Ucraina e guerra informatica

written by Leonid Savin | April 1, 2022
di Leonid Savin

Nella sua recente intervista al canale televisivo giapponese TBS, il presidente della Bielorussia Alexander Lukashenko [1] ha affermato che le armi informatiche sono più pericolose delle armi nucleari. Lukashenko ha spiegato che tali armi sono difficili da rilevare e che "non siamo pronti ad avere paura del crimine informatico e delle armi informatiche". C'è una logica nelle sue parole. Se consideriamo l'informatica come la scienza del feedback e dell'interazione uomo-macchina, allora anche le armi nucleari fanno parte dei cyber asset, anche se siamo abituati a pensare al "cyber" solo come a Internet e alle attuali applicazioni di controllo e comunicazione legate ai gadget tecnologici.

Le armi nucleari sono servite come strategia di deterrenza per decenni e sono state usate solo due volte, dagli Stati Uniti nel 1945 contro i civili nelle città giapponesi. Le armi informatiche, sin dalla loro comparsa sotto forma di malware, sono state utilizzate come mezzo di guerra segreto, sebbene il loro effetto sia principalmente un danno materiale e finanziario.

Fondamentalmente, "cyber" è un concetto ampio, come fenomeno e sfera di attività. Dai social media al fornire comando e controllo sul campo di battaglia, tutto questo è "cyber". L'intensa fase militare della guerra include inevitabilmente tecniche di manipolazione via Internet, ma anche in assenza di combattimento lo scontro invisibile non si ferma. Attacchi di hacking alle infrastrutture governative, hack nei sistemi informatici per rubare e distribuire dati, distribuire vari contenuti che fanno parte di informazioni e operazioni psicologiche: tutti questi elementi della guerra informatica sono costantemente utilizzati nel confronto tra Paesi.

La crisi ucraina non fa eccezione. I sistemi Starlink di Elon Musk sono utilizzati in Ucraina [2] per la ricognizione preliminare e il targeting. Varie piattaforme diffondono appelli alla violenza e raccolgono fondi. Ci sono casi di utilizzo ibrido di Internet. Il 14 marzo, le forze ucraine hanno lanciato un missile balistico Tochka-U a Donetsk. Venti persone sono state uccise e altre 30 ferite, tutte civili, compresi bambini. Il giorno prima, sui social network era apparso un appello ai residenti di Donetsk, a nome del Comitato delle Madri del Donbas, per partecipare a una manifestazione nella piazza centrale alle 12. Fu in questo momento che l'incidente si verificò nel centro della città. "Il Comitato delle Madri del Donbas" è una finta struttura creata dai servizi di sicurezza ucraini per portare avanti provocazioni.

Collettivi di hacker di diversi Paesi si sono divisi le posizioni: alcuni di loro stanno attaccando i siti web del governo russo, mentre altri stanno facendo lo stesso per l'Ucraina. Spesso è la società, non lo Stato, a subire tali attacchi.

Il 22 marzo si è saputo che la più grande azienda agricola russa, Miratorg, era stata attaccata da un malware crittografico. Secondo gli specialisti che si occupano del problema, il processo di recupero dei dati è difficile a causa del lavoro necessario per trovare un codice per il trojan stesso e per i file interessati.

Gli Stati Uniti, nel frattempo, stanno usando il conflitto per i propri scopi, inclusa la sicurezza informatica. Il 21 marzo, la Casa Bianca ha rilasciato una dichiarazione in cui si afferma che la Russia potrebbe lanciare attacchi informatici sul territorio degli Stati Uniti, quindi dobbiamo "accelerare il nostro lavoro per rafforzare la sicurezza informatica domestica e la resilienza nazionale". Secondo Biden, "la Russia potrebbe impegnarsi in attività informatiche dannose contro gli Stati Uniti, anche in risposta alle sanzioni

economiche senza precedenti che le abbiamo imposto insieme ai nostri alleati e partner. Questo è uno degli elementi strategici della Russia. Oggi, la mia amministrazione sta ripetendo questi avvertimenti sulla base dell'intelligence che il governo russo sta esplorando possibili opzioni di attacco informatico". Tutto questo è stato detto senza alcuna prova.

Poiché il conflitto esacerba la realtà politica, i suoi partecipanti sono costretti a riconsiderare molte disposizioni che in precedenza davano per scontate. Lunedì 21 marzo, il tribunale di Tverskoi a Mosca ha stabilito che Facebook e Instagram, applicazioni software di Meta Platforms, sono estremisti. Le loro attività sono ora completamente vietate in Russia. A Meta, infatti, è vietato aprire filiali e svolgere attività commerciali in Russia, in quanto tali attività sono dirette contro il Paese, i suoi cittadini e le forze armate.

In precedenza, su Facebook era stata diffusa una grande quantità di contenuti che chiedevano l'uccisione dei russi [3], con l'iniziativa della dirigenza aziendale. Entrambe le reti sono state bloccate in Russia all'inizio di marzo. Instagram ha ignorato più di 4.500 richieste di rimuovere i falsi sulle operazioni speciali delle truppe russe in Ucraina e incitamenti per manifestazioni non autorizzate.

Ora il tribunale ha posto fine alla questione. Il rappresentante di Meta in tribunale ha cercato di giustificare che gli utenti russi si affidano a Facebook e Instagram come piattaforme di comunicazione. Ha inoltre sottolineato che le informazioni che hanno causato le pretese delle autorità sono una parte trascurabile del flusso totale di informazioni e la società ha già pagato multe per violazioni. E il blocco comporterebbe la perdita di accesso a un'enorme quantità di "informazioni non controverse". Ma dato che i cittadini e le organizzazioni non saranno perseguiti per estremismo per l'utilizzo di Facebook e Instagram, tale accesso è praticamente preservato. L'unica domanda è sull'uso dei server VPN per aggirare il blocco. È improbabile, ovviamente, che la

maggior parte dei cittadini che hanno account Facebook e Instagram intraprendano tale azione.

L'importante è che Meta perda l'opportunità di fare soldi con i cittadini russi. Ordinare pubblicità su entrambi i social network o scambiare azioni Meta può qualificarsi come finanziamento di attività estremiste: questa è una responsabilità penale. Inoltre, qualsiasi esposizione pubblica di simboli – sul sito web, alle porte di negozi e caffè, sull'auto, sui social network, su manifesti e biglietti da visita – sarà motivo di responsabilità amministrativa fino a 15 giorni d'arresto.

Tuttavia, ci sono ancora altre organizzazioni in Russia che pongono rischi per la sicurezza e distribuiscono contenuti estremisti (o rimuovono contenuti russi). Google, di proprietà di Alphabet, ha dichiarato di aver bloccato l'accesso ai media statali russi in tutto il mondo e di aver rimosso i contenuti sulle azioni della Russia in Ucraina che violano le sue politiche. Google ha rimosso 1.000 canali e più di 15.000 video da YouTube [4]. Anche Apple ha seguito questo esempio e ha bloccato il traffico diretto e le segnalazioni di incidenti relativi all'Ucraina in collaborazione con le autorità locali. Con una mossa simile, Apple ha anche bloccato l'accesso alle app multimediali gestite dallo Stato, come RT News e Sputnik, in tutte le regioni dell'AppStore al di fuori della Russia. Apple ha anche sospeso le vendite di prodotti e smesso di esportare nel suo canale russo.

È molto probabile che YouTube sarà la prossima piattaforma ad essere bloccata in Russia. Molti esperti ritengono inoltre che sia necessario il monitoraggio di altre app e social network più piccoli, nonché di vari media occidentali che diffondono notizie false sulla Russia e che dovrebbero essere tutti bloccati e/o banditi in Russia.

Certamente, questi divieti dovrebbero essere considerati una misura importante e a lungo ritardata per ripristinare la

sovranità informativa della Russia. L'esperienza dei social network VKontakte e Telegram mostra che la Russia può avere le sue scoperte e applicazioni che non sono inferiori a quelle occidentali. E, molto probabilmente, anche altri Paesi seguiranno questo esempio. A cominciare dalla Russia, che non è l'unico Paese in cui i social network americani sono vietati. Facebook e Twitter sono bloccati in Cina dal 2009. Un'alternativa alle reti occidentali in Cina è la piattaforma multifunzionale WeChat. La situazione con queste reti è simile in Iran. Twitter è stato bandito in Corea del Nord dal 2016. Anche in Turkmenistan non ci sono social network. È probabile che presto altri Paesi prenderanno il comando, limitando l'influenza distruttiva esercitata dalle reti americane.

Ma la questione della regolamentazione legale di Internet in quanto tale rimane irrisolta. I dibattiti su questo sono in corso da anni e finora i Paesi si sono divisi in due campi: uno è a favore di un Internet sovrano e l'altro sta cercando di imporre una politica di multistakeholders, in cui si promuovono le proprie aziende come attori importanti nel commercio di Internet.

[1] https://president.gov.by/en/events/intervyu-yaponskomu-telekanalu-tbs-1647515901

[2] https://www.dw.com/en/ukraine-is-using-elon-musks-starlink-for-drone-strikes/a-61270528

[3] https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/

[4] https://www.engadget.com/youtube-russian-state-backed-media-184607588.html

Traduzione a cura di Costantino Ceoldo

Foto: Idee&Azione

1° aprile 2022