RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0129 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Arturo Di Corinto

Netwar, come cambia l'hacktivismo nella guerra cibernetica

La disponibilità delle tecnologie di comunicazione influenza le attività e la formazione stessa dei gruppi e dei movimenti della società civile. Con la diffusione di massa di Internet e del Web, la Rete è diventata un campo di battaglia per gli attivisti digitali. Molte delle pratiche di informazione, contestazione e sabotaggio tipiche dei movimenti di protesta sociale sono state digitalizzate e riversate in Rete. Protagonisti in questo scenario sono gli hacktivisti, gli hacker-attivisti che hanno usato la Rete per autorganizzarsi, fare propaganda, controinformazione, e condurre azioni politiche dirette. I loro obbiettivi e i loro metodi degli inizi erano quelli dell'infowar, la "guerra" d'informazione e propaganda, ma oggi gli hacktivisti sono entrati di prepotenza nelle guerre guerreggiate: spesso arruolati su una base ideologica, talvolta usati come mercenari, sono arrivati ad accompagnare i conflitti cinetici, le guerre vere e proprie. Si tratta di una mutazione graduale e forse attesa, ma poco presente nel dibattito pubblico e accademico. Con questo articolo vorremmo contribuire a tracciare l'evoluzione di questa trasformazione culminata nella creazione di vere e proprie milizie di hacktivisti digitali impegnati nel conflitto Russo-Ucraino.

Guerra dell'informazione – Guerra in Rete – Guerra cibernetica – Hacktivismo – Cybersicurezza

Netwar, hacktivism evolution in cyber warfare

The availability of communication technologies influences the activities and the very formation of civil society groups and movements. With the mass diffusion of the Internet and the Web, the Internet has become a battlefield for digital activists. Many of the infomration-related practices of information, protest and sabotage typical of social protest movements have been digitized and transferred online. The protagonists in this scenario are the hacktivists, who have used the Internet to self-organize, carry out propaganda activities, counter-information, and conduct direct political action. Their objectives and methods in the beginning were those of the infowar, the "war" of information and propaganda, but today the hacktivists have forcefully entered hybrid conflicts: often recruited on an ideological basis, sometimes used as mercenaries, have come to accompany kinetic conflicts, real wars. This is a gradual and perhaps expected mutation, but little present in the public and academic debate. With this article we would like to help trace of the evolution of this transformation which culminated in the creation of militias of digital hacktivists engaged in the Russian-Ukrainian conflict which is shaking Europe.

Infowar – Netwar – Cyberwar – Hacktivism – Cybersecurity

L'Autore è *Public Affairs and Communication Advisor* presso l'Agenzia per la cybersicurezza nazionale (ACN) e afferisce al Dipartimento di comunicazione e ricerca sociale di Sapienza - Università di Roma
Quanto dichiarato dall'Autore non impegna in alcun modo l'ACN

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Infowar, Netwar, cyberwar

Partiamo da una premessa, un conto è la contestazione digitale, l'infowar, altra cosa è la cyberwar che usa armi cibernetiche e viene praticata da eserciti, paramilitari e servizi segreti nel contesto dei conflitti tra Stati nazionali e mira a provocare danni a cose e persone. L'infowar è stata diversamente concettualizzata nella storia, ma ogni sua definizione operativa rimanda a una qualche forma di inquinamento dell'informazione.

Il defacciamento[1] dei siti (*web defacement*) di banche e governi, la creazione di luoghi digitali antagonisti in rete, i video virali del collettivo Anonymous, il cybersquatting[2] delle url e i siti clone di istituzioni come il Vaticano sono esempi di infowar, guerra dell'informazione[3]. E datano dalla metà degli anni Novanta del secolo scorso. Variamente concettualizati dai gruppi sociali, e da teorici come Ricardo Dominguez, Hakim Bey e Tommaso Tozzi[4], non implicano un danno irreversibile a cose e persone.

Nel novembre 1999, ad esempio, (r)TMark, gruppo di attivisti digitali, pubblica un sito[5] contente informazioni sul meeting di Seattle del 30 novembre del GATT (*Global Agreement on Tariffs and Trade*, predecessore del WTO, *World Trade Organization*). Il sito, formalmente identico a quello ufficiale dell'Organizzazione per il commercio mondiale, a dispetto alle aspettative dei visitatori mette in discussione gli assunti del libero mercato e della globalizzazione economica.

Nel febbraio 2001, invece, in occasione del Terzo Global Forum, quello sul governo elettronico tenutosi a Napoli il marzo successivo, alcuni attivisti napoletani clonano il sito della manifestazione ufficiale, ne modificano i contenuti e lo riversano su un loro dominio ocse.org che, successivamente censurato, viene trasferito sul sito www.noglobal.org/ocse. Anche in questo caso il sito plagiato dagli antiglobalizzatori conteneva una critica radicale al Forum che, secondo loro, era volto «a definire nuove modalità di sfruttamento e controllo sociale attraverso l'informatizzazione degli stati» anziché a promuoverne lo sviluppo democratico. In quell'occasione i contestatori digitali fecero anche un Netstrike (corteo telematico, antesignano dei

1. Con il termine *defacement* (in italiano *defacciamento*) si intende la modifica illecita della home page di un sito web (la sua "faccia") o la sostituzione di una o più pagine interne. Questo tipo di attacco viene eseguito all'insaputa di chi gestisce il sito ed è illegale in tutti i paesi del mondo.
2. *Cybersquatting*, o *domain squatting*, è l'attività di chi si appropria di nomi di dominio altrui corrispondenti a marchi commerciali, entità governative, personaggi famosi per realizzare un lucro sul trasferimento del dominio, per creare o un danno a chi non lo possa utilizzare oppure farne uno statement politico.
3. Di Corinto-Tozzi 2002; Di Corinto 2014.
4. Dominguez 2003; Bey 2007; Tozzi 2019.
5. https://web.archive.org/web/20120208220331/http://www.rtmark.com/gatt.html.

DDoS[6]), al sito di "FinecoOnLine"[7]) e lo usarono come occasione per avviare un dibattito pubblico sulla portata degli scambi finanziari on line e delle bolle speculative del mercato borsistico telematico.

Queste pratiche di attivismo digitale, o *hacktivism*[8], dall'unione delle due parole *hacking* e *activism*[9], non avevano niente a che vedere con le cyberguerre perché non miravano a distruggere e conquistare, ma ad occupare solo temporaneamente degli spazi di comunicazione per parlare all'opinione pubblica e ad una platea di altri cyberattivisti. Erano considerate pratiche di "guerriglia comunicativa" e di sabotaggio culturale[10].

L'antagonismo politico sociale in rete, secondo i suoi protagonisti, all'epoca rappresentava l'altra faccia della globalizzazione economica[11]. Così come si intensificavano gli scambi commerciali e l'economia diveniva "virtuale", così i movimenti sociali esprimevano bisogni universali "globalizzando la rivendicazione dei diritti" attraverso mezzi di comunicazione indifferenti alle frontiere e alle leggi degli Stati[12].

L'infowar degli hacktivisti (www.thehacktivist.com[13]) era qualcosa di assai diverso dalle cyberguerre e dal così detto "terrorismo informatico" o cyberterrorismo, e veniva praticata attraverso l'uso di *hacking skills* (capacità da hacker) per supportare l'azione diretta dei movimenti politici di base[14]. Gli hacker costruivano spazi e strumenti digitali per l'azione politica collettiva, come ad esempio strumenti di open publishing[15].

Il fax-strike, il Netstrike, il mass-mailing, il defacciamento dei siti web, sono le forme in cui in Italia, durante gli anni Novanta si è sovente articolata la protesta collettiva degli attivisti digitali. Seppure diversi, i *defacement* stessi – la sostituzione di una pagina web con un'altra o con un messaggio irridente e critico – somigliano da vicino alla copertura di un cartellone pubblicitario o alle scritte sui muri, sulla scia delle azioni degli attivisti del *Billboard Liberation Front*[16]. E anche in questo caso l'obiettivo era quello di appropriarsi di uno spazio per esprimere le proprie opinioni, anche quelle più estreme.

L'infowar è quindi per gli attivisti una guerra di parole, una guerra combattuta a colpi di propaganda, autorganizzata, dal basso. Ed è diversa dalla sua matrice linguistica che rimanda all'*Information Warfare*, intesa come un insieme di tattiche, tecniche e procedure belliche per assumere una superiorità informativa rispetto all'avversario tramite operazioni di spionaggio e sabotaggio[17].

2. La costruzione di uno spazio di *global public opinion*

Il concetto di infowar negli anni Novanta esonda dall'ambito militare e viene quindi appropriato dagli attivisti politici i quali, in aggiunta all'uso di strumenti tradizionali di comunicazione (volantini, affissioni, riviste), si "armano" di computer e cominciano ad usare la Rete come mezzo per comunicare le proprie ragioni ad una audience globale, sfruttando le peculiarità di un mezzo

6. DoS, *Denial of Service*, negazione di servizio ovvero blocco dei servizi web, causato da numerose richieste di accesso illegittime al servizio esposto. La sua variante più nota è il DDoS, il *Distributed Denial of Service attack*. Cfr. Brooks-Oxcelik-Oakley-Tusing 2021; Strano Network 1996
7. https://web.archive.org/web/20010201081900/http://www.netstrike.it/.
8. L'*hacktivism* è la convergenza dell'hacking con l'attivismo, dove "hacking" è qui usato per riferirsi a operazioni che sfruttano i computer in modi insoliti e spesso illegali, in genere con l'aiuto di software speciali ("strumenti di hacking"). In Denning 1999.
9. Denning 1999.
10. Critical Art Ensemble 1998; Piro 1998; Deseriis-Marano 2008.
11. .Zip!Puntozip 1997.
12. Klein 2000.
13. https://web.archive.org/web/*/www.thehacktivist.com.
14. Di Corinto-Tozzi 2002.
15. Veneziani 2006, pp. 210-220.
16. http://www.billboardliberation.com/.
17. Rapetto-Di Nunzio 2001.

potenzialmente accessibile a tutti da ogni dove, indipendentemente dalla collocazione spaziale e temporale degli attivisti e del pubblico per creare una nuova sfera pubblica[18]. Solo successivamente essi useranno la Rete come mezzo per realizzare azioni di interferenza sociale e di disobbedienza civile[19]. È in questo passaggio che i computer e la rete Internet diventano strumento e non solo teatro della contestazione, lo spazio dove la protesta, il rifiuto, la critica, espresse collettivamente, prendono forma e dalle parole si passa ai fatti. È questa la Netwar intesa come azione di guerriglia comunicativa e propaganda organizzata, che supera i concetti di blocco e sconfinamento in Rete tipici dell'infowar praticata dagli attivisti che così diventano Net Attivisti.

Ad esempio quando, nel 2014, in segno di protesta, gli attivisti digitali si coalizzano per impedire la sentenza capitale nei confronti del ventunenne Ali Mohammed al-Nimr, colpevole di aver incitato alla rivolta i suoi amici via SMS contro il governo saudita lanciando l'hashtag #OpNimr su Twitter, un elenco di tweet preimpostati che ogni net attivista può copiare, incollare e pubblicare, e solo dopo creando una lista di siti governativi da attaccare, riuscendo a mettere offline i siti del ministero dell'Economia e Finanze, della Giustizia e dell'Informazione del regime della famiglia Sahud con attacchi DDoS[20].

Infowar e Netwar sono quindi pratiche di conflitto tipiche dell'hacktivism, le cyberguerre no.

La cyberwar si riferisce alla guerra cibernetica propriamente detta, cioè a una guerra che usa l'informatica, la cibernetica e le reti di comunicazione al pari di armi convenzionali, per definizione appannaggio degli Stati e degli eserciti. La cyberwar, infatti, punta a smantellare i sistemi di comando, controllo e comunicazione del nemico in una maniera intenzionale e pianificata mettendo in campo ingenti risorse computazionali centralizzate facendo uso di cyber-armi come backdoor[21], botnet[22], malware[23], software exploits[24] e virus trojan[25], solo per citarne alcuni. La definizione generalmente accettata di guerra cibernetica, o cyberwar, è concettualizzata come una serie di attacchi informatici contro uno Stato-nazione, che causano danni significativi, dall'interruzione di sistemi informatici vitali fino alla perdita di vite umane. Secondo il *Tallinn Manual on the International Law Applicable to Cyber Operations* della Nato[26], un "attacco informatico" è «un'operazione informatica, offensiva o difensiva, che si prevede ragionevolmente possa causare lesioni o morte a persone o danni o distruzione di oggetti».

Questo tipo di guerra cibernetica, come tutte le guerre, produce tuttavia degli effetti di spillover anche sui civili, ad esempio interrompendo l'erogazione di energia elettrica all'interno di un

18. Meikle 2004.
19. Critical Art Ensemble 1998.
20. Di Corinto 2015.
21. Letteralmente "porta di servizio" collocata sul retro di un edificio. Viene chiamato così un canale occulto che consente l'accesso ad un sistema informatico eludendo le normali procedure di autenticazione.
22. Rete di computer utilizzata per attacchi da remoto, o per altre finalità, formata da computer infetti (*bot* o *zombie*) che, all'insaputa dei legittimi utenti, sono controllati da un utente malevolo (*botmaster*).
23. Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo abusivo e nascosto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.
24. Software impiegato per lo sfruttamento di vulnerabilità di un sistema al fine di accedervi abusivamente o porre in essere azioni malevoli.
25. Tipologia di malware che cela le proprie funzionalità (ad es. accesso non autorizzato, furto di credenziali, sabotaggio del sistema target) all'interno di un software legittimo (il nome deriva dal mitico Cavallo di Troia). A tale attacco sono spesso associate tecniche di ingegneria sociale, che inducono il target a scaricare/installare il software contenente il trojan.
26. Schmitt 2017.

determinato territorio, come accadrà in Ucraina nel 2015 ad opera di gruppi paramilitari russi[27].

E tuttavia le tecniche usate nei conflitti telematici sono per definizione ibride e molteplici[28]. Così come la protesta digitale può determinare l'interruzione di un servizio – si pensi agli attacchi DDoS dimostrativi che bloccano temporaneamente la funzionalità di un sito web pubblico – la cyberwar può fare uso di tecniche di propaganda tipiche dell'infowar per accompagnare l'attacco vero e proprio[29].

Le tecniche di infowar usate dagli attivisti sono quindi inizialmente un miscuglio di campagne di informazione e di strategie comunicative derivate dall'arte di avanguardia che mirano a mettere in cortocircuito l'informazione istituzionale cannibalizzando l'attitudine al sensazionalismo tipico dei media mainstream – tv, radio e giornali –, prendendosi gioco delle veline d'agenzia di stampa e del modo di costruire la notizia[30]. Le campagne di informazione e controinformazione su Internet sono l'equivalente digitale di forme di comunicazione più tradizionali, tipiche dei movimenti politici di base, in cui l'e-mail sostituisce il volantino, la petizione elettronica sostituisce il banchetto di firme all'angolo della strada, il sito web i manifesti murali e i cartelloni. Finché, portando alle estreme conseguenze la logica del "panico mediatico", usato con successo dagli epigoni della Beat Generation[31], si producono notizie false per creare diffidenza e allarme. È il caso dei finti virus o della soffiata relativa ad una improbabile intrusione dentro sistemi informatici protetti che prelude alla Netwar.

La Netwar, la "guerra" nei network digitali, ma sarebbe meglio chiamarla "guerriglia", si presenta come una forma di azione diretta che punta a creare disturbo e interferenza, ma anche danni nelle attività di comunicazione dell'avversario, si tratti di una lobby politica o di una azienda multinazionale, un governo locale o sovranazionale[32]. Sono iniziative collettive e pubbliche di comunicazione radicale. È il caso dei DDoS[33], del synflood[34], dei virus artistici[35], della divulgazione di dati personali.

Le cyberguerre, al contrario, non mirano a delegittimare oppure a contrastare l'avversario attraverso la propaganda, piuttosto mirano a interrompere e sabotarne i flussi informativi, danneggiando le sue infrastrutture economiche e sociali.

Assaggi di queste cyberguerre si sono avute all'epoca della crisi fra Usa e Cina a causa della bomba recapitata "per sbaglio" all'ambasciata cinese di Belgrado durante la guerra del Kosovo (1998-1999). In quel caso i computer del Pentagono e della Nasa furono bersagliati da milioni di lettere elettroniche con virus (*mailbombing*). Oppure nel caso del conflitto telematico che vede combattersi fino ai giorni nostri israeliani e palestinesi. Già nel 2000 i giornali di Tel Aviv riportarono la notizia di un attacco informatico DDoS, che aveva messo fuori uso il sito ufficiale di Hezbollah, mentre cyber attivisti arabi avevano deturpato i siti dell'Università ebraica di Gerusalemme e dell'accademia di Netanya ed erano penetrati nel sito della difesa israeliano.

Da allora le forme e gli strumenti della cyberguerra condotta in maniera coperta dagli Stati attraverso i loro "proxy", siano essi paramilitari, servizi segreti o Stati canaglia, ha visto una costante evoluzione. Dall'uso del virus Stuxnet[36], di fabbricazione americana-israeliana, che nel 2010 ha bloccato le centrali per l'arricchimento dell'uranio a Natanz, Iran, fino all'uso del malware Black

27. Greenberg 2019.
28. Rapetto-Di Nunzio 2001; Curioni-Giannuli 2019.
29. Microsoft Digital Security Unit 2022.
30. Deseriis-Marano 2008.
31. Autonome A.f.r.i.k.a. gruppe-Blisset-Brunzels 2001.
32. Di Corinto 2001.
33. Deseriis 2017, pp. 131-152.
34. Il *Synflood* è un'interferenza nei protocolli di comunicazione per causare "l'inondazione" ovvero la saturazione di un servizio digitale; Critical Art Ensemble 1998.
35. Tozzi 2019.
36. Zetter 2015.

Energy creato dal gruppo russo Sandworm[37], che ha interrotto l'erogazione di energia elettrica in Ucraina nel 2015 lasciando al buio e al freddo 225 mila ucraini all'antivigilia di Natale[38].

3. L'Hacktivism, origini ed evoluzione

Prima c'era l'*activism*. L'azione politica diretta nello spazio fisico cittadino che si concretizzava negli scioperi, nei cortei, e nell'occupazione di strade (*Reclaim the streets*), piazze e edifici. Poi è venuto l'*hack-tivism*, l'azione diretta in Rete con tecniche di hacking, e i cortei e le occupazioni sono diventate virtuali, dal *Netstrike* ai *Distributed Denial of Services* (DDoS).

Il termine *hacktivism* deriva dall'unione delle parole *hacking* e *activism*[39]. L'*Hacking* è la messa in opera di una particolare attitudine verso le macchine informatiche che presuppone storicamente la pratica di studiare i computer per migliorarne il funzionamento attraverso la cooperazione e il libero scambio di informazioni tra i programmatori, e la condivisione del sapere risultante per dare a tutti accesso illimitato alla conoscenza in essi incorporata[40]. *Activism* è il termine americano che indica le forme dell'azione diretta praticate dai movimenti politici di base (*grassroots movements*) come i sit-in, i cortei, i picchetti.

Successivamente è stato concettualizzato il mediattivismo o *media activism*[41], che si è sostanziato nel racconto mediatico delle proteste di piazza e nella diffusione virale dell'informazione in Rete usando anche le immagini in movimento e le street tv. Infine, col Web 2.0 ha fatto la sua comparsa il *clicktivism*, l'adesione a petizioni, mobilitazioni e proteste, reali e virtuali, con un colpo di click, senza staccare gli occhi dallo schermo del computer. Ma mentre questa nuova modalità di partecipazione coinvolgeva i grandi numeri dei social network, a compensare questa ondata di "slacktivism" – termine gergale per indicate "l'attivismo fannullone", cioè quello che dopo il click si disinteressa della reale entità del cambiamento prodotto –, si è assistito al revival dell'*hacktivism* col defacciamento dei siti web, i virus politici, gli attacchi DDoS organizzati.

Cosa è accaduto? È accaduto che la rivoluzione digitale ha messo nelle mani di molti individui strumenti di comunicazione efficienti e a basso costo in grado di connettersi alla Rete, mentre le crisi economiche e finanziarie ripetute hanno risvegliato la coscienza delle ingiustizie e portato singoli, gruppi e movimenti digitali a riorganizzarsi su due fronti: la comunicazione e il sabotaggio.

I movimenti sociali in Rete hanno sempre avuto una grande quantità di iniziative legate alla comunicazione e il loro rapporto avanguardistico e sperimentale con gli strumenti della comunicazione ha prodotto le fanzine ciclostilate, le radio indipendenti, il videoteatro, il documentario politico, fino ai siti web e ai software di comunicazione gratuiti[42]. Dall'italiana Radio Alice a Seattle 1999, fino alle azioni di Anonymous, è possibile ripercorrerne il filo conduttore che passa per Indymedia, Wikileaks e il movimento Occupy Wall Street.

Gli ingredienti della messa in opera della contestazione sono uguali e diversi, rappresentano in molti casi l'evoluzione tecnica e la convergenza di strumenti e forme di comunicazione precedenti: personal media prima (dal fax ai telefoni cellulari, dai camcorder ai videotelefoni, dai siti ai blog); software gratuiti e open source per l'editing di testi, audio e video; l'ubiquità dell'accesso a Internet (dai *Bulletin Board Systems*, BBS, al wi-fi), e poi social network e piattaforme di blogging e whistleblowing. Una "rimediazione" che consente di riunire i singoli media, prima isolati, sulla stessa piattaforma (convergenza digitale), e di portare uno stesso contenuto su piattaforme o media differenti (la divergenza digitale)[43], per realizzare una produzione di informazione indipendente, dal basso, orientata al sabotaggio dei flussi di comunicazione

37. Greenberg 2019.
38. Cyber Infrastructure & Security Agency 2021.
39. Di Corinto-Tozzi 2002.
40. Levy 1996.
41. Pasquinelli 2002.
42. Downing-Villareal Ford-Gil-Stein 2001; Meikle 2004.
43. Bolter-Grusin 2000.

di un potere «che non risiede più in strutture stabili e definite»[44] ma è organizzato intorno a dati, messaggi e informazioni.

Se la creazione di tool come software, server e servizi di messaggistica per la comunicazione indipendente ha subito un arresto con l'affermarsi dei social network e del Web 2.0 – che ha portato anche i gruppi di attivisti più radicali ad avere un account Facebook (il Partito Pirata[45]) –, si sono sviluppate nuove forme di comunicazione e sabotaggio a cavallo tra l'estrazione di informazione protetta e la sua comunicazione al pubblico più ampio, con una strategia di *hack and leak* ovvero "hackera e diffondi"[46].

È il caso di Wikileaks: ottenere informazioni sensibili e offrire al pubblico quelle di cui il potere si vergogna è stata la sua arma più potente fin dalle origini[47], ma prima c'erano stati gli hacker del Chaos Computer Club[48] che negli anni Ottanta, penetrati nel sistema informatico del Comune di Berlino, avevano acquisito le informazioni sulle case comunali sfitte per passarle al movimento dei senza casa. E hanno fatto scuola. Anche l'hacking può ricorrere alla violazione di sistemi informatici protetti (cracking) se ha un fine etico.

Nell'attacco al sito della Corte costituzionale ungherese da parte di Anonymous[49] nel marzo 2012, gli hacktivisti col volto di Guy Fawkes hanno cambiato il testo della Costituzione autoritaria voluta dal presidente Viktor Orban affermando il "diritto alla ribellione", con queste parole: «Gli ideologi e i governanti della tirannia, o anche i dittatori, non rappresentano che brevi periodi della storia. Il popolo ha il diritto di eliminare la tirannia e ribellarsi», aggiungendo poi un comma specifico: «[chiediamo] la pensione a 32 anni per gli informatici con il 150 per cento dello stipendio»[50].

Il retroterra teorico di molti di questi guerriglieri dell'informazione è l'etica hacker delle origini: consentire a chiunque l'accesso all'informazione, dovunque essa sia riposta e comunque sia custodita, con la ferma convinzione che l'accesso all'informazione renda tutti più liberi di fare e di scegliere[51]. Il paradigma dell'azione è la condivisione di saperi e conoscenze e la difesa dei beni comuni che si producono nei circuiti dell'interazione sociale, e che, secondo gli attivisti, necessita di pratiche non ortodosse. È questa l'idea che afferma definitivamente quella pratica creativa e disordinata che definiamo di hacktivism, e che vedrà la galassia dei collettivi hacktivisti di Anonymous protagonisti per oltre un decennio.

Sono infatti hacktivisti gli Anonymous organizzatori dell'operazione Payback[52], condotta nel 2010 contro i grandi produttori di contenuti creativi, le major hollywoodiane e le loro rappresentanze di categoria, contro le autorità di garanzia quali l'Agcom italiana e le collecting societies come la Siae. In queste iniziative c'era tutta la virulenza della contestazione verso chi si appropria del sapere altrui mettendoci sopra un marchio e pretendendo di limitarne la diffusione e la conoscenza se non dietro al pagamento di ogni file tracciabile e certificato.

Questi soggetti del conflitto in Rete non sono solo precari dell'industria culturale sfruttati e depressi dalla mancanza di lavoro[53]. Molti sono lavoratori che, in puro stile hacker, di giorno lavorano a far funzionare la macchina burocratica degli Stati, mantengono le linee di comunicazione a cavallo degli oceani e scelgono il payoff di prodotti pubblicitari, mentre la notte disfano la loro tela di Penelope. Una moltitudine che non è fatta soltanto di una minoranza colta, istruita, con eccellenti competenze informatiche, perché gli attacchi

44. Critical Art Ensemble 1995.
45. https://it.wikipedia.org/wiki/Partito_Pirata.
46. Rid 2022.
47. Assange 2012.
48. https://www.ccc.de/en/.
49. Coleman 2016.
50. La Repubblica 2012.
51. Levy 1996; Di Corinto-Tozzi 2002.
52. Olson 2012.
53. Tiddi 2002; Berardi Bifo 2011.

più virulenti sono stati portati con strumenti facili da usare come il Loic, *Low Orbit Ion Cannon*[54], e scaricabili sotto forma di codici software da installare sul computer, usare e cancellare subito dopo, ottenendo di avvicinare alla protesta ogni tipo di insoddisfazione verso i poteri costituiti.

Organizzazione senza capi, ma con dei leader, sostituibili, che hanno portato il conflitto all'interno delle reti di CIA, governi e servizi segreti, dal 2004 ad oggi Anonymous si presenterà come il capostipite di una nuova generazione di hacktivisti che conduce battaglie sociali a colpi di mouse e che agiscono per contagio ed emulazione[55].

In tutto questo, l'emergere di una nuova socialità è stato modellato dalla Rete assumendo molte forme. Dagli Indignados spagnoli a quelli greci, che però hanno costruito i loro propri social network al riparo dei dipartimenti di intelligence di tutto il mondo i quali usano Facebook e X (Twitter) per controllare i movimenti sociali, difendendosi dall'espropriazione dei propri dati per finalità commerciali. Tra queste si annoverano quelle scelte dai giovani magrebini che durante la così detta Primavera Araba tra il 2010 e il 2011 attraverso Facebook e YouTube hanno trovato le parole per contestare le dittature, si sono uniti ai coetanei per non sentirsi più soli e trovare il coraggio di scendere in piazza, anche a costo di farsi ammazzare, come quando nella Casbah di Tunisi nel 2010 furono «allestite tende e gruppi di lavoro che si occupavano di Internet, media e attivismo in rete»[56].

Così il sapere comunicativo diffuso dei "Millennial", unito alla potenzialità della comunicazione telematica ha prodotto i nuovi contestatori della rete in un procedimento alchemico accelerato dalla crisi globale, che è crisi della finanza, dell'economia, della società, della rappresentanza democratica, dello Stato-nazione[57].

Dietro alle loro sortite c'era una consapevolezza, teorizzata da Hakim Bey[58], e Ricardo Dominguez del Teatro del disturbo elettronico[59], per la quale il potere, da materiale che era, si stava sempre più smaterializzando e non coincideva più con luoghi fisici, portaerei e palazzi, ma coi flussi di comunicazione digitale che possono essere dirottati o sabotati.

Gli hacktivisti oggi però non sono più i soggetti del conflitto sociale in rete che rivendicavano dignità e libertà, reddito e tempo libero, democrazia e giustizia, autodeterminazione.

4. La nuova era dell'hacktivism, l'occupazione dell'agenda mediatica e dei flussi di comunicazione

L'hacktivism è stato a lungo associato a gruppi come Anonymous, gruppi decentralizzati e destrutturati composti da privati cittadini con differenti background. Anonymous ha lanciato numerose campagne (chiamate "Operazioni" e introdotte dal prefisso #Op) contro target individuati in base alle inclinazioni e agli interessi dei suoi membri. Tra le più note, l'operazione contro la chiesa di Scientology, che segna l'avvio del fenomeno, e l'operazione PayBack contro la Sony Corporation. Come racconta Geoff White[60], gli hacktivisti hanno spesso incarnato, in varia misura, una cultura tecnocratica, creativa, e ludica, ma chiunque, a prescindere dalla fede politica, è sempre stato il benvenuto nei gruppi di hacktivisti che si rifacevano alla galassia di questi "anonimi" nati sul forum visuale 4Chan e che avevano un solo imperativo, "Non attaccare i Media".

Altre iniziative di questi hacktivisti old school includono campagne come l'Operazione KKK di Anonymous contro i membri e sostenitori del Ku Klux Klan[61], l'Operazione Lolita, il cui obiettivo era quello di fermare lo smercio di pedopornografia in Rete, fino ad arrivare alle azioni della corrente scissionista di Anonymous, LulzSec, responsabile di attacchi informatici eclatanti alla HBGary, società

54. Di Corinto 2010.
55. Goode 2015, pp. 74-86.
56. Massarelli 2012, p. 40.
57. Klein, 2000.
58. Bey 2007.
59. Dominguez 2003.
60. White 2022.
61. Di Corinto 2014.

di cybersicurezza che aveva lavorato a incastrare sia gli Anonymous sia Julian Assange, il fondatore di Wikileaks, e che, da loro hackerata, ha dovuto terminare le attività.

Altre campagne, di profilo opposto tra di loro, a dimostrazione della variabilità di interessi dei gruppi eterogenei di hacktivisti che di volta in volta usano la sigla Anonymous per le proprie rivendicazioni, sono state #OpIsrael e #OpPalestine e, nel 2016, #OpTrump e #OpHilaryClinton.

Dal 2020 ad oggi però l'hacktivism ha cambiato natura. Per effetto di numerosi conflitti, locali e regionali, in uno scenario geopolitico dalle frontiere mobili, alcuni gruppi hacker hanno modificato le loro attività e la loro attenzione rispetto all'ideologia dell'azione diretta che mira al cambiamento sociale. Il fenomeno dell'hacktivism oggi non sembra più riguardare gruppi eterogenei, le crew, che si uniscono temporaneamente intorno a parole d'ordine precise, o a una causa specifica, il *single issue activism*, per vendicare un comportamento o riparare un torto. Oggi i gruppi di hacktivisti sono strutturati e organizzati con strumenti di attacco/difesa sofisticati e vengono supportati dai governi seppure raramente in maniera esplicita, fatta eccezione per l'IT Army ucraino[62] quando i primi cyberattacchi che hanno accompagnato l'invasione russa dell'Ucraina nel 2021 hanno generato la chiamata alle armi dei cittadini ucraini, e migliaia di attivisti hanno bloccato per ore banche e ministeri russi e, presumibilmente aiutati dai servizi di intelligence occidentali, rubato dati governativi usando il nome di Anonymous come copertura.

Le imprese, i governi e le infrastrutture critiche di molti paesi sono stati bersagliati da questa forma di hacktivism. Dal 2021 al 2023 tutti i paesi del G20 hanno subito pesanti attacchi mossi dai gruppi di attivisti, che in alcuni casi hanno avuto un impatto significativo. Gli attacchi recenti, per lo più di tipo DDoS, hanno interessato non solo i governi di questi paesi, ma anche grandi aziende come Lockheed Martin, azienda americana operante nel campo della difesa.

In questo contesto, il conflitto Russo-Ucraino, successivo all'invasione russa del Donbass, ha rappresentato un forte elemento di stimolo alla partecipazione degli hacktivisti nelle azioni collaterali alla guerra che ne è divampata.

5. Il caso di studio di Killnet, Legion e NoName(057)16

I principali gruppi di hacktivisti che hanno agito negli ultimi due anni condividono diverse caratteristiche proprie delle organizzazioni strutturate: una chiara ideologia politica, una gerarchia dei membri e una leadership definita, con un processo di reclutamento formale. Gli specialisti dell'IT Army Ucraino, ad esempio, in una prima fase sono stati selezionati attraverso l'analisi dei curricula e a monte di un continuo processo di reclutamento sui canali Telegram[63]. Sul fronte opposto, quello russo, è stato messo a disposizione degli hacktivisti un sofisticato tool di attacco come parte del DDoSia project realizzato dagli hacktivisti filorussi di NoName(057)16[64].

Lanciato nel 2022 e successore della botnet Bobik, lo strumento di attacco DDoSia è progettato per mettere in scena attacchi DDoS contro obiettivi situati principalmente in Europa, Australia, Canada e Giappone. Nel periodo che va dall'8 maggio al 26 giugno 2023 i paesi più attaccati sono stati Lituania, Ucraina, Polonia, Italia, Repubblica Ceca, Danimarca, Lettonia, Francia, Regno Unito e Svizzera per un totale di 486 diversi siti web colpiti. Le implementazioni di DDoSia basate su Python e Go scoperte fino ad oggi lo rendono un programma multipiattaforma in grado di essere utilizzato su sistemi Windows, Linux e macOS. DDoSia viene distribuito attraverso un processo completamente automatizzato su Telegram che consente alle persone di registrarsi all'iniziativa di crowdsourcing in cambio di un pagamento in criptovaluta e di un archivio .zip contenente il toolkit di attacco. Ciò che è degno di nota della nuova versione è l'uso della crittografia per mascherare l'elenco degli obiettivi da attaccare, un fatto che dimostra come lo strumento venga mantenuto attivamente dagli operatori.

I gruppi hacktivisti si coordinano quindi nella selezione dei bersagli, si coalizzano, si fondono, e collaborano, svolgendo anche consistenti attività di propaganda finalizzate a pubblicizzare

62. https://t.me/itarmyofukraine2022.
63. https://t.me/itarmyofukraine2022/1637.
64. https://t.me/c/1228309110/34219.

e promuovere i loro risultati, veri o presunti che siano, sui canali Telegram, sul Web e in televisione, come accaduto per Killnet, di cui parleremo più avanti. Questi hacktivisti, secondo i rapporti di Microsoft e Google/Mandiant[65], si mobilitano in seguito a eventi politici, e operano di concerto con enti governativi, raggiungendo obiettivi strategici e ad ampio spettro con un discreto tasso di successo, e un maggiore impatto sociale favorito dal sensazionalismo mediatico di questi attacchi.

L'evoluzione di questa forma di hacktivism è iniziata, secondo alcune ricerche, silenziosamente, nel Medio Oriente ad opera di diversi gruppi come Hackers of Savior, Black Shadow e Moses Staff. Tali gruppi hanno concentrato gli attacchi esclusivamente su Israele. La maggior parte di questi non ha nascosto i rapporti con la propaganda antisraeliana promossa dal regime iraniano. Parallelamente, altri gruppi, fra i quali Predatory Sparrow, si sono concentrati nell'attacco di bersagli iraniani e pro-iraniani: il loro unico piano comune essendo l'opposizione al regime degli Ayatollah.

In realtà l'embrione di queste attività, basate su individuazione del nemico con strumenti di Open Source Intelligence (Osint)[66], tramite l'esfiltrazione di dati strategici, la corruzione dei database avversari, fino all'inoculazione di malware, va rintracciato nel mondo hacktivista nella guerra senza quartiere che Anonymous – chiunque si celasse sotto questa sigla – ha condotto contro l'Isis[67].

L'hacktivism adesso è parte essenziale della guerra ibrida combattuta tra la Federazione Russa e l'Ucraina. Mentre una serie di attacchi, contro l'Estonia nel 2007, la Georgia nel 2008, l'Ucraina nel 2014, hanno ricevuto una provvisoria attribuzione – si tratterebbe infatti di paramilitari e servizi segreti russi, in particolare del GRU, il servizio segreto militare russo e solo in misura ridotta di hacktivisti –, nella prima parte del 2021, sono emerse altre formazioni, evidenziando un rapporto più diretto tra criminalità cibernetica, hacktivism e hacking di Stato.

Secondo Google-Mandiant[68], quando gli hacker governativi russi attaccano, passano i dati rubati agli hacktivisti entro 24 ore dall'irruzione in modo da consentire loro di effettuare nuovi attacchi e diffondere propaganda filorussa. Ad agire in questo modo sarebbero in particolare quattro gruppi non governativi: XakNat Team, Infoccentr, CyberArmyofRussia_Reborn e Killnet.

Tuttavia, mentre XakNat si coordinerebbe con l'intelligence russa, Killnet, con cui collabora, è pronta ad attaccare chiunque se pagata. Nel corso del 2022 il collettivo, che ha anche bersagliato l'Italia, ha però incominciato ad ammantare le proprie azioni di patriottismo, diventando una celebrità grazie alle ospitate nella televisione russa.

Negli gli ultimi mesi del 2022 e per tutto il 2023, NoName057(16) ha individuato come obiettivi degli attacchi i Paesi nell'Unione Europea dichiaratamente impegnati a sostenere l'Ucraina come Polonia, Lituania, Lettonia, Slovacchia e Finlandia, nonché l'Italia, a più riprese. NoName057(16) ha anche attaccato il sito del parlamento finlandese, dopo che la Finlandia aveva espresso interesse nell'unirsi alla NATO.

Il gruppo ha apertamente dichiarato i propri piani a supporto degli interessi russi, come emerge nel manifesto di NoName057(16)[69], che ha indirizzato, con regolarità, gli attacchi verso l'Ucraina con l'intenzione di espandere il proprio raggio d'azione.

L'altro schieramento è composto da altrettanto numerosi gruppi di hacktivisti che si sono mobilitati per sostenere l'Ucraina. Alcuni, come l'Esercito IT ucraino, sono ufficialmente controllati dal governo. L'IT Army è stato creato qualche giorno dopo l'inizio dell'invasione russa e comprende volontari provenienti da tutto il mondo per sostenere l'Ucraina seguendone le direttive, ma è composto anche da esperti dell'intelligence ucraina. Ad affiancarli in alcune azioni eclatanti il gruppo Ghostsec, noto almeno dal 2015 per le incursioni contro il cybercaliffato, la cyber-unit dell'Isis, quando, staccatisi da Anonymous, hanno incominciato a occuparsi di cyber-intelligence e antiterrorismo

65. Mandiant Intelligence 2022.
66. Osint è la raccolta di informazioni da fonti aperte
67. Di Corinto 2015a.
68. Mandiant Intelligence 2022.
69. Ninotti-Colatin 2022.

per trasformarsi poi in GhostSecSecurity prima di scomparire e riapparire nel cyberspace del conflitto russo-ucraino con lo stesso nome[70].

Secondo l'azienda di sicurezza informatica CyberKnow a maggio 2023 si contavano 112 gruppi di hacker attivisti che parteggiano per l'una o per l'altra parte nel conflitto russo ucraino (figura 1).

Figura 1. A maggio *2023 sono 112 i gruppi hacktivisti attivi nel conflitto russo-ucraino copyright CyberKnow*

Uno dei maggiori attori hacktivisti all'interno di questa galassia resta Killnet, un gruppo che è stato pubblicamente annunciato attorno al febbraio 2022, all'inizio del conflitto russo-ucraino. Durante la guerra in Ucraina ha rivendicato attacchi DDoS ai siti governativi rumeni, polacchi e di aziende americane. Sul proprio canale Telegram ha dichiarato che il suo obiettivo è attaccare "i Paesi Nato e l'Ucraina".

Il collettivo Legion ad essi affiliato si presenta come una versione russa di Anonymous. Perlomeno ne emulano il linguaggio e l'estetica sia nei messaggi che nelle immagini. Ma a differenza di Anonymous, che dopo l'invasione russa si è apertamente schierato a favore dell'Ucraina, Legion sostiene azioni a favore della Russia. Killnet è diventato piuttosto noto dopo il 3 aprile 2022, da quando cioè un altro gruppo di hacker, Bluehornet/Atw, ha diffuso alcuni dati personali di quelli che sarebbero alcuni dei leader del gruppo e rivelato l'esistenza della botnet di Killnet. Bluhornet è un gruppo antagonista di Killnet nella controparte virtuale della guerra cinetica tra Russia e Ucraina.

Il gruppo ha iniziato le sue attività aggressive a marzo 2022, con obiettivi primariamente ucraini, ma già ad aprile il gruppo aveva completamente cambiato l'oggetto della sua attenzione supportando gli interessi geopolitici russi in tutto il mondo. Tra fine febbraio e settembre 2022, il gruppo ha affermato di aver portato a termine più di 550 attacchi. Solo 45 di questi però erano indirizzati all'Ucraina: meno del 10% del numero di attacchi totale[71].

Molti di questi attacchi erano diretti a obiettivi di alto profilo come i principali siti governativi, grosse compagnie finanziarie, aeroporti e altri bersagli. Mentre in alcuni casi è difficile comprendere l'impatto reale, in altri casi gli attacchi hanno chiaramente avuto successo, provocando l'inattività

70. Di Corinto 2022.

71. Check Point Research 2022.

dei principali siti web, molti dei quali fornitori di servizi pubblici essenziali.

Ecco di seguito alcuni esempi.

1. A marzo, l'aeroporto internazionale di Bradley in Connecticut (US) ha subìto un attacco DDoS che ha interessato il proprio sito web. Le autorità statunitensi hanno confermato un tentato attacco DDoS su larga scala sul sito dell'aeroporto.

2. Ad aprile, alcuni siti web che appartengono al governo rumeno, come quello del Ministero della Difesa, quello della Polizia di Confine, quello della Compagnia Nazionale dei Trasporti Ferroviari e una banca commerciale, sono stati resi irraggiungibili per diverse ore. Questi attacchi si sono verificati in risposta ad una affermazione fatta dal leader rumeno del partito Socialdemocratico Marcel Ciolacu, che si è offerto di procurare armi all'Ucraina.

3. A maggio, ingenti attacchi DDoS sono stati portati a termine contro due fra i maggiori Paesi europei:

– sono stati coinvolti diversi bersagli tedeschi, incluso il governo e siti web dei politici, fra questi, il sito del partito a cui appartiene il cancelliere Olaf Scholz, il sito del Ministero della Difesa, quello del Parlamento, quello della Polizia Federale e diverse autorità della polizia statale. Secondo gli osservatori, una risposta agli sforzi dell'amministrazione Scholz di fornire equipaggiamento militare all'Ucraina, autorizzando il trasferimento di 50 Gepard anti-aircraft, e annunciando la consegna di 7 sistemi di artiglieria semoventi e a fuoco rapido.
– Anche il Senato italiano, il Ministero della Difesa e l'Istituto superiore di sanità sono stati presi di mira con attacchi da negazione di servizio ai propri siti web.

4. A giugno, due significative onde di attacchi sono state portate a termine contro la Lituania e la Norvegia in risposta agli sviluppi geopolitici che sono avvenuti fra questi Paesi e la Russia:

– seguendo la decisione del governo lituano di fermare il transito di beni russi verso Kaliningrad, un'ondata rilevante di attacchi ha colpito i servizi pubblici lituani e il settore privato. Durante l'attacco, Jonas Skardinskas, il capo della cybersecurity presso il Centro di Cyber Sicurezza Nazionale Lituano, ha avvisato che i disagi con i trasporti, i settori finanziari e quello energetico sarebbero potuti continuare per diversi giorni amplificando l'impatto dell'attacco. Ad un certo punto la maggioranza dei siti web lituani non era accessibili tramite indirizzi IP esterni al paese, più probabilmente come misura preventiva finalizzata a mitigare la portata dell'attacco.
– Lo stesso mese, diverse organizzazioni norvegesi sono state disconnesse. Si pensa che questo attacco sia stato eseguito come risultato di una disputa riguardante il transito attraverso il territorio norvegese verso un estrattore di carbone sotto il controllo russo situato nell'Artico.

5. A luglio, Killnet ha concentrato i propri sforzi sulla Polonia e causato l'indisponibilità di molti siti web. Molti degli attacchi sono stati diretti ai portali governativi, le autorità di tassazione e i siti web della polizia.

6. Agosto è stato un mese piuttosto intenso per Killnet. È cominciato con un attacco in Lettonia: dopo aver dichiarato la Russia come "un Paese rappresentante del terrorismo", il sito del Parlamento ha subìto un ingente attacco DDoS. Successivamente (nello stesso mese), l'Estonia ha affrontato l'attacco più esteso da quello del 2007, effettuato in risposta alla rimozione del monumento al soldato sovietico. L'efficacia di questi attacchi è stata discutibile, in quanto sembra che l'Estonia fosse ben preparata per questo genere di eventualità. Ad agosto, Killnet ha anche iniziato a concentrarsi sugli USA. Il gigante della produzione americana Lockheed Martin è stato pesantemente bersagliato da Killnet come conseguenza del rifornimento al sistema militare dell'esercito ucraino. Parallelamente Killnet ha anche bersagliato la US Electronic Health Monitoring e Tracking System e il Senato statunitense, che stava dibattendo la possibilità di inviare un aiuto addizionale all'Ucraina.

7. A settembre il gruppo ha bersagliato l'Asia per la prima volta indirizzando i suoi sforzi in particolare al Giappone, a causa del supporto giapponese all'Ucraina.

6. Disinformazione ed interferenze hacker

Con l'evolversi del conflitto scaturito dalla contesa delle Isole Kuril, Killnet ha attaccato con successo diversi siti giapponesi, incluso l'e-government, i siti

di trasporto pubblico della città di Tokyo e Osaka, i sistemi di pagamento JCB e Mixi, il secondo più grande sito web giapponese.

Come ci sono riusciti? I più grandi gruppi di hacktivisti che sono emersi nel corso degli ultimi due anni sono caratterizzati da operazioni ben strutturate che li mettono nelle condizioni di essere efficaci e di attrarre persone con maggiori skill. Queste persone sono solitamente motivate da una chiara ideologia legata allo Stato e i loro obiettivi sono parte di un manifesto che contiene un elenco di regole da seguire.

Per esempio, Killnet ha più di 100.000 iscritti nei suoi canali Telegram ed «è organizzata secondo una struttura militare con una gerarchia marcatamente top-down. Killnet consiste in un insieme di squadre preparate ad eseguire attacchi che rispondono ad un ordine principale. Attualmente esistono una dozzina di sottogruppi fra i quali il primario è Legion. Tutti questi gruppi sono guidati da un hacker anonimo con nickname KillMilk, che ha annunciato la sua intenzione di distaccarsi dal gruppo a luglio, rimanendo ancora coinvolto nelle attività del gruppo. Legion e le squadre (conosciute come: "Jacky", "Mirai", "Impulse", "Sakurajima", "Rayd", "Zarya", "Vera", "Phoenix", "Kajluk", "Sparta" and "DDOSGUNG") sono considerate le forze speciali di Killnet, con Legion identificata come la sua forza di cyber-intelligence»[72].

Tanti piccoli team organizzati attorno al maggiore gruppo e al suo leader, che assegna ordini d'attacco a ciascun capogruppo dando vita a infrastrutture indipendenti e migliorando così le probabilità di sopravvivenza dell'intera organizzazione. Questo metodo si è dimostrato efficace dal momento che la squadra continua a reclutare membri, crescendo numericamente. La pagina Telegram contiene regole, discussioni riguardanti gli obiettivi e le istruzioni rispetto a creare/unirsi a nuove squadre per i membri che cercano autonomia o un avanzamento gerarchico. L'evoluzione di Killnet li ha messi nella situazione in cui gli altri gruppi vogliono collaborare con loro, o ufficialmente unire le forze.

Un nuovo interessante fenomeno riguarda i metodi di reclutamento del gruppo. Diversamente da Anonymous, che è orgoglioso di dare il benvenuto a chiunque, senza imporre alcun prerequisito riguardante skill o piani specifici, la nuova era hacktivista accetta solo membri che rispettano prerequisiti minimi. Molti gruppi, come Killnet e le sue squadre, scelgono di investire in programmi di recruitment, pubblicizzati sui propri canali Telegram. Alcuni gruppi hanno istituito un processo di preselezione per assumere solo hacker competenti o esperti di un particolare campo, per ridurre il rischio di fare errori che potrebbero compromettere le operazioni.

In ogni caso, Check Point Software ha recentemente osservato che KillNet affida le istruzioni sugli attacchi DDoS alle masse, forse a causa della mancanza di forza-lavoro necessaria per portare a termine le azioni pianificate e in molteplici occasioni ha offerto ricompense economiche agli affiliati.

Il processo di recruitment è simile per molti gruppi russi. Per esempio, XakNet (che si definisce come il "Team dei Patrioti Russi") è un gruppo di utenti russi attivo all'incirca da marzo 2022. Il gruppo minacciava di contrattaccare per qualunque attacco cyber rivolto contro la Russia e avrebbe individuato diverse entità interne all'Ucraina che hanno rubato dati ufficiali del governo ucraino. XakNet ha dichiarato che non recluteranno hacker, *pentesters* (specialisti nell'esecuzione di test di vulnerabilità di siti web), o specialisti Osint senza esperienza e capacità dimostrate.

Un altro gruppo piuttosto rigido sul reclutamento è quello filorusso di NoName057(16) che investe parte delle sue risorse per offrire un training adeguato ai seguaci tramite canali Telegram, piattaforme di e-learning, tutorial, corsi e attività di mentoring, svolta anche nei canali di supporto in lingua inglese.

I gruppi di hacktivisti si sforzano costantemente di utilizzare strumenti più avanzati per eseguire i loro attacchi, dal momento che più gli attacchi arrecano danni più il gruppo guadagna in termini di notorietà ed esposizione. Nonostante i segnali dell'uso di tecniche avanzate, la maggior parte dell'attività rimane concentrata attorno agli attacchi DDoS tramite il ricorso a enormi botnet (rete di computer zombie sotto il controllo di un'unica entità). Questi attacchi sono tuttavia differenti, suddivisi in attacchi DDoS volumetrici, applicativi

72. Check Point Research 2022.

e infrastrutturali[73], rispetto ai quali non è possibile abbassare la guardia.

7. Conclusioni

Una delle escalation più significative dei vari conflitti che si sono verificati negli ultimi anni può essere identificata come l'attivismo politico nel cyberspazio. Per circa trent'anni, l'hacktivism ha rappresentato un modo per rivendicare il proprio protagonismo, individuale e collettivo, e non sembrava porre rischi significativi alle organizzazioni globali pur provocando danni variamente quantificabili[74]. Oggi, all'inizio degli anni Venti del nuovo secolo, essendo diventato più organizzato, strutturato e sofisticato, l'hacktivism ha inaugurato una nuova era. Solo nel conflitto Russo-Ucraino si contano ben 112 gruppi di hacktivisti che parteggiano per l'una o per l'altra parte in guerra. E i numeri aumentano costantemente. Poiché molti gruppi di hacktivisti hanno un'agenda politica legata agli Stati, questi ultimi potrebbero essere interessati a supportarli in maniera sempre più rilevante e non solo in tempo di guerra.

Il coinvolgimento di attori non statali, il loro utilizzo da parte dei governi, gli attacchi alle infrastrutture civili anche attraverso *ransomware gangs* per attaccare la catena di approvigionamento delle aziende dei paesi alleati coi belligeranti, con l'obbiettivo sia di interferire con la produzione di armi che con l'erogazione di servizi essenziali, sta trasformando Internet in una trincea di guerra. Amaro preludio della fine dell'utopia di un mondo pacifico perché iperconnesso e interdipendente grazie alla Rete.

Riferimenti bibliografici

I. Agrafiotis, J.R.C. Nurse, M. Goldsmith et al. (2018), *A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding, how they propagate*, in "Journal of Cybersecurity", vol. 4, 2018, n. 1

J. Assange (2012), *Internet è il nemico. Conversazione con Jacob Appelbaum, Andy Muller-Mauguhn e Jeremie Zimmermann*, Giangiacomo Feltrinelli Editore

Autonome A.f.r.i.k.a. gruppe (a cura di), L. Blisset, S. Brunzels (2001), *Comunicazione-guerriglia. Tattiche di agitazione gioiosa e resistenza ludica all'oppressione*, DeriveApprodi, 2001

F. Berardi Bifo (2011), *La sollevazione. Collasso europeo e prospettive del movimento*, Manni Editori, 2011

H. Bey (2007), *T.A.Z. Zone Temporaneamente Autonome*, ShaKe, 2007; tit. or. *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*, Autonomedia, 1991

J.D. Bolter, R. Grusin (2000), *Remediation: Understanding New Media*, Mit Press, 2000

R.R. Brooks, I. Oxcelik, J. Oakley, N. Tusing (2021), *Distributed Denial of Service (DDoS): A History*, IEEE, 2021

Check Point Research (2022), *The New Era of Hacktivism. State Mobilized Hacktivism Proliferates to the West and Beyond*, 29 September 2022

G. Coleman (2016), *I Mille volti di Anonymous. La vera storia del gruppo hacker più provocatorio al mondo*, Stampa Alternativa, 2016; tit. or. *Hacker, Oaxes, Whistleblower, Spy: The Many Faces of Anonymous*, Verso, 2014

Critical Art Ensemble (1998), *Disobbedienza Civile Elettronica e altre idee impopolari: come sopravvivere e resistere nella società del controllo*, Castelvecchi, 1998; tit or. *Critical Arts Ensemble, Civil Disobedience,* Autonomedia, 1996

73. Csirt Italia 2022.

74. Agrafiotis-Nurse-Goldsmith et al. 2018.

Critical Art Ensemble (1995), *Sabotaggio elettronico. Il primo gruppo americano di critica e attacco ai mass media*, Castelvecchi, 1995

Csirt Italia (2022), *Attacchi DDOS ai danni di soggetti nazionali ed internazionali avvenuti a partire dall'11 Maggio 2022: Analisi e mitigazione*, 13 maggio 2022

A. Curioni, A. Giannuli (2019), *Cyberwar. La guerra prossima ventura*, Mimesis edizioni, 2019

Cyber Infrastructure & Security Agency (2021), *Cyber-Attack Against Ukrainian Critical Infrastructure*, 20 July 2021

D.E. Denning (1999), *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Global Problem Solving Information Technology and Tools, December 10, 1999

M. Deseriis (2017), *Hacktivism, On The use of botnet in Cyberattacks,* in "Theory, Culture and Society", vol. 34, 2017, n. 4

M. Deseriis, G. Marano (2008), *Net.Art. L'arte della connessione*, Shake, 2008

A. Di Corinto (2022), *#OpRussia: Anonymous dichiara guerra a Putin nel cyberspazio*, in "La Repubblica", 4 marzo 2022

A. Di Corinto (2015), *Anonymous minaccia l'Arabia saudita: "Non uccidete Alì"*, in "La Repubblica", 30 settembre 2015

A. Di Corinto (2015a), *Anonymous: "Abbiamo violato la rete jihadista"*, in "La Repubblica", 8 febbraio 2015

A. Di Corinto (2014), *Anonymous ruba gli account del Ku Klux Klan: operazione "Giù il cappuccio", rivelati esponenti*, in "La Repubblica", 18 novembre 2014

A. Di Corinto (2014), *Un dizionario hacker*, Manni Editori, 2014

A. Di Corinto (2010), *Con Wiki, senza amare Julian. Hacker italiani a favore della trasparenza ma non dell'australiano*, in "Il Sole 24 Ore", 14 dicembre 2010

A. Di Corinto (2001), *Don't hate the media, become the media*, in AA.VV., "La sfida al G8", Manifestolibri, 2001

A. Di Corinto, T. Tozzi (2002), *Hacktivism. La libertà nelle maglie della rete*, Manifestolibri, 2002

R. Dominguez (2003), *Illegal Knowledge? Strategies for new media activism*, in "Electronic Book Review", 2003

J.D. Downing, T. Villareal Ford, G. Gil, L. Stein (2001), *Radical Media. Rebellious communication and Social Movements*, Sage Publications Inc., 2001

L. Goode (2015), *Anonymous and the Political Ethos of Hacktivism*, in "Popular Communication", vol. 1, 2015, n. 1

A. Greenberg (2019), *Sandworm. A new era of cyberwar and the hunt for Kremlin's most dangerous hackers*, DoubleDay, 2019

N. Klein (2000), *No Logo: Taking Aim at the Brand Bullies*, Picador, 2000

S. Levy (1996), *Hackers, gli eroi della rivoluzione informatica*, ShaKe Edizioni Underground, 1996; tit. or. *Hackers, Heroes of the informatic revolution*, Anchor Press/Doubleday, 1984

Mandiant Intelligence (2022), *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant Intelligence, 2022

F. Massarelli (2011), *La collera della Casbah. Voci di rivoluzione da Tunisi*, Agenzia X, 2011

G. Meikle (2004), *Disobbedienza civile elettronica. Mediattivismo, come costruire una nuova sfera pubblica*, Apogeo, 2004

Microsoft Digital Security Unit (2022), *An overview of Russia's cyberattack activity in Ukraine*, 27 April 2022

L. Ninotti, S. De Tomas Colatin (2022), *Analysis of the Russian-Speaking Threat Actor NoName 057(16)*, 13 October 2022

P. Olson (2012), *We Are Anonymous: Inside the Hacker World of LulzSec*, Little, Brown and Company, 2012

M. Pasquinelli (a cura di) (2002), *Media Activism. Strategie e pratiche della comunicazione indipendente*, DeriveApprodi, 2002

N. Piro (a cura di) (1998), *Cyberterrorismo. Come si organizza un rapimento virtuale*, Castelvecchi, 1998

U. Rapetto, R. Di Nunzio (2001), *Le Nuove Guerre. Dalla Cyberwar ai Black Bloc, dal sabotaggio mediatico a Bin Laden*, RCS Libri, 2001

La Repubblica (2012), *Anonymous attacca la Costituzione "Il popolo deve difendersi dai tiranni"*, 5 marzo 2012

T. Rid (2022), *Misure Attive. Storia segreta della disinformazione*, Luiss University Press, 2022; tit. or. *Active Measures: The Secret History of Disinformation and Political Warfare*, Ferrar Straus & Giroux, 2021

M.N. Schmitt (2017) (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017

Strano Network (1996), *Net strike, no copyright, Et (:- Pratiche antagoniste nell'era telematica*, AAA Edizioni, 1996

A. Tiddi (2002), *Precari. Percorsi di vita tra lavoro e non lavoro*, DeriveApprodi, 2002

T. Tozzi (2019), *Le radici dell'hacktivism in Italia, 1969-1989. Dallo sbarco sulla Luna alla caduta del muro di Berlino*, Accademia di Belle Arti di Firenze, 2019

M. Veneziani (2006), *Controinformazione. Stampa Alternativa e giornalismo d'inchiesta dagli anni Settanta ad oggi*, Castelvecchi, 2006

G. White (2022), *Crime dot com. Il potere globale dell'hacking dai virus ai brogli elettorali,* Odoya, 2022; ed or. *Crime Dot Com: From Viruses to Vote Rigging, How Hacking Went Globa*, Reaktion publishing, 2020

K. Zetter (2015), *Countdown to zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, 2015

.Zip!puntozip (1997), *Hot Web. Guida ai siti alternativi e radicali su Internet*, Castelvecchi, 1997

Sitografia

https://t.me/itarmyofukraine2022
https://t.me/itarmyofukraine2022/1637
https://t.me/c/1228309110/34219
https://www.ccc.de/en/
https://web.archive.org/web/20010201081900/http://www.netstrike.it/
http://www.billboardliberation.com/
https://it.wikipedia.org/wiki/Partito_Pirata
https://web.archive.org/web/20120208220331/http://www.rtmark.com/gatt.html
https://web.archive.org/web/*/www.thehacktivist.com