Quali i primi risvolti cibernetici derivanti dal conflitto ucraino

Autor(en): **Giedermann, Stefano**

Objekttyp: **Article**

Zeitschrift: **Rivista Militare Svizzera di lingua italiana : RMSI**

Band (Jahr): **95 (2023)**

Heft 2

PDF erstellt am: **05.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-1046583

Quali i primi risvolti cibernetici derivanti dal conflitto ucraino

col
Stefano Giedemann

colonnello Stefano Giedemann,
C CYBINT, SM spec cyber

Esaminando retrospettivamente il primo anno di ostilità, sulla base di alcune tesi correnti proviamo a derivare possibili riflessioni riguardo l'efficacia militare delle operazioni informatiche russe, le ragioni per cui queste non hanno avuto un maggiore impatto strategico e le possibili lezioni. Basandoci su analisi disponibili al grande pubblico, questo approccio ci permette di comprendere meglio scenari di conflitti moderni e il ruolo cibernetico.

Premessa

La guerra in Ucraina è la prima significativa conflagrazione tra due realtà tecnologicamente avanzate nell'era cibernetica in un campo di battaglia aperto. Questo contesto ci spinge a verificare concretamente la natura della guerra moderna e l'uso della tecnologia digitale. Altrimenti detto, se i piani strategici s'intersecano spesso in modo non sempre facilmente rilevabile nelle dimensioni politiche-diplomatiche, economico-finanziarie, dell'informazione e quelle tradizionalmente cinetiche, ora concorre pure la dimensione della tecnologia digitale a ricercare quel vantaggio che permette di sbilanciare il centro di gravità strategico avversario e, di conseguenza, determinare le sorti finali del conflitto.

Per facilitare questa breve analisi, è utile ricordare che, in termini di sicurezza informatica, con *azioni cibernetiche* ci si riferisce all'uso di dispositivi dotati di capacità elaborativa e relative comunicazioni, da una parte per attaccare gli equivalenti della controparte, più comunemente il tutto volto a degradare l'infrastruttura critica dell'avversario (con una perdita significativa di informazioni e/o capacità di funzionamento). In aggiunta possiamo posizionare le azioni criminali come "attacco informatico", mentre le azioni di soggetti legati agli stati nazionali, in particolare quelle offensive, come "guerra cibernetica".

Tesi

Premessa la complessità di ottenere una effettiva oggettività nei fatti e nelle opinioni, alla lettura di diversa documentazione liberamente accessibile, la maggior parte degli osservatori occidentali concorda sul fatto che le operazioni cibernetiche russe non hanno avuto un grande impatto strategico in Ucraina, anche se sul perché c'è meno consenso. Alcuni citano l'incapacità o la reticenza informatica della Russia, mentre altri sottolineano gli sforzi difensivi dell'Ucraina e dei suoi alleati. Gli analisti variano anche nel concentrarsi sulle circostanze di questa particolare guerra o sul ruolo del cyberspazio nella guerra in generale.
Senza entrare in aspetti prettamente legati alla tattica e alla tecnica, una selezione e analisi di alcuni di questi fattori a livello strategico-operativo rivela che probabilmente erano in gioco diversi e ulteriori elementi, in parte correlabili con l'evoluzione stesso del conflitto.

Fattori

La dottrina cibernetica russa enfatizza l'intelligence, la sovversione e la guerra psicologica – Il Direttorato generale per le informazioni militari, ovvero il servizio informazioni delle Forze armate russe "GRU", è stato il principale attore degli attacchi informatici. Microsoft ha dichiarato a dicembre dello scorso anno che tutti gli attacchi distruttivi contro obiettivi ucraini a sostegno dello sforzo bellico russo sono stati responsabilità di attori associati al GRU. Sebbene questa entità faccia parte dell'esercito, il GRU è un elemento a livello nazionale non strutturato per operare in stretta integrazione con truppe regolari in condizioni di combattimento su larga scala. Questo può aiutare a spiegare perché il GRU è riuscito a eseguire una campagna strategica cibernetica, come quella contro l'infrastruttura Viasat in concomitanza con l'invasione iniziale, ma successivamente non è riuscito a mostrare molto coordinamento tattico con le unità russe sul terreno. Tuttavia, le operazioni di raccolta informazioni e propaganda – presumibilmente un punto di forza del GRU – non sono sembrate così efficaci come i suoi attacchi informatici. Tutto ciò suggerisce che una solida dottrina non è sufficiente per raggiungere determinati successi in un contesto operativo coordinato.

Le forze informatiche russe erano troppo piccole per contribuire in modo significativo a una guerra su vasta scala – Per ottenere una significativa differenza nello sforzo bellico, le operazioni informatiche russe dovrebbero scalare per adattarsi alle dimensioni della guerra stessa. Non è chiaro se la Russia abbia preso provvedimenti per far crescere le sue forze informatiche, prima o dopo

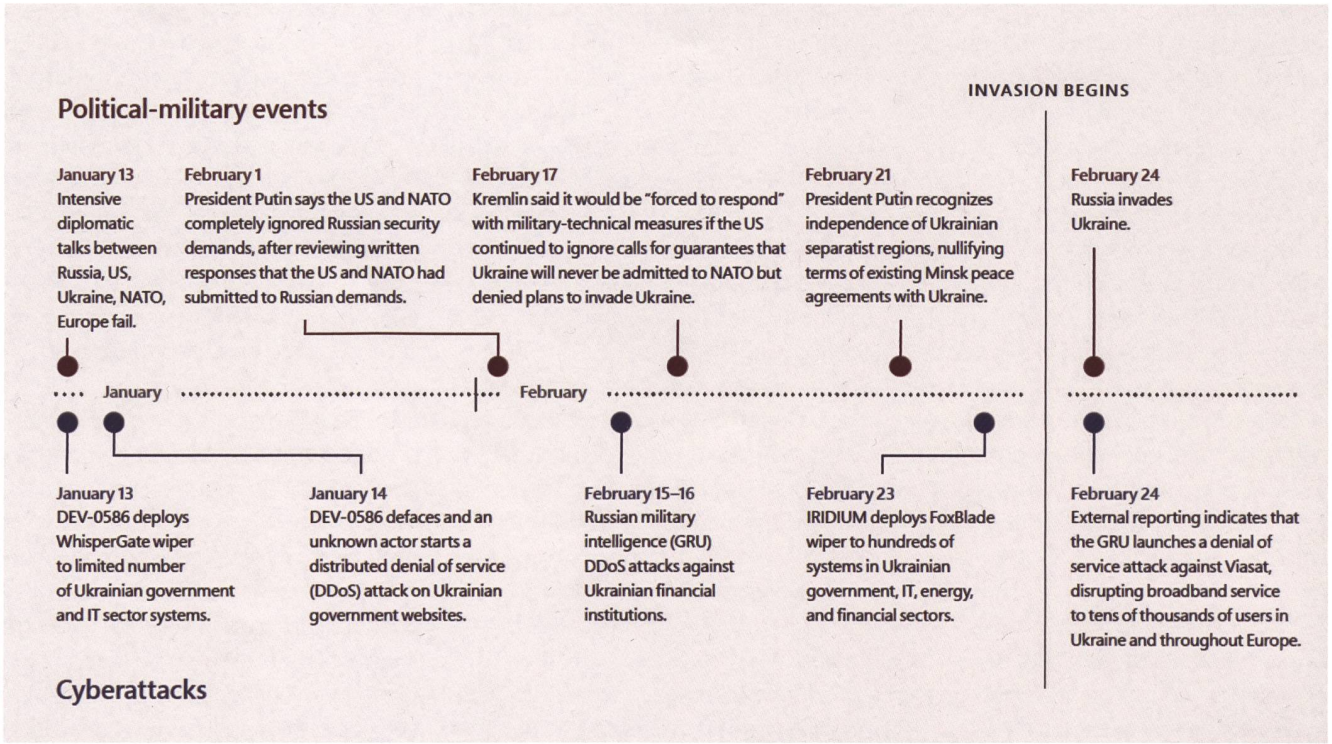
l'invasione. Il grande e altamente capace ecosistema del crimine informatico russo non ha partecipato visibilmente alla guerra, nella misura in cui molti avevano previsto sebbene le premesse lo erano. Sembrerebbe che solo alcuni presunti gruppi criminali russi e collettivi di hacker abbiano preso di mira l'Ucraina (XakNet in particolare sembra abbia effettuato diverse operazioni degne di nota), mentre la gran parte dell'attività criminale è stata negazione temporanea del servizio di basso livello (DDoS). Ulteriori indicazioni mostrano che il grosso dei gruppi ha continuato a concentrarsi su obiettivi non ucraini, con attacchi ransomware decisamente molto più lucrosi.

La Russia è stata lenta a rigenerare la capacità cibernetica una volta utilizzata – Se le forze informatiche russe fossero riuscite in qualche modo a mantenere il ritmo significativo delle operazioni viste all'inizio della guerra, avrebbero potuto avere impatti strategici più importanti nel tempo. La costatazione è inversa, con un forte calo in quantità e qualità di attacchi informatici dopo le prime settimane di conflitto. Il declino dei nuovi "wipers" e i relativi cambiamenti tattici da parte degli hacker russi suggeriscono una scorta limitata di risorse tecniche da mettere in campo con successo.

La Russia ha scelto di non concentrare la sua piena capacità cibernetica sull'Ucraina – La Russia si è astenuta dal condurre significativi attacchi informatici distruttivi o dirompenti contro gli alleati occidentali dell'Ucraina, complice i rischi nella complessa interpretazione "dell'Articolo 5" della NATO: fa eccezione ottobre, quando il GRU ha effettuato un attacco ransomware alle società di logistica e trasporto, due in Ucraina e uno in Polonia, probabilmente identificate come centrali nel supporto delle operazioni avversarie. Per contro le attività informatiche nell'ambito dello spionaggio informatico su larga scala e altre penetrazioni di rete su scala globale contro obiettivi occidentali sono risultate stabili o sono aumentate dall'inizio dell'invasione, a giudicare da numerosi rapporti dei governi occidentali e delle società di sicurezza informatica.

La Russia ha preservato le infrastrutture ucraine per facilitare l'eventuale occupazione – Analizzando le fasi strategiche con conflitto bellico, nel periodo iniziale di febbraio e marzo le attività nel contesto cibernetico e cinetico erano allineate ed effettivamente mirate alla rapida occupazione con successivo controllo del territorio. Per contro con il cambiamento del quadro strategico gli attacchi informatici sui sistemi di controllo industriale sono scemati da aprile fino a luglio. Solo a partire da agosto, dopo la necessaria preparazione operativa è rilevabile un netto riorientamento delle attività nella combinazione spazio-temporale tra azioni di disturbo cyber e la distruzione cinetica delle infrastrutture critiche, in particolare quelle legate all'approvvigionamento energetico. Queste attività hanno portato con sé altri importati fattori, quali il ricercare effetti ulteriori nella dimensione strategica, ovvero il minare la resilienza psicologica nella popolazione con l'arrivo dell'inverno.

Gli attacchi informatici della Russia hanno avuto un impatto psicologico e politico molto minore rispetto ai suoi attacchi cinetici – La violenza rilevata da ambo le parti sul campo di battaglia è ampiamente visibile tramite i media

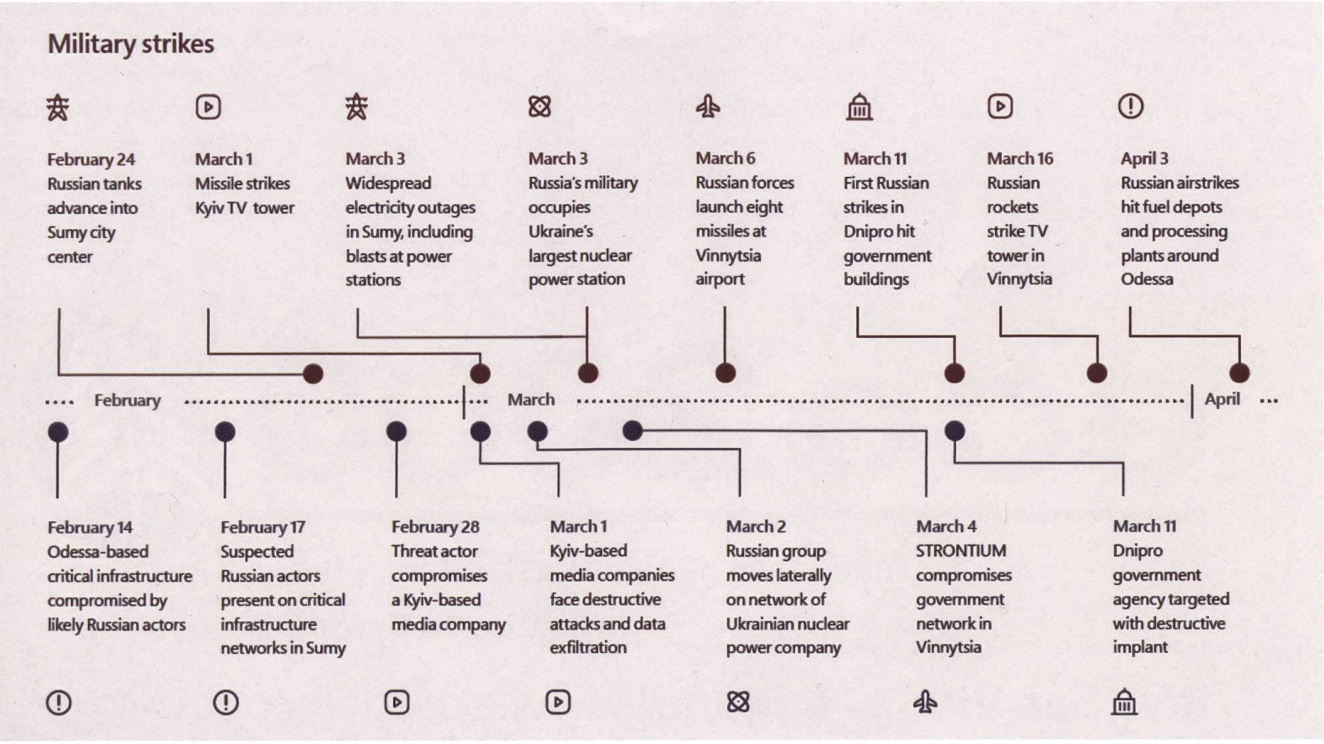


occidentali, in particolare verso una società europea che non era pronta ad accettare un conflitto di tale portata ai propri confini orientali. Alla luce di quanto, è difficile immaginare qualsiasi campagna cibernetica, non importa quanto ben costruita e persistente, che non possa aggiungere significativi elementi a questo trauma sociale e psicologico. Tuttavia, sappiamo poco delle dinamiche della politica e del morale ucraini in tempo di guerra. Plausibilmente, il sostegno popolare ucraino per continuare a perseguire la guerra è dipeso in parte dalla capacità iniziale e continua degli ucraini di ascoltare i loro leader tramite le piattaforme social, accedere ai servizi di base e comunicare con i familiari. Se così fosse una campagna, altamente efficace e sostenuta, d'interruzioni informatiche da parte di Mosca avrebbe forse potuto contribuire a far cedere il fronte interno, in particolare quello non filo-russo o di origini non russe, costringendo Kiev a sedersi rapidamente al tavolo delle trattative di fronte ad una spaccatura interna della nazione.

L'infrastruttura digitale nazionale dell'Ucraina era strutturalmente resiliente – L'infrastruttura tecnologica nazionale dell'Ucraina, anche prima della guerra, seppure non altamente moderna era sufficientemente resiliente in molti modi, non da ultimo con significativi contributi occidentali avvenuti dopo i fatti del 2014. È possibile identificare una bassa concentrazione del mercato della tecnologia a più livelli e un numero relativamente elevato di strutture d'interconnessione, il che significa che non ci sono punti critici evidenti o reti individuali la cui perdita avrebbe comportato un effetto paralizzante di Internet in Ucraina. Inoltre, il paese ha subito un fiorente aumento della forza lavoro di professionisti IT e ingegneri di rete, e questo elemento umano si è dimostrato agile, collaborativo e altamente motivato a mantenere la connettività digitale di fronte agli attacchi cinetici e cibernetici.

Alcuni sistemi miliari chiave ucraini non sono ancora stati digitalizzati o collegati in rete – Non sono stati segnalati attacchi di attrezzature militari ucraine dell'era sovietica, molte delle quali presumibilmente hanno una connettività limitata o assente. Ma allo stesso modo, non ci sono stati rapporti credibili e specifici che le moderne apparecchiature in rete dell'Ucraina siano state violate. Ad esempio, le operazioni dei droni ucraini si sono dimostrate vulnerabili al jamming russo e alla ricerca nell'ambito della guerra elettronica, ma non si trova traccia evidente di tentativi di hacking. Naturalmente, il governo ucraino e i suoi fornitori, inclusi gli alleati, non sono propensi nel pubblicizzare eventuali successi avversari nell'ambito specifico. Tuttavia un importante numero di attacchi informatici potrebbero trovare una correlazione nell'accelerazione degli aggiornamenti nelle componenti tecnologiche occidentali avvenute nel periodo.

Gli investimenti a lungo termine nell'ecosistema della difesa informatica dell'Ucraina hanno dato i loro frutti – Dal 2017 circa, gli Stati Uniti hanno ampliato molteplici iniziative per rafforzare la sicurezza informatica del governo ucraino e delle infrastrutture critiche. Inoltre, numerosi altri governi stranieri e società di sicurezza informatica hanno investito nello sviluppo di capacità informatiche ucraine per diversi anni. Le istituzioni ucraine hanno fatto investimenti paralleli propri completando nel tempo la postura informatica. Tutto ciò



concorre alle difese informatiche dell'Ucraina in tempo di guerra come dimostra il fatto che, se dal 2015 al 2017 l'Ucraina è stata vittima di tre attacchi informatici russi eccezionalmente dannosi con due interruzioni di corrente elettrica e l'attacco NotPetya, dal 2018 fino all'invasione della Russia del 2022 non ci sono stati eventi relativamente gravi; e ciò nonostante il conflitto in corso nel Donbass e l'occupazione della Crimea.

L'"IT Army of Ucraine" ha permesso ai professionisti e attivisti informatici globali di aumentare le capacità del personale ucraino – Sebbene questa organizzazione, forte di quasi 300 mila cyber combattenti nelle prime settimane dall'invasione russa secondo il New York Times, fosse stata originariamente annunciata come avente missioni sia difensive che offensive, la ricerca suggerisce che presto divenne di natura puramente offensiva e con successi limitati dal punto di vista operativo. Maggiore successo è rilevabile nella sfera psicologica, determinato dall'eco generato nell'enfasi portata dai media occidentali a fronte di alcune limitate azioni, ma dal forte impatto spettacolare, di fatto confermando che qualsiasi altro beneficio sia stato, lo è da annoverare in termini indiretti e non in modo determinante.

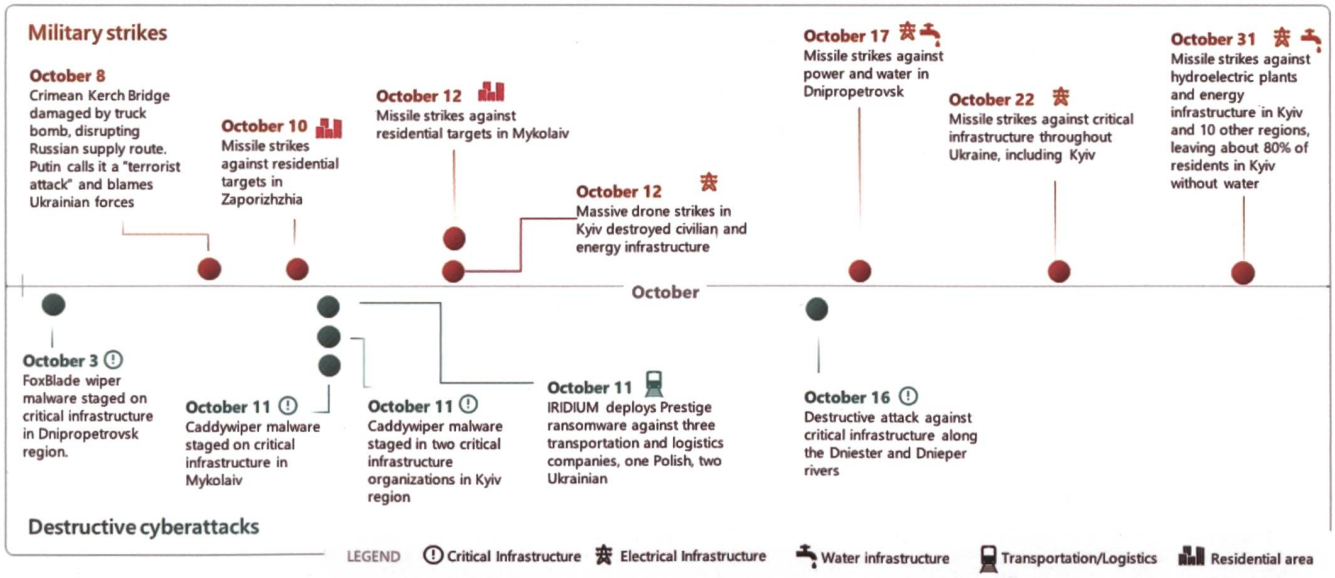
I fornitori di servizi cloud hanno aiutato l'Ucraina a migrare i dati chiave verso server sicuri al di fuori del paese – L'Ucraina ha intrapreso una migrazione cloud subito dopo l'invasione russa, allorquando la Russia ha danneggiato un data center del governo ucraino grazie a un attacco con un missile da crociera. Le agenzie governative ucraine e le società occidentali hanno definito questo passo fondamentale per la sicurezza informatica e la resilienza digitale del paese. A questa affermazione si contrappone la realtà, con necessità temporali di settimane per assicurare un'impresa così enorme e complessa. Questo suggerisce che la migrazione al cloud non può spiegare completamente il successo delle difese informatiche dell'Ucraina, sia nelle prime fasi della guerra che successivamente in quanto questa nuova tecnologia introduce nuove problematiche, quali le interruzioni del servizio e la vulnerabilità della sicurezza informatica, determinate dalle interfacce di configurazione, e l'accesso delle risorse cloud. La migrazione al cloud in particolare verso i provider come Amazon, Google e Microsoft, ha certamente migliorato la sicurezza informatica dell'Ucraina, ma probabilmente questo non è l'unico fattore decisivo.

Le aziende di sicurezza informatica hanno fornito sicurezza avanzata degli endpoint, intelligence sulle minacce e condivisione delle informazioni – Microsoft ha sostenuto che le recenti innovazioni nella sicurezza end-point, nell'intelligence sulle minacce e nella condivisione delle informazioni sono stati alcuni dei fattori più importanti nelle difese informatiche ucraine. La società ha pure dichiarato che i rilevamenti comportamentali, che sfruttano l'apprendimento automatico, hanno fatto uso di modelli di attacco noti per identificare e bloccare con successo ulteriori attacchi senza previa conoscenza del malware sottostante, né tantomeno interventi espliciti umani. Anche altre aziende, come Amazon e Google, hanno fornito uno stretto supporto alla sicurezza informatica all'Ucraina, mentre l'intelligence sulle minacce da parte di aziende e governi occidentali hanno contribuito a esporre e mitigare attività dannose. L'impatto di questi sforzi è difficile da giudicare data la complessità operativa, ma la loro portata è difficile da sottovalutare. Questa straordinaria concentrazione di capacità di sicurezza informatica presenta grandi ostacoli anche per un avversario determinato e con tante risorse come la Russia.

I sistemi Starlink hanno rafforzato la sicurezza e la resilienza delle telecomunicazioni ucraine – Il principale funzionario della sicurezza informatica ucraina ha citato Starlink come la forma più utile di assistenza digitale che l'Ucraina ha ricevuto durante la guerra. Secondo quanto riferito, Starlink ha dato numerosi contributi tangibili allo sforzo bellico, come il consentire il controllo dei droni ucraini, aiutare le truppe ucraine assediate a rimanere in contatto con i loro comandanti come pure facilitare le comunicazioni del presidente Volodymyr Zelenskyy con i leader mondiali e il pubblico globale. Sebbene l'architettura di Starlink è risultata relativamente

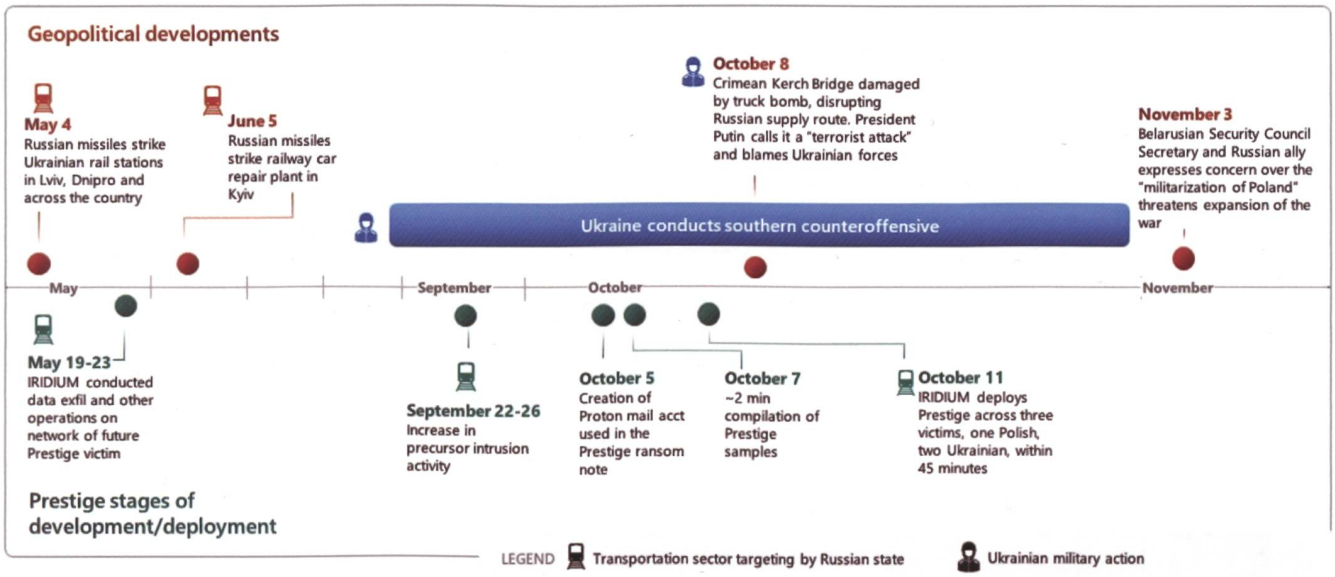
resistente agli attacchi informatici e al jamming, agli utenti di Starlink è stato chiesto di limitare la loro dipendenza perché i suoi segnali rappresentano un rischio di scoperta e targeting da parte delle forze russe. In questo senso viene però da ritenere che alcuni suoi utenti siano più importanti di altri nello sforzo bellico, dove le forze in prima linea verosimilmente sono tra gli utenti Starlink quelli decisivi. Nel citare Starlink come il canale più importante per il comando e il controllo, essi descrivono tali interruzioni come il fattore critico di successo nelle comunicazioni sul campo di battaglia. Ulteriori ricerche potrebbero indagare la misura in cui altre comunicazioni essenziali, come i dati governativi, militari e delle infrastrutture critiche, fluiscono su Starlink e sui vari altri sistemi di telecomunicazione dell'Ucraina.

Timeline of Russian cyber and military attacks on critical infrastructure in October



MICROSOFT CONFIDENTIAL Digital Security Unit

Prestige ransomware deployment underscores Russian military focus on logistics



MICROSOFT CONFIDENTIAL Digital Security Unit

Gli ucraini hanno utilizzato app di messaggistica straniere che la Russia non è in grado o non vuole colpire con attacchi informatici – Le app di messaggistica e altre app di comunicazione, come Signal, Telegram, Twitter e Zello, erano ampiamente utilizzate in Ucraina prima dell'invasione russa, rendendole canali familiari e preziosi una volta iniziata la guerra. Sono a lungo utilizzati dal governo e dai media ucraini, diventando fonti centrali d'informazione sulla politica e sulla vita quotidiana oltre che di propaganda, favorendo la tenuta del fronte interno. Inevitabile il riferimento a questo mezzo importante per il presidente Volodymyr Zelensky per rassicurare il suo popolo, in particolare nei primi giorni della guerra, quando mantenere il morale era essenziale. La Russia ha pure usato essa stessa queste stesse piattaforme per fare propaganda alla popolazione ucraina. Sono necessarie ulteriori ricerche per comprendere i molti effetti di queste piattaforme sulla progressione della guerra, che di fatto hanno sostituito altri canali fino a prima noti e diffusi come le pagine web tradizionali, inducendo allo sviluppo di nuovi motori di ricerca e analisi dei relativi contenuti.

Le operazioni cyber difensive degli Stati Uniti e della NATO, comprese quelle offensive, sono state efficaci – Il ministro della sicurezza informatica ucraino ha descritto come una costante sinergia tra il suo governo, il Cyber Command degli Stati Uniti e la National Security Agency (NSA) per proteggere le reti ucraine, in particolare delle istituzioni governative e delle installazioni militari. Ma non ci sono informazioni pubbliche sulla natura e la portata di queste attività o sul loro impatto, che verosimilmente hanno una portata ben maggiore di quanto affermato. In questo senso, desta interesse la recente pubblicazione da parte della Casa Bianca della nuova strategia nazionale nell'ambito della sicurezza cibernetica.

Conclusioni

Abbiamo presentato diversi fattori nella sfera delle operazioni cibernetiche mostrando che l'inversione di tendenza di alcuni di essi non è al momento stata sufficiente a migliorare significativamente l'utilità militare complessiva delle operazioni cibernetiche russe. Diversamente, il reputato scarso successo della Russia in Ucraina sembra, alla prova dei fatti, essere stato sovrastimato da altri fattori esterni. Tra questi citeremo l'evitare la propagazione di azioni nell'ambito della guerra cibernetica e dei relativi effetti all'infuori del contesto stretto del conflitto, ingenerando effetti a catena difficilmente prevedibili.

Conseguenze

L'attuale conflitto moderno a carattere ibrido, con importanti coinvolgimenti della sfera operativa cibernetica, sta mostrando almeno tre importanti elementi sul quale riflettere.

Il primo è la dipendenza ormai consolidata dei provider di servizi di tecnologia a vario titolo e che fungono da *proxy regolari*. Essendo sempre più permeati nelle infrastrutture e nella società civile, in caso di conflitto diventano un elemento centrale nel disegno più ampio della resilienza. Inoltre essendo parte direttamente coinvolte, essi si aggiungono e/o si sostituiscono de facto al ruolo dello Stato anche nelle attività di Threat Detection and Response, oltre che dell'Intelligence. A titolo di solo esempio, i documenti e le informazioni pubblicate dalla Microsoft nella fattispecie mostrano livelli di capacità importanti ritenute impensabili fino a poco tempo fa.

Il secondo è il ruolo dei *proxy irregolari*, determinati da gruppi di cyber criminali che possono entrare e uscire nel conflitto secondo proprie dinamiche di opportunità. Analogamente nell'ambito cinetico, essi possono acquisire e scambiare tecnologia che possono poi altrimenti esercitare a scopo di lucro, generando – a differenza di organi centralmente gestiti – dinamiche a geometria variabile che contribuiscono potenzialmente a destabilizzare il resto dell'ambiente operativo non implicato direttamente nel conflitto.

Il terzo è *l'uso duale delle tecnologie*, come ad esempio quello di Starlink e dei droni a basso costo, dove i primi entrano per stessa ammissione della NATO come infrastruttura critica nel supporto alle truppe ucraine posizionando lo stesso imprenditore Elon Musk come attore in causa nel conflitto, mentre i secondi – grazie ad ulteriori accorgimenti come quelli offerti da Pallantir nell'ambito dell'AI per il rilevamento, la gestione e attribuzione degli obbiettivi – diventano un nuovo ed efficace elemento nel combattimento a livello tattico militare.

Ulteriori riflessioni con la progressione del conflitto e il necessario diradamento della nebbia che lo avvolge nei diversi ambiti, ci permetteranno di consolidare le tesi e le relative ulteriori conseguenze. Quello che è certo, che l'attuale conflitto – inutilmente cruento e che necessita una rapida risoluzione per tutte le parti in causa mediata da un'organizzazione universalmente riconosciuta – pone nuovi e chiari accenti dell'ecosistema cibernetico, sia esso militare sia civile. ◆

Bibliografia consultabile in Internet

- 4WardPro, Russia-Ucraina, come stanno cambiando gli scenari dei cyber attacchi, Marzo 2023
- Canadian Forces College, The bear went under the mountain, Dicembre 2016
- Cf2R, Un an après, forces et faiblesses des armée russe et ukrainienne, Marzo 2023
- CSS ETH Zürich, Addendum to Cyber and Information warfare in the Ukrainian conflict, Ottobre 2018
- CSS ETH Zürich, Goodbye Cyberwar, Ukraine as Reality Check, Maggio 2022
- CSS ETH Zürich, The IT army of Ukraine, Giugno 2022
- CSS ETH Zürich, Software Supply Chain Attacks, Gennaio 2023
- DIIS, Russian hybrid warfare, Giugno 2017
- ECCRI, Cyber operations during the 2022 Russian invasion of Ukraine, Luglio 2022
- ENISA, Identifying Emerging Cyber Security Threats and Challenges for 2030, Marzo 2023
- GCSP, The Russia-Ukraine war's implications for global security, Agosto 2022
- Google, Fog of war, Febbraio 2023
- Insikt Group, Russian information operations aim to divide the western coalition on Ukraine, Luglio 2022
- ISPSW, Over five years of Russian hybrid warfare against Ukraine provide lessons, Gennaio 2020
- ISW, Russian hybrid warfare, Settembre 2020
- Microsoft, Special report on Ukraine, Aprile 2022
- Microsoft, Defending Ukraine: Early Lessons from the Cyber War, Giugno 2022
- Microsoft, Digital Defence Report 2022, Ottobre 2022
- Microsoft, Is Russia regrouping for renewed cyberwar?, Marzo 2023
- Microsoft, A year of Russian hybrid warfare in Ukraine, Marzo 2023
- Microsoft, Collaboration is crucial to strengthening cybersecurity, Marzo 2023
- NATO, Handbook of Russian information Warfare, Novembre 2016
- NATO, Strengthening security & defence, stabilizing, deterrence, Agosto 2019
- PSC, Supporting Ucraine, Compendium to US Assistance Initiatives, Febbraio 2023
- RAND, Understanding Russian hybrid warfare and what can be done about it, Marzo 2017
- RUSI, Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine, Novembre 2022
- Security Council of Ukraine, Cyber, artillery and propaganda, Dicembre 2022
- Security Week, A year of conflict, Cybersecurity industry assesses impact of Russia-Ukraine war, Febbraio 2023
- Security Week, Preparing for a Russian cyber offensive against Ukraine this winter, Dicembre 2022
- The White House, National cybersecurity strategy, Marzo 2023
- Thales, A year of Cyber Conflict in Ukraine, the extensive analysis, Aprile 2023
- US Congressional Research Service, Russia's war in Ukraine, Settembre 2022
- WEF, Global Cybersecurity Outlook 2023, Gennaio 2023