

https://blog.smat-app.com/p/kremlin-hunting

https://time.com/6158437/telegram-russia-ukraine-information-war/

https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375

https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart

https://liveuamap.com/

https://eyesonrussia.org/

https://apnews.com/article/elon-musk-twitter-inc-technology-misinformation-social-media-e9fa93bc9132a4adf8535a8a34bebec9

BIOGRAFIA

Mirko Lapi

Consulente in ambito di *Intelligence* e Sicurezza delle Informazioni, ha trascorso 27 anni nelle Forze Armate, 16 dei quali all'interno del II° Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa con l'incarico di analista e docente di *Intelligence*. Ha operato in svariati contesti di crisi, tra cui Afghanistan, Libano e Balcani, ove ha svolto incarichi relativi all'analisi e alla protezione delle informazioni. Attualmente è socio ordinario Socint e Presidente di Osintitalia, Associazione di Promozione Sociale che divulga l'*Open Source Intelligence* in una prospettiva sociale e solidale.

CYBER CRIME CONFERENCE

11-12 MAGGIO 2023

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine per conoscere l'agenda e partecipare alla **11ª Edizione della Cyber Crime Conference**