Kamil Goryń
https://orcid.org/0000-0003-3021-028X
Wydział Stosunków Międzynarodowych Uniwersytetu w Białymstoku

Konflikt w cyberprzestrzeni na przykładzie wojny w Ukrainie. Studium aktywności z lat 2022–2023

Zarys treści: Współczesne konflikty międzynarodowe charakteryzują się dynamiką i zróżnicowaniem, co utrudnia ich systematyzację, szczególnie w kontekście działań poniżej progu wojny i operacji w cyberprzestrzeni. Artykuł analizuje konflikt w cyberprzestrzeni podczas wojny w Ukrainie, pokazując, jak działania cybernetyczne wspierają operacje kinetyczne oraz kampanie dezinformacyjne.

Outline of content: Contemporary international conflicts are marked by their dynamic nature and diversity, which makes it challenging to categorise them, particularly regarding warfare and cyber operations that fall below the threshold of armed conflict. This article examines the conflict in cyberspace during the war in Ukraine, highlighting how cyber operations support kinetic actions and disinformation campaigns.

Słowa kluczowe: operacje dezinformacyjne Federacji Rosyjskiej, bezpieczeństwo cyfrowe, wojna w Ukrainie

Keywords: disinformation operations of the Russian Federation, digital security, war in Ukraine

Współczesne konflikty międzynarodowe charakteryzują się wysoką dynamiką i zróżnicowanym teatrem działań. Próba ich usystematyzowania jest o tyle trudna, iż intensywność większości z nich wpisuje się w tzw. agresję poniżej progu wojny oraz obejmuje różnorodne teatry i warunki działań. Przez to zbieranie, agregowanie i analiza informacji na ich temat stanowi zadanie wymagające szerokiej wiedzy eksperckiej odnoszącej się nie tylko do kompetencji w obszarze czegoś, co można określić mianem wojny kinetycznej[1], ale również coraz szerszego spektrum działań prowadzonych w cyberprzestrzeni i infosferze.

[1] Powszechne rozumienie konfliktu zbrojnego obejmujące fizyczną eliminację przeciwnika w ramach walki zbrojnej.

PL ISSN 1230-5057 http://dx.doi.org/10.12775/SDR.2024.2.10

Kolejnym wyzwaniem jest ewolucja pojęć używanych do uchwycenia w ramy teoretyczne działań podejmowanych przez różne podmioty na arenie międzynarodowej. Przykład takiego pojęcia stanowić może „wojna hybrydowa", która co do zasady w swoim zakresie pojęciowym pokrywa się w dużej mierze z pojęciem „maskirowki"[2]. Z jednej strony to naturalna próba opisania obserwowanej rzeczywistości, z drugiej jednak strony w swoich rozważaniach wielu badaczy wydaje się pomijać opracowania i solidne podstawy teoretyczne oraz praktyczne, uzyskane w trakcie rywalizacji bloków zachodniego i wschodniego przed rozpadem ZSRR. Co jest zjawiskiem dodatkowo interesującym, gdy uwzględnimy fakt, iż wielu polskich badaczy ma dostęp do rodzimych opracowań obejmujących techniki pracy operacyjnej z PRL. Ich analiza wskazuje, iż co do zasady metodyka pracy pozostaje niezmienna, a kluczowe zmiany zachodzą głównie w obszarze wykorzystywanej technologii, która na przestrzeni lat ewoluuje.

Nie można również zignorować sytuacji rosnącego znaczenia podmiotów niepaństwowych. Na przestrzeni lat, zwłaszcza uwzględniając obszar nowych technologii, zauważyć można rosnące znaczenie w polityce międzynarodowej organizacji o charakterze komercyjnym, których rola była do tej pory bardziej służebna. Jednak wraz ze wzrostem ich wpływu na otoczenie i rosnącym monopolem w zakresie dostarczania kluczowych usług (systemy operacyjne, poczta, usługi wyszukiwania itp.) zwiększyła się także ich podmiotowość. Co obok obecnie odrobinę przebrzmiałych prywatnych firm wojskowych (ang. skrót PMC), których roli w wywieraniu wpływu na różne państwa nie należy jednak ignorować, stanowi kolejny element komplikujący współczesne środowisko bezpieczeństwa.

Powyższe bardzo skrótowe omówienie kontekstu globalnego pozwala na lepsze zakotwiczenie w otaczającej rzeczywistości problemu badawczego będącego tematem poniższego opracowania. Mianowicie na próbę odpowiedzi na pytanie: „Czym charakteryzuje się współczesny konflikt prowadzony w cyberprzestrzeni?". Oczywiście ze względu na złożoność omawianego tematu konieczne jest narzucenie pewnych ograniczeń badawczych. Pierwsze z nich to skoncentrowanie się na jednym konflikcie, który stanowić będzie oś spajającą poszczególne przejawy walki w cyberprzestrzeni. Najbardziej reprezentatywnym przykładem jest obecnie trwająca wojna w Ukrainie, gdyż obejmuje ona działania w cyberprzestrzeni, które z jednej strony stanowią wsparcie działań kinetycznych, a z drugiej wykorzystują działania kinetyczne do zwiększenia skuteczności kampanii dezinformacyjnych prowadzonych w rzeczywistości wirtualnej. Należy też narzucić ograniczenia czasowe, gdyż celem tej analizy nie jest opis wydarzeń historycznych, ponieważ *modus operandi* poszczególnych aktorów ulega zmianie. Dalej jednak niezbędne jest zachowanie pewnego buforu i oparcie się na wydarzeniach odsuniętych w czasie, ze względu na konieczność oczekiwania na publikację rzetelnych źródeł umożliwiających analizę omawianego tematu.

---

[2] Por. I. Dąbrowska, *Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika*, „Przegląd Bezpieczeństwa Wewnętrznego" (2021), nr 25, https://abw.gov.pl/download/18/3855/Ksiega-PBW25-15112021-NOWY.pdf (dostęp: 4.06.2024).

Po zdefiniowaniu problemu badawczego czas na przedstawienie hipotezy roboczej, która została zweryfikowana w procesie badawczym. Jej pierwotna wersja brzmiała: Współczesny konflikt w cyberprzestrzeni charakteryzują wysoka złożoność i szeroka sieć powiązań z działaniami kinetycznymi. Rosnące zaawansowanie techniczne usług kluczowych dla funkcjonowania państwa sprawia, iż rośnie powierzchnia ataku i możliwość oddziaływania na nie przez wrogich aktorów państwowych i niepaństwowych. Z tego względu do skutecznej prewencji i reagowania niezbędne jest podejmowanie szeroko zakrojonych działań pozwalających na rozpoznanie aktywności uderzających w kluczowe obszary funkcjonowania współczesnego państwa.

W zakresie metodyki przeprowadzone badania skupiają się na analizie danych z ogólnodostępnych źródeł opisujących omawiany konflikt. Na podstawie tak uzyskanego materiału metodą dedukcji wyciągnięto wnioski służące do weryfikacji postawionej hipotezy badawczej. Jednocześnie od strony metodyki wykorzystano metody badawcze stosowane w ramach CTI[3] (Cyber Threat Intelligence), stanowiącej jeden z najbardziej interdyscyplinarnych obszarów powiązanych z cyberbezpieczeństwem, który w ramach zakresu tematycznego obejmuje możliwie szeroki kontekst charakteryzujący nie tylko metody, ale również motywy adwersarzy identyfikowanych w cyberprzestrzeni.

Istotny jest fakt, iż w wykorzystanych materiałach widać wyraźne wskazanie agresora, którego działania ofensywne są opisywane i charakteryzowane. W tym wypadku to Federacja Rosyjska, która dokonała agresji na Ukrainę. Ukraina natomiast, wraz ze wspierającymi ją podmiotami, opisywana jest z perspektywy podmiotu podejmującego działania defensywne. W tym zakresie wiadomo, iż ofensywna aktywność w cyberprzestrzeni była i jest podejmowana również przez stronę ukraińską. Niemniej – zapewne celem zachowania skuteczności działań – w przytaczanych raportach informacje na temat działań ofensywnych Ukrainy jeśli się pojawiają, to wyłącznie w zakresie szczątkowym. Można jednak przyjąć założenie, iż ofensywna aktywność pokrywa się rodzajowo z podejmowaną przez stronę rosyjską, gdyż pod wieloma względami charakter podejmowanych działań podyktowany jest wyłącznie posiadanymi możliwościami, a nie ich subiektywną oceną moralną.

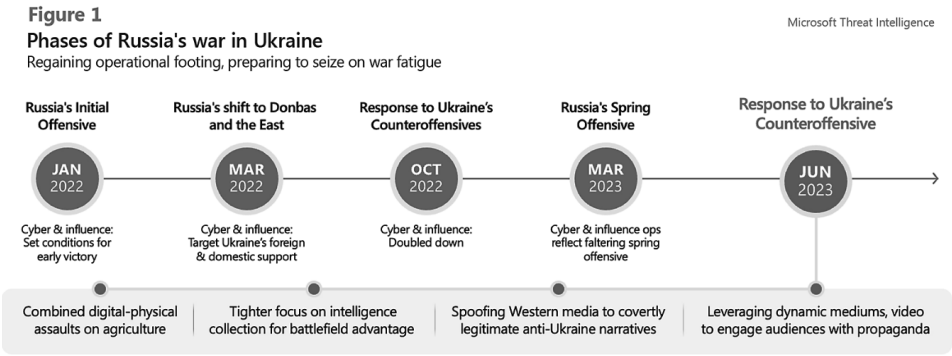
Jednym z przekrojowych opisów działań podejmowanych przez Rosję w stosunku do Ukrainy w 2022 i 2023 r. jest raport „Russian threat actors dig in, prepare to seize on war fatigue" z grudnia 2023 r.[4]

---

[3] Na potrzeby tego opracowania stosowana będzie definicja CTI przytoczona przez Bartosza Jerzmana, a mianowicie „Cyber Threat Intelligence to ocena zdolności, celów i sposobów działania grup adwersarzy opracowana na podstawie analiz narzędzi, infrastruktury oraz danych z incydentów. Zadaniem CTI jest wsparcie decyzyjne w procesie proaktywnego wzmacniania zdolności defensywnych", B. Jerzman, *Wprowadzenie do Cyber Threat Intelligence*, w: *Wprowadzenie do bezpieczeństwa IT*, red. M. Sajdak, Kraków 2023, s. 308.

[4] Por. Microsoft Threat Intelligence, *Russian threat actors dig in, prepare to seize on war fatigue*, https://go.microsoft.com/fwlink/?linkid=2252570 (dostęp: 29.05.2024).

Rysunek 1. Microsoft Threat Intelligence. Przekrój rosyjskiej aktywności



Źródło: https://go.microsoft.com/fwlink/?linkid=2252570 (dostęp: 29.05.2024).

Opisany w raporcie wycinek rosyjskiej aktywności wycelowanej w Ukrainę koncentrował się na operacjach kombinowanych obejmujących działania kinetyczne skupione na przemyśle zbożowym. W założeniu miały one nasilić kryzys związany z niedoborami ziarna dostępnego na rynkach międzynarodowych. Głównym odbiorcą ukraińskich produktów rolnych były i pozostają ubogie kraje globalnego Południa[5]. Kinetyczne ataki na infrastrukturę zbożową oraz blokady morskie wymuszane przez Rosję stanowiły fizyczny aspekt działań podejmowanych w celu uderzenia w ukraińską ekonomię. W latach 2022–2023 produkcja zbóż w Ukrainie spadła o ok. 30%[6]. Jednocześnie drastycznie wzrosła cena zboża na światowych rynkach, co bezpośrednio wpływało na bezpieczeństwo żywnościowe głównych odbiorców ukraińskiej produkcji rolnej. Niska efektywność działań zbrojnych podejmowanych przez Federację Rosyjską i brak możliwości utrzymania fizycznej blokady morskiej wymusiły jednak zmianę strategii działania. Z jednej strony Rosja przystąpiła na pewien czas do porozumienia, które pozwoliło na uformowanie korytarza morskiego umożliwiającego najkorzystniejszy ekonomicznie transport zbóż drogą morską, z drugiej jednak strony nie rezygnowała ona ze swoich planów w stosunku do Ukrainy.

Zintensyfikowane zostały działania realizowane w cyberprzestrzeni. Polegały one z jednej strony na przełamywaniu technicznych zabezpieczeń i wykorzystywaniu luk w celu sparaliżowania usług świadczonych drogą elektroniczną. Z drugiej strony stanowiły narzędzie pozwalające na uzyskanie dostępu do informacji i wykorzystywanie ich w celu działań propagandowych.

---

[5] Por. *Ukrainian gain exports explained*, https://www.consilium.europa.eu/en/infographics/ukrainian-grain-exports-explained/ (dostęp: 29.05.2024); *How the Russian invasion of Ukraine has further aggravated the global food crisis*, https://www.consilium.europa.eu/en/infographics/how-the-russian-invasion-of-ukraine-has-further-aggravated-the-global-food-crisis/ (dostęp: 29.05.2024).

[6] Por. *How the Russian invasion of Ukraine…*

W tym zakresie szczególnie interesujący wydaje się sposób, w jaki łączone były działania kinetyczne, propagandowe oraz cyber celem uzyskania zakładanych efektów. Aby jednak prawidłowo uchwycić ich kontekst, należy zaznaczyć, iż w wypadku ofensywnej aktywności w cyberprzestrzeni, skierowanej przeciwko Ukrainie, nie mamy do czynienia z jednym aktorem. W cytowanych powyżej raportach CTI znaleźć możemy informacje o tym, iż udało się dokonać atrybucji niektórych wrogich aktywności w cyberprzestrzeni i połączyć je z grupami APT[7] powiązanymi z rosyjskim wywiadem wojskowym (GRU) oraz Federalną Służbą Bezpieczeństwa FR (FSB). Jest to istotne, gdyż w pierwszej kolejności pokazuje, iż charakterystyka zrealizowanych działań pozwoliła na jednoznaczne przypisanie ich do poszczególnych aktorów (dokonanie atrybucji), i wskazuje, iż nie mówimy w tym zakresie o homogenicznym zagrożeniu. Podobnie jak w przypadku różnych rodzajów sił zbrojnych czy też różnorodnej charakterystyki poszczególnych jednostek wojskowych funkcjonujących w ramach jednego rodzaju wojsk, w cyberprzestrzeni budowana jest specjalizacja w zakresie realizowanych działań.

Poza grupami APT koniecznie należy wspomnieć również o grupach przestępczych, najczęściej nastawionych na zdobycie korzyści majątkowych, które także stanowią poważne zagrożenie dla kluczowych usług realizowanych przez administrację publiczną. Jednak w kontekście tego artykułu zostały one wyłącznie wspomniane dla zachowania klarowności.

Kolejną podgrupę, którą w tym zakresie najtrudniej scharakteryzować, jednak jej aktywność jest istotna z punktu rozważania cyberzagrożeń możliwych do zaobserwowania podczas wojny w Ukrainie, stanowią tzw. haktywiści, a więc „grupy aktorów związane z […] dokonywaniem ataków «dla sprawy», tzn. z pobudek społecznych lub politycznych. Najczęstszą formą takiej aktywności jest prowadzenie rozproszonych ataków odmowy usługi – DDoS (Distributed Denial of Service). Haktywiści to rzadko kiedy grupy dobrze zorganizowane; powstają często w sposób spontaniczny, pod wpływem wydarzeń społecznych lub politycznych”[8].

Wstępna typologia charakteryzująca różne grupy przeciwników pokazuje, iż próba uchwycenia w ramy teoretyczne wyłącznie przejawów konfliktu obecnych w cyberprzestrzeni stanowi niełatwe zadanie. Jednak dla lepszego zrozumienia, z jak dużym wyzwaniem należy się zmierzyć w celu zapewnienia bezpieczeństwa w cyberprzestrzeni, niezbędne jest zagłębienie się w bardziej techniczny opis działań podejmowanych przez poszczególnych aktorów. W tym obszarze ponownie warto sięgnąć do raportu firmy Microsoft, w którym zidentyfikowany został szereg działań wykonywanych przez grupę APT, nazwaną Seashell Blizzard[9].

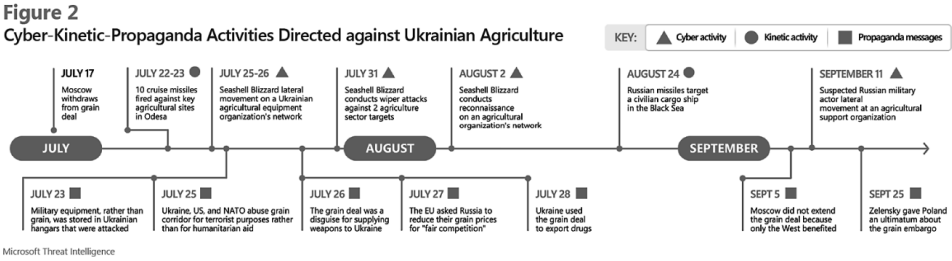
---

[7] Advanced Persistent Threat – adwersarz/przeciwnik posiadający zdolności do realizowania długofalowych działań z wykorzystaniem zaawansowanych narzędzi, realizujący cele państwowe, w tym dostarczanie informacji wywiadowczych. Por. B. Jerzman, *op. cit.*, s. 313–314.

[8] *Ibidem*, s. 314.

[9] Istotna uwaga odnośnie do nazewnictwa poszczególnych grup. Nie istnieje jedna zunifikowana metoda nazywania poszczególnych aktorów. Praktycznie każda grupa analityczna posiada w tym

Rysunek 2. Microsoft Threat Intelligence. Komplementarność działań kinetycznych, dezinformacyjnych oraz aktywności w cyberprzestrzeni



Źródło: https://go.microsoft.com/fwlink/?linkid=2252570 (dostęp: 29.05.2024).

Analizując powyższy diagram, zauważyć możemy, iż działania kinetyczne stanowiące jeden z pierwszych etapów były następnie wspierane przez aktywność w cyberprzestrzeni. W części zadań opierały się one na uzyskiwaniu dostępu do sieci komputerowej i budowaniu metod persystencji w celu utrwalenia dostępu do danych. Jednocześnie uzyskane dane wykorzystywano w działaniach propagandowych. Warto też zaznaczyć, iż jakość przekazu propagandowego wspierającego atak na przemysł rolny Ukrainy w wielu obszarach przypominała bardziej teorie spiskowe (np. sugestie, iż korytarz zbożowy wykorzystywany jest jako kanał przerzutowy do eksportu narkotyków), kierowane w pewnym zakresie na potrzeby wewnętrznej propagandy rosyjskiej. Jednak inne działania skupiały się w dużej mierze na podważeniu wsparcia dla Ukrainy wśród opinii publicznej na świecie.

Jednocześnie celem ataków nie były wyłącznie organizacje ukraińskie, ale także różnorodne organizacje pozarządowe oraz międzynarodowe, zaangażowane w rozwiązanie konfliktu i wsparcie dla walczącej Ukrainy.

Od strony technicznej podstawowy element działań w cyberprzestrzeni dla obu ze zidentyfikowanych grup APT stanowiło gromadzenie informacji na temat potencjalnych celów. W przypadku grupy Aqua Blizzard, powiązanej z FSB, na liście celów na przestrzeni lat znajdowały się ukraińskie podmioty wojskowe, NGO oraz organy mające związek z wymiarem sprawiedliwości. Lista wykorzystywanych przez nie narzędzi, jak również przeprowadzonych kampanii wskazuje, iż najprawdopodobniej jest to grupa posiadająca nie tylko bardziej zawężone cele, ale także mniejsze możliwości operacyjne[10]. Zidentyfikowano wykorzystanie przez tę grupę trzech rodzajów oprogramowania, a mianowicie PowerPinch, Pteranodon

zakresie własne metodyki, stąd w zależności od źródła wykorzystanych informacji ten sam adwersarz może być opisany za pomocą innej nazwy. Przykładowo firma Microsoft grupy powiązane z Rosją określa przydomkiem „Blizzard" (zob. https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming [dostęp: 29.05.2024]). Inne nazwy stosowane w przypadku wymienionego wyżej aktora to np. Sandworm Team, Voodoo Bear, IRIDIUM. Brak spójności w zakresie nazewnictwa niewątpliwie nie sprzyja łatwemu i usystematyzowanemu opisowi poszczególnych grup.

[10] Por. https://attack.mitre.org/groups/G0047/ (dostęp: 29.05.2024).

oraz QuietSieve do zdobywania dostępu i wykradania informacji. Analiza macierzy MITRE ATT&CK[11], przygotowanej dla tej grupy, pokazuje, iż na przestrzeni lat efektem jej działań były wykradanie informacji i działania psychologiczne mające na celu wskazanie zaatakowanym podmiotom, iż adwersarz posiadał dostęp do systemów wewnętrznych.

W przypadku grupy Sandworm/Seashell Blizzard możemy mówić o znacznie szerszym spektrum działań. Z jednej strony aktywność tej grupy w analizowanym okresie obejmowała realizowanie cyberataków wspierających działania podejmowane przeciwko ukraińskiemu przemysłowi zbożowemu. Z drugiej strony pamiętać należy, iż to właśnie ta grupa APT odpowiada za atak z wykorzystaniem oprogramowania NotPetya w 2017 r., a także ataki na inne obiekty infrastruktury krytycznej w analizowanym okresie. Co więcej, jej aktywność nie ograniczała się geograficznie wyłącznie do Ukrainy, ale obejmowała również ataki z wykorzystaniem oprogramowania ransomware, skierowane do podmiotów państwowych i niepaństwowych sprzyjających Ukrainie. Natomiast analiza macierzy MITRE ATT&CK, gdzie zmapowano techniki i taktyki Sandworm Team, wskazuje, iż efektem ich działań, poza eksfiltracją danych, jest doprowadzanie do ich zaszyfrowania bądź szerzej rozumianej niedostępności. Działania te mają charakter bardziej agresywny niż te realizowane przez grupę Aqua Blizzard. Zaznaczyć należy jednak, iż cele i narzędzia poszczególnych grup na przestrzeni lat ulegają zmianie. Szczególnie w wypadku grup APT, które są zadaniowane politycznie. Co może być powodem tego, iż w 2023 r. zaobserwowano spadek operacji, których celem była destrukcja danych czy szerzej zaburzenie funkcjonowania systemów teleinformatycznych. Wzrosła natomiast liczba działań szpiegowskich. Obserwując konflikt, zauważyć można było, iż 50% działań o charakterze destrukcyjnym miało miejsce w pierwszych sześciu tygodniach intensyfikacji konfliktu[12], nastąpił wzrost działań polegających na rozsyłaniu wiadomości phishingowych, wykradaniu poświadczeń, umacnianiu persystencji w sieciach, gdzie uzyskano wcześniej dostęp, i wykradaniu danych[13]. Nie oznacza to jednak, iż adwersarze nie podejmowali działań w zakresie wypracowywania nowych narzędzi, które mogły być wykorzystane przeciwko Ukrainie. Ciekawie o sukcesywnym zdobywaniu i utrwalaniu zdolności do penetrowania infrastruktury IT oraz OT wypowiedzieli się pracownicy Mandiant we wpisie zatytułowanym *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*[14]. Autorzy opisali, jak śledzili aktywność

[11] Zob. https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0047%2FG0047-enterprise-layer.json (dostęp: 29.05.2024).

[12] Por. Microsoft Digital Defense Report 2023, Microsoft Threat Intelligence, https://go.microsoft.com/fwlink/?linkid=2249025&clcid=0x409&culture=en-us&country=us (dostęp: 29.05.2024).

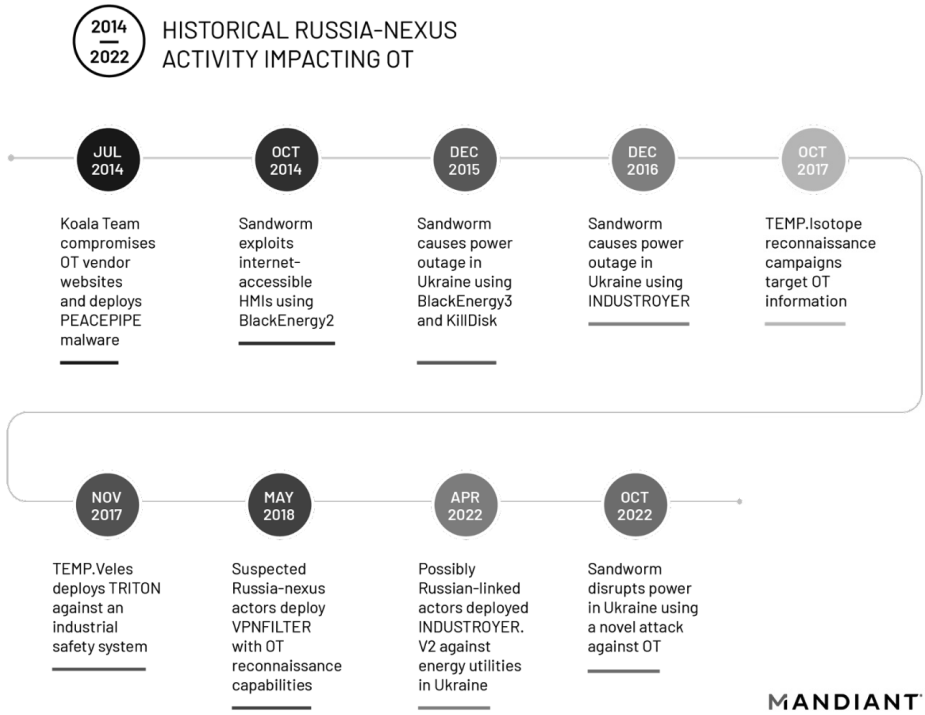
[13] Por. *ibidem*.

[14] K. Prosaka, J. Wolfram, J. Wilson, D. Black, K. Lunden, D. Kapellmann Zafra, N. Brubaker, T. McLellan, C. Sistrunk, *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology (dostęp: 30.05.2024).

aktora, którą w późniejszym czasie udało im się przypisać do grupy Sandworm. Zidentyfikowali oni nie tylko przejawy aktywności w Ukrainie, ale generalnie w skali globalnej. Interesujące jest to, jak w sposób długotrwały i celowany rozwijano kolejne narzędzia bądź wersje wykorzystywanych wcześniej narzędzi.

Dzięki pracy analitycznej możliwe było nie tylko zbudowanie szerszego zrozumienia wykorzystywanych narzędzi, ale także wypracowanie metod ich wykrywania wraz ze wskazówkami pozwalającymi na przeprowadzenie tzw. hardeningu systemów umożliwiającego zmitygowanie ataków.

Rysunek 3. Rozwój narzędzi aktora Sandworm/Seashell Blizzard/Nexus na przestrzeni lat



Źródło: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology (dostęp: 30.05.2024).

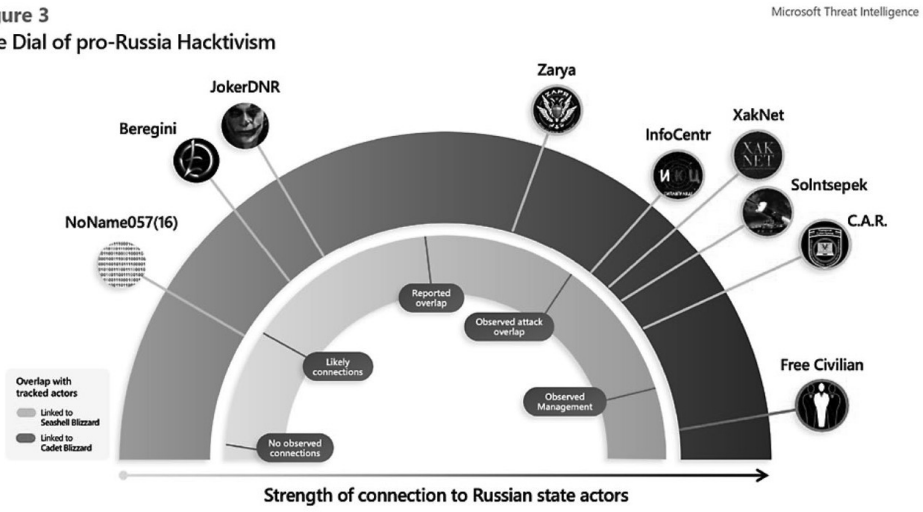
Na powyższej grafice widać, jak na przestrzeni lat rozwijane były poszczególne narzędzia, które w późniejszym czasie grupa APT wykorzystała w celu przeprowadzenia ataków wspierających cele polityczne Federacji Rosyjskiej.

Inną rodzajowo aktywnością charakteryzują się działania podejmowane przez podmioty prywatne realizujące zadania na rzecz aktorów państwowych. W tym zakresie jednym z najlepszych przykładów są tzw. fabryki trolli powiązane z Wagner PMC, którym kierował Jewgienij Prigożyn. Bez wątpienia działania te prowadzono w cyberprzestrzeni, jednak nie skupiały się one na wykorzystaniu kompetencji technicznych, a na budowaniu struktur koncentrujących się na sianiu dezinformacji.

Zdolności w tym zakresie również kształtowane były na przestrzeni lat, jednak skupiano się na korzystaniu z zachodnich platform i mediów społecznościowych do wykreowania kont podszywających się pod prawdziwych użytkowników i rozprzestrzeniania narracji sprzyjającej polityce rosyjskiej. Analiza rodzajowa prowadzonej aktywności pokazuje, iż organizacja o charakterze *stricte* militarnym została wykorzystana przez Rosję do zbudowania zdolności pozwalających na proces demokratycznego wyłaniania władz czy też społeczną percepcję światowych wydarzeń. Przykładami takich działań były: opłacanie influencerów w mediach społecznościowych w celu nakłonienia ich do głoszenia rosyjskiej propagandy, masowe komentowanie wpisów polityków zachodnich celem spotęgowania kremlowskiej narracji czy manipulowanie sondażami prowadzonymi za pomocą mediów społecznościowych[15].

Wybuch pełnoskalowego konfliktu w Ukrainie nie pozostał obojętny dla opinii publicznej. Jest to oczywiście truizm, jednak należy zaznaczyć, iż swój sprzeciw bądź poparcie różnorodne osoby wyrażały w zróżnicowany sposób. Media społecznościowe zostały zalane częściowo inspirowanym i opłacanym przez aktorów państwowych przekazem, a jednocześnie wiele osób chciało podejmować bardziej aktywne działania w celu wspierania jednej ze stron. Doprowadziło to do intensyfikacji zjawiska haktywizmu, opisanego powyżej.

Rysunek 4. Prorosyjscy haktywiści i ich powiązania z grupami APT



From July 2022 to August 2023, Microsoft Threat Analysis Center (MTAC) identified several incidents when a pro-Russia Telegram channel targeted an organization, defaced its website, and claimed it performed a destructive attack. Our data shows some of the incidents had overlap with methods, malware, and infrastructure used by Russian military actors. Above is our current assessment of the relative proximity of many active pro-Russia hacktivist personas to the Russian state, based on first-party data, MTAC analysis of social media posts, and open-source reporting.

Źródło: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue/ (dostęp: 28.05.2024).

[15] Por. *'Troll factory' spreading Russian pro-war lies online, says UK*, https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk (dostęp: 24.05.2024).

W odróżnieniu od wcześniej opisywanych rodzajów aktorów w tym zakresie znacznie łatwiej jest znaleźć przykłady działań ofensywnych wspierających zarówno stronę ukraińską, jak i rosyjską. Na rysunku 4 zobrazowane zostały ciekawe zjawiska. W pierwszej kolejności widać, iż można zidentyfikować różnorodne grupy haktywistów, którzy podejmują różne jakościowo działania. Niewątpliwie każda grupa motywowana jest ideologicznie, jednak w przypadku niektórych widać, iż były one aktywnie wspierane bądź wykorzystywane przez grupy APT. Owo wsparcie bądź wyzyskanie w działaniach miało zróżnicowany charakter, częściowo obejmując wyłącznie udostępnienie narzędzi, które można było wykorzystać w atakach. W innych przypadkach dochodzono do zarządzania działaniami grupy m.in. po to, aby dokonać ataku w cyberprzestrzeni wyprzedzającego działania kinetyczne[16].

Sam haktywizm nie był przeznaczony wyłącznie dla osób wspierających inwazję rosyjską. Po intensyfikacji konfliktu w lutym 2022 r. pojawiło się bardzo dużo serwisów, które umożliwiały łatwe „dołączenie" do ataków DDoS na serwisy i portale rosyjskie. Stanowiło to specyficzny wyraz wsparcia dla Ukrainy, który z perspektywy państw zachodnich był jednak dość problematyczny. Po pierwsze, każde celowe działanie mające na celu zakłócenie funkcjonowania systemów teleinformatycznych stanowi naruszenie prawa w praktycznie wszystkich systemach prawnych krajów zachodnich. Po drugie, działania haktywistów mogą realnie zagrozić operacjom ofensywnym prowadzonym przez strony, które wspierają. Szerzej na ten temat napisał Adam Haertle w artykule umieszczonym w serwisie Zaufana Trzecia Strona:

> W sieci pojawił się na przykład ogromny zrzut danych białoruskiej fabryki broni. W jaki sposób tą akcją zaszkodziły Ukrainie osoby za nim stojące? Niestety tego rodzaju ataki, zarówno wycieki, jak i samo przełamywanie zabezpieczeń, może być poważnym problemem dla wywiadów innych krajów, które w tej samej sieci już się dawno zadomowiły. Jest całkiem możliwe, że w sieci tej białoruskiej fabryki leżał sobie implant amerykański czy brytyjski i czekał na swoją okazję, by przerwać produkcję, zmienić proporcje składu materiałowego kluczowego elementu uzbrojenia, ujawnić listę odbiorców sprzętu czy w inny, skuteczny sposób zakłócić działanie zakładu. Po opublikowaniu wycieku systemy IT przejdą dużo bardziej skrupulatny audyt, pojawią się kolejne zabezpieczenia sieci i jest spora szansa, że te działania mogą przeszkodzić wywiadom, które mogły działać skuteczniej niż publikacja 200 GB dumpu losowych danych online. Podsumowując tę część – grzebiąc w krytycznych systemach, możecie przeszkodzić komuś, kto już tam mieszka i może osiągnąć efekt o wiele większy od tego, co sami zaplanowaliście[17].

Co to oznacza w praktyce? Tak jak zaobserwowali badacze zajmujący się CTI, charakter działań grup APT reprezentujących Rosję uległ zmianie i skupił się na utrwalaniu persystencji i długotrwałym pozyskiwaniu danych. Można więc założyć,

---

[16] Por. J. Coker, *RSAC: Threat Actors Weaponize Hacktivism for Financial Gain*, https://www.infosecurity-magazine.com/news/hacktivism-financial-gain-threat/ (dostęp: 19.05.2024).

[17] Zob. https://zaufanatrzeciastrona.pl/post/dlaczego-nie-powinniscie-hakowac-ani-ddosowac-rosyjskiej-infrastruktury-it/ (dostęp: 10.01.2024).

iż wiele państw zachodnich również takie działania podejmuje. Natomiast haktywiści swoją aktywnością mogą doprowadzić do skutecznego zaalarmowania operatorów infrastruktury teleinformatycznej o występujących w niej lukach.

Ostatnim z obszarów, który uwidocznił się po wybuchu pełnoskalowego konfliktu w Ukrainie, jest uzależnienie infrastruktury ICT od dostawców sprzętu i oprogramowania niepodzielających naszych celów strategicznych. Zrozumienie pełnej skali wyzwań wymaga w tym zakresie przyjęcia roli „adwokata diabła" i uchwycenia perspektywy rosyjskiej. Niemniej wyzwanie to jest jak najbardziej realne. Otóż Rosja, budując swoje sieci teleinformatyczne z wykorzystaniem zachodniego sprzętu i oprogramowania, w chwili gdy podjęła decyzję o pełnoskalowej inwazji, doprowadziła do sytuacji, w której zaprzestano świadczenia jej określonych usług. Jest to o tyle istotne, gdy mówimy o wykorzystaniu sprzętu komputerowego bądź oprogramowania opartego okresowo na odnawianych licencjach bądź wymagającego wsparcia technicznego z kraju, który traktujemy jako przeciwnika. W tym wypadku zauważyć możemy, iż korporacje takie jak Alphabet, Microsoft czy Cisco aktywnie wspierały obronę ukraińskiej infrastruktury ICT, ale jednocześnie w wielu aspektach przestały świadczyć usługi na rzecz agresora.

Podsumowując, przekrojowa analiza danych opisujących konflikt rosyjsko-ukraiński pokazuje dość reprezentatywne spektrum zagrożeń występujących obecnie w cyberprzestrzeni. Z jednej strony wynika to z faktu, iż nie da się teraz prowadzić „wyizolowanego" konfliktu w takiej skali. Skuteczne porażenie zdolności obronnych Ukrainy wymaga uderzenia w podmioty ją wspierające. Oznacza to nie tylko ataki na infrastrukturę krytyczną sojuszników Ukrainy, ale także wpływanie na opinię publiczną w ramach operacji w cyberprzestrzeni. Ich skuteczność podyktowana jest koniecznością ciągłego rozwoju narzędzi i wyszukiwania kolejnych podatności. Zarówno tych technicznych, pozwalających na uzyskanie dostępu do systemów teleinformatycznych, głównie po to, aby zapewnić sobie stały dopływ kluczowych informacji o działaniach przeciwnika, jak i budowania sieci wpływów w mediach społecznościowych. W tym zakresie celem jest wykorzystanie technologii i usług świadczonych na rzecz społeczności zachodnich, aby wywierać wpływ i realizować zamierzenia agresora.

Nie da się dokonać jednoznacznego podziału na rodzaj aktywności i zagrożeń, dominujących w danym momencie. Niezbędne jest prowadzenie przekrojowego modelowania zagrożeń w celu identyfikacji trendów w działaniach adwersarzy. Część grup przestępczych rzeczywiście kieruje się głównie zyskiem i oczekuje okupu za rozszyfrowanie danych, jednak jest to inne gatunkowo wyzwanie niż mitygowanie zagrożeń generowanych przez zadaniowane i finansowane przez państwo grupy APT.

Pod względem teoretycznym złożoność współczesnych wyzwań dla cyberbezpieczeństwa wskazuje, iż z powodzeniem można stosować ramy teoretyczne wykute dla pojęcia „wojna hybrydowa", jak i metodyki badania przejawów „maskirowki". Szczególnie gdy w wyniku atrybucji jesteśmy w stanie przypisać działania do podmiotów powiązanych z Federacją Rosyjską.

W wyniku przeprowadzonej procedury badawczej wstępnie postawiona hipoteza okazała się prawdziwa, wymaga ona jednak uzupełnienia i przybiera następującą formę: Współczesny konflikt w cyberprzestrzeni charakteryzują wysoka złożoność i szeroka sieć powiązań z działaniami kinetycznymi. Priorytet wybranego rodzaju aktywności uzależniony jest od możliwości osiągnięcia celów politycznych za pomocą wybranych środków. Przez co prym działań kinetycznych nad działaniami w cyberprzestrzeni zmienia się dynamicznie. Rosnące zaawansowanie techniczne usług kluczowych dla funkcjonowania państwa sprawia, iż rośnie powierzchnia ataku i możliwość oddziaływania na nie przez wrogich aktorów państwowych i niepaństwowych. Z tego względu do skutecznej prewencji i reagowania niezbędne jest podejmowanie szeroko zakrojonych działań pozwalających na rozpoznanie aktywności uderzających w kluczowe obszary funkcjonowania współczesnego państwa.

Powyższa hipoteza nie pozwala oczywiście w pełni odpowiedzieć na postawione pytanie badawcze i wymaga dalszych badań. Niemniej stanowi ona dobry punkt wyjścia próby uogólnienia charakterystyki wyzwań wynikających z zagrożeń obecnych we współczesnej cyberprzestrzeni.

Conflict in Cyberspace on the Example of the War in Ukraine. A Study of Activity, 2022–2023

Abstract

The article analyses the cyberaspects of the Ukraine-Russia war in 2022–2023, considering both kinetic operations and disinformation campaigns. The author presents the tools and methods used by the Advanced Persistent Threat groups linked to Russia as well as by private actors and hacktivists. The aim is to show how cyber operations complement warfare by supporting disinformation and destabilisation campaigns.

The analysis is based on CTI (Cyber Threat Intelligence) reports, which present data collected for incident prevention and response. The author employs deduction and desk-based analysis to confirm the hypothesis that cyber and kinetic activities support each other. Among the key findings, it is noted that modern cyber conflicts are complex and dynamic, necessitating comprehensive defence strategies. Russian operations conducted by groups such as Sandworm have targeted critical infrastructure operators, aiming to increase pressure on Ukraine and its international partners who are assisting in its defence efforts.

Конфликт в киберпространстве на примере войны в Украине. Исследование активности в 2022–2023 годах

Аннотация

В статье «Конфликт в киберпространстве на примере войны в Украине» анализируются кибераспекты украинско-российского конфликта 2022–2023 гг., учитывая как кинетические действия, так и дезинформационные кампании. Автор представляет инструменты

и методы, используемые группами APT (Advanced Persistent Threat), связанными с Россией, а также частными лицами и хактивистами. Цель – показать, как кибероперации дополняют военные действия, поддерживая дезинформационные и дестабилизационные кампании.

Анализ основан на отчетах CTI (Cyber Threat Intelligence), в которых представлены данные, собранные в рамках предотвращения и реагирования на инциденты. Автор использует дедуктивный и кабинетный анализ для проверки гипотезы о взаимной поддержке кибер- и кинетических действий. Среди ключевых выводов отмечается, что современный киберконфликт многогранен и динамичен, поэтому требует комплексных оборонных стратегий. Российские операции, проводимые, в частности, такими группами, как Sandworm, были направлены на операторов критической инфраструктуры с целью оказать многократно увеличенное давление на Украину и ее международных партнеров, поддерживающих ее в оборонительной войне.

Bibliografia

Coker J., *RSAC: Threat Actors Weaponize Hacktivism for Financial Gain*, https://www.infosecurity-magazine.com/news/hacktivism-financial-gain-threat/ (dostęp: 19.05.2024).

Dąbrowska I., *Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika*, „Przegląd Bezpieczeństwa Wewnętrznego" (2021), nr 25, https://abw.gov.pl/download/18/3855/Ksiega-PBW25-15112021-NOWY.pdf (dostęp: 4.06.2024).

How the Russian invasion of Ukraine has further aggravated the global food crisis, https://www.consilium.europa.eu/en/infographics/how-the-russian-invasion-of-ukraine-has-further-aggravated-the-global-food-crisis/ (dostęp: 29.05.2024).

https://attack.mitre.org/groups/G0047/ (dostęp: 29.05.2024).

https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming (dostęp: 29.05.2024).

https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0047%2FG0047-enterprise-layer.json (dostęp: 29.05.2024).

Jerzman B., *Wprowadzenie do Cyber Threat Intelligence*, w: *Wprowadzenie do bezpieczeństwa IT*, red. M. Sajdak, Kraków 2023, s. 308.

Microsoft Digital Defense Report 2023, Microsoft Threat Intelligence, https://go.microsoft.com/fwlink/?linkid=2249025&clcid=0x409&culture=en-us&country=us (dostęp: 29.05.2024).

Microsoft Threat Intelligence, *Russian threat actors dig in, prepare to seize on war fatigue*, https://go.microsoft.com/fwlink/?linkid=2252570 (dostęp: 29.05.2024).

Prosaka K., Wolfram J., Wilson J., Black D., Lunden K., Kapellmann Zafra D., Brubaker N., McLellan T., Sistrunk C., *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology (dostęp: 30.05.2024).

'Troll factory' spreading Russian pro-war lies online, says UK, https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk (dostęp: 24.05.2024).

Ukrainian gain exports explained, https://www.consilium.europa.eu/en/infographics/ukrainian-grain-exports-explained/ (dostęp: 29.05.2024).

Kamil Goryń, dr; adiunkt na Wydziale Stosunków Międzynarodowych Uniwersytetu w Białymstoku. W pracy badawczej skupia się na wpływie nowoczesnych technologii na stosunki międzynarodowe, ze szczególnym uwzględnieniem różnorodnych obszarów wpisujących się w ramy cyberbezpieczeństwa (k.goryn@uwb.edu.pl).

Kamil Goryń, PhD, is an assistant professor, employee of the Department of International Relations, University of Białystok. His research focuses on the impact of modern technologies on international relations, with a particular emphasis on the various areas that fall under the umbrella of cyber security. He supports his research with practical experience gained through his work as an engineer and cybersecurity consultant gained in the IT industry (k.goryn@uwb.edu.pl).

Wpłynęło do redakcji: 15.05.2024 Zatwierdzono do druku: 19.09.2024