European Repository of Cyber Incidents

Rok działań wojennych w Ukrainie: dziewięć uwag na temat operacji cybernetycznych

Kerstin Zettl-Schabath, Uniwersytet w Heidelbergu
Sebastian Harnisch, Uniwersytet w Heidelbergu
Tłumaczenie polskie: Joanna Kulesza, Uniwersytet Łódzki

Federacja Rosyjska i jej pełnomocnicy przeprowadzili liczne operacje cybernetyczne przeciwko Ukrainie i państwom wspierającym jej prawo do samostanowienia. Bezpośrednio po inwazji z 2014 roku te operacje powodowały poważne szkody i wywoływały niepokoje w samej Ukrainie, jak i w innych państwach. Po rosyjskiej inwazji w 2022 roku wielu obserwatorów obawiało się jeszcze skuteczniejszych ataków rosyjskich na infrastrukturę krytyczną lub realizacji przez Rosję operacji zintegrowanych, konwencjonalno-cybernetycznych. Rok po rozpoczęciu konfliktu trwają dyskusje na temat powodów, dla których rosyjskie działania w cyberprzestrzeni nie spełniły tych oczekiwań. Uczestnicy tych debat szukają odpowiedzi na pytanie o to, czy większość operacji została skutecznie udaremniona przez ukraińską cyberobronę i podmioty ją wspomagające, czy raczej rosyjskie jednostki państwowe i wspomagające je podmioty niepaństwowe nie były w stanie lub nie chciały zrealizować skutecznych operacji cybernetycznych o szerszym zasięgu. Niezależnie od treści tych rozważań, niniejszy artykuł zawiera dziewięć spostrzeżeń na temat możliwych do zidentyfikowania wzorców konfliktu cybernetycznego ukształtowanych w pierwszym roku działań wojennych w Ukrainie. Koncentrujemy się w nim na interakcjach pomiędzy państwami a podmiotami niepaństwowymi oraz na wzorcach operacyjnych. Czynimy to w oparciu o nasze własne dane z projektu EuRepoC, ale także wykorzystując analizy przygotowane przez innych badaczy. Zakładamy, że w nadchodzących latach środowisko cyberzagrożeń będzie ulegało dalszej dywersyfikacji, kształtując nowy krajobraz cyberbezpieczeństwa międzynarodowego. Teza ta niedawno znalazła odzwierciedlenie w raporcie ENISA, zawierającym prognozę zagrożeń cyberbezpieczeństwa do roku 2030.

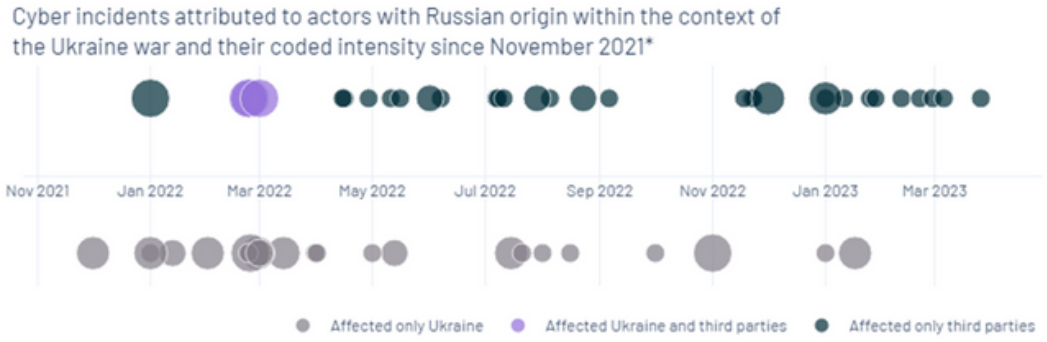
Niezależnie jednak od tego rosnącego poziomu zagrożeń, państwa powinny zadbać także o zwiększenie swoich możliwości reagowania na zagrożenia wielowymiarowe, omówione w tym artykule.

Analizując zmieniające się motywacje sprawców, towarzyszące ich działaniom elementy polityki państw czy same metody ich działania, odnotowujemy, że coraz bardziej zacierają się sfery działania podmiotów państwowych i niepaństwowych. Identyfikujemy ponadto istotne trendy odnotowane podczas przebiegu takich konfliktów, które prawdopodobnie ukształtują przyszłe środowisko operacyjne.

1. Cyberataki w Ukrainie nie osiągnęły progu intensywności ataków zbrojnych.

- Przed 24 lutego 2022 r. eksperci z zakresu cyberbezpieczeństwa zapowiadali niespotykany dotąd poziom ofensywnych cyberoperacji rosyjskich, bezpośrednio wspierających konwencjonalne działania wojenne w Ukrainie. Tak się nie stało - zamiast takiej eskalacji odnotować można raczej zmienną intensywności ataków cybernetycznych w pierwszym miesiącu operacji wojskowych, głównie operacji skierowanych przeciwko ukraińskim celom strategicznym, takim jak podmioty rządowe lub sieci telekomunikacyjne, zaś siła tych ataków z czasem spadła (patrz wykres poniżej). Wspólny raport firm iant z lutego 2023 r. pokazuje, że w pierwszych czterech miesiącach otwartego konfliktu miało miejsce więcej szkodliwych operacji niż w ciągu ośmiu lat ją poprzedzających (tj. od czasu aneksji Krymu w 2014 r.), zaś ich kulminacja nastąpiła w czasie inwazji w lutym 2022 r.
- Omawiając podejmowane przez strony konfliktu rodzaje operacji informacyjnych, autorzy raportu wskazują, że Rosja i podmioty działające na jej rzecz skoncentrowały się przede wszystkim na dezinformacji i szpiegostwie. Działania te miały prawdopodobnie na celu wprowadzenie w błąd co do rodzajów i skali ataków konwencjonalnych oraz przemieszczania się wojsk okupacyjnych, zaś próby uszkodzenia infrastruktury krytycznej miały jedynie charakter posiłkowy. Warto zauważyć, że większość rosyjskich operacji była skierowana na cele niewojskowe, a poważne zakłócenia fizyczne były raczej wyjątkiem niż regułą. Co ważne, atak hackerski na satelitę firmy Viasat zrealizowany na godzinę przed inwazją na Ukrainę pozostaje najbardziej jak dotąd nieudolną rosyjską operacją cybernetyczną, której celem było zakłócenie ukraińskiej komunikacji wojskowej, opartej o wykorzystanie satelity KA-SAT. Alternatywnie, włamanie do sprzętu Viasat mogło stanowić jedynie atak wspierający szerzej przeprowadzoną operację informacyjną, mając na celu uzależnienie Ukrainy od komunikacji naziemnej, łatwiejszej do przechwycenia.

- Rosyjskie operacje dezinformacyjne i szpiegowskie w dużej mierze wpisują się w istniejący już rosyjski schemat wojny informacyjnej w Ukrainie, wymierzonej także w państwa NATO i UE. Niesłusznie wskazują więc niektórzy eksperci, iż połączone operacje konwencjonalno-cybernetyczne były częste. Jednoczesne cyfrowe i konwencjonalne ataki wojskowe stanowią niewystarczające kryterium dla oceny efektywności działania i zdolności operacyjnych Rosji. Niespójne rosyjskie cyberoperacje pozwalają natomiast sądzić, że najprawdopodobniej nie były one wcześniej skoordynowane z konwencjonalnymi działaniami wojennymi, rozpoczętymi 24 lutego. Co więcej, strona rosyjska nie doceniła ukraińskiej cyberobrony i skuteczności otrzymanego przez nią wsparcia. Niezależnie od trudnej sytuacji rosyjskich sił na kilku frontach, malejąca liczba operacji cybernetycznych od lipca 2022 r. pozwala wnioskować, iż nastąpiło pewne "zmęczenie operacyjne", które może, choć nie musi oznaczać ograniczoną liczbę zasobów ludzkich, dostępny w cyberoperacjach realizowanych przez rosyjskie agencje bezpieczeństwa (FSB), wywiadu (SWR) i wojsko (GRU), ograniczoną możliwość wykorzystania serwerów proxy na potrzeby skoordynowanych operacji cybernetycznych oraz straty w personelu IT, wynikające z emigracji lub tymczasowej zmiany celów kolejnych ataków (zob. wykres poniżej).
- Jak dotąd, według naszej wiedzy, żaden rząd (w tym także rząd Ukrainy czy Rosji) nie uznał, że operacje cybernetyczne w Ukrainie lub związane z nimi incydenty w państwach trzecich stanowiły bezprawne "użycie siły", naruszając zakaz zawarty w art. 2 ust. 4 Karty Narodów Zjednoczonych i zwyczajowe prawo międzynarodowe. Poszlaki sugerują raczej, że rządy wahały się nad (lub nie były zainteresowane) sugerowaniem, że "próg użycia siły zbrojnej" został przekroczony. Mimo to Wiktor Żora, dyrektor ds. transformacji cyfrowej w Państwowej Służbie Specjalnej Komunikacji i Ochrony Informacji (SSSCIP) Ukrainy, przekonywał w styczniu 2023, że rosyjskie cyberataki, przeprowadzane równolegle do ataków fizycznych na ukraińską ludność cywilną, można także zakwalifikować jako zbrodnie wojenne. Aby ten argument był zasadny, rzekoma "koordynacja" między atakami fizycznymi i cybernetycznymi musiałaby być poparta analizą techniczną, która zawierałaby więcej dowodów niż tylko ich koordynację w czasie. Niezależnie od istniejącej, powszechnej zgody państw co do tego, że prawo międzynarodowe znajduje zastosowanie w cyberprzestrzeni tak samo jak poza nią oraz że państwa także tam powinny przestrzegać zasad odpowiedzialności międzynarodowej, niewiele wysiłku włożono w faktyczną implementację tych reguł w odniesieniu do rzeczywistych przykładów. Choć różne są powody, dla których państwa ukrywają szczegóły swoich operacji i dochowują poufności, warto odnotować, że taka praktyka może przyczynić się do powstania niepożądanej przepaści pomiędzy uznaniem obowiązywania norm prawa międzynarodowego a ich implementacją, również w kontekście wojny w Ukrainie.[1]

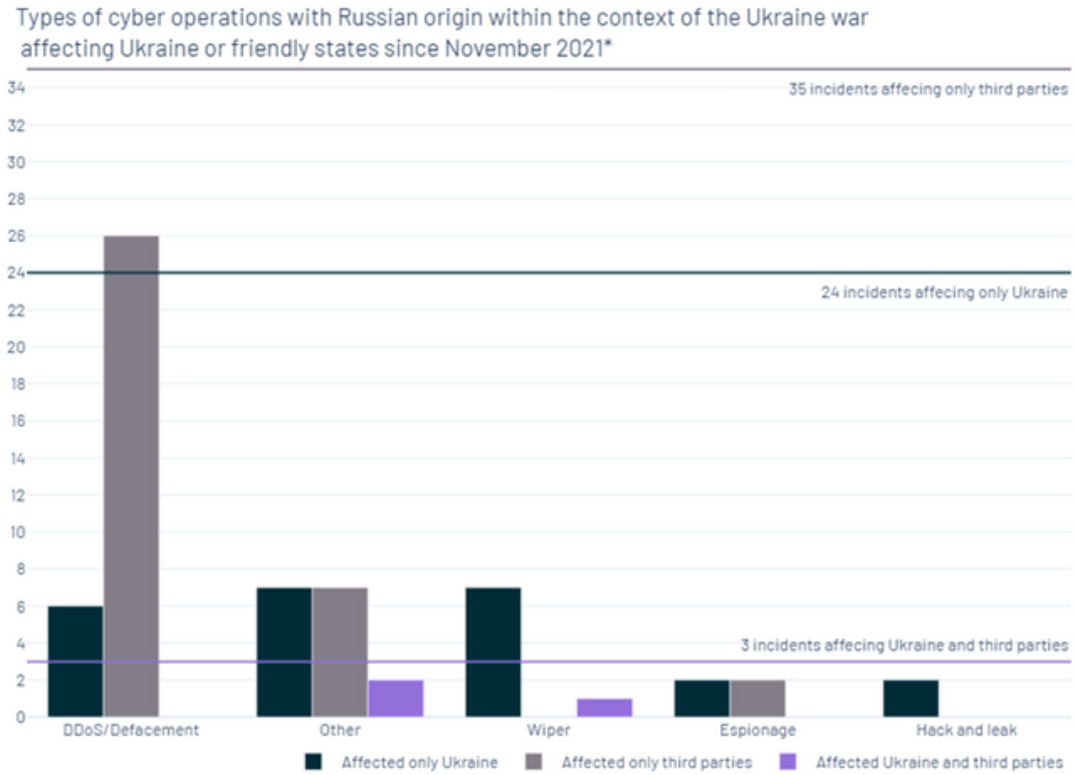


Przykład: Cyberincydenty wywołane przez Rosję po 1 listopada 2021 r. w związku wojną w Ukrainie w oparciu o przyjęte w naszej metodologii zasady atrybucji. | Wykres przedstawia 62 incydenty. Każdy krąg oznacza incydent, jego kolor wskazuje na udział stron trzecich, a rozmiar odzwierciedla jego ważoną intensywność cybernetyczną | * odniesienie do daty rozpoczęcia incydentu. Źródło: zbiór danych EuRepoC 1.0 na dzień 17.04.2023 r. - DOI 10.5281/zenodo.7848941

2. Podmioty rosyjskie skutecznie wykorzystują operacje cybernetyczne jako

- Z danych EuRepoC wynika, że zdecydowana większość rosyjskich operacji cybernetycznych przeciwko celom ukraińskim oraz tych, które zostały przypisane podmiotom lojalnym wobec Kremla, to działania o charakterze szpiegowskim lub o niskim poziomie „dolegliwości". Operacje te obejmują dezinformację, realizowaną za pomocą ataków DDoS w połączeniu z atakami mającymi na celu zniszczenie reputacji celu ataku (ang. defacement) lub operacjami typu hack-and-leak (patrz wykres poniżej). Rosyjskie podmioty państwowe przeprowadziły szereg operacji ofensywnych przeciwko celom infrastruktury krytycznej, ale podmioty prywatne z Ukrainy i państw ją wspierających były w stanie udaremnić takie operacje, albo niezwłocznie odzyskać kontrolę nad przejętym systemem. Niektóre firmy zajmujące się cyberbezpieczeństwem i wspierające władze ukraińskie, jak Microsoft, raportowały o znacznej ilości udanych rosyjskich operacji cybernetycznych, realizowanych równolegle z operacjami konwencjonalnymi, jednak ustaleń tych nie potwierdzają dane i analizy EuRepoC. Po pierwsze, doniesienia o skoordynowanych operacjach sił rosyjskich nie są wystarczająco szczegółowe ani obszerne, aby móc udowodnić wykorzystanie szczególnie zaawansowanych metod integracji ataków fizycznych i cybernetycznych. Po drugie, jeśli siły rosyjskie były zdolne do tak wysoce zintegrowanych działań wojennych, w tym operacji cybernetycznych, powinny były skorzystać z tej zdolności przede wszystkim w krytycznych fazach rosyjskich operacji konwencjonalnych, czego nie zrobiły. Po trzecie, należałoby przyjąć, że z upływem czasu siły rosyjskie powinny być w stanie dokonać postępów na polu walki, podczas gdy aktualne rosyjskie cyberoperacje charakteryzuje niezmieniony lub wręcz niższy stopień zaawansowania, przede wszystkim w porównaniu z coraz lepszą sytuacją wojsk Rosji w walce konwencjonalnej, w szczególności po częściowej mobilizacji we wrześniu 2022 r. Ten brak koordynacji pomiędzy rosyjskimi atakami cybernetycznymi a konwencjonalnymi podkreślono także we wspólnym raporcie holenderskiej Służby Wywiadu i Bezpieczeństwa (AIVD) oraz Służby Wywiadu i

Bezpieczeństwa Wojskowego (MIVD). Podkreślono tam również skuteczność ukraińskich wysiłków obronnych realizowanych wspólnie z partnerami z Zachodu.

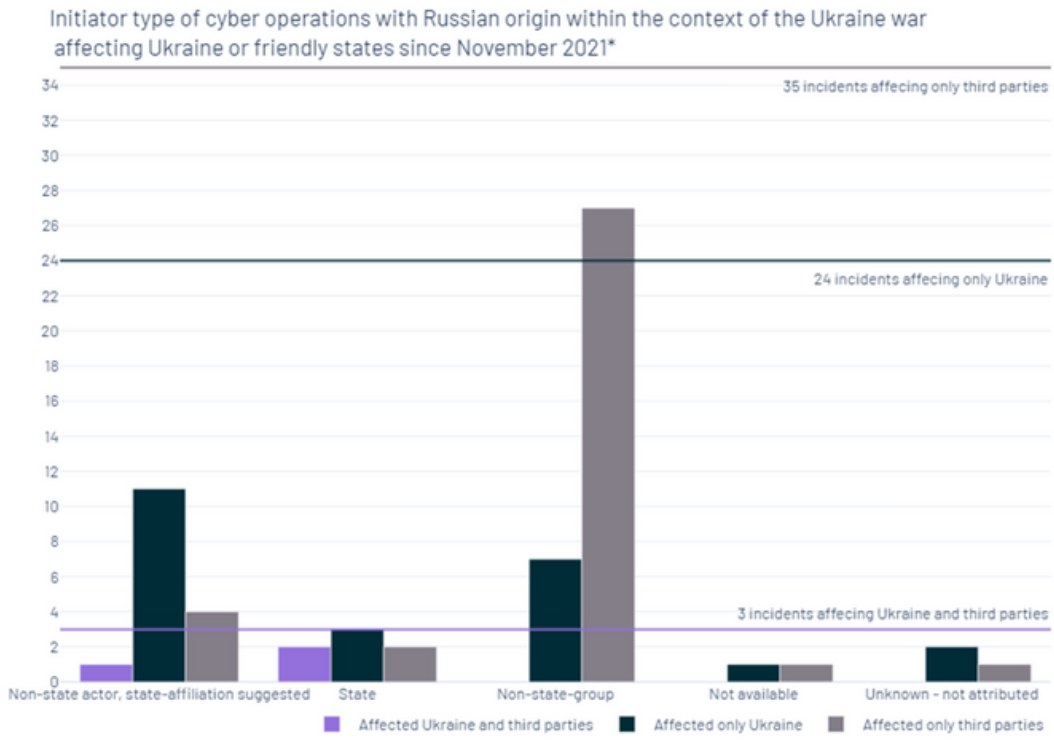


Przykład: Cyberincydenty oficjalnie przypisane Rosji, odnotowywane od listopada 2021 r. w związku z wojną w Ukrainie. Na wykresie przedstawiono liczbę typów operacji przez nas zbadanych, zróżnicowanych według udziału podmiotów trzecich, wyróżnionych wśród 62 zdarzeń analizowanych w zestawie danych. | * odniesienie do daty rozpoczęcia incydentu. | Typ operacji jest określany przez kombinacje typów incydentów: DDoS/Defacement (zakłócenia bez przejęcia), Hack and leak (kradzież danych i doxing), Wiper (zakłócenia przepływu danych i ich przejęcie z nadużyciem), szpiegostwo (kradzież danych), inne: (inne kombinacje). | Źródło: zbiór danych EuRepoC 1.0 na dzień 17.04.2023 r. - DOI 10.5281/zenodo.7848941

3. Rosyjskim władzom udało się zmobilizować niepaństwowych cyberprzestępców, państwowe grupy APT, grupy przestępców korzystających z ransomware i haktywistów w celu zintensyfikowania operacji cybernetycznych w Ukrainie (patrz wykres poniżej). Realizowane w następstwie tych działań operacje nie wykazują jednak nowych schematów koordynacji operacyjnej, a sposoby działania lub wybór metod nie wykazują znacznych różnic w stosunku do ataków z lat poprzednich.

- Po roku wojny podmioty działające z upoważnienia lub pod kontrolą Rosji nie były w stanie przeprowadzić operacji bardziej destrukcyjnych niż te, które realizowały przed rozpoczęciem działań wojennych 24 lutego 2022 r. Przeciwnie, intensywność i częstotliwość operacji cybernetycznych ustabilizowała się po wczesnej przerwie na przełomie marca i kwietnia 2022 r. W szczególności współpracujące z państwem grupy APT, takie jak APT28, nadal skupiają swoje działania na szpiegostwie, podczas gdy grupy cyberprzestępcze, które przysięgły wierność Kremlowi, kontynuują ataki ransomware. Z kolei rosyjscy hakerzy, deklarujący patriotyczne motywy swoich

działań, tacy jak ci z grupy Killnet, nadal korzystają przede wszystkim z ataków DDoS i ataków typu *defacement*, polegających na włamaniu się na strony i zmianę ich treści, które czasami nazywane są "uciążliwościami" (ang. *nuisance*, zob. też przypis 5). Ogólnie rzecz biorąc, grupy te nie były w stanie zastąpić słabej rosyjskiej obrony cybernetycznej, co spowodowało wzrost liczby ataków na rosyjskie systemy informatyczne po rozpoczęciu działań wojennych.



Przykład: Cyberincydenty oficjalnie przypisane Rosji, odnotowywane od listopada 2021 r. w związku z wojną w Ukrainie. Na wykresie przedstawiono liczbę typów operacji, zróżnicowanych według udziału podmiotów trzecich, wyróżnionych wśród 62 zdarzeń analizowanych w zestawiel * odwołując się do daty rozpoczęcia cyberincydentu. Źródło. Zbiór danych EuRepoC 1.0 na dzień 17.04.2023 r. - DOI 10.5281/zenodo.7848941

- Co więcej, zdolności cybernetyczne pomiotów niepaństwowych działających na rzecz Rosji wydają się być niższe zarówno podczas operacji defensywnych, jak i ofensywnych od możliwości ochotniczej Ukraińskiej Cyberarmii, innych grup haktywistów, nie deklarujących powiązań z żadnym państwem, takich jak Anonymous, czy podmiotów prywatnych, pomagających Ukrainie, takich jak Microsoft. Jest oczywiste, że drenaż mózgów w rosyjskim sektorze IT, w połączeniu z zachodnimi sankcjami, jeszcze bardziej przechyli równowagę niepaństwowych sił cybernetycznych pomagających obu stronom na korzyść Ukrainy.

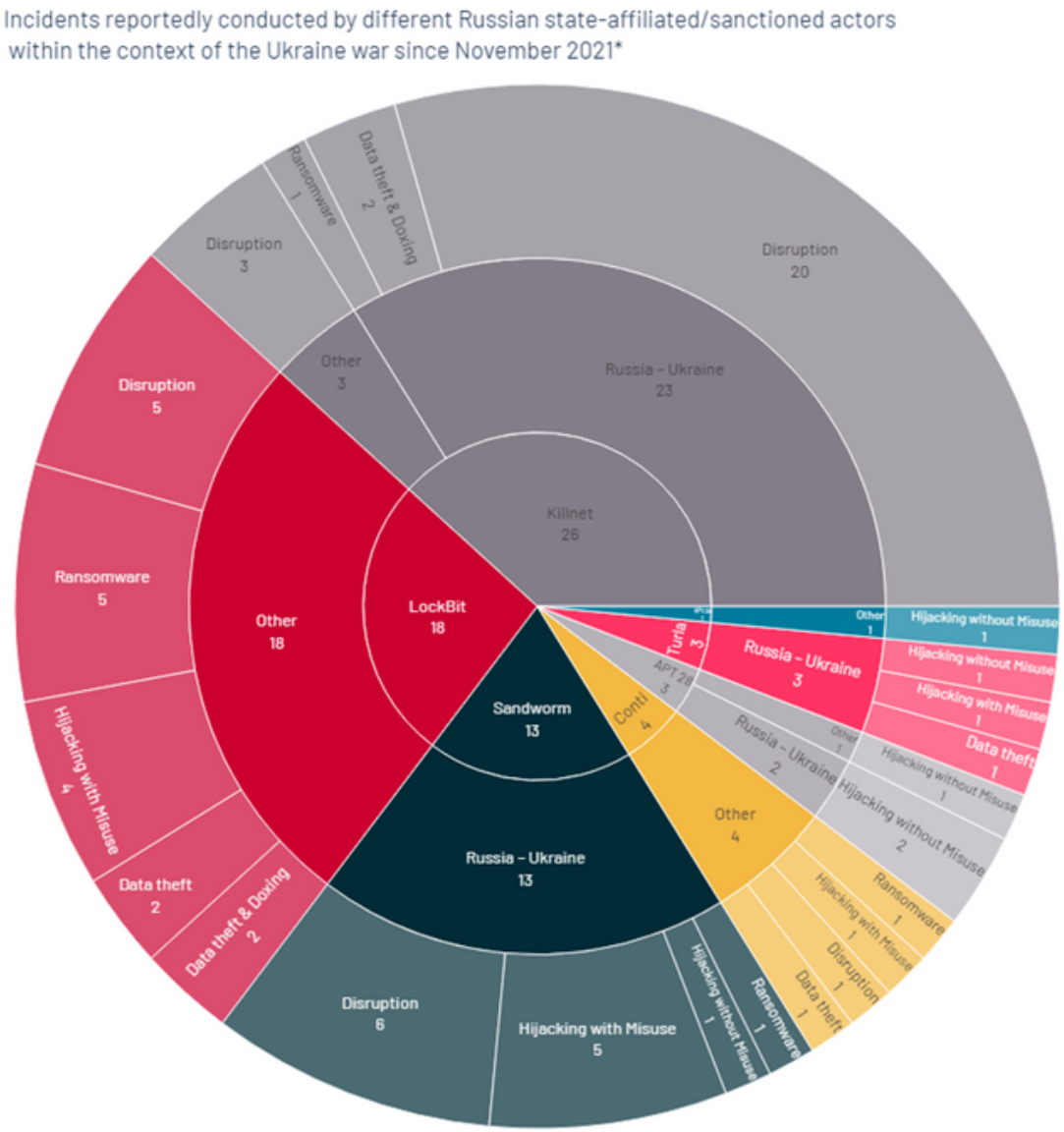
4. "Drenaż mózgów" z rosyjskiego sektora technologicznego i przymusowa rekrutacja ekspertów IT od września 2022 r., np. z więzień, zapowiadają potencjalne przegrupowanie rosyjskich państwowych jednostek cybernetycznych i grup cyberprzestępczych we Wspólnocie Niepodległych Państw.

- Ostatnie raporty dotyczące cyberzagrożeń zawierają sugestie, jakoby skład grup cyberprzestępczych zmienił się w konsekwencji ich reorientacji politycznej. Po tym, jak grupa ransomware Conti zadeklarowała lojalność wobec Kremla w następstwie inwazji, doszło do wewnętrznego rozłamu między jej prorosyjskimi i proukraińskimi członkami. Jednak inne grupy cyberprzestępcze wykorzystujące przede wszystkim szkodliwe oprogramowanie typu ransomware, takie jak LockBit lub ALPHV (BlackCat), rzekomo unikają opowiadania się po którejś ze stron konfliktu, przedkładając wspólne interesy ekonomiczne członków grup nad potencjalnie rozbieżne postawy narodowo-patriotyczne.
- Według stanu na koniec marca 2023 r. niewiele wskazuje na to, że przegrupowanie personelu operacyjnego w rosyjskich jednostkach państwowych spowodowało dramatyczne zmiany w taktyce, technikach i procedurach (TTP), np. odnośnie do wykorzystania złośliwego oprogramowania.

5. W porównaniu z tajnymi operacjami szpiegowskimi prowadzonymi przez "klasyczne" rosyjskie grupy APT, takie jak Sandworm czy APT28, grupy ransomware powiązane z Rosją, np. Conti, zdominowały publiczne doniesienia o konfliktach cybernetycznych.

- Najbardziej znane rosyjskie grupy APT, czasami nazywane "wspaniałą czwórką" (Sandworm, Turla, APT28 i APT29), nie zmieniły znacząco swojego schematu operacyjnego wobec Ukrainy po rozpoczęciu działań wojennych. Raczej prowadziły dalej realizowane wcześniej działania (patrz wykres poniżej), np. szpiegostwo polityczne przeciwko członkom NATO, które oczywiście obejmuje obecnie znacznie więcej informacji związanych z Ukrainą. Na przykład w 2022 r. grupa APT28 uzyskała dostęp do amerykańskiego dostawcy łączności satelitarnej, co podkreśla rosnące strategiczne znaczenie sieci satelitarnych jako celów cyberataków. Z kolei powiązana z GRU grupa APT Sandworm zachowała swój (bardziej) destrukcyjny profil operacyjny, przeprowadzając kilka ataków na cele ukraińskie (przykłady: CaddyWiper, NikoWiper), ale nie spowodowała większych szkód. Warto zauważyć, że żadna z wyżej wymienionych grup APT nie była odpowiedzialna za "jeden decydujący cyberatak", który mógłby zmienić przebieg wojny na korzyść Rosji. Serwery proxy wspierające działania o charakterze szpiegującym, takie jak Turla, atakowały ukraińskie instytucje także w okresie poprzedzającym inwazję, wykorzystując złośliwe oprogramowanie ANDROMEDA od grudnia 2021 r.

- Wzorce operacyjne grup wykorzystujących oprogramowanie ransomware, takich jak Conti czy LockBit, zakłóciły działanie różnych sektorów kluczowych dla państw na całym świecie, powodując np. stan wyjątkowy w Kostaryce w maju 2022 r., ale ich działania wobec celów ukraińskich były słabo skoordynowane lub mało skuteczne.
- Podmioty stosujące hybrydowy model ataków, tj. te które nie działają wyłącznie z wykorzystaniem narzędzi hakerskich lub dezinformacyjnych, a raczej łączą je z metodami konwencjonalnymi, takie jak Ghostwriter, wymagają większej uwagi ze strony podmiotów państwowych, jakwynika z raportu Uniwersytetu w Cardiff. Autorzy wskazują, że wyraźny podział kompetencji pomiędzy podmiotami administracji państwowej na zagrożenia cybernetyczne i fizyczne czyni je „ślepymi" na tego rodzaju operacje hybrydowe, nazywając to zjawisko "ślepotą na powiązania".

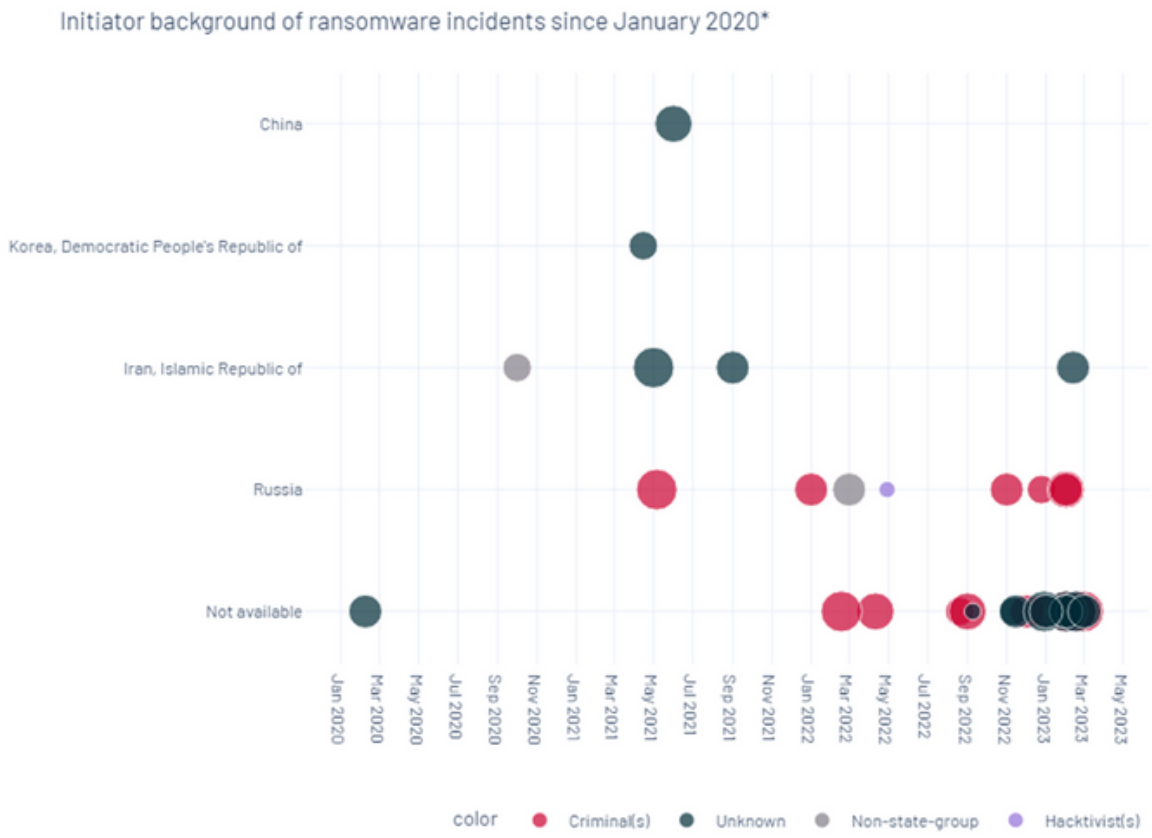


Przykład: Typy cyberincydentów inicjowanych przez rosyjskie podmioty państwowe/objęte sankcjami od listopada 2021 r. na podstawie publicznej atrybucji. Na wykresie przedstawiono 68 typów zakodowanych łącznie dla 40 zdarzeń, z podziałem na rolę każdego podmiotu wskazaną w wewnętrznym okręgu, jego udział w działaniach offline wskazany w środkowym okręgu oraz udział i liczbę określonych typów zdarzeń dla każdego podmiotu odzwierciedloną w zewnętrznym okręgu. Należy pamiętać, że każdy incydent może obejmować wiele typów zdarzeń. | * odniesienie do daty rozpoczęcia incydentu. | Źródło: zbiór danych EuRepoC 1.0 na dzień 17.04.2023 r. - DOI 10.5281/zenodo.7848941

6. (Rosyjskie) kampanie z wykorzystaniem szkodliwego oprogramowania ransomware nabierają charakteru hybrydowego, łącząc cele finansowe i polityczne.

- Według dostępnych doniesień, częstotliwość operacji ransomware spadła w 2022 r. w porównaniu z 2021 r., podczas gdy średnie zyski z ich realizacji wzrosły, co spowodowało, że sprawcy koncentrują się na bardziej wartościowych celach, takich jak infrastruktura krytyczna, ze szczególnym uwzględnieniem sektora ochrony zdrowia, produkcji przemysłowej i energetyki. Jednak nakierowanie prawodawstwa krajowego na walkę z cyberatakami wykorzystującymi oprogramowanie ransomware w połączeniu z pakietami sankcji przeciwko podmiotom rosyjskim skutecznie zniechęca ofiary do uiszczania okupu.
- Z operacyjnego punktu widzenia przestępcze motywacje mające na celu zdobycie "szybkiego zysku" niejednokrotnie powiązane były z motywacją geopolityczną państw udzielających schronienia cyberprzestępcom, na przykład poprzez zachęcanie ich do atakowania infrastruktury krytycznej państw, z którymi konkurowały. Ta prawidłowość znajduje odzwierciedlenie także w ilości ataków ransomware przypisywanych cyberprzestępcom działającym z terytorium lub pod kontrolą Rosji lub podmiotów z nimi powiązanych, które od 2022 r. często atakują organy władzy lub państwową infrastrukturę krytyczną, w konsekwencji czego zostały włączone do bazy danych EuRepoC (zob. poniżej). Odmienny pogląd na kwalifikację tego typu operacji realizowanych na korzyść państw uznaje je za działania indywidualne jednostek, mające na celu wyłącznie korzyść finansową, bez bezpośredniego zaangażowania państw.
- Z politycznego punktu widzenia przypisanie państwu wysoce destrukcyjnych operacji typu ransomware w trakcie działań wojennych może okazać się jeszcze istotniejsze niż w czasie pokoju, ponieważ tylko ono pozwoli jednoznacznie ocenić tempo eskalacji konfliktu. Biorąc pod uwagę, że kradzieże kryptowalut nadal generują znacznie wyższe zyski niż ataki typu ransomware, to te pierwsze powinny cieszyć się większą popularnością w czasie pokoju. Jednakże, gdy operacje z wykorzystaniem oprogramowania typu ransomware wynikają z motywacji zarówno ekonomicznych, jak i politycznych, mogą stanowić przedmiot świadomego „wyboru" cyberprzestępców i ich mocodawców, ponieważ zdobyty okup może być wykorzystany także do finansowania dalszych operacji cybernetycznych, tworząc w ten sposób samonapędzający się model działania.
- W tym kontekście kilka państw zachodnich zintensyfikowało wysiłki na rzecz przeciwdziałania operacjom typu ransomware w 2022 roku. Środki prawne i polityczne podjęte przez państwa obejmują akty oskarżenia, aresztowania, naciski dyplomatyczne na państwa, w których działają grupy cyberprzestępców wykorzystujących ransomware, a także realizowane są coraz częściej (wspólne) działania organów ścigania, mające na celu np. likwidowanie sieci botnetów lub

sankcje wobec producentów kryptowalut. Poza Stanami Zjednoczonymi, państwa sprzymierzone, takie jak Wielka Brytania i Korea Południowa, niedawno również obrały ten kierunek działania.

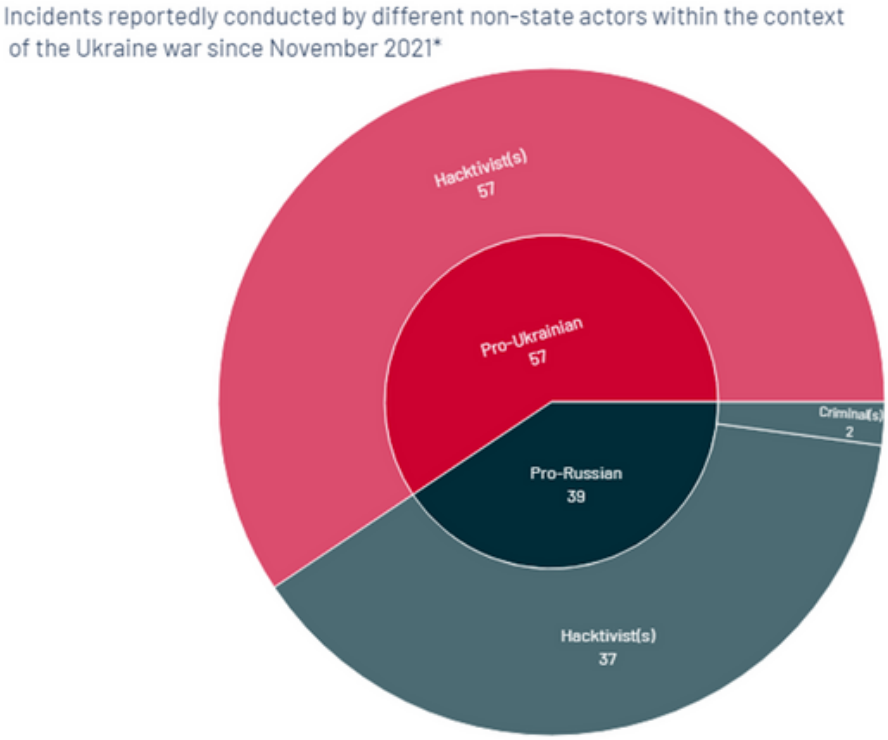


Przykład: Cyberincydenty z wykorzystaniem oprogramowania typu "ransomware" od stycznia 2020 r. | Grafika przedstawia łącznie 43 incydenty w podziale na udział każdego rodzaju podmiotu inicjującego oraz jego państwa pochodzenia. Każdy okręg odzwierciedla zdarzenie, jego kolor symbolizuje rodzaj podmiotu inicjującego, a rozmiar odzwierciedla jego ważoną moc. | * W odniesieniu do daty rozpoczęcia incydentu. | Źródło: zbiór danych EuRepoC 1.0 na dzień 17.04.2023 r. - DOI 10.5281/zenodo.7848941

7. Analizując potencjalne konsekwencje prawne działań "cyberochotników", państwa stosują odmienne praktyki.

- Od początku działań wojennych rząd Ukrainy aktywnie i otwarcie rekrutował hakerów do swojej "armii IT". Wobec prowadzonej przez władze państwowe rekrutacji i koordynacji działań tej grupy można uznać, że działa ona pod „efektywną kontrolą" ukraińskiego Ministerstwa Transformacji Cyfrowej. O ile jej członkowie nie powinni być uznawani za żołnierzy „strony walczącej" w międzynarodowym konflikcie zbrojnym, o tyle władze ukraińskie (i inne państwa świadomie dające im schronienie) mogą zostać pociągnięte do odpowiedzialności prawnej za (niektóre) ich działania.[II]
- Jednocześnie rosyjski rząd ogłosił niedawno plany zwolnienia od odpowiedzialności karnej haktywistów działających w kraju i za granicą z pobudek patriotycznych, argumentując, że ma na celu stworzenie ponadnarodowej koalicji hakerów, podobnej do ukraińskiej ochotniczej cyberarmii. (Poniższy wykres ilustruje proporcje proukraińskich i prorosyjskich niepaństwowych cyberataków odnotowanych przez EuRepoC od listopada 2021 r.)

- W miarę jak ewoluuje praktyka państwowa (np. ostatnio Belgia była pierwszym państwem europejskim, który wprowadził własne zasady udzielania "bezpiecznego schronienia" etycznym hakerom), otwarte pozostają kwestie dotyczące statusu podmiotów niepaństwowych działających na rzecz lub pod kontrolą państw-stron zaangażowanych w międzynarodowy konflikt zbrojny oraz tego, w jaki sposób zasady prawa międzynarodowego, takie jak zasada należytej staranności, mają wpływ na odpowiedzialność prawną podmiotów państwowych i niepaństwowych.



Przykład: Cyberincydenty zainicjowane przez podmioty niepaństwowe w związku z wojną w Ukrainie od listopada 2021 r. | Grafika przedstawia 96 incydentów z podziałem na udział liczbowy/liczbę podmiotów, które były beneficjentami incydentu w okręgu wewnętrznym oraz udział/liczbę typów podmiotów odzwierciedloną w okręgu zewnętrznym. Liczba ta jest wynikiem ustalenia podmiotu inicjującego zgodnie z publiczną atrybucją i państwem, w interesy którego nakierowany był atak: rosyjscy lub białoruscy hacktywiści atakujący Ukrainę lub zaprzyjaźnione państwa traktowani będą jako prorosyjscy; podmioty ukraińskie o sympatiach prorosyjskich realizujące działania wymierzone w Ukrainę lub państwa z nią zaprzyjaźnione traktowane będą także jako prorosyjskie; podmioty ukraińskie lub zaprzyjaźnione, realizujące działania wymierzone w Rosję lub Białoruś, traktowane będą jako proukraińskie; zaś podmioty rosyjsko-białoruskie realizujące działania wymierzone w interesy Rosji lub Białorusi traktowane będą jako proukraińskie. | * odniesienie do daty rozpoczęcia incydentu. | Źródło: zbiór danych EuRepoC 1.0 na dzień 17.04.2023 r. - DOI 10.5281/zenodo.7848941

8. Pomoc cybernetyczna apństw trzecich, w szczególności Stanów Zjednoczonych, Wielkiej Brytanii i państw członkowskich UE, jest istotnym nowym elementem polityki bezpieczeństwa zaobserwowanym podczas działań wojennych w Ukrainie.

- Ukraina odniosła niezwykły sukces w mobilizowaniu międzynarodowej pomocy cybernetycznej ze strony państw, firm technologicznych i akademii, co można postrzegać jako szczególną formę "cyber soft power". Pomoc cybernetyczna dla Ukrainy realizowana jest na dwa sposoby: poprzez zewnętrzne agencje państwowe bezpośrednio wspierające władze ukraińskie w obronie ich sieci oraz, pośrednio, poprzez państwa zachodnie pozwalające na wykorzystanie ich jurysdykcji przez firmy prywatne chroniące ukraińskie dane państwowe, strony internetowe i bezpieczeństwo sieci. Ten stan rzeczy rodzi pytanie o to, czy pomoc cybernetyczna nie realizująca znamion udziału w konflikcie zbrojnym może skutkować przewidzianą przez prawo międzynarodowe reakcją Rosji.
- O ile trudno jest oddzielić konsekwencje dostaw broni konwencjonalnej przez państwa UE i NATO do Ukrainy od konsekwencji towarzyszącej im pomocy cybernetycznej, o tyle można przyjąć, że konsekwencje tej ostatniej były umiarkowane lub niskie. W szczególności TAG Google odnotował w 2022 r. wzrost liczby ataków phishingowych na państwa NATO o 300% w porównaniu z 2020 r., z czego większość pochodziła od wspieranej przez rząd białoruskiej grupy o nazwie PUSHCHA. Nie jest jednak jasne, czy te działania o motywacji geopolitycznej, np. przeciwko polskim organizacjom rządowym lub wojskowym, są bezpośrednio związane z polskimi dostawami broni do Ukrainy, czy też stanowią zwykły element działań o charakterze wywiadowczym i są następstwem innych efektów konfliktu, np. mają na celu monitorowanie ruchu ukraińskich uchodźców.

W szczególności kilkakrotnie wykryliśmy, że konkretna decyzja polityczna podjęta przez państwo lub podmiot udzielający pomocy, Polskę, UE i Niemcy, wydaje się wywoływać reakcję cybernetyczną (na niskim poziomie) prorosyjskich hakerów (przykłady poniżej). 27 października 2022 r. skoordynowany atak DDoS uderzył w polski Sejm, dzień po tym, jak ten przyjął uchwałę uznającą "reżim rosyjski za terrorystyczny". Analogicznie, pod koniec listopada 2022 r. Parlament Europejski stanął w obliczu ataku DDoS po tym, jak zagłosował za uznaniem Rosji za "państwowo wspierające terroryzm". Wiele wskazuje na to, że te "głośne i krótkie operacje" regularnie przyciągają większą uwagę opinii publicznej niż na przykład bardziej efektywne ataki na infrastrukturę krytyczną. W konsekwencji opinia publiczna odnośnie do dynamiki konfliktów cybernetycznych w państwach udzielających pomocy Ukrainie może być zmanipulowana przez atakującego, który dąży do maksymalnego efektu politycznego przy minimalnym wysiłku technicznym.

Zdarzenia/decyzje polityczne

Reakcja(e) w cyberprzestrzeni

2022

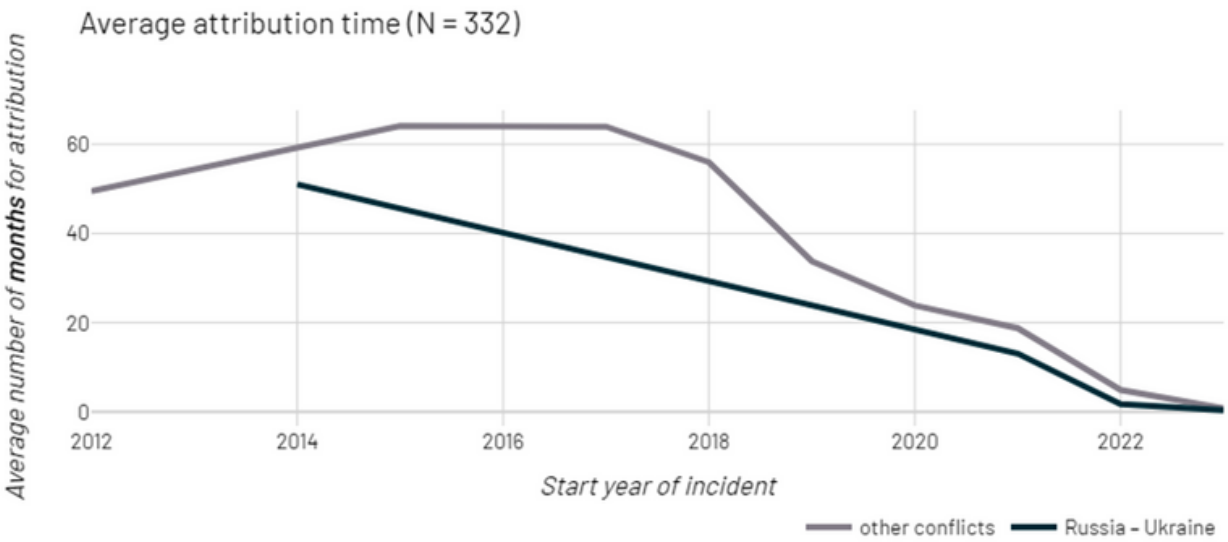
Polska staje się "hubem logistycznym" dla dostaw broni do Ukrainy	02/03	03	Rosyjska sponsorowana przez państwo grupa hakerska IRIDIUM wykorzystuje nowe oprogramowanie ransomware Prestige do atakowania firm transportowych i logistycznych w Ukrainie i w Polsce
Marcel Ciolacu, przewodniczący rumuńskiej Izby Deputowanych, rzekomo obiecuje Ukrainie "maksymalną pomoc" w dostawach śmiercionośnej broni	04	29.04	Prorosyjska grupa Killnet atakuje rumuńskie strony internetowe sektora państwowego i prywatnego
Litwa zakazuje tranzytu towarów przez swoje terytorium do rosyjskiego okręgu kaliningradzkiego z powodu sankcji UE	06	06	Prorosyjskie grupy Killnet i NoName057(16) atakują litewskie witryny internetowe firm prywatnych i agencji rządowych
Norwegia blokuje rosyjskie ładunki na archipelagu Svalbard, przekazuje Ukrainie artylerię rakietową dalekiego zasięgu (MLRS) i zabiega o członkostwo Finlandii i Szwecji w NATO	06/07	29.07	Prorosyjska grupa NoName057(16) atakuje norweskie strony rządowe za pomocą ataków DDoS
Były minister obrony Mołdawii Anatol Salaru krytykuje Władimira Putina i agresję Rosji do Ukrainy	08	23.08	Prorosyjska grupa Killnet atakuje mołdawskie witryny internetowe firm prywatnych i agencji rządowych
Polski Sejm przyjmuje uchwałę, która określa Rosję jako "reżim terrorystyczny"	26.10	27.10	Skoordynowany atak DDoS uderza w witrynę polskiego Sejmu
Starlink kontynuuje finansowanie usługi bezprzewodowego dostępu do Internetu satelitarnego do Ukrainy	10	18.11	Prorosyjska grupa Killnet przyznaje się do ataku DDoS na amerykańską firmę Starlink
Parlament Europejski uznaje Rosję za państwo sponsorujące terroryzm	23.11	23.11	Prorosyjska grupa Killnet atakiem DDoS wyłącza stronę internetową Parlamentu Europejskiego

2023

Niemcy zapowiadają, że wyślą czołgi Leopard do Ukrainy	25.01	25.01	Prorosyjska grupa haktywistów Killnet zakłóca działanie stron internetowych niemieckich podmiotów prywatnych i państwowych
Premier Włoch Giorgia Meloni z wizytą w Kijowie	21.02	21.02	Prorosyjska grupa NoName057 realizuje ataki DDoS na włoskie strony internetowe

9. Zmniejsza się średnia ilość czasu niezbędna do dokonania (publicznego) przypisania operacji cybernetycznej według metodologii EuRepoC (patrz poniżej).

- To, co dotyczy cyberoperacji w ogóle, dotyczy również cyberincydentów podczas działań wojennych w Ukrainie: publikacja informacji i raportów na temat ich przebiegu jest zawsze pierwszym krokiem w kierunku przypisania oraz kwalifikacji politycznej i prawnej. Cyberoperacje ze swej natury są tajne, nieraz nie dochodzi do ich wykrycia, przez co cyberoperacje mogą pozostawać poza świadomością publiczną przez długi czas. Poza tzw. "czasem oczekiwania" przy przeprowadzaniu cyberoperacji, tj. okresem między pierwszym dostępem do sieci docelowych a momentem, w którym ów nieautoryzowany dostęp zostanie zauważony przez ofiarę lub podmioty zewnętrzne (np. firmy informatyczne), średni czas między datą rozpoczęcia a publicznym przypisaniem operacji znacznie się skrócił (zob. poniżej).
- Z punktu widzenia wykrywalności i zapobiegania atakom, ów czas pomiędzy inicjacją incydentu a jego atrybucją może być świadomie determinowany przez ofiarę, np. poprzez monitorowanie działań napastnika w spenetrowanym systemie bez natychmiastowego blokowania mu dostępu. Jeśli tak, ofiara może zdecydować się na wydłużenie odstępu czasowego pomiędzy średnim czasem wykrycia (MTTD; Mean Time to Detect) a średnim czasem reakcji (MTTR; Mean Time to React). W wielu z tych przypadków strategiczna decyzja o opóźnieniu atrybucji pozostaje nieznana opinii publicznej, co z kolei może wpłynąć na poprawność interpretacji wzorców wykrywania, przypisywania i ostatecznie reagowania na incydenty cybernetyczne.



Przykład: Wszystkie incydenty zakodowane według metodologii EuRepoC od marca 2022 r., które zostały przypisane atakującemu. | Wykres przedstawia liczbę miesięcy między zgłoszonymi datami rozpoczęcia i atrybucji dla wszystkich 332 incydentów. Na wykresie rozróżnia się incydenty związane z wojną przeciwko Ukrainie i inne incydenty. | Źródło: zbiór danych EuRepoC 1.0 na dzień 17.04.2023 r. - DOI 10.5281/zenodo.7848941

[I] Weźmy pod uwagę rzekomą operację Głównego Zarządu Wywiadu Ministerstwa Obrony Ukrainy (GURMO) przeciwko przedsiębiorstwu energetycznemu Rosnieftu w Biełgorodzie, o której poinformował wyłącznie jeden z amerykańskich ekspertów ds. cyberbezpieczeństwa, ale nie powtórzyły tego inne główne serwisy informacyjne ani firmy zajmujące się analizą zagrożeń cybernetycznych. Dla kontekstu warto wskazać, iż operacje GURMO zostały zgłoszone przez amerykańskiego eksperta ds. cyberbezpieczeństwa Jeffreya Carra, który z kolei twierdzi, że pomagał GURMO w zbieraniu funduszy na planowaną platformę OSINT do śledzenia rosyjskich terrorystów w Ukrainie i w jej sąsiedztwie przed 24 lutego 2022 r. Następnie, 5 kwietnia, Carr opublikował artykuł o rzekomej ofensywnej operacji cybersabotażu przeprowadzonej przez GURMO przeciwko kilku rosyjskim instalacjom naftowym, w tym przeciwko przedsiębiorstwu Rosnieft w Biełgorodzie.
Podobno 1 kwietnia doszło do pożaru w magazynie Rosnieftu, a rosyjscy urzędnicy obwiniali za zniszczenia ataki ukraińskich helikopterów, zaś władze ukraińskie ostatecznie zaprzeczyły tym doniesieniom. Gubernator Biełgorodu twierdził jednak, że dwóch pracowników firmy zostało rannych. Wynika z tego zatem, że jeśli operacja cybernetyczna GURMO spowodowała (bezpośrednio) pożar w zakładzie naftowym, jak twierdzi Carr, i jeśli pożar spowodował obrażenia fizyczne dwóch pracowników, jak twierdzi gubernator Biełgorodu, to operacja ta mogła przekroczyć próg użycia siły. Biorąc jednak pod uwagę, że twierdzenia Carra nie spotkały się z dużym zainteresowaniem i nie zostały podchwycone przez rosyjskie media ani rosyjskich urzędników, można stwierdzić, że albo twierdzenia Carra zostały uznane za niewiarygodne, albo zostały (celowo) zlekceważone. W tym drugim przypadku, biorąc pod uwagę, że władze rosyjskie nie unikały w przeszłości oskarżania Ukrainy o ataki na terytorium Rosji, można domniemywać, że celowe zlekceważenie (udanej) ukraińskiej operacji cybernetycznej przeciwko rosyjskiej infrastrukturze krytycznej może być wyrazem intencji władz rosyjskich zminimalizowania szkód w reputacji i umniejszenia samych konsekwencji ataku. Utrzymując atak lub jego skutki w tajemnicy, rosyjskie władze mogły chcieć zbagatelizować wewnętrzne koszty agresji na Ukrainę, jednocześnie unikając oczekiwań eskalacji operacji cybernetycznych przeciwko Ukrainie, co z kolei mogło skutkować kolejnymi ukraińskimi cyberatakami, ujawniając słabą cyberobronę Rosji. Epizod ten jeszcze bardziej podkreśla rolę "tajności" i "poufności" przy budowaniu politycznych scenariuszy dotyczących teorii konfliktów cybernetycznych, (nie)ujawnianie cyberataków w całości lub ich niektórych elementów może być świadomym wyborem władz i agencji bezpieczeństwa, zarówno ze strony atakujących, jak i atakowanej.

[II] Po tym, jak proukraińska grupa haktywistów NB65 ogłosiła, że w marcu wyłączyła centrum kontroli rosyjskiej agencji kosmicznej, Rosja ostrzegła, że cyberatak na jej satelity byłby deklaracją wojny. Incydent ten wyraźnie wskazuje, że podmioty niepaństwowe mogą poprzez swoje działania eskalować konflikty międzypaństwowe. Rosja mogłaby pociągnąć do odpowiedzialności międzynarodowej Ukrainę lub państwo trzecie, w którym przebywa sprawca cyberataku, przypisując jej kontrolę nad owymi działaniami lub zaniechanie powstrzymania sprawców niepaństwowych przed prowadzeniem operacji cybernetycznych, co byłoby równoznaczne z użyciem siły, o czym pisali Martin Müller i Sebastian Harnisch.

Wykresy zamieściliśmy dzięki uprzejmości Jonasa Hemmelskampa.

O autorach:

- **Dr. Kerstin Zettl-Schabath** jest pracownikiem naukowym w Instytucie Nauk Politycznych (IPW) na Uniwersytecie w Heidelbergu.
- **Prof. Dr. Sebastian Harnisch** jest profesorem stosunków międzynarodowych i polityki zagranicznej na Uniwersytecie w Heidelbergu.
- **Jonas Hemmelskamp** jest studentem nauk politycznych i asystentem naukowym w Instytucie Nauk Politycznych (IPW) na Uniwersytecie w Heidelbergu.
- **Tłumaczenie polskie: Dr Joanna Kulesza** jest adiunktem w Katedrze Prawa Międzynarodowego i Stosunków Międzynarodowych Wydziału Prawa i Administracji Uniwersytetu Łódzkiego oraz kierownikiem centrum badawczego Lodz Cyber Hub.