Dimensiunea cibernetică a conflictului Rusia – Ucraina
Deslușirea primei etape

De când au atras atenția în cadrul conflictului din Kosovo în 1999, atacurile cibernetice au devenit un element esențial al conflictelor din era modernă, fapt demonstrat inclusiv de atacurile cibernetice efectuate de actori statali, non-statali și semi-statali pe parcursul conflictului actual dintre Rusia și Ucraina. Astfel, este necesar ca trendurile activității cyber din timpul conflictului să fie înțelese, începând cu ziua invadării (24 februarie 2022), până la terminarea celei de-a doua etape a conflictului (12 mai 2022). În acest context, este important de luat în considerare prezicerea experților, potrivit căreia tipul activităților cibernetice vor varia pe parcursul următoarelor etape.

Înainte de a analiza trendurile observate în activitatea cibernetică a Rusiei și a Ucrainei, împreună cu alte părți terțe, este important de înțeles că informațiile despre conflicte cibernetice au atât limitări, cât și o doză de subiectivitate pe care cercetătorii trebuie să o ia în calcul. Joseph Fitsanakis a punctat următoarele limitări și prejudecăți:

- Rezistența adversarilor și a actorilor cibernetici nu este studiată
- Clasificarea informațiilor referitoare la atacuri cibernetice de către agenții guvernamentale
- Presiunea reproducerii propagandei dominante de către anumite secțiuni ale mass-mediei occidentale
- Concentrarea exclusiv pe actori cibernetici răuvoitori non-vestici
- Instinctul de a atribui prematur atacuri cibernetice unor suspecți previzibili în aparență

În ciuda acestor limitări, este important de discutat strategia Rusiei în spațiul cibernetic și de a o compara cu strategiile folosite în trecut. De asemenea, este esențial de înțeles baza pe care Ucraina și-a pus-o atât în mobilizarea suportului internațional, cât și în formarea unei armate "cyber". În plus, analizarea rolului pe care actorii terți l-au avut, în special Belarus și China, este instrumentală în evaluarea dimensiunii cibernetice a conflictului.

Strategia Rusiei

Atacurile cibernetice efectuate de Rusia pot fi împărțite în trei categorii: atacuri asupra încrederii, atacuri bazate pe capabilități și atacuri bazate pe control. Atacurile asupra încrederii se referă la atacurile cibernetice care diminuează încrederea publică în abilitatea guvernului de a-și proteja cetățenii și de a-i aproviziona cu servicii esențiale. În prima săptămână din martie 2022, se presupune că niște actori cibernetici ruși au fost implicați în lansarea unor atacuri DDOS (atacuri cibernetice în care serverele website-urilor sunt inundate cu trafic până când devin instabile) împotriva website-ului Ministerului Apărării din Ucraina. În mod similar, actorul cibernetic rus FancyBear a fost găsit responsabil de implicarea într-o campanie de phishing împotriva unei companii media ucrainene, UkrNet.

Atacurile bazate pe capabilități sunt atacurile cibernetice în care puterea adversarului este subminată prin exploatarea armelor cibernetice, cu scopul de a obține acces la infrastructura critică a adversarului și de a-i distruge capabilitățile. Spre exemplu, atunci când armata rusă invada Ucraina pe data de 24 februarie 2022, câțiva atacatori, despre care se presupune că sunt de naționalitate rusă, au distrus zeci de mii de modem-uri de internet prin satelit în Ucraina și Europa de Est. Acesta este considerat a fi unul din cele mai mari atacuri cibernetice din cadrul unui război și a cauzat o întrerupere masivă a comunicațiilor la începerea conflictului. În prima fază a războiului, actorul cibernetic proeminent rus, Sandworm, a fost în mare parte absent din motive necunoscute. Totuși, grupul și-a făcut simțită prezența în cea de-a două etapă, când a fost dezvăluit faptul că a încercat să cauzeze o cădere de electricitate printr-un malware (software malițios), care ar fi putut afecta două milioane de oameni.

Atacurile bazate pe control se referă la atacurile fizice asupra unor infrastructuri cibernetice, în care obiectivul este să obții control asupra infrastructurii critice a adversarului. Din acest punct de vedere, sunt două atacuri cibernetice care ies în evidență. Pe 1 martie 2022, o lovitură de proiectil asupra turnurilor de televiziune din Kiev a coincis cu un atac cibernetic asupra unor companii media. Câteva zile mai târziu, când armata rusă a ocupat cea mai mare centrală nucleară din Europa –Zaporojie - un actor cibernetic rus a fost detectat în rețelele unei companii de energie nucleară din Ucraina.

Tipurile de atacuri pe care actorii cibernetici ruși le-au lansat în Ucraina sunt în concordanță cu comportamentul lor în spațiul cibernetic timp de mai bine de un deceniu, de la atacurile cibernetice rusești împotriva Estoniei (a se vedea Fig. 1). În afară de Estonia, entități din Georgia și Ucraina au fost anterior vizate de aceste atacuri cibernetice.

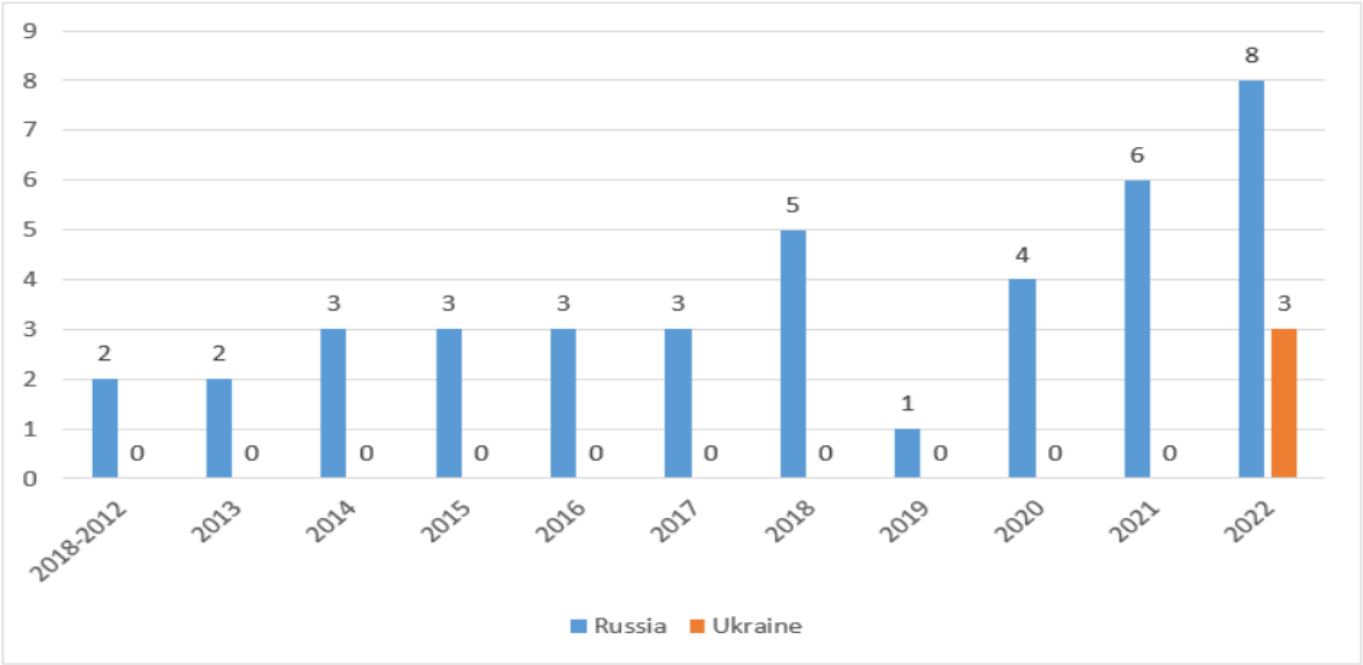
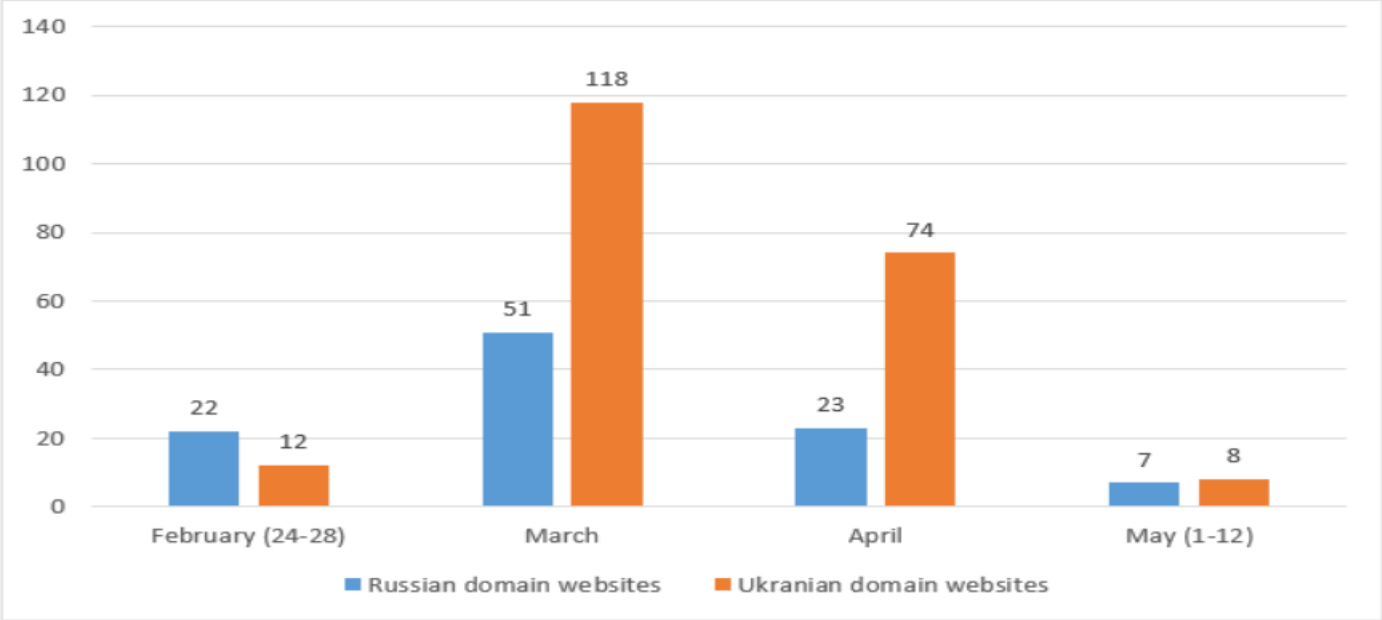


Fig.1: Atacuri cibernetice publice, stat contra stat, între Rusia si Ucraina (Sursa: Monitorul de Operațiuni Cibernetice CFR)

În legătură cu "defacement-ul" website-urilor, o arhivă de site-uri compromise, Zone H, a documentat faptul că aproximativ 210 domenii aparținând unor website-uri ucrainene au suferit un astfel de atac (a se vedea Fig.2). Este important de menționat faptul că nu poate fi clarificat câte dintre ele au fost efectuate de actori ruși. De când a început invazia, a fost scos în evidență numărul redus de atacuri cibernetice la scară mare efectuate de către actorii cibernetici ruși. Au fost găsite două motive cheie care motivează acest aspect: o eficacitate ridicată de atacuri cinetice și dificultatea de a planifica și executa atacuri cibernetice întru-un timp atât de scurt.

Fig.2: Categorizarea pe luni a domeniilor website-urilor desfigurate din Rusia și Ucraina (Sursă: Zone-H)



Răspunsul Ucrainei

Pentru a contracara activitățile cibernetice ale Rusiei, Ucraina a adoptat o strategie pe două direcții, prin mobilizarea suportului internațional și crearea unei armate de profesioniști în securitate cibernetică,

cunoscuți ca “armata IT a Ucrainei”. Armata IT, care este estimată a avea mai mult de 400.000 de voluntari, este împărțită în două unități: unitatea de apărare (responsabilă pentru protejarea infrastructurii critice a Ucrainei) și unitatea de ofensivă (ce are responsabilitatea de a spiona cibernetic armata rusă). Guvernul a pornit o inițiativă de coordonare a hacktiviștilor și a unor grupuri de hacktiviști, atât pentru lansarea unor atacuri DDOS împotriva băncilor din Rusia, cât și pentru compromiterea website-ului care aparține Guvernului Rusiei. Armata IT a primit o listă ce conținea mai mult de 30 de ținte, inclusiv companii mari care susțin infrastructura Rusiei.

Pe de altă parte, grupul proeminent și descentralizat de hacktiviști, Anonymous, a declarat război cibernetic Rusiei. Această grupare de hackeri pretinde că a atacat servicii majore ale Rusiei de streaming și broadcasting, pentru a difuza clipuri cu războiul din Ucraina. De asemeana, hacktiviștii pro-Ucraina sunt suspectați că ar fi folosit un wiper (un tip de malware care șterge datele de pe hard drive-ul computerului infectat) pentru a ataca entități ruse.

În același timp, companii vestice de tehnologie au sărit în ajutorul Ucrainei în multiple moduri. De exemplu, Google și-a extins normele de eligibilitate pentru serviciul său gratuit de protecție împotriva atacurilor DDOS, Project Shield, oferindu-l autorităților ucrainene. La momentul actual, mai mult de 150 de organizații din Ucraina folosesc acest serviciu. Alte companii de tehnologie, precum Microsoft, se ocupă atât cu identificarea amenințărilor asupra Ucrainei, cât și cu corectarea vulnerabilităților și împărtășirea informațiilor. Niște reportaje de presă sugerează că echipele de apărare cibernetică din Statele Unite și Marea Britanie erau deja în Ucraina din decembrie 2021. în urma invaziei, Ucraina a încurajat hacktiviștii să apere țară împotriva actorilor cibernetici ruși. Conform Zone-H, în jur de 100 de domenii de website rusești au fost compromise (Fig.2). Este neclar câte dintre ele au fost atacate de actori cibernetici ucraineni.

Rolul părților terțe

Pe lângă actorii cibernetici ruși și ucraineni, actori cibernetici din Belarus au fost implicați în desfășurarea de activități în domeniul cibernetic. Actorul cibernetic din Belarus UNC1151 a fost detectat instalând un backdoor (printr-o modalitate nedocumentată de acces la sistemul informatic) pe sistemele guvernamentale ucrainene. De asemenea, actorul cibernetic a fost implicat în lansarea de campanii de tip phishing împotriva guvernelor și organizațiilor militare poloneze și ucrainene. Pe de altă parte, actorul cibernetic „Mustang Panda” din China, care se concentrează puternic pe țintele din Asia de Sud-Est, folosește situația din Ucraina pentru a viza entitățile europene prin capcane sub forma unor atașamente răuvoitoare.

Tendințe viitoare

În cazul unui conflict prelungit, nu poate fi exclusă posibilitatea de răspândire a atacurilor cibernetice. în acest sens, este important să înțelegem că actorii cibernetici ai guvernului rus s-ar putea să nu se implice neapărat în atacuri cibernetice de propagare din cauza activităților cibernetice legate de Ucraina. Cu toate acestea, există posibilitatea ca grupurile de hacktiviști ruși să fie implicate în lansarea de atacuri cibernetice împotriva Statelor Unite, UE și NATO (în special Polonia, România etc.). Astfel, tipul de atacuri cibernetice pe care actorii cibernetici ruși le-ar putea desfășura ar putea fi DDOS.

Un alt factor cheie, care ar putea determina măsura în care actorii cibernetici ai guvernului rus s-ar putea implica în lansarea de atacuri cibernetice dincolo de Ucraina, este stabilizarea angajamentelor militare ruse în Ucraina. Atacurile cibernetice lansate de către actori cibernetici ruși ca represalii împotriva Statelor Unite și a entităților UE se vor încadra probabil într-un test în cinci puncte care variază de la a nu viza entități la nivelul cărora atacurile pot fi văzute ca un act de război de către victime, până la evitarea țintirii acelor entități a căror impactare ar putea duce la o escaladare a situației generale. Prin urmare, există o mare posibilitate ca cinci tipuri de entități – servicii financiare, instituții de învățământ, retail, administrații locale și mici departamente/agenții federale – să fie vizate de actorii cibernetici ruși.

Cu toate acestea, impactul general al atacurilor cibernetice asupra conflictului în curs de desfășurare poate fi cu adevărat determinat odată cu încheierea sa. Până atunci, este important ca observatorii conflictului cibernetic să examineze comportamentele actorilor cibernetici cu scepticism.

Sursa: The Cyber Dimension of the Russia-Ukraine Conflict - Unpacking the Early Phase - Pakistanpolitico

Autor: Fahad Nabeel, Pakistan Politico