Volontari cibernetici: il caso dell'«IT Army» ucraino

Formazione

Secondo le informazioni disponibili, subito dopo l'invasione russa del 24 febbraio 2022, Mychajlo A. Fedorov, Vice Primo ministro e Ministro della Trasformazione digitale dell'Ucraina, ha avuto un incontro con Yegor Aushev, noto imprenditore ucraino nel campo delle tecnologie informatiche, per discutere la possibilità di formare un'organizzazione di volontari con il compito di contribuire a proteggere le infrastrutture digitali dell'Ucraina (Soesanto 2023, 94).

Il 26 febbraio 2022, il Ministero della Trasformazione digitale ha annunciato l'apertura di un canale della piattaforma Telegram del neocostituito «IT Army of Ukraine» ("Esercito cibernetico dell'Ucraina"). Questo canale Telegram ha rapidamente attirato notevole attenzione, anche al di là dei confini nazionali, giungendo a superare, al suo apice, la soglia dei 300.000 utenti iscritti. L'IT Army si è poi provvisto anche di un sito web e di un profilo su Twitter. Altri Ministeri ucraini hanno sostenuto l'iniziativa: in particolare, il Ministero ucraino dell'Istruzione e della Scienza ha invitato gli appartenenti al mondo della ricerca scientifica e dell'istruzione superiore a unirsi all'organizzazione (Soesanto 2023, 94).

Organizzazione

Secondo alcuni esperti (Soesanto 2022; 2023), l'IT Army conserverebbe un team «interno» (*in house*) composto con ogni probabilità da esperti dei servizi di *intelligence* e delle forze armate dell'Ucraina, nonostante le smentite dalle autorità di Kyiv a questo riguardo (Waterman 2023). Laddove effettivamente presente, tale assetto organizzativo consentirebbe al governo ucraino di guidare l'IT Army con il vantaggio della *plausible deniability* ("negazione plausibile").

In ogni caso, come è stato notato (Soesanto 2023, 95), l'IT Army non funziona in modo isolato; infatti, intorno all'organizzazione originaria si è sviluppato un intero «ecosistema» digitale, comprendente numerosi altri gruppi per attacchi DDoS[1], sviluppatori di strumenti per tale tipo di attacchi, *hacktivists*, piattaforme per *data leak* ("fuga di dati") e appunto volontari con base in Ucraina e all'estero (si veda, per esempio, Tidy 2022).

IT Army, di fatto, ha anche potuto beneficiare del sostegno attivo o passivo di aziende tecnologiche e informatiche con base negli Stati Uniti e in Europa, comprese alcune tra le più note e rilevanti del mondo (da ultimo, si veda Srivastava 2023).

Attività

Alle attività a protezione dell'Ucraina, l'organizzazione inizialmente è intervenuta su siti web russi con l'obiettivo di diffondere disinformazione e seminare sfiducia tra gli avversari. Successivamente ha avviato operazioni più avanzate, tra cui campagne cibernetiche di natura offensiva che hanno condotto alla violazione di popolari piattaforme russe, al sabotaggio di imprese e, persino, di reti elettriche in Russia.

I volontari partecipano direttamente a queste attività cibernetiche di carattere offensivo. Sino a ottobre 2022, essi trovavano direttamente sul canale Telegram di internet persino una lista di obiettivi russi, che cambiava più volte alla settimana, insieme con strumenti che consentivano e consentono loro di partecipare ad attacchi cibernetici DDoS.

[1] Con l'espressione DDoS (*Distributed Denial of Service*) si designa un malfunzionamento dovuto a un attacco cibernetico che causa la saturazione deliberata delle risorse di un sistema informatico, come un sito web su un web server, fino a renderlo non più in grado di erogare il servizio; a differenza del semplice DoS (*Denial of Service*), nel caso dell'attacco DDoS il traffico che colpisce la vittima proviene da molteplici fonti.

I volontari non devono possedere, necessariamente, elevate conoscenze e competenze tecniche per contribuire all'azione dell'IT Army: infatti l'organizzazione oggi mette anche a disposizione una *botnet* che consente agli utenti interessati di partecipare con facilità ad attacchi cibernetici coordinati (Shore 2022; Fendorf 2023).

A essere colpita dalle operazioni cibernetiche è una vasta gamma di obiettivi economici e governativi. Secondo le analisi disponibili (Fendorf 2023), il tipo di bersaglio più colpito sarebbe il settore finanziario, principalmente con attacchi DDoS, ma anche con l'esposizione di informazioni sensibili; seguirebbero, in ordine decrescente di operazioni rivendicate, aziende tecnologiche e informatiche, siti e reti governative, organi di stampa e istituzioni culturali, il settore commerciale, trasporti pubblici, il settore energetico, aziende manufatturiere. Ad oggi, altri settori cruciali, come quello sanitario, non sono stati invece interessati da attacchi cibernetici dell'IT Army.

A differenza della grande maggioranza delle organizzazioni o dei collettivi *cyber* associati a uno Stato, l'IT Army fornisce un registro pubblico delle proprie operazioni cibernetiche. In aggiunta agli attacchi, la piattaforma online dell'IT Army offre l'opportunità di condividere documenti trafugati e altro materiale (per esempio, Fendorf 2023).

Ruolo e *status* dei volontari

Il numero esatto dei volontari attivi dell'IT Army è ignoto, per quanto presumibilmente significativo. Analogamente, con poche eccezioni, non si conoscono nemmeno i loro profili e le loro motivazioni individuali. Secondo alcuni esperti, è ragionevole ipotizzare che una parte di essi possa aver avuto in passato esperienze in campo militare o di *intelligence* (Soesanto 2023, 98-99). Si può anche supporre che questi soggetti siano motivati principalmente dal desiderio di contribuire alla difesa dell'Ucraina; a differenza dei combattenti stranieri che sono accorsi fisicamente nell'area del conflitto (cfr. Marone 2022), questi volontari cibernetici possono naturalmente prestare la loro assistenza a distanza, da posizioni di sicurezza e *comfort*.

A questo proposito, è opportuno aggiungere che al momento lo stesso *status* giuridico di questi volontari cibernetici operanti in Stati membri dell'Unione Europea e/o della NATO appare piuttosto incerto (si vedano Biggerstaff 2023; Waterman 2023). Ai volontari dell'IT Army viene raccomandato, peraltro, di utilizzare una rete privata VPN; ciò fa sì che un volontario possa risultare attivo in un Paese in cui non si trova veramente (Soesanto 2023, 99).

Da parte sua, già a marzo 2022, la Federazione Russa ha ufficialmente condannato un'«aggressione cibernetica» a suo danno, imputando presunte responsabilità anche all'«Occidente» (Shore 2022).

Evoluzione

A giudicare dal numero di iscritti al canale Telegram ufficiale, dopo un picco di partecipazione nella primavera del 2022, il numero dei volontari dell'IT Army si è ridotto, pur rimanendo consistente. L'organizzazione ha cercato di affrontare questa sfida con diverse strategie e accorgimenti, tra cui il ricorso a elementi di «*gamification*» e di competizione tra volontari; per esempio, nell'ottobre 2022 ha introdotto una modalità attraverso cui gli utenti possono verificare le statistiche relative al proprio contributo ad attacchi DDoS (Soesanto 2023, 101).

Nonostante queste difficoltà, secondo gli esperti, l'IT Army ha mostrato un buon livello di organizzazione e notevole flessibilità ed è stato in grado di affinare la sua azione nel corso del tempo (in particolare, Soesanto 2023).

Conclusioni

La formazione dell'IT Army ucraino rappresenta un fenomeno senza precedenti. Questa organizzazione composta ufficialmente da volontari, formata subito dopo l'invasione russa del

2022, ha consentito all'Ucraina di potenziare le proprie capacità cibernetiche (Ling 2022), peraltro nel confronto diretto con uno Stato, la Federazione Russa, ben noto per la sua abilità ed esperienza nella sfera *cyber*. L'azione dell'IT Army, non priva di aspetti controversi, non si colloca però nell'ambito tradizionale dello sforzo centralizzato di uno Stato sovrano, tanto più in tempo di guerra, ma prevede il contributo di migliaia di volontari attivi in tutto il mondo, in virtù di modalità organizzative apparentemente caratterizzate da un elevato livello di decentralizzazione. Il fattore della dispersione dei volontari dell'IT Army in numerosi Paesi, tra cui Paesi occidentali, chiama anche in causa la questione delicata non soltanto del loro *status* giuridico, ma anche delle potenziali responsabilità degli Stati di cui sono cittadini o residenti (si veda, tra gli altri, Shore 2022).

Bibliografia

- Biggerstaff W.C (2023). The Status of Ukraine's "IT Army" Under the Law of Armed Conflict. *Articles at War*, The Lieber Institute at West Point, 10 maggio, testo disponibile al sito: https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/ (consultato il 18 luglio 2023).
- Fendorf K. (2023). The Dynamics of the Ukrainian IT Army's Campaign in Russia. *Lawfare*, 15 giugno, testo disponibile al sito: https://www.lawfaremedia.org/article/the-dynamics-of-the-ukrainian-it-army-s-campaign-in-russia (consultato il 18 luglio 2023).
- Ling J. (2022). Ukraine's Online Volunteers Go After Russian Targets. *Foreign Policy*, 3 maggio, testo disponibile al sito: https://foreignpolicy.com/2022/05/03/ukraine-it-army-hackers-russia-war/ (consultato il 18 luglio 2023).
- Marone F. (2022). *I combattenti stranieri a sostegno dell'Ucraina*. Osservatorio Strategico 01-22, IRAD – CASD, Ministero della Difesa, testo disponibile al sito: https://www.difesa.it/SMD_/CASD/IM/CeMiSS/DocumentiVis/Osservatorio_Strategico_2022/Osservatorio_Strategico_2022_n_1/09_Marone_OS_1_ITA_2022.pdf (consultato il 18 luglio 2023).
- Shore J. (2022). Don't Underestimate Ukraine's Volunteer Hackers. *Foreign Policy*, 11 aprile, testo disponibile al sito: https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/ (consultato il 18 luglio 2023).
- Soesanto S. (2022). *The IT Army of Ukraine*. CSS Cyberdefense Report. Center for Security Studies (CSS), ETH Zürich, testo disponibile anche al sito: https://css.ethz.ch/en/center/CSS-news/2022/06/the-it-army-of-ukraine.html (consultato il 18 luglio 2023).
- Soesanto S. (2023). Ukraine's IT Army. *Survival*, 65: 93-106.
- Srivastava M. (2023). Ukraine innovates on cyber defence. *Financial Times*, 18 luglio, testo disponibile al sito: https://www.ft.com/content/94f3274b-7b9f-458f-bb62-4e061d987281 (consultato il 19 luglio 2023).
- Tidy J. (2022). Meet the hacker armies on Ukraine's cyber front line. *BBC News*, aprile, testo disponibile al sito: https://www.bbc.com/news/technology-65250356 (consultato il 18 luglio 2023).
- Waterman S. (2023). Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts. Newsweek, 21 febbraio, testo disponibile al sito: https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970 (consultato il 18 luglio 2023).