BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Perspectiva SSSCIP asupra atacurilor cibernetice derulate în contextul conflictului militar dintre Federația Rusă și Ucraina (ianuarie 2022 – ianuarie 2024)

SSSCIP's Perspective on the cyber-attacks unfolded in the context of the military conflict between Russia and Ukraine (January 2022 – January 2024)

Drd. Mihai OLTEANU*

*Universitatea Națională de Apărare „Carol I", București, România

Abstract

Lucrarea de față evaluează raportările SSSCIP privind atacurile cibernetice derulate asupra Ucrainei în perioada ianuarie 2022 – ianuarie 2024. De la exploatarea malware-ului CaddyWiper, atribuit de SSSCIP către APT SANDWORM, la campaniile sofisticate ale FSB și atacul cibernetic asupra Kyivstar, lucrarea prezintă o perspectivă a atacurilor cibernetice de origine rusă derulate asupra Ucrainei, așa cum au fost raportate de autoritatea ucraineană în domeniu. Scopul articolului este acela de a identifica modul în care SSSCIP (principala instituție responsabilă pe componenta de securitate cibernetică) a raportat atacurile cibernetice asupra infrastructurilor IT&C ucrainene, completitudinea datelor publicate, precum și modalitatea în care sunt prezentate campaniile. Pentru realizarea acestui scop, au fost evaluate toate raportările SSSCIP din perioada de referință și au fost incluse în studiu doar acelea care s-au materializat și au afectat infrastructuri IT&C. În concluzii, vor fi evidențiate, în principal, limitările raportărilor SSSCIP și, secundar, perspectiva SSSCIP privind domeniile care au fost cel mai des vizate de atacuri cibernetice și capabilitățile actorilor ruși.

This paper evaluates the reports of the SSSCIP regarding cyber-attacks carried out against Ukraine from January 2022 to January 2024. From the exploitation of the CaddyWiper malware, attributed by SSSCIP to APT SANDWORM, to the sophisticated campaigns of the FSB and the cyber-attack on Kyivstar, the paper provides an insight into Russian-origin cyber-attacks against Ukraine, as reported by the main Ukrainian authority in the field, SSSCIP.
The purpose of the article is to identify how SSSCIP reported cyber-attacks on Ukrainian IT&C infrastructures, the completeness of the published data, and the way the campaigns are presented. To achieve this goal, all SSSCIP reports from the reference period were evaluated, and only those that materialized and affected IT&C infrastructures were included in the study. In conclusion, the paper will primarily highlight the limitations of SSSCIP reports and, secondarily, SSSCIP's perspective on the domains most frequently targeted by cyber-attacks and the capabilities of Russian actors.

Cuvinte-cheie:
SSSCIP; Ucraina; APT; securitate cibernetică; Federația Rusă; conflict militar.

Keywords:
SSSCIP; Ukraine; APT; cyber security; Russia; military conflict.

Info articol
Primit: 1 februarie 2024; Evaluat: 26 februarie 2024; Acceptat: 13 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Olteanu, M. 2024. „Perspectiva SSSCIP asupra atacurilor cibernetice derulate în contextul conflictului militar dintre Federația Rusă și Ucraina (ianuarie 2022 – ianuarie 2024)". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(1): 26-43. https://doi.org/10.53477/2065-8281-24-02

Pe parcursul ultimelor decenii, evoluția continuă a tehnologiei și extinderea semnificativă a proceselor de digitalizare de la nivelul statelor și companiilor private au determinat o creștere constantă a importanței domeniului securității cibernetice. Această creștere a determinat modificări substanțiale ale celor mai importante sectoare ale societății, notabile în domeniile politic, economic și militar. Concomitent, amenințările cibernetice au crescut în complexitate, gama de ținte existente fiind mult mai variată, compromiterea acestora oferind oportunități financiare, politice și militare (Furstenau și alții 2020).

În context politic, atacurile cibernetice au devenit una dintre principalele preocupări la nivelul statelor și organizațiilor internaționale, deoarece compromiterea unor infrastructuri IT&C poate genera dezavantaje strategice. Aspecte, precum influențarea proceselor electorale, manipularea deciziilor politice și subminarea stabilității instituțiilor guvernamentale, au devenit amenințări la adresa domeniului politic. Instrumentalizarea atacurilor cibernetice s-a cristalizat într-un mijloc strategic de atingere a obiectivelor geopolitice atât pentru actorii statali, cât și pentru cei nonstatali (Visvizi și Lytras 2020, 333-336). Un exemplu în acest sens este actorul cibernetic APT28, care, conform raportărilor companiilor din industria de securitate cibernetică, acționează pentru a susține interesele Federației Ruse (FR) și a reușit compromiterea unor ținte de interes strategic de la nivelul unor state (precum Georgia, Polonia și Ungaria) sau organizații (precum NATO și OSCE) (Mcwhorter 2014).

În domeniul economic, digitalizarea extensivă a mediului de afaceri a generat inerent o serie de amenințări cibernetice, care pot afecta nu doar confidențialitatea informațiilor, ci și integritatea financiară și reputația organizațiilor. Furtul de date, spionajul industrial și diversele forme de șantaj cibernetic reprezintă elemente de risc la nivelul mediului public și al celui privat, care pot afecta buna funcționare a entităților economice (Hernandez-Castro și Cartwright 2020). Incidente notabile, precum campania cibernetică WannaCry, au ilustrat potențialul distructiv al amenințărilor cibernetice, având un impact direct asupra sectoarelor economice și industriale (Hernandez-Castro, Cartwright și Stepanova 2017).

În sfera militară, dependența sporită de sisteme informatice avansate a expus infrastructura militară la riscuri cibernetice semnificative. Complexitatea operațiunilor militare moderne impune o interconectivitate crescută între sistemele de comunicații și control, amplificând astfel vulnerabilitățile la atacurile cibernetice. De asemenea, atacurile cibernetice au devenit un instrument folosit de state, inclusiv ca parte a conflictelor militare, notabil în acest sens fiind conflictul dintre FR și Ucraina (UA), început în februarie 2022. Literatura de specialitate existentă până în acest moment oferă analize

[1] WannaCry a reprezentat o campanie cibernetică de tip ransomware, care a avut loc în mai 2017. Odată infectat un sistem, WannaCry cripta fișierele utilizatorilor și solicita plata unei răscumpărări în moneda virtuală Bitcoin, pentru eliberarea acestora. Atacul a avut impact global, afectând organizații importante, inclusiv sistemul de sănătate din Marea Britanie, companii din sectoarele energetic și financiar, generând alarmă cu privire la vulnerabilitatea infrastructurilor critice în fața amenințărilor cibernetice (Mohurle și Patil 2017).

privind atacurile cibernetice asupra unor domenii specifice, fără a exista evaluări extinse cu privire la cele mai importante campanii cibernetice, indiferent de ținta acestora, derulate împotriva UA, începând cu anul 2022. În context, scopul acestui studiu este acela de a analiza raportările oficiale, realizate de autoritățile ucrainene cu privire la cele mai importante atacuri cibernetice din perioada ianuarie 2022 – ianuarie 2024, care au afectat diverse sectoare de activitate. După analizarea acestora, vor fi formulate o serie de concluzii, în principal cu privire la modul de raportare al SSSCIP și, în plan secund, cu privire la atacurile cibernetice, în contextul conflictului dintre FR și UA.

Pentru derularea acestui studiu, vor fi folosite, cu precădere, raportările realizate de SSSCIP[2] UA, principalul serviciu ucrainean privind securitatea cibernetică, aflat sub controlul Președintelui, care desfășoară atât activități pentru stabilirea politicilor în domeniul protecției infrastructurilor IT&C (inclusiv rețelele clasificate ale UA) (Cyber Security Intelligence 2022), cât și intervenții, în cazul unor atacuri cibernetice (prin intermediul CERT-UA) (Temple-Raston 2023). Motivul axării pe raportările SSSCIP este acela că lucrarea își propune să analizeze atacurile cibernetice din perspectiva UA.

[2] Державна служба спеціального зв'язку та захисту інформації України – Serviciul de Stat pentru Comunicații Speciale și Protecția Informațiilor.

Este important de precizat faptul că atacurile cibernetice din cuprinsul rapoartelor SSSCIP variază în complexitate și relevanță din două puncte de vedere: (1) impactul pe care l-au produs asupra infrastructurilor IT&C atacate și (2) nivelul capabilităților tehnice deținute de atacator (Agrafiotis și alții 2018). În acest sens, este relevant că cele mai comune tipuri de atacuri cibernetice sunt cele de *phishing*, care presupun utilizarea unor tehnici de inginerie socială pentru a încerca să convingă ținta să acceseze un conținut cu potențial malware (Khonji, Iraqi și Jones 2013, 2091-2121). Cele mai multe atacuri de tip phishing nu au succes, aspect determinat de factori multipli, printre care capabilitățile reduse ale atacatorilor și utilizarea unor tehnici de inginerie socială documentate insuficient sau a unor programe malware cu nivel redus de complexitate, ușor de detectat de către soluțiile de securitate cibernetică (Patil și alții 2022). Astfel, din punct de vedere metodologic, pentru ca rezultatele din cadrul acestui articol să fie relevante, vor fi excluse acele raportări ale SSSCIP care fac referire doar la campanii de tip phishing despre care nu se menționează că au avut un impact la adresa infrastructurilor IT&C țintite. În acest sens, este important de menționat că, în intervalul de referință, au fost întocmite 435 de rapoarte publice de către SSSCIP, însă, în urma analizei preliminare, 394 dintre acestea fac referire strict la campanii cibernetice de tip phishing. Despre acestea, nu este menționat că ar fi reușit să compromită oricare dintre țintele urmărite, motiv pentru care nu au fost incluse în cadrul articolului. Pe baza acestor criterii, au fost selectate 41 de articole, care vor fi evaluate pentru evidențierea unor concluzii privind securitatea cibernetică, în contextul conflictului dintre FR și UA.

Literatura de specialitate în domeniu

În ceea ce privește analiza asupra componentei atacurilor cibernetice, în contextul conflictului dintre FR și UA, lucrările existente urmăresc impactul atacurilor asupra anumitor domenii sau în perioade de timp reduse. Davydiuk și Zubok fac o evaluare a domeniului energetic din UA din perspectiva rezilienței la atacuri cibernetice și a posibilității generării unor efecte în cascadă asupra altor sectoare de activitate, aspecte care dezavantajează UA în cadrul conflictului (Davydiuk și Zubok 2023, 121-139). Au fost publicate analize similare, inclusiv, asupra sectorului financiar din UA, cu privire la caracteristicile atacurilor și amenințărilor cibernetice, în contextul conflictului FR-UA. Astfel, sunt analizate tendințele atacurilor cibernetice asupra industriei financiare, fiind identificată utilizarea activă a mesajelor SMS și a e-mailurilor cu linkuri sau coduri malware (Kloba și Kloba 2022, 19-28). CERT-EU a publicat constant evaluări asupra unor atacuri cibernetice, derulate împotriva UA și identificate de diverse entități publice sau private (CERT-EU 2023). Totuși, aceste lucrări adoptă o perspectivă focalizată strict pe anumite domenii de activitate (precum cele centrate pe sectoarele energetic și financiar) sau urmăresc o evaluare, din perspectiva entităților externe conflictului. Comparativ, această lucrare vizează strict raportările realizate de UA prin instituțiile abilitate.

Marcus Willet analizează posibilitatea escaladării conflictului dintre FR și UA la nivelul comunității internaționale, prin implicarea NATO (pe baza dreptului internațional), ca urmare a unor atacuri cibernetice mai ample (Willett 2022, 7-26). Evoluția conflictului, din perspectiva securității cibernetice, este analizată inclusiv considerând implicarea unor actori nonstatali neanticipați în februarie 2022, dar care au avut un rol semnificativ (Lonergan, Smith și Mueller 2023, 85-102). Richard Wilson include, în lucrarea sa, posibilitatea ca atacurile cibernetice, în contextul conflictului FR-UA, să conducă la declanșarea unor evenimente de natură nucleară, în mod intenționat sau incidental (Wilson și Fitz 2023, 440-448). De asemenea, există lucrări care au încercat să construiască o strategie pe componenta de securitate cibernetică, menită să permită asigurarea rezilienței, concluzionând că îmbunătățirea sistemului de securitate cibernetică se află într-o fază incipientă (Tarasenko și alții 2022, 583-599).

Literatura în domeniu include o serie de lucrări privind implicarea unor entități nonstatale, atrase în conflictul dintre FR și UA, cu precădere a entității denumite Ukraine IT Army, creată de autoritățile de la Kiev cu scopul de a reuni experți, indiferent de proveniența acestora, pentru a ajuta UA să combată atacurile cibernetice (Soesanto 2023, 93-106). Similar, Smith și Dean evaluează eficiența Ukraine IT Army și capacitatea de a gestiona aproximativ 200.000 de experți voluntari care au decis să se alăture entității (Smith și Dean 2023, 103-119). Există lucrări care evaluează implicarea unor entități externe pentru a sprijini UA, precum marile companii din domeniul tehnologic (de exemplu, Google, Microsoft, Meta, Apple și Amazon), și impactul generat de acest aspect (Matania și Sommer 2023). Alături de companiile private, au existat și state sau organizații internaționale (precum UE) care au trimis echipe ce pot sprijini UA pe componenta de asigurare a securității cibernetice (Sullivan 2023, 9-23).

Analiza atacurilor cibernetice asupra UA pe parcursul anului 2022

Pe parcursul anului 2022, au fost identificate un număr semnificativ de atacuri cibernetice derulate asupra infrastructurilor IT&C de pe teritoriul UA, cele mai relevante în acest sens fiind:

- În noaptea dintre 13 și 14 ianuarie 2022, website-urile mai multor organizații publice din UA au fost țintele unui atac cibernetic. Conform SSSCIP, atacul a inclus afișarea unor imagini provocatoare, în unele cazuri, criptarea sau ștergerea datelor (SSSCIP 2022a). Atacul a fost estimat ca fiind planificat în avans și a implicat diverse tipuri de malware, inclusiv distructiv (denumit WhisperKill), care avea drept scop indisponibilizarea infrastructurilor (CERT-UA 2022a). SSSCIP nu a inclus date cu privire la posibila asociere sau atribuire a campaniei de atacuri unei entități statale sau nonstatale. Conform Microsoft, țintele au fost atât organizații guvernamentale și nonguvernamentale, cât și companii private (Microsoft 2022).
- La data de 15 februarie 2022, un atac semnificativ de tip DDoS[3] a vizat compromiterea unor infrastructuri IT&C care aparțin unor organizații publice (printre care website-ul Ministerului Apărării și cel al Forțelor Armate) și private (precum Privatbank și Oschadbank, care au fost compromise) (SSSCIP 2022e). Conform autorității ucrainene, aceeași campanie de atacuri cibernetice a fost identificată și în seara zilei de 23 februarie 2022, cu o zi înainte de invazia FR în UA. De această dată, atacurile cibernetice s-au intensificat, fiind vizate website-urile Cabinetului de Miniștri, Verkhovna Rada (Parlamentul UA), Ministerului Afacerilor Externe și Serviciului de Securitate. În aceeași zi, SSSCIP raporta o intensificare a campaniilor de distribuție malware, a încercărilor de penetrare a infrastructurilor IT&C publice și private și a tentativelor de distrugere a datelor. De această dată, SSSCIP preciza că este clar faptul că aceste campanii au fost derulate de *„statul agresor"* (SSSCIP 2022r).

  Prezintă relevanță în context faptul că intensificarea atacurilor cibernetice s-a sincronizat cu debutul conflictului, ceea ce creează premisele unor acțiuni conjugate din partea FR asupra UA (Lewis 2022).

  La data de 6 martie 2022, SSSCIP publica o statistică, prin care anunța că numărul de atacuri cibernetice este în continuare unul record, ajungând la 2.800. De asemenea, a fost înregistrat un număr record, de 271 de atacuri de tip DDoS în 24 de ore. Aceste acțiuni au fost atribuite în totalitate Federației Ruse, autoritatea ucraineană susținând că sunt derulate în completarea atacurilor din aer, apă și de pe uscat (SSSCIP 2022q).

  Mai mult, la data de 25 martie SSSCIP a anunțat că, numai în săptămâna 15-22 martie, a înregistrat 60 de atacuri cibernetice, dintre care 11 asupra autorităților locale și centrale, 8 asupra sectorului de apărare, 6 asupra sectorului financiar, 6 asupra organizațiilor comerciale,

[3] Atacurile cibernetice de tip DDoS vizează întreruperea serviciilor, ca urmare a unor încercări repetate de epuizare a unei aplicații prin trafic de date excesiv (Microsoft, fără an).

4 asupra sectorului de telecomunicații, 2 asupra domeniului energetic, iar restul au vizat alte entități publice și private (SSSCIP 2022p).

➢ La data de 15 martie 2022, SSSCIP publica informații privind un nou malware care urmărește ștergerea datelor din sistemele compromise, denumit în industria de specialitate CaddyWiper. Prezintă relevanță că este primul caz în care SSSCIP citează două companii private (Eset și Microsoft) cu privire la identificarea acestui malware (SSSCIP 2022b). Campania a vizat entități din domeniul energetic și a avut drept obiectiv întreruperea alimentării cu energie electrică pe teritoriul UA, fiind atribuită actorului cibernetic de origine rusă APT SANDWORM (CERT-UA 2022b).

Prezintă interes și faptul că APT SANDWORM a fost atacatorul către care a fost atribuită campania cibernetică, din anul 2015, derulată asupra UA, care a avut drept țintă rețeaua energetică națională (Paverman 2019).

➢ La data de 6 aprilie 2022, SSSCIP a publicat date cu privire la un atac cibernetic care a avut drept țintă infrastructura UKRTELECOM, cea mai mare companie ucraineană de telefonie mobilă. Conform investigațiilor, atacul a avut un nivel ridicat de complexitate și a fost lansat de pe teritoriile ocupate la acel moment de către FR, iar scopul a fost acela de a prelua controlul infrastructurii de comunicații. În context, UKRTELECOM a fost nevoită să reducă la 13% capacitatea infrastructurii, pentru a permite echipelor de specialiști să prevină materializarea intențiilor atacatorilor. UKRTELECOM și SSSCIP au reușit refacerea infrastructurii și au menționat că nu dețin date suficiente încât să atribuite campania unui atacator specific (SSSCIP 2022c).

➢ La data de 11 aprilie 2022, a fost comunicat un anunț privind dificultățile de asigurare a comunicațiilor mobile pe teritoriul UA, SSSCIP derulând constant eforturi pentru menținerea activității furnizorilor de Internet și a celor de telecomunicații, precum Vodafone. Conform estimărilor, la acel moment doar 65% din infrastructura telecom a rămas operațională, afectând astfel posibilitatea ca cetățenii să comunice pe teritoriul UA (SSSCIP 2022i).

➢ La data de 12 aprilie 2022, SSSCIP a anunțat desfășurarea unor acțiuni de prevenire a unei noi campanii cibernetice derulate de APT SANDWORM, care a vizat întreruperea alimentării cu energie electrică pe teritoriul UA, urmărind compromiterea echipamentelor de rețea de la nivelul întreprinderilor private. Similar exemplului din data de 15 martie 2022, SSSCIP anunța faptul că a avut parte de sprijinul ESET și MICROSOFT în eforturile de prevenire a materializării atacului cibernetic. UA a declarat, de asemenea, faptul că menține cooperarea cu statele europene prin schimbul de informații cu privire la acest atac cibernetic. Totuși, SSSCIP menționează că scopul cooperării este acela de a identifica existența altor infrastructuri energetice de pe teritoriul UA compromise de APT SANDWORM (SSSCIP 2022h).

➢ O zi mai târziu, la data de 13 aprilie 2022, SSSCIP anunța că a primit informații de la partenerii internaționali privind compromiterea unei companii de distribuție a energiei electrice de către actorul rus APT SANDWORM, scopul fiind acela de a întrerupe alimentarea cu energie electrică a unei părți importante din teritoriul UA. La momentul intervenției,

atacul cibernetic era în desfășurare, reușind compromiterea unor resurse, însă fără a materializa intenția finală. Mai mult, SSSCIP a anunțat continuarea creșterii numărului atacurilor cibernetice, în special de tip DDoS, fiind identificate aproximativ de 25 de ori mai multe atacuri de acest tip, comparativ cu anul anterior (SSSCIP 2022l).

- Ulterior, la data de 16 aprilie 2022, SSSCIP anunța o nouă campanie de atacuri cibernetice de tip DDoS care a avut drept țintă website-urile unor autorități publice, reușind indisponibilizarea temporară a acestora. În urma intervenției echipelor tehnice, website-urile au fost repuse în funcțiune (SSSCIP 2022n).
- Pe parcursul lunii mai 2022, au fost continuate încercările de întrerupere a comunicațiilor, atacatorii reușind oprirea permanentă a acestora în zona Kherson, ocupată de FR. Locuitorii nu mai aveau acces la comunicații mobile sau Internet, iar SSSCIP anunța că nu poate face nimic în acest sens, zona aflându-se sub ocupație militară, iar echipamentele, controlate. Concomitent, autoritățile ucrainene anunțau că, în absența mijloacelor de comunicare, soldații FR patrulează și transmit prin sisteme audio știri propagandiste, pentru influențarea cetățenilor fără acces la comunicații în afara zonei. Mai mult, SSSCIP anunța că estimează că cetățenilor din zona Kherson le va fi oferit accesul la rețeaua telecom a FR, controlată de statul agresor (SSSCIP 2022m). La finalul anului, în noiembrie 2022, SSSCIP comunica faptul că a reușit restabilirea accesului la posturile de radio și televiziune ucrainene în Kherson, cu ajutorul companiei poloneze Emitel SA (SSSCIP 2022t).
- La data de 6 iunie 2022, SSSCIP informa că se află în derulare o campanie cibernetică, dublată de acțiuni propagandiste, prin care s-a reușit compromiterea celor mai importante rețele de televiziune ucrainene, în cadrul cărora s-au difuzat știri rusești. Știrile au fost difuzate în timpul în care televiziunile ucrainene transmiteau meciul de calificare al echipei naționale la campionatul mondial de fotbal. Cel mai probabil, atacatorii au reușit să obțină acces la un nod de comunicații TV, prin intermediul căruia au transmis traficul modificat (SSSCIP 2022j).

Până la finalul anului 2022, nu au fost publicate alte atacuri cibernetice de către SSSCIP, cu toate că au existat anumite campanii, raportate de industria privată, printre care întreruperile de energie electrică, din intervalul 10-12 octombrie 2022, conform raportării MANDIANT (Proska și alții 2023). De asemenea, SSSCIP nu a publicat un raport cu privire la campania asupra modemurilor satelitare VIASAT care funcționează în bandă KA și care au fost indisponibilizate pe teritoriul UA și al multor state europene (printre care Polonia, Marea Britanie, Franța), ca efect secundar (Boschetti, Gordon și Falco 2022). Cu toate acestea, multe state europene au atribuit această campanie cibernetică Federației Ruse, în anul 2022 (Steinbrecher 2022). Singura mențiune cu privire la această campanie, făcută de SSSCIP, a fost la data de 2 iulie 2022, când a precizat că UA folosește infrastructura satelitară STARLINK, pusă la dispoziție de către Elon Musk, pentru a asigura comunicațiile de rezervă, în cazul unui atac cibernetic asupra infrastructurii principale (SSSCIP 2022o).

Pe parcursul anului 2022, au mai existat raportări statistice privind intensitatea atacurilor cibernetice (de 3 ori mai mare decât în anul anterior (SSSCIP 2022u), domeniile vizate (cu precădere telecomunicații, medical și guvernamental (SSSCIP 2022g) și atacatori (în special grupări motivate ideologic și actori statali (SSSCIP 2022d). Totuși, un aspect de interes este cel din raportul din data de 1 mai 2022, când SSSCIP anunța că indiciile existente conduc către ipoteza conform căreia intensitatea atacurilor cibernetice ruse la adresa UA a atins un nivel maxim, serviciul ucrainean estimând că nu vor exista operațiuni cibernetice mai puternice (SSSCIP 2022k). Acest aspect poate indica o încercare de creștere a încrederii sociale și de menținere a atitudinii ofensive față de FR la un nivel ridicat, similar celui anterior conflictului militar (Paniotto 2020, 3-14). Pe de altă parte, este posibil ca UA să fi acționat în vederea promovării unei imagini puternice față de statul agresor, pentru a slăbi susținerea conflictului militar de către populația rusă din FR, aflată în proporție de 60% în anul 2022 (Kizilova 2022, 2-5). Demersul a fost susținut două luni mai târziu, când SSSCIP anunța faptul că intensitatea atacurilor cibernetice a continuat să se mențină la același nivel ridicat, însă calitatea acestora se afla pe un trend descendent (SSSCIP 2022f).

Un alt aspect care indică o abordare deosebită din partea SSSCIP este relevat într-un comunicat, din data de 1 mai 2022, în care UA transmitea că atacurile cibernetice rusești îndreptate împotriva infrastructurilor proprii sunt, de asemenea, un potențial atac asupra altor state partenere. Exemplificând, SSSCIP menționează că, în anul 2014, alegerile din UA au fost ținta unor atacuri cibernetice de origine rusă, iar doi ani mai târziu, același mod de operare a fost observat și în cadrul proceselor electorale ale SUA (SSSCIP 2022s). Astfel, având în vedere antecedentele pe componenta de securitate cibernetică, UA reiterează indirect necesitatea de a fi sprijinită pe parcursul conflictului, acesta nefiind de interes doar pentru cele două state participante (Ratten 2022, 265-271).

Analiza atacurilor cibernetice asupra UA pe parcursul anului 2023

În cursul anului 2023, SSSCIP a publicat un număr mai mic de comunicate cu privire la atacurile cibernetice comise împotriva rețelelor și sistemelor informatice proprii, cele mai relevante în acest sens fiind următoarele:

- La data de 1 ianuarie 2023, a fost publicat un comunicat care atribuia atacurile cibernetice, derulate prin intermediul malware-ului CaddyWiper, în luna ianuarie 2022, actorului cibernetic de origine rusă APT SANDWORM (SSSCIP 2023l), a cărui activitate este atribuită public serviciului militar de informații al FR (Akimenko și Giles 2020, 67-75).
- La data de 18 ianuarie 2023, SSSCIP a publicat o analiză privind o campanie cibernetică, ce a vizat compromiterea unor ținte din domeniul mediatic, cu precădere agenția de știri UKRINFORM. Comunicatul subliniază încercările FR de compromitere a factorilor de informare pentru populație, având drept

scop principal dezinformarea cetățenilor și, ulterior, influențarea acestora (SSSCIP 2023a).

➢ La data de 1 februarie 2023, au fost publicate o serie de investigații tehnice privind campaniile cibernetice, derulate de serviciul rus FSB asupra infrastructurilor informatice de pe teritoriul UA, fiind precizat faptul că activitatea este desfășurată prin atacuri cibernetice cu un nivel ridicat de complexitate și precizie, în contrast cu campaniile de atacuri de tip DDoS. Mai mult, SSSCIP precizează că acest tip de operațiuni ale FSB reprezintă cea mai mare amenințare cibernetică identificată pe parcursul conflictului militar (SSSCIP 2023k).

➢ O zi mai târziu, SSSCIP publica date cu privire la un atac cibernetic de tip watering hole[4], care a presupus crearea unui website, în cadrul căruia era folosită imaginea ministerului ucrainean de externe pentru a crea aparențele unui website legitim. Odată accesat, website-ul oferea vizitatorilor un program care urma să fie descărcat sub aparența unei aplicații ce putea identifica dacă sistemul utilizatorului este compromis. În realitate, aplicația avea conținut malware care ar fi infectat computerul vizitatorului website-ului, în cazul în care era instalată (SSSCIP 2023f). Campania este singura de acest tip, raportată de SSSCIP, și avea la bază exploatarea dorinței cetățenilor de a se informa cu privire la stadiul conflictului, pe baza unei surse guvernamentale de încredere.

➢ La data de 1 iulie 2023 a fost publicată o analiză cu privire la creșterea numărului atacurilor cibernetice care vizează, cu precădere, companii din domeniul IT&C de pe teritoriul UA. Scopul acestor atacuri a fost declarat ca fiind acela de a compromite aceste companii în vederea obținerii controlului asupra produselor software comercializate în UA și, ulterior, asupra utilizatorilor acestor soluții. De asemenea, SSSCIP menționează că industria privată evaluează că poate gestiona pe cont propriu acest tip de amenințări, însă există contraexemple recente care arată că mari companii din domeniu au fost compromise (SSSCIP 2023c).

➢ La 5 iulie 2023, SSSCIP a comunicat date cu privire la o campanie cibernetică ce a reușit compromiterea paginii de Facebook utilizată de Serviciul Național de Statistică al UA, atacatorii postând pe această pagină faptul că și infrastructura instituției a fost compromisă, fiind astfel indisponibilizat accesul la date statistice economice și sociale. În fapt, conform SSSCIP, atacatorii au reușit doar compromiterea paginii de Facebook, fără a avea acces la infrastructura Serviciului Național de Statistică, mesajul postat în numele instituției fiind fals (SSSCIP 2023e). Este posibil ca scopul acestor acțiuni să fi fost acela de destabilizare a încrederii populației în statisticile oficiale, publicate de UA. Astfel de acțiuni de propagandă au fost desfășurate constant de FR pe parcursul conflictului cu UA, având drept scop scăderea încrederii societății în autorități (Geissler și alții 2023).

[4] Watering hole – atac cibernetic care se bazează pe identificarea acelor website-uri utilizate, cu precădere, de grupul țintă și clonarea sau modificarea acestora astfel încât să compromită vizitatorii acelui domeniu (Krithika 2017).

➢ La data de 19 iulie 2023, SSSCIP a publicat o investigație tehnică cu privire la două aplicații malware cu complexitate tehnică ridicată, denumite CAPIBAR și KAZUAR, utilizate de APT TURLA, atribuit serviciului de informații al FR, FSB, pentru compromiterea unor ținte de pe teritoriul UA. SSSCIP notează faptul că a transmis toate rezultatele investigațiilor tehnice, inclusiv industriei private de specialitate (SSSCIP 2023j).

➢ La data de 13 decembrie 2023, SSSCIP anunța că, în urmă cu o zi, infrastructura IT&C a operatorului de telecomunicații Kyivstar a fost compromisă, astfel fiind indisponibilizată furnizarea serviciilor specifice către aproximativ 24 de milioane de clienți, câteva zile (Balmforth 2024). Pentru a reuși repunerea în funcțiune a operatorului, SSSCIP a solicitat ca serviciile roaming să fie oprite pe o perioadă limitată de timp, situație în care clienții nu au mai putut comunica în afara teritoriului ucrainean (SSSCIP 2023d). Prezintă relevanță faptul că SSSCIP nu a anunțat impactul atacului cibernetic pe website-ul oficial, însă declarațiile suplimentare, făcute de către directorul instituției pentru publicații europene, au relevat că infrastructura IT&C a Kyivstar a fost afectată în totalitate, malware-ul utilizat reușind să șteargă majoritatea datelor (Gatlan 2024), atacul fiind caracterizat drept cel mai mare din istorie asupra industriei telecom (Sapuppo 2023).

➢ Ultimul atac cibernetic, publicat de SSSCIP în perioada de referință, prezintă o campanie derulată de actorul cibernetic rus APT28, care a vizat atât ținte de pe teritoriul UA, cât și rețele și sisteme informatice din Polonia. SSSCIP transmite astfel din nou mesajul că atacurile cibernetice asupra UA nu sunt incidente izolate din punct de vedere geografic, ci pot afecta inclusiv state membre ale UE sau NATO (SSSCIP 2023i).

Prezintă interes faptul că, pe parcursul anului 2023, SSSCIP a avut o serie de raportări statistice cu privire la cele mai țintite domenii de către atacatorii cibernetici, astfel fiind menționate organizații comerciale, industria telecom, dezvoltatori software, aparatul guvernamental, sectorul de industrie și apărare, precum și autorități locale (SSSCIP 2023h). Mai mult, SSSCIP precizează faptul că, începând cu luna septembrie 2022, monitorizează cel puțin șapte actori cibernetici care vizează constant infrastructuri ale UA, toți fiind asociați guvernului FR (SSSCIP 2023g), precum și 23 de grupuri catalogate drept hacktiviste (SSSCIP 2023b).

De asemenea, este important de precizat că, până la finalul lunii ianuarie 2024, nu au fost publicate noi rapoarte cu privire la alte atacuri cibernetice derulate împotriva infrastructurilor IT&C de pe teritoriul UA.

Concluzii

Din punct de vedere metodologic, acest articol a urmărit, într-o primă etapă, selectarea și prezentarea celor 41 de rapoarte realizate de SSSCIP, în perioada ianuarie 2022 – ianuarie 2024, cu privire la atacurile cibernetice cu un nivel ridicat

de complexitate și care au reușit să producă un impact asupra infrastructurilor IT&C ucrainene, fiind astfel excluse acele campanii cibernetice tip phishing. Ulterior prezentării rapoartelor menționate, se remarcă o serie de aspecte de interes cu privire la modul de funcționare al instituției, la raportarea acesteia față de atacurile cibernetice, comise asupra infrastructurilor IT&C ucrainene, și față de modul de operare al actorilor cibernetici de origine rusă.

În primul rând, se remarcă faptul că cele mai vizate domenii în cadrul campaniilor cibernetice au fost cel al comunicațiilor și cel energetic. Acest aspect poate fi explicat prin faptul că domeniul energetic constituie o resursă foarte importantă atât pentru statul atacat, asigurând funcționarea de bază a acestuia (Kozak, Klaban și Šlajs 2023, 1-6), cât și pentru statul agresor, reprezentând un element care poate crea panică în rândul populației, odată ce a fost indisponibilizat (Lee 2022). În ceea ce privește zona de telecomunicații, rolurile principale ale acesteia sunt determinate de informarea populației cu privire la starea conflictului (în special prin posturile TV și radio) și de posibilitatea cetățenilor de a comunica între ei din motive de siguranță sau de a avea acces la persoane din afara statului (Bratich 2020, 311-332). Impactul se remarcă, cu precădere, în zona Kherson, unde trupele FR au acționat pentru a opri accesul la informații ucrainene, precum și posibilitatea de a comunica cu persoane din afara arealului. În ceea ce privește exponenții mediului hacktivist, aceștia au urmărit compromiterea website-urilor unor autorități publice atât pentru scăderea încrederii în instituțiile publice, cât și pentru a crea un sentiment de panică în rândul civililor, care, deși nu interacționau direct cu conflictul, puteau conștientiza efectele acestuia (Hupperich 2023). Un exemplu evidențiat în acest sens este compromiterea paginii de Facebook a Serviciului Național de Statistică al UA, acțiune care, deși nu a afectat datele instituției, a urmărit scăderea încrederii populației în informațiile publicate de aceasta.

În ceea ce privește capabilitățile actorilor cibernetici de origine rusă, se remarcă faptul că acestea au avut o varietate foarte mare, pornind de la atacuri distructive, precum cel derulat prin intermediul malware-ului CaddyWiper, până la campanii cibernetice de tip DDoS, care urmăreau indisponibilizarea temporară a unor resurse (Liedekerke și Frankenthal 2023). Conform rapoartelor SSSCIP, serviciile FR identificate cu precădere au fost FSB și GRU, evidențiindu-se actorul cibernetic APT SANDWORM, atribuit serviciului militar de informații (McFail, Hanna și Rebori-Carretero 2021, 2-3). De asemenea, poate fi punctat un anume nivel de sincronizare între forțele militare și capacitățile cibernetice, având în vedere raportarea SSSCIP care anunța o campanie cibernetică, derulată cu o zi înaintea invaziei UA, al cărei scop era probabil de susținere a forțelor armate ale FR în cadrul conflictului ce urma să aibă loc (Radu 2022, 533-544). De asemenea, prezintă interes creșterea semnificativă a numărului de atacuri cibernetice, ceea ce conduce la concluzia că segmentul cyber a avut un rol relevant din derularea conflictului din perioada ianuarie 2022 – ianuarie 2024.

Referitor la modul de funcționare al SSSCIP și la raportarea instituției față de campaniile cibernetice, se remarcă faptul că, inițial, atacurile cibernetice nu au fost

atribuite cu prea mare certitudine FR, aspect modificat pe parcursul timpului. Cu toate acestea, SSSCIP nu a publicat date tehnice suficiente încât să dovedească aceste acțiuni de atribuire publică, ceea ce conduce la concluzia că raportările au avut fundamente strategice politice, nu de natură tehnică. Astfel, retorica raportărilor a migrat către formulări care subliniau faptul că atacurile au fost derulate cu certitudine de către statul agresor. Mai mult, SSSCIP a evidențiat pe parcursul timpului din ce în ce mai multe raportări, în care preciza că nivelul de cooperare cu industria privată din domeniul IT&C este ridicat, nominalizând, cu precădere, companiile ESET și MICROSOFT, aspect ce poate urmări reliefarea existenței unei cooperări dezvoltate care sprijină UA în prevenirea și combaterea atacurilor cibernetice (Lilly și alții 2023, 71-83). Un alt aspect punctat de SSSCIP în repetate rânduri este faptul că impactul acțiunilor ofensive de natură cibernetică nu se resimte doar asupra UA, ci și asupra partenerilor, indiferent de localizarea acestora. Astfel, este posibil ca SSSCIP să fi urmărit creșterea solidarității față de UA în cadrul conflictului cu FR.

Un alt aspect important de remarcat este acela că, în cei doi ani de analiză, nu a fost prezentat niciun atac cibernetic materializat ca fiind asociat sau atribuit unor entități de origine diferită decât cea rusă. SSSCIP nu a raportat atacuri cibernetice de origine chineză, iraniană sau nord-coreeană, deși există actori cibernetici asociați acestor state, cu un nivel ridicat de activitate în mod obișnuit (Assoudeh 2020). Astfel, o ipoteză în acest sens ar putea fi aceea că SSSCIP a urmărit construirea unei retorici care să fie concentrată în totalitate asupra FR (nu asupra prezentării autentice a faptelor), sens în care a evitat publicarea unor rapoarte care să arate că ar exista și alte entități care urmăresc compromiterea unor rețele și sisteme din UA.

În final, este necesar de punctat că raportările SSSCIP s-au dovedit, în unele instanțe, ca fiind incomplete sau lacunare. Un exemplu relevant în acest sens este campania cibernetică asupra infrastructurii satelitare a VIASAT, neraportată de SSSCIP în totalitate, în special din punct de vedere tehnic. Un alt exemplu este cel referitor la raportul din data de 13 decembrie 2023, referitor la atacul cibernetic asupra operatorului Kyivstar, în care nu s-a precizat dimensiunea impactului atacului cibernetic derulat împotriva infrastructurii UA. Aceste aspecte conduc către două posibile concluzii: (1) decizia de a se raporta lacunar anumite incidente sau de a nu se raporta deloc a fost una de natură strategică, pentru a evita scăderea încrederii în rândul populației sau (2) rata ridicată a atacurilor cibernetice a generat greșeli de comunicare, SSSCIP nefiind capabil să mențină ritmul raportărilor racordat la numărul atacurilor cibernetice.

Referințe

Agrafiotis, Ioannis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese și David Upton. 2018. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity* 4 (1). https://doi.org/10.1093/cybsec/tyy006.

Akimenko, Valeriy și Keir Giles. 2020. "Russia's Cyber and Information Warfare." *Asia Policy, National Bureau of Asian Research* 27 (2): 67-75. doi:10.1353/asp.2020.0014.

Assoudeh, Mitra. 2020. "Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective." *Reno ProQuest Dissertations Publishing.* http://hdl.handle.net/11714/7624.

Balmforth, Tom. 2024. "Exclusive: Russian hackers were inside Ukraine telecoms giant for months". https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

Boschetti, Nicolò, Nathaniel G. Gordon și Gregory Falco. 2022. "Space Cybersecurity Lessons Learned from the ViaSat Cyberattack." https://doi.org/10.2514/6.2022-4380.

Bratich, Jack. 2020. "Civil Society Must Be Defended: Misinformation, Moral Panics, and Wars of Restoration." *Communication, Culture and Critique* 13 (3): 311-332. https://doi.org/10.1093/ccc/tcz041.

CERT-EU. 2023. "Russia's war on Ukraine: one year of cyber operations". https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf.

CERT-UA. 2022a. "Fragment of the study of cyberattacks 14.01.2022". https://cert.gov.ua/article/18101.

—. 2022b. "Sandworm Group Cyberattack (UAC-0082) on Ukrainian energy objects using INDUSTROYER2 and CADDYWIPER malware (CERT-UA#4435)". https://cert.gov.ua/article/39518.

Cyber Security Intelligence. 2022. "State Service of Special Communications & Information Protection of Ukraine (SSSCIP)". https://www.cybersecurityintelligence.com/state-service-of-special-communications-and-information-protection-of-ukraine-ssscip-7222.html.

Davydiuk, Andrii și Vitalii Zubok. 2023. "Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn, ESTONIA: IEEE. 121-139. doi:10.23919/CyCon58705.2023.10181813.

Furstenau, Leonardo Bertolin, Michele Kremer Sott, Andrio Jonas Ouriques Homrich și Liane Mahlmann Kipper. 2020. "20 Years of Scientific Evolution of Cyber Security: a Science Mapping." *International Conference on Industrial Engineering and Operations Management.* Dubai, UAE: IEOM Society International. https://www.researchgate.net/publication/340413661_20_Years_of_Scientific_Evolution_of_Cyber_Security_a_Science_Mapping.

Gatlan, Sergiu. 2024. *"Russian hackers wiped thousands of systems in KyivStar attack".* https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/.

Geissler, Dominique, Dominik Bär, Nicolas Pröllochs și Stefan Feuerriegel. 2023. "Russian propaganda on social media during the 2022 invasion of Ukraine." *EPJ Data Science* 12 (1). doi:10.1140/epjds/s13688-023-00414-5.

Hernandez-Castro, Julio, Edward Cartwright și Anna Stepanova. 2017. "Economic Analysis of Ransomware." https://ssrn.com/abstract=2937641.

Hernandez-Castro, Julio și Edward Cartwright. 2020. "An economic analysis of ransomware and its welfare consequences." *The Royal Society Open Science.*

Hupperich, Thomas. 2023. "On DDoS Attacks as an Expression of Digital Protest in the Russo-Ukrainian War 2022." *2023 International Symposium on Networks, Computers and Communications.* Doha, Qatar: IEEE. doi:10.1109/ISNCC58260.2023.10323968.

Khonji, Mahmoud, Youssef Iraqi și Andrew Jones. 2013. "Phishing Detection: A Literature Survey." *IEEE Communications Surveys & Tutorials* 15 (4): 2091 - 2121. doi:10.1109/SURV.2013.032213.00009.

Kizilova, Kseniya. 2022. "Assessing Russian Public Opinion on the Ukraine War." *Social Science Open Access Repository* 2-5. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-86994-6.

Kloba, Lev și Taras Kloba. 2022. "Cyber threats of the banking sector in the conditions of the war in Ukraine." *Financial and Credit Activity - Problems of Theory and Practice* 5 (46): 19-28. doi:10.55643/fcaptp.5.46.2022.3883.

Kozak, Pavel, Ivo Klaban și Tomáš Šlajs. 2023. "Industroyer cyber-attacks on Ukraine's critical infrastructure." *2023 International Conference on Military Technologies (ICMT).* Brno, Czech Republic: IEEE. 1-6. doi:10.1109/ICMT58149.2023.10171308.

Krithika, N. 2017. "A study on wha (watering hole attack)–the most dangerous threat to the organisation." *International Journal of innovations in Scientific and Engineering Research (IJISER)* 4 (8): 196-198. https://web.archive.org/web/20180421102442id_/http://www.ijiser.com/paper/2017/vol4issue8/Aug2017p101.1.pdf.

Lee, Chia-yi. 2022. "Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructur." *Energy Research & Social Science* 87 (8): 102459. doi:10.1016/j.erss.2021.102459.

Lewis, James A. 2022. "Cyber War and Ukraine." https://www.csis.org/analysis/cyber-war-and-ukraine.

Liedekerke, Arthur de și Kira Frankenthal. 2023. "The Cyber Dimension in Russia's War of Aggression." doi:10.5771/9783748917205-239.

Lilly, Bilyana, Kenneth Geers, Greg Rattray și Robert Koch. 2023. "Business@War: The IT Companies Helping to Defend Ukraine." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (IEEE) 71-83. doi:10.23919/CyCon58705.2023.10181980.

Lonergan, Erica D, Margaret W Smith și Grace B. Mueller. 2023. "Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine." *15th International Conference on Cyber Conflict (CyCon).* Tallinn, ESTONIA: IEEE. 85-102. https://doi.org/10.23919/CyCon58705.2023.10182101.

Matania, Eviata și Udi Sommer. 2023. "Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations." https://doi.org/10.1177/00471178231211500.

McFail, Michael, Jordan Hanna și Daniel Rebori-Carretero. 2021. "Detection Engineering in Industrial Control Systems. Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study." *The MITRE Corporation* 2-3. https://www.mitre.org/sites/default/files/2022-04/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf.

Mcwhorter, Dan. 2014. "APT28 Malware: A Window into Russia's Cyber Espionage Operations?". https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations.

Microsoft. fără an. „Definiția atacurilor DDoS". Accesat 14 ianuarie 2023. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-ddos-attack.

—. 2022. "Destructive malware targeting Ukrainian organizations". https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

Mohurle, Savita și Manisha Patil. 2017. "A brief study of Wannacry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science* 8 (5). https://www.ijarcs.info/index.php/Ijarcs/article/view/4021.

Paniotto, Volodymyr. 2020. "The Attitude of Ukraine's Population to Russia and Russia's Population to Ukraine (2008–2020)." *NaUKMA Research Papers Sociology* 3: 3-14. doi:10.18523/2617-9067.2020.3.3-14.

Patil, Dharmaraj, Tareek Pattewar, Shailendra Pardeshi, Vipul Punjabi și Rajnikant Wagh. 2022. "Learning to Detect Phishing Web Pages Using Lexical and String Complexity Analysis." https://eudl.eu/doi/10.4108/eai.20-4-2022.173950.

Paverman, Joseph Herbert. 2019. "An Examination of Cyber-Attacks Carried Out by Russia to Perpetuate Expansion." *Utica College ProQuest Dissertations Publishing*. https://www.proquest.com/openview/a0cb326bdab5e2f4c65f0baca4d2ab47/1?pq-origsite=gscholar&cbl=18750&diss=y.

Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler Mclellan și Chris Sistrunk. 2023. "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology". https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

Radu, Claudiu-Cosmin. 2022. "Russia's approach to cyberspace." *International Scientific Conference Strategies XXI. Volume XVIII*. București: "Carol I" National Defence University Publishing House. 533-544. https://doi.org/10.53477/2971-8813-22-61.

Ratten, Vanessa. 2022. "The Ukraine/Russia conflict: Geopolitical and international business strategies." *Thunderbird - International Business Review* 65 (2): 265-271. https://doi.org/10.1002/tie.22319.

Sapuppo, Mercedes. 2023. "Ukrainian telecoms hack highlights cyber dangers of Russia's invasion". https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-telecoms-hack-highlights-cyber-dangers-of-russias-invasion/.

Smith, Margaret W. și Thomas Dean. 2023. "The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* 103-119. doi:10.23919/CyCon58705.2023.10182061.

Soesanto, Stefan. 2023. "Ukraine's IT Army." *Global Politics and Strategy* 65 (2): 93-106. https://doi.org/10.1080/00396338.2023.2218701.

SSSCIP. 2022a. "A fragment of the January 14 cyber attack investigation has been published". https://www.cip.gov.ua/en/news/opublikovano-fragment-doslidzhennya-kiberatak-14-sichnya.

—. 2022b. ”A new program erasing data from computers has been detected”. https://www.cip.gov.ua/en/news/viyavleno-novu-programu-yaka-stiraye-dani-z-komp-yuteriv.

—. 2022c. ”Cyberattack against Ukrtelecom on March 28: the details”. https://www.cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali.

—. 2022d. ”Cyberattacks against Ukraine are carried out by Russian military hackers”. https://www.cip.gov.ua/en/news/cyberattacks-against-ukraine-are-carried-out-by-russian-military-hackers.

—. 2022e. ”Cyberattacks on the sites of military structures and state banks”. https://www.cip.gov.ua/en/news/shodo-kiberataki-na-saiti-viiskovikh-struktur-ta-derzhavnikh-bankiv.

—. 2022f. ”Four Months of War: Cyberattack Statistic”. https://www.cip.gov.ua/en/news/chotiri-misyaci-viini-statistika-kiberatak.

—. 2022g. ”Hackers mainly attack state institutions, telecommunication operators, local authorities, logistics companies and medical resources of Ukraine”. https://www.cip.gov.ua/en/news/khakeri-atakuyut-perevazhno-derzhavni-ustanovi-operatoriv-zv-yazku-miscevi-organi-vladi-logistichni-kompaniyi-ta-mediaresursi-ukrayini.

—. 2022h. ”Heavy cyberattack on Ukraine’s energy sector prevented. https://www.cip.gov.ua/en/news/poperedzhena-masshtabna-kiberataka-na-energetichnii-sektor-ukrayini.

—. 2022i. ”Latest update on networks operation in Ukraine as of April 11, 15:00”. https://www.cip.gov.ua/en/news/operativna-informaciya-derzhspeczv-yazku-pro-robotu-mobilnogo-zv-yazku-internetu-ta-cifrovogo-telebachennya-v-ukrayini-stanom-na-15-00-11-kvitnya-2022-roku.

—. 2022j. ”Russian cyberattack on the OLL.TV service”. https://www.cip.gov.ua/en/news/kiberataka-rosiyi-na-servis-oll-tv.

—. 2022k. ”Russian cyberwarfare against Ukraine seem to have reached its peak”. https://www.cip.gov.ua/en/news/rosiiski-kibernastupalni-operaciyi-na-ukrayinu-imovirno-dosyagli-svogo-maksimalnogo-potencialu.

—. 2022l. ”Russian hackers attempted to cut electricity supply to many Ukrainians”. https://www.cip.gov.ua/en/news/rosiiski-khakeri-namagalisya-pozbaviti-dostupu-do-elektroenergiyi-znachnu-kilkist-ukrayinciv.

—. 2022m. ”Russian Invaders Disabled Communication Services in the South of Ukraine”. https://www.cip.gov.ua/en/news/rosiiski-okupanti-vidklyuchili-zv-yazok-na-pivdni-ukrayini.

—. 2022n. ”SSSCIP’s State Centre of Cybersecurity has neutralized an attack on public authorities’ websites”. https://www.cip.gov.ua/en/news/derzhavnii-centr-kiberzakhistu-derzhspeczv-yazku-neitralizuvav-ataku-na-saiti-derzhavnikh-organiv.

—. 2022o. ”Starlink in Ukraine: How Elon Musk’s Satellite Internet is Helping Now and What the Prospects Are”. https://www.cip.gov.ua/en/news/starlink-v-ukrayini-yak-suputnikovii-internet-vid-ilona-maska-dopomagaye-zaraz-ta-yaki-perspektivi.

—. 2022p. *”Statistics of Cyber Attacks on Ukrainian Critical Information Infrastructure: 15-22 March”*. https://www.cip.gov.ua/en/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya.

—. 2022q. ”The war continues not only on land, in the air and at sea. Cyberspace has also become an arena for hostilities”. https://www.cip.gov.ua/en/news/the-war-continues-not-only-on-land-in-the-air-and-at-sea-cyberspace-has-also-become-an-arena-for-hostilities.

—. 2022r. "Today's attacks are a continuation of the attacks that took place on February 15". https://www.cip.gov.ua/en/news/23-lyutogo-2022-roku-stavsya-chergovii-akt-kiberagresiyi-proti-ukrayini.

—. 2022s. "Ukraine is not the only target for russian hackers, but a major one". https://www.cip.gov.ua/en/news/ukrayina-ne-yedina-cil-rosiiskikh-khakeriv-prote-odna-z-golovnikh.

—. 2022t. "Ukrainian television and radio are back in Kherson". https://www.cip.gov.ua/en/news/do-khersona-povernulosya-ukrayinske-telebachennya-i-radio.

—. 2022u. "Within a month of war, there were already three times more hacker attacks than during the same period last year". https://www.cip.gov.ua/en/news/za-misyac-viini-vzhe-stalosya-maizhe-vtrichi-bilshe-khakerskikh-atak-riznogo-vidu-nizh-za-analogichnii-period-minulogo-roku.

—. 2023a. "A Cyberattack Failed to Disrupt Ukrinform News Agency". https://www.cip.gov.ua/en/news/kiberataka-ne-zmogla-zupiniti-robotu-informaciinogo-agentstva-ukrinform.

—. 2023b. "At least 23 russian cyber terrorist groups act against Ukraine". https://www.cip.gov.ua/en/news/proti-ukrayini-pracyuyut-shonaimenshe-23-rosiiski-kiberteroristichni-khakerski-grupi.

—. 2023c. "Attacks against IT companies and specialized software developers as a threat to critical infrastructure". https://www.cip.gov.ua/en/news/ataki-na-it-kompaniyi-ta-specializovanikh-rozrobnikiv-pz-yak-zagroza-kritichnii-infrastrukturi.

—. 2023d. "CERT-UA experts are investigating a cyberattack against Kyivstar telecom operator's network". https://www.cip.gov.ua/en/news/fakhivci-cert-ua-doslidzhuyut-kiberataku-na-merezhu-telekom-operatora-kiyivstar.

—. 2023e. "Cyberattack on the State Statistics of Ukraine: the enemy reports another non-existent «victory»". https://www.cip.gov.ua/en/news/kiberataka-na-derzhstat-ukrayini-vorog-ukotre-prozvituvav-pro-peremogu-yakoyi-ne-bulo.

—. 2023f. "Cybercriminals tried to steal data, disguising themselves as Ukrainian MFA". https://www.cip.gov.ua/en/news/kiberzlovmisniki-namagalisya-vikradati-dani-maskuyuchis-pid-ukrayinske-mzs.

—. 2023g. "How russian and pro-russian hackers attack Ukraine". https://www.cip.gov.ua/en/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu.

—. 2023h. "Local public authorities are among the key targets for russian hackers". https://www.cip.gov.ua/en/news/miscevi-organi-vladi-odna-z-osnovnikh-mishenei-rosiiskikh-khakeriv.

—. 2023i. "Russian hackers attacked users in Ukraine and Poland once again: this time they used emails containing links to «documents»". https://www.cip.gov.ua/en/news/rosiiski-khakeri-vchergove-atakuvali-koristuvachiv-ukrayini-ta-polshi-cogo-razu-za-dopomogoyu-elektronnikh-listiv-z-posilannyami-na-dokumenti.

—. 2023j. "Russian hacking group Turla attacks defense forces using CAPIBAR and KAZUAR malware — CERT-UA investigation". https://www.cip.gov.ua/en/news/rosiiske-ugrupuvannya-turla-spryamovuye-ataki-proti-sil-oboroni-vikoristovuyuchi-shkidlivi-programi-capibar-ta-kazuar-doslidzhennya-cert-ua.

—. 2023k. ”Targeted cyberattacks remain among the major cyber threats posed by the FSB hackers — Report”. https://www.cip.gov.ua/en/news/targetovani-kiberataki-zalishayutsya-odniyeyu-z-osnovnikh-kiberzagroz-vid-khakeriv-iz-fsb-zvit.

—. 2023l. ”The attack on Ukrinform might have been carried out by the Sandworm hacking group, associated with russian GRU: preliminary results of CERT-UA investigation”. https://www.cip.gov.ua/en/news/ukrinform-mogli-atakuvati-khakeri-z-ugrupuvannya-sandworm-pov-yazanogo-z-rosiiskim-gru-poperedni-dani-doslidzhennya-cert-ua.

Steinbrecher, Dominique. 2022. ”Viasat KA-SAT attack (2022)”. https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022).

Sullivan, Scott. 2023. ”Unpacking Cyber Neutrality.” *15th International Conference on Cyber Conflict (CyCon).* Talinn, ESTONIA: IEEE. 9-23. https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.

Tarasenko, Oleh, Dmytro Mirkovets, Artem Shevchyshen, Oleksandr Nahorniuk-Danyliuk și Yurii Yermakov. 2022. ”Cyber security as the basis for the national security of Ukraine.” *Cuestiones Politicas* 40 (73): 583-599. https://doi.org/10.46398/cuestpol.4073.33.

Temple-Raston, Dina. 2023. ”In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans”. https://therecord.media/victor-zhora-interview-click-here-ousted.

Visvizi, Anna și Miltiadis D. Lytras. 2020. ”Government at risk: between distributed risks and threats and effective policy-responses.” *Transforming Government: People, Process and Policy* 14 (3): 333-336. https://doi.org/10.1108/TG-06-2020-0137.

Willett, Marcus. 2022. ”The Cyber Dimension of the Russia–Ukraine War.” *Global Politics and Strategy* 64 (5): 7-26. https://doi.org/10.1080/00396338.2022.2126193.

Wilson, Richard L. și Alexia Fitz. 2023. ”Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues.” *Proceedings of the 18th International Conference on Cyber Warfare and Security Vol. 18 No. 1.* Baltimore, MD: Towson University. 440-448. https://doi.org/10.34190/iccws.18.1.1050.