European Repository of Cyber Incidents

Major Cyber Incidents

KA-SAT 9A

Inne nazwy incydentu: Viasat, AcidRain

Opis

Niskoorbitalne satelitarne usługi szerokopasmowego dostępu do Internetu, oferowane przez amerykańską firmę telekomunikacyjną Viasat (sieć KA-SAT 9A) zostały zakłócone w niektórych częściach Europy, gdy w lutym 2022 r. rozpoczęła się rosyjska ofensywa wojskowa przeciwko Ukrainie. Chociaż atak spowodował przede wszystkim istotne zakłócenia w ukraińskiej łączności satelitarnej we wczesnych godzinach rosyjskiej inwazji 24 lutego 2022 r., miał również wpływ na obniżenie wydajności sieci KA-SAT w znacznej części Europy Zachodniej. Firma SentinelOne, zajmująca się badaniem cyberzagrożeń, znalazła pewne "istotne podobieństwa" między komponentami AcidRain, wykorzystanymi w tym ataku, a złośliwym oprogramowaniem VPNFilter. To ostatnie jest powszechnie stosowane przez rosyjską grupę APT Sandworm, powiązaną z rosyjską agencją wywiadu wojskowego GRU, choć SentinelOne powstrzymał się od jednoznacznego przypisania ataku AcidRain grupie Sandworm. Na poziomie politycznym kilka rządów zdecydowało się publicznie przypisać Rosji włamanie do KA-SAT, powołując się na ustalenia wywiadu USA i Wielkiej Brytanii opublikowane 10 maja 2023 r. Jak dotąd incydent Viasat jest powszechnie postrzegany jako najbardziej szkodliwa operacja cybernetyczna w trakcie rosyjskiej wojny przeciwko Ukrainie, choć uważa się, że miał ograniczony wpływ na konwencjonalną kampanię wojskową.

Ramy czasowe
od 24 lutego do 15 marca 2022 r.

Inicjator
Rosyjski wywiad wojskowy: GRU (prawdopodobnie grupa Sandworm)

Typ zdarzenia
Wiper: zakłócenie komunikacji, porwanie (Hijacking) z bezprawnym wykorzystaniem zasobów (Misuse)

Cel ataku
Infrastruktura telekomunikacyjna (Internet satelitarny) na Ukrainie i w całej Europie

Tło wydarzeń

Atak nastąpił równolegle z rozpoczęciem rosyjskiej ofensywy wojskowej przeciwko Ukrainie, która obejmowała serię cyberataków. Rosyjska ofensywa lądowa, stanowiąca punkt kulminacyjny wieloletniej rosyjskiej agresji na Ukrainę, rozpoczęła się wczesnym rankiem 24 lutego 2022 r. z czterech różnych kierunków. Ta ofensywa lądowa była wspierana przez pociski, rakiety i ostrzał artyleryjski ukraińskich miast i infrastruktury.

Jednocześnie od końca 2021 r. nasilało się inwigilowanie sieci komputerowych ("cyberszpiegostwo") i cyberataki na ukraińskie cele cywilne, wojskowe i infrastrukturę krytyczną. [1]

Wpływ i znaczenie

Włamanie do KA-SAT wywarło szkodliwy wpływ głównie na działanie modemów użytkowników w europejskiej sieci satelitarnej EUTELSAT na terytorium Ukrainy i Europy Zachodniej. Ponadto zakłócona została zdalna komunikacja niezbędna do działania blisko 5 800 turbin wiatrowych niemieckiego producenta Enercon, gdzie połączenie zostało przerwane, zaś turbiny nadal działały. [2] W rezultacie niezbędne było dostarczenie 30 000 nowych modemów celem ustabilizowania systemu Enercon, a wymiany trzeba było dokonać na miejscu. [3]

Warto zauważyć, że zarówno ukraińskie wojsko, jak i policja korzystały z modemów, których dotyczył problem. Były one prawdopodobnie niezbędne do normalnego funkcjonowania inteligentnych systemów uzbrojenia oraz w manewrach połączonych sił zbrojnych Ukrainy, które w coraz większym stopniu opierają się na połączeniach internetowych. [4] Tak więc, mimo że atak na naziemną infrastrukturę modemów i routerów satelity KA-SAT zakończył się sukcesem i został opisany w bazie EuRepoC jako charakteryzujący się najwyższą intensywnością (4 z 15), na podstawie oświadczeń publicznych i doniesień medialnych stwierdzamy, że jego wojskowe znaczenie operacyjne było ograniczone.

Rys. 1: Incydenty cybernetyczne z zakodowanym sektorem odbiornika pochodzące z Rosji i wymierzone w Ukrainę od listopada 2021 r.*, z podziałem na sektor docelowy (N = 28)

Uwaga: Rozmiar okręgów przedstawia średnią intensywność incydentów dla każdego sektora i miesiąca, zaś kolor odzwierciedla liczbę incydentów. Próbka obejmuje incydenty w bazie danych EuRepoC, które pochodzą z Rosji i są wymierzone w Ukrainę, uwzględniając cele ataków. Incydenty są wyświetlane wielokrotnie, jeśli dotyczyły więcej niż jednego celu. | * według daty rozpoczęcia incydentu.

Według doniesień medialnych, cyberatak mógł mieć na celu wyłącznie zakłócenie lub wręcz eliminację komunikacji wojskowej Ukrainy podczas rosyjskiej inwazji. Dalsze skutki uboczne mogły być niezamierzone. Początkowo atak ten był postrzegany jako wynik istotnej słabości ukraińskiej obrony podczas rosyjskiej ofensywy, zwłaszcza uwzględniwszy potencjalną przewagę Ukrainy, uzyskaną dzięki koordynacji działań wojskowych w oparciu o inteligentne systemy satelitarne, i tym samym był szeroko komentowany w mediach. Wypowiedzi Wiktora Żory, zastępcy przewodniczącego i dyrektora ds. transformacji cyfrowej Państwowej Służby Łączności Specjalnej i Ochrony Informacji Ukrainy, wywołały dezorientację: po stwierdzeniu na konferencji prasowej na początku maja, że wydarzenie Visat spowodowało "naprawdę ogromne szkody w komunikacji na samym początku wojny", w wywiadzie z dziennikarką Kim Zetter we wrześniu 2022 r., stwierdził, że atak "nie miał" istotnego wpływu na ukraińską komunikację wojskową. [5]

Z perspektywy czasu widać, że atak hackerski miał ograniczony wpływ na komunikację wojska i policji, ponieważ mogły one polegać na analogowych telefonach stacjonarnych, a komunikacja cyfrowa stanowiła jedynie uzupełnienie tego kanału komunikacji. [5] W związku z tym ukraińskie kierownictwo polityczne, wywiad wojskowy oraz łączność oddziałów dowodzenia i kontroli utrzymały funkcjonalność dzięki łączności naziemnej (linie telefoniczne i łączność radiowa). Ukraińskim władzom udało się również w ciągu dwóch dni przywrócić łączność satelitarną i internetową. [5]

Pomimo ograniczonego wpływu militarnego, po ataku ukraiński wicepremier i minister transformacji cyfrowej Mychajło Fedorow za pośrednictwem Twittera zwrócił się o pomoc do Elona Muska. Prośba ta została spełniona i spowodowała, że firma Starlink zapewniła Ukrainie satelitarną łączność internetową. [6] Zapewniając bezproblemowy, szybki dostęp do Internetu, Starlink pozwolił Ukrainie korzystać nie tylko ze stabilnego cywilnego dostęp do Internetu, ale zagwarantował także kluczową przewagę militarną. Precyzyjne ataki dronów na rosyjskie cele, a także synchronizacja postępów i ruchów sił ukraińskich były możliwe tylko dzięki satelitom niskoorbitującym Starlink, zapewniającym szybki przepływ danych. Mimo że Musk ograniczył korzystanie z Internetu satelitarnego dla celów wojskowych, jego działanie unaocznia wyzwania wynikające z rosnącego zaangażowania firm prywatnych (działających w obszarze technologii kosmicznych) w konflikty o wysokiej intensywności. Otwarte pozostają pytania o militaryzację tego typu usług komercyjnych i ich dostawców, działających bez upoważnienia ze strony ministerstw obrony, a tym samym o to, czy można je uznać za legalne cele wojskowe. [35]

Szersza perspektywa I: Militaryzacja przestrzeni kosmicznej

Począwszy od lat 30. XX wieku, rozwój systemów rakietowych przez nazistowskie Niemcy miał obejmować wojskowe cele kosmiczne. [7] W okresie zimnej wojny i po wyniesieniu pierwszego satelity na orbitę po raz pierwszy opracowano wojskowe systemy kosmiczne, które dziś są wykorzystywane przez coraz większą liczbę państw do wspierania naziemnych operacji wojskowych. [8] W tym kontekście militaryzacja przestrzeni kosmicznej opisuje wykorzystanie technologii kosmicznych do celów wojskowych. [9] Wraz z rozwojem nowych systemów satelitarnych do obserwacji pogody, gromadzenia informacji, łączności i nawigacji wzrosło uznanie dla ich wykorzystania w kontekście wojskowym, zwiększając tym samym znaczenie dotyczących ich polityk bezpieczeństwa. [8] [10] Wraz z przyspieszeniem cyfryzacji, wcześniej konwencjonalna kinetyczna militaryzacja przestrzeni kosmicznej przekształciła się w niekinetyczny i nieelektroniczny sposób zakłócania satelitów z Ziemi, głównie w celu zakłócenia komunikacji wychodzącej lub przychodzącej.

Szersza perspektywa II: Broń i cele współczesnych działań wojennych

Atakowanie wojskowych i cywilnych systemów dowodzenia i komunikacji jest cechą działań wojennych. Podstawy doktrynalne stosowania środków bojowych dowodzenia i kierowania (command-and-control warfare; C2W) znalazły odzwierciedlenie np. w polityce USA pod koniec lat 80. i na początku lat 90., której cele skoncentrowane były na wywołaniu paraliżu operacyjnego. [13] Zdolność do samodzielnego lub skoordynowanego działania obejmująca działania ofensywne i manewry, mające na celu wywołanie takich skutków w cyberprzestrzeni, stanowi podstawową cechę wojsk cybernetycznych. [14]

Znaczenie ataku Viasat należy oceniać w kontekście całokształtu jego przyczyn, celów i działań Rosji i Ukrainy pod koniec lutego 2022 r. Atak można uznać za udany w sensie technicznym, jeśli celem było spowodowanie jakiejś formy zakłóceń w atakowanych systemach. Równie skuteczna okazała się reakcja ukraińskiego rządu, polegająca na zastąpieniu jednego kanału łączności satelitarnej innym, co umożliwiło rządowi i dowództwu wojskowemu kontynuowanie dowodzenia i zapewnienie komunikacji za pośrednictwem satelitów. Z drugiej strony możliwe jest, że atak KA-SAT/Viasat nie stanowił głównego wektora rosyjskiego cyberataku, stosowania środków bojowych C2W lub wojny informacyjnej, a miał raczej charakter ataku wspierającego; próbą zmuszenia ukraińskich przywódców do korzystania przede wszystkim z łączności stacjonarnej, co według Wiktora Żory miało miejsce. Telefony stacjonarne mogą być łatwo namierzone i łatwiej podsłuchiwać je przy użyciu konwencjonalnych narzędzi. Dopóki rosyjskie myślenie i strategia operacyjna pozostają niejawne, oceny powodzenia i znaczenia ataku Viasat można jedynie szacować.

Nowatorski charakter ataku

Atak na system i usługi KA-SAT pokazuje, że cyberataki na infrastrukturę krytyczną są wykorzystywane i można się spodziewać, że będą nadal wykorzystywane podczas konfliktów zbrojnych. Komercyjne systemy kosmiczne mogą być postrzegane jako korzystne cele w atakach mających na celu wsparcie naziemnych operacji wojskowych, ponieważ standardy cyberbezpieczeństwa dla satelitów komercyjnych i rządowych/wojskowych różnią się, co sprawia, że satelity komercyjne są potencjalnie bardziej podatne na ataki. [12] Co więcej, skutki takich ataków nie ograniczają się do konkretnych podmiotów i systemów (w tym systemów wojskowych). W przypadku KASAT miał miejsce efekt domina, obejmujący wiele systemów infrastruktury krytycznej daleko poza granicami Ukrainy.

Przypisanie odpowiedzialności

Viasat zbadał incydent we współpracy z firmą Mandiant, zajmującą się cyberbezpieczeństwem, a także z "organami ścigania oraz amerykańskimi i międzynarodowymi agencjami rządowymi". [14] 30 marca koncern wydał wstępne oświadczenie, w którym potwierdził, że ataki wymierzone były przede wszystkim w Ukrainę. [15] 31 marca firma Sentinel Labs, także zajmująca się cyberbezpieczeństwem, oceniła "ze średnią pewnością, że istnieją podobieństwa rozwojowe między AcidRain a szkodliwą wtyczką VPNFilter etapu 3". [16] Jak twierdzi firma, FBI i Departament Sprawiedliwości USA pierwotnie przypisały kampanię VPNFilter rosyjskiemu rządowi i APT 28. Amerykańska Agencja Bezpieczeństwa Narodowego (NSA) oraz Agencja Cyberbezpieczeństwa i Infrastruktury (CISA) przypisały go później konkretnie grupie Sandworm na podstawie analizy zachowań realizowanych w związku z atakami[16], które obejmowały wcześniejszy sabotaż ukraińskiej infrastruktury krytycznej i wywołały tam fizyczne skutki (np. atak na ukraińską sieć energetyczną na przełomie 2015 i 2016 roku). Opierając się na tych poszlakach, tj. czasie realizacji operacji oraz jej zbieżności z początkiem wojny konwencjonalnej i wykrytych podobieństwach wynikających z badań kryminalistycznych, włamanie do KA-SAT zostało technicznie przypisane Rosji.

10 maja brytyjskie Narodowe Centrum Cyberbezpieczeństwa (NCSC) dokonało politycznego przypisania ataku. Opierając się na danych wywiadowczych USA i Wielkiej Brytanii NCSC oceniło, że Rosja (a konkretnie wywiad wojskowy, GRU) była prawie na pewno odpowiedzialna za włamanie do Viasat. [17] Stany Zjednoczone[18], Wielka Brytania [17], Kanada [19] i Australia [20] przypisały incydent Rosji w indywidualnych oświadczeniach wygłoszonych wspólnie z Wysokim Przedstawicielem Unii Europejskiej. [21] Następnie Macedonia Północna, Czarnogóra, Serbia, Albania, Bośnia i Hercegowina, Islandia, Liechtenstein, Norwegia, Ukraina, Mołdawia i Gruzja przyłączyły się do oświadczenia Unii Europejskiej. [21] Warto zauważyć, że te publiczne atrybucje nie określały, która konkretnie grupa powiązana z GRU była odpowiedzialna za atak, pomimo zgłoszonych dowodów wskazujących na grupę Sandworm.

Oś czasu operacji i atrybucja

24 lutego 2022	HermeticWiper na ukraińskich komputerach rządowych; Atak na komputery z systemem Windows
24 lutego 2022	Wiper AcidRain na satelitach KA-SAT 9A Rosja atakuje Ukrainę
02:00 UTC	Rosja rozpoczyna ataki rakietowe na Ukrainę
03:02 UTC	Viasat wykrywa złośliwy ruch na modemach
04:15 UTC	Viasat wykrywa modemy wychodzące z sieci
15 marca	Viasat oficjalnie ustabilizowany

Źródła: [16] [14] [17]

Specyfikacja techniczna

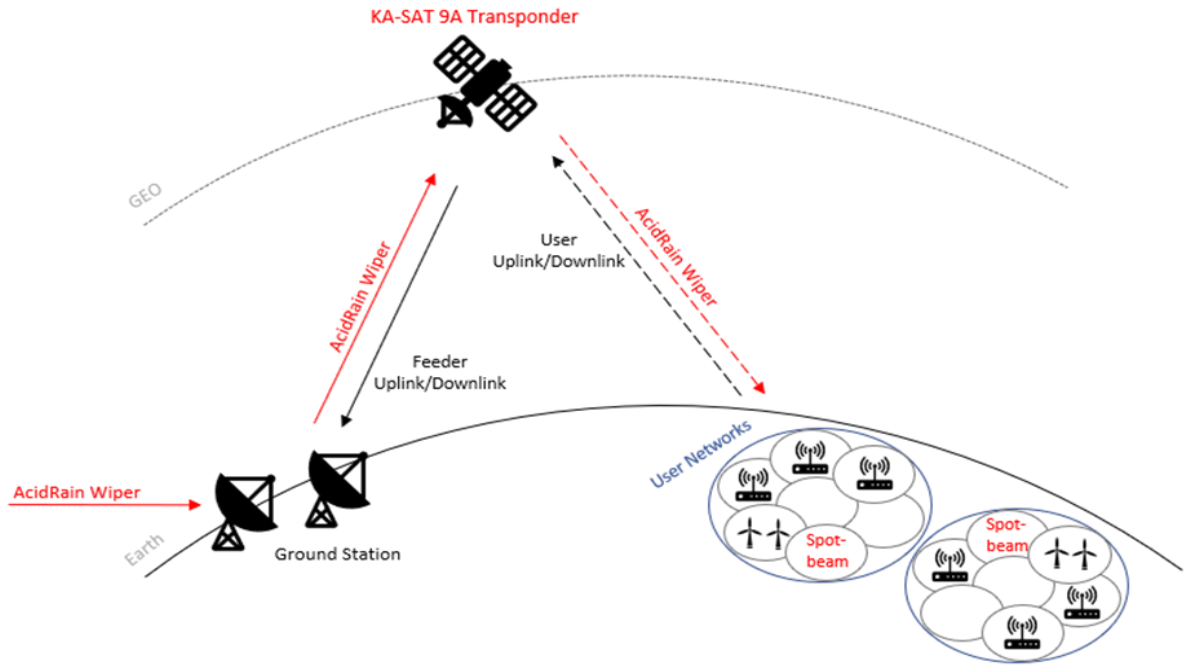
Atak nie dotknął samego geostacjonarnego satelity szerokopasmowego KA-SAT 9A, ale naziemną infrastrukturę obsługujących go modemów i routerów. Operacja składała się z dwóch faz: w pierwszej operator wykrył atak DDoS, który pochodził z kilku modemów SmurfBeam2 i SmurfBeam2+ i był wymierzony w inne modemy. Następnie modemy przeszły na stałe w tryb offline, ponieważ ich system został usunięty. [15] Najprawdopodobniej źródłem dostępu był cyberatak na łańcuch dostaw. W trakcie ataku źle skonfigurowana aplikacja VPN prawdopodobnie dała atakującym dostęp do zaufanego segmentu zarządzania siecią KA-SAT. Umożliwiło to jednoczesne wydawanie poleceń wykonywanych na dużej liczbie modemów domowych. [15] Analiza przeprowadzona przez społeczność zajmującą się bezpieczeństwem IT sugeruje, że dostępne polecenia zarządzania systemem obejmowały możliwość uruchamiania dowolnych kodów na modemach. Złośliwy kod binarny zawierający złośliwe oprogramowanie typu wiper "AcidRain" został prawdopodobnie wykorzystany w ten sposób. [22] Wydaje się prawdopodobne, że polecenia te były również wykorzystywane do uruchamiania innych szkodliwych kodów, w tym początkujących ataki DDoS na modemy. "AcidRain" poinstruował modemy, aby nadpisały swoją pamięć flash, najpierw usuwając wszystkie niestandardowe pliki w systemie, a następnie nadpisując całą pamięć masową. [16] W tym celu wiper zastosował atak brute-force (łamanie haseł i kluczy kryptograficznych poprzez wielokrotne wpisywanie różnych kombinacji danych dostępowych), iterując wszystkie możliwe identyfikatory urządzeń. Ta metoda stwarzała wrażenie, jakby złośliwe oprogramowanie było mniej sterowalne niż inne wipery, których działanie byłoby skuteczniejsze wobec plików systemowych atakowanych urządzeń, bowiem niezwłocznie usunęłoby kluczowe pliki, zamiast ponawiać próby z użyciem wszystkich możliwych identyfikatorów. Odróżnia to również "AcidRain" od bardzo podobnych modułów czyszczących złośliwego oprogramowania "VPNFilter", które

zostało powiązane ze sponsorowaną przez państwo rosyjską grupą "Sandworm". SentinelOne postawił hipotezę, że mógł to być świadomy wybór, aby zachować narzędzie "ogólne i wielokrotnego użytku". [16] Warto zauważyć, że SentinelOne zasugerował, iż kod "AcidRain" był gorszej jakości niż kod "VPNFilter". [16] Złośliwe oprogramowanie w końcu zrestartowało terminale, które nie były w stanie powrócić do pracy bez danych z pamięci flash. To skutecznie wyłączyło tysiące modemów, które nie posiadały dostępu do danych, bez aktualizacji oprogramowania układowego albo ich całkowitej wymiany. Chociaż modemy nie zostały fizycznie zniszczone przez złośliwe oprogramowanie, przywrócenie ustawień fabrycznych byłoby konieczne, aby przywrócić działanie systemu. [15] Decyzja o ograniczeniu operacji do odwracalnych skutków może być przejawem zamiaru cyberprzestępcy ograniczenia potencjalnej eskalacji ataku.

Okoliczności umożliwiające dokonanie ataku

Atak ten był możliwy dzięki złożonej sieci użytkowników sieci KA-SAT, "źle skonfigurowanej" aplikacji VPN oraz niewystarczającym procedurom bezpieczeństwa w protokołach i oprogramowaniu modemów. W związku z tym, że różne podmioty miały dostęp do sieci, ryzyko wykorzystania jej najsłabszego ogniwa stało się wysokie. Według operatora, do początkowego dostępu użyto źle skonfigurowanej aplikacji VPN [15], a z raportów wynika, że prawdopodobnie nie było wystarczających środków bezpieczeństwa stosowanych przez użytkowników w zaufanych sieciach VPN (np. "polityka zerowego zaufania"). Ponadto modemy były niewystarczająco zabezpieczone - zawierały zintegrowaną opcję zdalnego wykonywania kodu. Wreszcie wydaje się, że środki zaradcze zastosowane przez operatora, pomimo iż zauważył niepokojący ruch w sieci, nie powstrzymały ataku. [15]

Rys. 2: Wiper "spada" z satelity



Udział sektora prywatnego

Viasat [15]
Skylogic [analiza, zapobieganie eskalacji ataku i odzyskanie zdolności operacyjnej] [15]
SentinelOne [analiza] [16]
Eutelsat [15]
Mandiant [15]

Ocena prawna

Kilka państw i prawników skomentowało incydent Viasat, który został uznany za jeden z najważniejszych, historycznych incydentów oficjalnie przypisanych państwu. O odpowiedzialność za to włamanie oskarżyło Rosję prawie 20 państw, w tym kilkanaście państw członkowskich UE i kraje Sojuszu Pięciorga Oczu. [25] Większość krajów potwierdziła szkodliwe skutki uboczne incydentu, podkreślając, że pierwotnym celem było zakłócenie ukraińskiego systemu dowodzenia i kontroli podczas inwazji. [17] [18] [21] USA i Kanada potępiły atak, stwierdzając, że podważa on porządek międzynarodowy oparty na zasadach prawa i uzasadnia działania Stanów Zjednoczonych i ich sojuszników zmierzające do podjęcia "kroków defensywnych przeciwko nieodpowiedzialnym działaniom Rosji". [18] [19] W swoim oświadczeniu Wielka Brytania doprecyzowała charakter i zakres szkód: "nieprowokowana agresja" dotknęła prywatnych i komercyjnych użytkowników Internetu, a także farmy wiatrowe w Europie Środkowej. [17] UE zakwalifikowała również atak na Viasat jako mający umożliwić i ułatwić agresję wojskową na Ukrainę. Wskazała także, iż miał on jednocześnie wywołać długotrwałe przerwy w komunikacji oraz zakłócenia działania organów publicznych, przedsiębiorstw i użytkowników w Ukrainie, wpływając jednocześnie na sytuację w kilku państwach członkowskich UE. [21] UE wstrzymała się jednak od jakichkolwiek ocen prawnych, stwierdzając jedynie, że zachowanie Rosji było "sprzeczne z oczekiwaniami wszystkich członków ONZ co do odpowiedzialnego zachowania państwa". [21]

Australia określiła incydent jako zagrożenie dla międzynarodowego pokoju i bezpieczeństwa. [20] Kraje skandynawskie wydały wspólne oświadczenie, w którym wskazały, że "podmioty państwowe przeprowadzające cyberataki na infrastrukturę krytyczną robią to z wyraźnym naruszeniem prawa międzynarodowego i nie wywiązują się z realizacji dobrowolnych niewiążących norm, które wszystkie państwa członkowskie zatwierdziły w drodze konsensusu w rezolucji Zgromadzenia Ogólnego 70/237". [26] Uznając takie zachowanie za niedopuszczalne, państwa skandynawskie wezwały Radę Bezpieczeństwa do potępienia wszelkiej działalności cybernetycznej wykonywanej w imieniu państw, o ile ta jest sprzeczna z prawem międzynarodowym, oraz do podjęcia działań na rzecz powstania Rady, która będzie w stanie identyfikować naruszenia prawa międzynarodowego w cyberprzestrzeni, które zagrażają międzynarodowemu pokojowi i bezpieczeństwu. [26] Ponadto Estonia zakwalifikowała incydent Viasat jako naruszenie prawa międzynarodowego: "Te cyberataki są sprzeczne z prawem międzynarodowym i dlatego jednoznacznie je potępiamy". [27] Kilku uczonych wypowiedziało się na temat incydentu i jego implikacji w świetle prawa konfliktów zbrojnych [28] [29] i

międzynarodowego prawa kosmicznego. [30] [31] [32] Incydent został skomentowany przez Cyber Peace Institute [33] i został włączony do zestawu narzędzi CCD COE Cyber Law Toolkit. [34]

Źródła

[1] Matthias Schulze and Mika Kerttunen (2023). Cyber Operations in Russia's War against Ukraine. Uses, limitations, and lessons learned so far. SWP Comment 2023/C 23 April 17. Dostępne pod: https://www.swp-berlin.org/publikation/cyber-operations-inrussias-war-against-ukraine [Kopia archiwalna dostępna: 09.05.2023].

[2] Moritz Tremmel (2022). Wiper legte Satelliten-Netzwerk lahm, Golem. Dostępne pod: https://www.golem.de/news/viasat-wiper-legte-satelliten-netzwerk-lahm-2204- 164366.html [Kopia archiwalna dostępna: 09.05.2023].

[3] Martin Matishak (2022). Western powers blame Russia for Ukraine satellite hack, The Record. Dostępne pod: https://therecord.media/eu-uk-blame-russia-for-ukrainesatellite-hack [Kopia archiwalna dostępna: 09.05.2023].

[4] James Pearon, Raphael Satter, Christopher Bing, and Joel Chectman (2022). Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say, Reuters. Dostępne pod: https://www.reuters.com/world/europe/exclusive-us-spy-agency-probessabotage-satellite-internet-during-russian-2022-03-11/ [Kopia archiwalna dostępna: 09.05.2023].

[5] Kim Zetter (2022). Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says. Dostępne pod: https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact [Kopia archiwalna dostępna: 25.05.2023].

[6] Mykhailo Fedorov (2022). Statement on Twitter. Dostępne pod: https://twitter.com/FedorovMykhailo/status/1497543633293266944 [Kopia archiwalna dostępna: 09.05.2023].

[7] Jürgen Scheffran (2020). Militarisierung des Weltraums und Möglichkeiten der Rüstungskontrolle: Eine zivilgesellschaftliche Perspektive, BBE-Newsletter für Engagement und Partizipation in Deutschland. Berlin: Bundesnetzwerk Bürgerschaftliches Engagement.

[8] SSI 2019.

[9] Kai-Uwe Schrogl, ed. (2020). Handbook of Space Security. Policies, Applications and Programs, 2nd edition. Basel: Springer International Publishing.

[10] Peter Malanczuk (1991). "Erdfernerkundung," in: Karl-Heinz Böckstiegel (ed.), Handbuch des Weltraumrechts. Köln/Berlin/Bonn/München: Carl Heymanns Verlag KG: 307-347.

[11] Stephan Hobe (2019). Space Law. Baden-Baden: Nomos.

[12] Clémence Poirier (2022). The War in Ukraine from a Space Cybersecurity Perspective, ESPI Short Report. Dostępne pod: https://www.espi.or.at/wpcontent/uploads/2022/10/ESPI-Short-1-Final-Report.pdf [Kopia archiwalna dostępna: 09.05.2023].

[13] Joint Chiefs of Staff (1996). Joint Doctrine for Command and Control Warfare (C2W), JP 3-13.1. Dostępne pod:

https://www.bits.de/NRANEU/others/jpdoctrine/jp3_13_1.pdf [Kopia archiwalna dostępna: 09.05.2023]. 9
[14] Information Office of the State Council of the People's Republic of China (2011). China's National Defense in 2010. Dostępne pod: http://www.china.org.cn/government/whitepaper/node_7114675.htm [Kopia archiwalna dostępna: 09.05.2023].
[15] Viasat (2022). KA-SAT Network cyber attack overview. Dostępne pod: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attackoverview [Kopia archiwalna dostępna: 09.05.2023].
[16] Juan Andrés Guerro-Saade (2022). AcidRain | A Modem Wiper Rains Down on Europe, SentinelOne. Dostępne pod: https://www.sentinelone.com/labs/acidraina-modem-wiper-rains-down-on-europe/ [Kopia archiwalna dostępna: 09.05.2023].
[17] Foreign, Commonwealth & Development Office of the UK (2022). Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. Dostępne pod: https://www.gov.uk/government/news/russia-behind-cyber-attack-witheurope-wide-impact-an-hour-before-ukraine-invasion [Kopia archiwalna dostępna: 09.05.2023].
[18] Anthony J. Blinken (2022). Attribution of Russia's Malicious Cyber Activity Against Ukraine, United States Department of State. Dostępne pod: https://web.archive.org/web/20231004140606/https://www.state.gov/attribution- of-russias-malicious-cyber-activity-against-ukraine/ [Kopia archiwalna dostępna: 09.05.2023].
[19] Global Affairs Canada (2022). Statement on Russia's malicious cyber activity affecting Europe and Ukraine. Dostępne pod: https://www.canada.ca/en/globalaffairs/news/2022/05/statement-on-russias-malicious-cyber-activityaffecting-europe-and-ukraine.html [Kopia archiwalna dostępna: 09.05.2023].
[20] Marise Payne, Peter Dutton, and Karen Andrews (2022). Attribution to Russia for malicious cyber activity against European networks, Australian Minister for Foreign Affairs. Dostępne pod: https://www.foreignminister.gov.au/minister/marisepayne/media-release/attribution-russia-malicious-cyber-activity-againsteuropean-networks [Kopia archiwalna dostępna: 09.05.2023].
[21] Council of the European Union (2022). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, European Council. Dostępne pod: https://www.consilium.europa.eu/en/press/pressreleases/2022/05/10/russian-cyber-operations-against-ukraine-declarationby-the-high-representative-on-behalf-of-the-european-union/ [Kopia archiwalna dostępna: 09.05.2023].
[22] Ruben Santamarta (2022). VIASAT incident: from speculation to technical details, Reversemode. Dostępne pod:

https://www.reversemode.com/2022/03/viasat-incident-from-speculationto.html [Kopia archiwalna dostępna: 09.05.2023].
[23] Michael N. Schmitt (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. 10
[24] United Nations General Assembly (2013). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report A 68/98 (24 June); United Nations General Assembly (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report A 70/174 (22 July); United Nations General Assembly (2021). Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Report A 76/135 (14 July).
[25] Kevin Poireault (2023). Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites, InfoSecurity Magazine. Dostępne pod: https://web.archive.org/web/20231004121828/https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack/ [Kopia archiwalna dostępna: 04.10.2023].
[26] Marie-Louise Koch Wegter (2023). Nordic Statement at Arria Meeting on the Responsibility of States to Cyberattacks, Ministry of Foreign Affairs of Denmark. Dostępne pod: https://web.archive.org/web/20231004122045/https://fnnewyork.um.dk/en/statements/nordic-statement-at-arria-formula-meeting-on-the-responsibility-of- states-to-cyberattacks [Kopia archiwalna dostępna: 04.10.2023].
[27] Republic of Estonia Ministry of Foreign Affairs (2023). Estonia joins the statement of attribution on cyberattacks against Ukraine. Dostępne pod: https://web.archive.org/web/20231004135244/https://vm.ee/en/news/estonia- joins-statement-attribution-cyberattacks-against-ukraine [Kopia archiwalna dostępna: 04.10.2023].
[28] Aurel Sari (2023). International Law and Cyber Operations: Current Trends and Developments, Council of Europe Committee of Legal Advisers on Public International Law. Dostępne pod: https://web.archive.org/web/20231004135653/https://rm.coe.int/64th-cahdi-pr- aurel-sari-presentation/1680aaaf48 [Kopia archiwalna dostępna: 04.10.2023].
[29] Kristen E. Eichensehr (2023). Ukraine, Cyberattacks, and the Lessons for International Law. In the American Journal of International Law. Dostępne pod: https://web.archive.org/web/20231004135739/https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ukraine-cyberattacks-andthe-lessons-for-international-law/69B36016B06998BCE1EC67C757CDF34D [Kopia archiwalna dostępna: 04.10.2023].
[30] Jennifer A. Cannon (2023).Targeting Dual-Use Satellites. Lessons Learned from Terrestrial Warfare. In the Air and Space Operations Review, Vol. 2(2). Dostępne pod

https://web.archive.org/web/20231004135841/https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-2_Number-2/Cannon.pdf [Kopia archiwalna dostępna: 04.10.2023].
[31] European Space Policy Institute (2022). The war in Ukraine from a space cybersecurity perspective, ESPI Short Report 1. Dostępne pod: https://web.archive.org/web/20231004121842/https://www.espi.or.at/wp11content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf [Kopia archiwalna dostępna: 04.10.2023].
[32] Tara Brown (2022). The Risk of Commercial Actors in Outer Space Drawing States into Armed Conflict, West Point Ukraine Symposium. Dostępne pod: https://web.archive.org/web/20231004140215/https://lieber.westpoint.edu/commercial-actors-outer-space-armed-conflict/ [Kopia archiwalna dostępna: 04.10.2023].
[33] Cyber Peace Institute (2022). Case Study Viasat. Dostępne pod: https://web.archive.org/web/20231004140448/https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat [Kopia archiwalna dostępna: 04.10.2023].
[34] Cooperative Cyber Defence Centre of Excellence (2022). Viasat KA-SAT Attack (2022). Dostępne pod: https://web.archive.org/web/20231004140714/https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_%282022%29 [Kopia archiwalna dostępna: 04.10.2023].
[35] Sandra Erwin (2023). Limits on Ukraine's use of Starlink for war operations is a lesson for U.S. military. Dostępne pod: https://spacenews.com/limits-onukraines-use-of-starlink-for-war-operations-is-a-lesson-for-u-s-military/

Ostatnia aktualizacja: 04.10.2023