Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 33, s. 149–177

https://doi.org/10.4467/20801335PBW.25.024.22641

ARTYKUŁ

# Przestępczość cybernetyczna jako metoda adaptacji Koreańskiej Republiki Ludowo-Demokratycznej do reżimu sankcyjnego

## Cybercrime as an adaptation method of the Democratic People's Republic of Korea to the sanctions regime

SEBASTIAN JEŻ

Uniwersytet Warszawski

https://orcid.org/0009-0001-3605-3054

Abstrakt

Działania ofensywne Koreańskiej Republiki Ludowo-Demokratycznej w cyberprzestrzeni stanowią jedno z poważniejszych zagrożeń globalnego cyberbezpieczeństwa. Pomimo sankcji międzynarodowych reżim KRLD skutecznie wykorzystuje operacje cyberprzestępcze do generowania przychodów budżetowych sięgających miliardów dolarów. Celem artykułu jest ocena skali, charakteru oraz znaczenia cyberprzestępczości finansowej w strategii ekonomicznej i operacyjnej Korei Północnej w warunkach reżimu sankcyjnego. Omówiono północnokoreańskie grupy cybernetyczne, największe cyberataki o charakterze zarobkowym przypisywane KRLD, a także przedstawiono mechanizmy przeciwdziałania cyberprzestępczości sponsorowanej przez państwo wdrażane przez rządy i organizacje międzynarodowe. Wyniki analizy wskazują, że działania ofensywne KRLD w cyberprzestrzeni pełnią funkcję strategicznego narzędzia umożliwiającego reżimowi nie tylko efektywne pozyskiwanie środków finansowych, lecz także realizację celów politycznych

i projekcję siły w cyberprzestrzeni. Te ustalenia uwidaczniają konieczność przewartościowania dotychczasowych strategii przeciwdziałania tego rodzaju cyberprzestępczości, ze szczególnym uwzględnieniem izolowanych reżimów.

Słowa kluczowe Korea Północna, cyberbezpieczeństwo, cyberprzestępczość, szpiegostwo cybernetyczne, wojna cybernetyczna, atrybucja publiczna, grupa Lazarus

Abstract Offensive activities of the Democratic People's Republic of Korea in cyberspace constitute one of the more serious threats to global cybersecurity. Despite international sanctions, the DPRK regime effectively employs cybercriminal operations to generate state revenues amounting to billions of dollars. The aim of the article is to assess the scale, nature and significance of financial cybercrime within North Korea's economic and operational strategy under the sanctions regime. North Korean cyber groups, the largest profit-driven cyber attacks attributed to the DPRK, were discussed, and mechanisms implemented by governments and international organisations to counter state-sponsored cybercrime were presented. The results of the analysis indicate that North Korea's offensive cyber activities serve as a strategic tool enabling the regime not only to effectively obtain financial resources, but also to achieve political objectives and project power in cyberspace. These conclusions highlight the need to re-evaluate existing strategies for combating this type of cybercrime, particularly considering isolated regimes.

Keywords North Korea, cybersecurity, cybercrime, cyber espionage, cyber warfare, public attribution, Lazarus group

## Wprowadzenie

Operacje cybernetyczne prowadzone przez hakerów sponsorowanych przez państwo (ang. *state-sponsored cyber threat*), których głównym celem jest uzyskanie bezpośrednich korzyści finansowych, stanowią jeden z najnowszych trendów w działaniach aktorów tego typu. We wczesnej fazie występowania państwowych operacji w cyberprzestrzeni dominowały działania o charakterze szpiegowskim, cyberterrorystycznym oraz wojennym. Od ok. 2013 r. zauważalna jest intensyfikacja działań

cyberprzestępczych ukierunkowanych na realizację operacji o wysokim potencjale finansowym. Jednymi z pierwszych przykładów tego zjawiska były operacje dokonywane przez państwa o ograniczonych zasobach, które funkcjonując w warunkach sankcji międzynarodowych, stopniowo adaptowały cyberprzestępczość jako narzędzie generowania dochodów[1].

Szczególną uwagę zwraca Koreańska Republika Ludowo-Demokratyczna (KRLD), która w ostatnich latach przeprowadziła jedne z najbardziej dotkliwych ataków pod względem strat finansowych poniesionych przez ofiary. Kluczowym aspektem tych działań jest to, że odpowiedzialne za nie jednostki nie funkcjonują jako niezależne, luźno powiązane grupy przestępcze, lecz stanowią integralny element operacyjny reżimu. Zarządzanie tymi operacjami oraz ich kontrola bezpośrednio przez struktury państwowe kwalifikują je jako przejaw cyberprzestępczości sponsorowanej przez państwo[2].

Celem artykułu jest analiza skali, charakteru oraz znaczenia cyberprzestępczości finansowej w strategii ekonomicznej i operacyjnej Korei Północnej w warunkach reżimu sankcyjnego. Przyjęta w pracy hipoteza zakłada, że cyberprzestępczość finansowa stanowi istotny i systematyczny element strategii operacyjnej Korei Północnej, umożliwiający skuteczne omijanie sankcji międzynarodowych oraz finansowanie celów politycznych i wojskowych reżimu. W celu realizacji założeń badawczych zastosowano studium przypadku, uznawane za odpowiednią metodę w sytuacjach, w których badacz dysponuje ograniczoną kontrolą nad analizowanym zjawiskiem, a przedmiotem analizy nie są procesy jedynie historyczne, lecz współczesne[3]. Ta metoda pozwoliła na pogłębioną analizę badanego problemu, co jest szczególnie istotne ze względu na ograniczony dostęp do danych pierwotnych oraz wysoki poziom złożoności analizowanego zjawiska. Studium przypadku uzupełniono metodą porównawczą, aby móc zestawić przypadki cyberprzestępczości w różnych kontekstach operacyjnych. Ponadto wykorzystano technikę analizy źródeł zastanych, obejmującą krytyczny przegląd literatury przedmiotu, raportów organizacji międzynarodowych oraz dostępnych danych ilościowych.

Zrozumienie cyberprzestępczości finansowej KRLD wymaga osadzenia jej w szerszym kontekście strategicznym. W ostatnich dekadach adaptacja strategii

---

[1] J. DiMaggio, *Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej*, Warszawa 2023, s. 57.

[2] K. Chung, K. Lee, *Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle*, Seoul 2017, s. 23–26.

[3] R.K. Yin, *Studium przypadku w badaniach naukowych. Projektowanie i metody*, Kraków 2015, s. 47–87.

asymetrycznych przez Koreę Północną była świadomą odpowiedzią na złożone wyzwania związane z bezpieczeństwem militarnym oraz sytuacją gospodarczą. Przełom XX i XXI w. przyniósł zmianę w równowadze sił na Półwyspie Koreańskim, częściowo wynikającą z dynamicznego rozwoju Republiki Korei i jednoczesnej stagnacji gospodarczej KRLD[4].

Aspiracje zjednoczeniowe Pjongjangu, które przez lata determinowały jego politykę zagraniczną, zaczęły napotykać nowe bariery. Pomimo znacznych inwestycji w sektor obronny KRLD stopniowo dostrzegała ograniczenia swoich konwencjonalnych zdolności wojskowych, zwłaszcza w kontekście zmieniającej się globalnej dynamiki układu sił po zakończeniu zimnej wojny. Zmniejszenie wsparcia zewnętrznego, głównie ze strony Rosji i Chin, oraz utrzymująca się silna obecność wojskowa Stanów Zjednoczonych w Korei Południowej skłoniły reżim do przewartościowania priorytetów strategicznych i intensyfikacji działań asymetrycznych[5].

Korea Północna, pomimo izolacji na arenie międzynarodowej, konsekwentnie rozwija zaawansowane strategie mające na celu podważanie pozycji swoich głównych rywali – Stanów Zjednoczonych oraz Republiki Korei. Pjongjang intensyfikuje działania na rzecz wzmacniania zdolności operacyjnych i koncentruje się na rozbudowie potencjału w zakresie działań asymetrycznych zarówno w wymiarze konwencjonalnym, jak i cybernetycznym. Rozwój technologii oraz metod operacyjnych w cyberprzestrzeni stanowi najważniejszy element tej strategii i umożliwia KRLD realizację działań wywiadowczych, sabotażowych oraz tych ukierunkowanych na pozyskiwanie środków finansowych[6].

Szczególna specyfika ataków cybernetycznych przeprowadzanych przez państwa wynika przede wszystkim z trudności w ich szybkiej i precyzyjnej atrybucji – identyfikacja sprawcy bywa procesem długotrwałym i niejednoznacznym, co ogranicza możliwość natychmiastowej odpowiedzi. Atakujący często korzystają z podmiotów pośrednich, takich jak prywatne grupy hakerskie, firmy najemne lub nieformalne organizacje, które celowo działają w sposób utrudniający jednoznaczne powiązanie ich aktywności z państwem zlecającym. Ta złożoność wymaga zastosowania zaawansowanych metod analizy umożliwiających prześledzenie całego łańcucha dowodów – od taktyk, technik i procedur, przez konkretne osoby, aż po sponsorów instytucjonalnych. Proces ten dodatkowo komplikuje fakt, że niektóre państwa posługują się atrybucją publiczną w sposób mało transparentny,

[4] J. Jun, S. LaFoy, E. Sohn, *North Korea's Cyber Operations: Strategy and Responses*, Center for Strategic & International Studies, *2023*, s. 11–15.

[5] Tamże.

[6] Tamże, s. 24–25.

co sprawia, że końcowe przypisanie odpowiedzialności politycznej często opiera się na dowodach o zróżnicowanej jakości[7].

Sama atrybucja ataków jest zagadnieniem niezwykle szerokim i wymagałaby osobnego opracowania. Warto jednak zaznaczyć, że w literaturze przedmiotu wyróżnia się kilka jej typów[8]. Pierwszym z nich jest atrybucja techniczna, mająca na celu identyfikację konkretnego urządzenia końcowego, serwera lub innej formy infrastruktury wykorzystywanej do przeprowadzenia ataku. Stanowi ona punkt wyjścia dla dalszych analiz. Na jej podstawie możliwe staje się przejście do atrybucji organizacyjnej lub osobowej, która koncentruje się na ustaleniu tożsamości osób lub grup stojących za działaniami ofensywnymi. W jej ramach próbuje się odpowiedzieć na pytanie, kto bezpośrednio odpowiada za atak oraz jakie środowisko – organizacja czy grupa przestępcza – może za nim stać, jeśli takowe jest zaangażowane. Wyniki obu tych procesów tworzą fundament dla atrybucji politycznej, będącej najbardziej złożonym i wrażliwym etapem przypisywania odpowiedzialności. Polega ona na powiązaniu zebranych danych technicznych, wywiadowczych i organizacyjnych z interesami oraz działaniami konkretnego państwa, które mogło zlecić atak[9].

Każdy rodzaj atrybucji wiąże się z unikalnymi wyzwaniami – od technicznych[10], które utrudniają prowadzenie śledztwa, przez brak jednoznacznych regulacji w prawie międzynarodowym[11], aż po ryzyko arbitralności decyzji wynikającej z uwarunkowań politycznych[12]. Wielowymiarowy charakter procesu atrybucji, zwłaszcza w kontekście przypisywania odpowiedzialności konkretnemu państwu, sprawia, że jest ona szczególnie narażona na kontestację. Ten problem ujawnia się zarówno na arenie międzynarodowej, zwłaszcza w relacjach między antagonistycznymi reżimami, jak i w dyskursie eksperckim, w którym różnice w podejściu metodologicznym oraz ograniczona dostępność dowodów dodatkowo komplikują osiągnięcie konsensusu.

---

7 M. Mueller i in., *Cyber Attribution: Can a New Institution Achieve Transnational Credibility?*, „The Cyber Defense Review" 2019, t. 4, nr 1, s. 107–122; H. Lin, *Attribution of Malicious Cyber Incidents*, „Aegis Paper Series" 2016, nr 1607, s. 30–42; W. Banks, *Cyber Attribution and State Responsibility*, „International Law Studies" 2021, t. 97, s. 1058–1072.

8 T. Rid, B. Buchanan, *Attributing Cyber Attacks*, „Journal of Strategic Studies" 2015, t. 38, nr 1–2, s. 4–37. http://dx.doi.org/10.1080/01402390.2014.977382.

9 H. Lin, *Attribution of Malicious Cyber Incidents*…, s. 1–26.

10 J.A. Guerrero-Saade, C. Raiu, *Walking in your enemy's shadow: when fourth-party collection becomes attribution hell*, Virus Bulletin, 2017, s. 1–12.

11 K.E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, „UCLA Law Review" 2020, t. 67, s. 559–597.

12 T. Rid, B. Buchanan, *Attributing Cyber Attacks*…, s. 4–37.

Ponadto istotnym wyzwaniem analitycznym pozostaje wysokie ryzyko błędów oraz manipulacji, w tym celowo przeprowadzanych operacji pod fałszywą flagą, mających na celu przypisanie odpowiedzialności innemu podmiotowi niż faktyczny sprawca[13].

W kontekście działań Korei Północnej, której modus operandi bywa często naśladowany przez inne grupy hakerskie, wzrasta ryzyko błędnego bądź celowego przypisania jej operacji przeprowadzonych przez inne podmioty. Tego rodzaju zabiegi otwierają przestrzeń dla politycznych manipulacji oraz działań maskujących, stanowiących część szerszych kampanii informacyjnych realizowanych przez państwa trzecie. Z tego względu dane ilościowe powinny być traktowane z dużą rezerwą, jako że mogą odzwierciedlać nie tylko realną skalę działań, lecz także skutki błędnych lub intencjonalnie zniekształconych atrybucji.

W świetle tych ustaleń kluczowe staje się zrozumienie, w jakim stopniu działalność ukierunkowana na pozyskiwanie zasobów finansowych w cyberprzestrzeni przekształciła się w trwały i systemowo wykorzystywany komponent strategii operacyjnej Korei Północnej. Zdolność reżimu do prowadzenia skoordynowanych działań nastawionych na generowanie przychodów wskazuje na rosnącą profesjonalizację oraz instytucjonalne zakorzenienie tego podejścia w strukturach państwowych. Jednocześnie z uwagi na ograniczoną przejrzystość procesów atrybucji oraz niepełną wiarygodność danych ilościowych konieczne jest zachowanie krytycznego podejścia interpretacyjnego. Analiza tego zjawiska pozostaje jednak niezbędna dla zrozumienia współczesnej dynamiki zagrożeń cybernetycznych oraz narzędzi wykorzystywanych w działaniach asymetrycznych stosowanych przez izolowane reżimy.

## Praca przymusowa jako narzędzie uzyskiwania dochodów

Zrozumienie relacji między reżimem a jednostką wymaga uwzględnienia wysokiego stopnia arbitralności, który charakteryzuje północnokoreański system władzy. Koreańska Republika Ludowo-Demokratyczna, jako współczesne państwo totalitarne, dysponuje rozbudowanymi mechanizmami kontroli i represji, które trudno analizować w odniesieniu do zachodnich wartości, takich jak prawa człowieka, rządy prawa, demokratyczna legitymizacja władzy czy transparentność instytucji państwowych. Istotnym czynnikiem w tym kontekście jest również wpływ propagandy oraz mechanizmów represji na przeciętnego obywatela. Tym złożonym wymiarem analizy zajmowali się wybitni badacze, w tym

[13] F. Skopik, T. Pahi, *Under false flag: using technical artifacts for cyber attack attribution*, „Cybersecurity" 2020, t. 3, s. 1–20. https://doi.org/10.1186/s42400-020-00048-4.

Jan Baszkiewicz, który wnikliwie opisał mechanizmy kontroli i podporządkowania jednostki w systemach totalitarnych. Jego ujęcie pozwala dostrzec, że w państwach funkcjonujących w warunkach ścisłej kontroli ideologicznej terror i przemoc pełnią funkcję nie tylko narzędzi represji, lecz także stabilizatorów systemu, które kształtują społeczną dynamikę lojalności i strachu[14]. W tym kontekście sektor publiczny w KRLD funkcjonuje w warunkach istotnie odmiennych od tych charakterystycznych dla państw demokratycznych.

Korea Północna od lat wykorzystuje pracę przymusową jako jedno z kluczowych narzędzi generowania dochodów dla reżimu przez delegację obywateli do pracy zarówno w kraju, jak i za granicą. Ten proceder obejmuje wiele sektorów, w tym budownictwo, przemysł stoczniowy, rolnictwo, gastronomię, górnictwo oraz branżę IT. Rzetelne źródła wskazują również na udział północnokoreańskich pracowników w konfliktach zbrojnych, w szczególności w trwającej wojnie rosyjsko-ukraińskiej[15]. Wysyłani pracownicy często podlegają surowej kontroli państwowej, a znaczna część ich wynagrodzenia jest konfiskowana i przekazywana bezpośrednio do budżetu reżimu[16].

Zaangażowanie Korei Północnej w sektor IT wykracza poza działalność hakerską. Od lat reżim realizuje skoordynowany program infiltracji globalnego rynku IT przez wykorzystywanie północnokoreańskich specjalistów zatrudnianych na zdalnych stanowiskach w zagranicznych firmach, szczególnie w Stanach Zjednoczonych (tzw. *IT worker schemes*). Przez działanie pod fałszywymi tożsamościami i posługiwanie się skradzionymi danymi osobowymi północnokoreańscy informatycy znajdują zatrudnienie w międzynarodowych przedsiębiorstwach, zwłaszcza w sektorach technologii, finansów i przemysłu. Ich aktywność stanowi istotne źródło dochodów dla reżimu, a dla globalnego bezpieczeństwa – poważne zagrożenie. Dzięki dostępowi do wewnętrznych sieci korporacyjnych mogą prowadzić działania wywiadowcze, a w dłuższej perspektywie przygotowywać grunt pod cyberataki[17].

Stany Zjednoczone wielokrotnie podejmowały działania prawne przeciwko północnokoreańskim schematom infiltracji sektora IT, mającym na celu generowanie dochodów dla reżimu oraz uzyskiwanie dostępu do systemów korporacyjnych.

---

[14] J. Baszkiewicz, *Władza*, Wrocław 1999, s. 165–166.

[15] J. Garamone, *Pentagon Says 10K North Korean Troops in Kursk Oblast*, U.S. Department of War, 4 XI 2024 r., https://www.defense.gov/News/News-Stories/Article/Article/3955757/pentagon-says-10k-north-korean-troops-in-kursk-oblast/ [dostęp: 18 III 2025].

[16] S.R. Stewart, *DPRK Overseas Financial Networks*, w: *People for Profit: North Korean Forced Labour on a Global Scale*, R.E. Breuker, I.B.L.H. van Gardingen (red.), Leiden 2018, s. 120–125.

[17] C. Starks i in., *Staying a Step Ahead: Mitigating the DPRK IT Worker Threat*, Mandiant, 23 IX 2024 r., https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat [dostęp: 8 III 2025].

Jednym z przykładów takich działań jest oskarżenie w grudniu 2024 r. 14 obywateli Korei Północnej o udział w wieloletnim procederze nielegalnego uzyskiwania zatrudnienia jako zdalni specjaliści IT, co pozwoliło na transfer co najmniej 88 mln dolarów na rzecz Pjongjangu[18].

## Struktura sektora cybernetycznego Korei Północnej

Rozwój północnokoreańskiego sektora technologii informacyjnej rozpoczął się już w latach 80. XX w., jednak najważniejsze etapy intensyfikacji tych działań przypadły na koniec lat 90. W tym okresie wdrożono serię pięcioletnich strategii rozwojowych ukierunkowanych na postęp w obszarze nauki i technologii, ze szczególnym naciskiem na informatykę. Konsekwencją tych inicjatyw było zwiększenie krajowych zdolności produkcyjnych w zakresie oprogramowania i sprzętu, a także priorytetowy rozwój technologii sterowania numerycznego, infrastruktury światłowodowej oraz sieci komunikacyjnych przeznaczonych do zastosowań rządowych, badawczych i wojskowych[19].

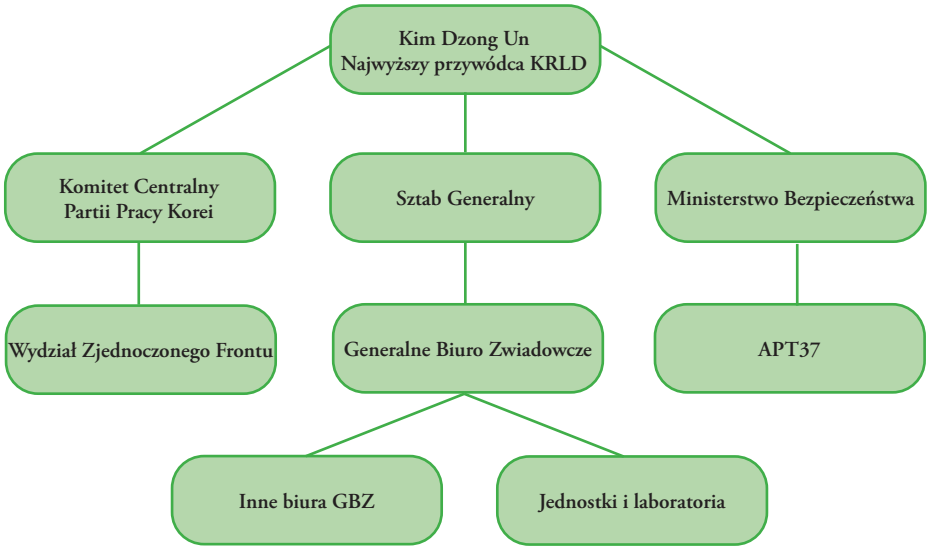
Literatura przedmiotu niemal jednomyślnie wskazuje, że kompetencje w zakresie prowadzenia większości operacji ofensywnych należą do Generalnego Biura Zwiadowczego (GBZ), północnokoreańskiej agencji wywiadowczej utworzonej w 2006 r. (rysunek 1)[20]. Oprócz elitarnych jednostek hakerskich działających w ramach GBZ w Korei Północnej funkcjonują także mniej wyspecjalizowane formacje, które prowadzą operacje w cyberprzestrzeni, jednak pozostają podporządkowane innym instytucjom państwowym[21].

[18] United States of America v. J. Song Hwa, R. Kyong Sik, K. Ryu Song et al., United States District Court for the Eastern District of Missouri, CR 4:24CR648 MTS/JSD, 2024.

[19] J. Jun, S. LaFoy, E. Sohn, *North Korea's Cyber Operations*…, s. 52–53.

[20] K. Ji Young, L. Jong In, K. Kyoung Gon, *The All-Purpose Sword: North Korea's Cyber Operations and Strategies*, w: *2019 11th International Conference on Cyber Conflict: Silent Battle*, T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (red.), Tallinn 2019, s. 2–6; M. Barnhart i in., *Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations*, Mandiant, 23 III 2022 r., https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government#intelligencesubmenu [dostęp: 19 XII 2024]; K. Chung, K. Lee, *Advancement of Science and Technology*…, s. 23–26.

[21] M. Barnhart i in., *Not So Lazarus*…




**Rysunek 1.** Struktura sektora cybernetycznego Koreańskiej Republiki Ludowo-Demokratycznej.

Źródło: opracowanie własne na podstawie: M. Barnhart i in., *Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations*, Mandiant, 23 IIII 2022 r., https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government#intelligencesubmenu [dostęp: 19 XII 2024].

Wydział Zjednoczonego Frontu, funkcjonujący w strukturach Komitetu Centralnego Partii Pracy Korei, odgrywa kluczową rolę w realizacji operacji propagandowych. Jednym z jego fundamentalnych narzędzi jest rozbudowana sieć, licząca tysiące członków, których działalność koncentruje się na promowaniu proreżimowych narracji oraz systematycznym podważaniu wiarygodności przeciwników. Ten mechanizm opiera się na skoordynowanych działaniach dezinformacyjnych prowadzonych w przestrzeni cyfrowej i jest powszechnie określany mianem armii trolli[22]. Analiza przeprowadzona w ramach badań nad strategiami propagandowymi wykazała, że Korea Północna, w przeciwieństwie do większości państw, nie opiera swoich działań w tym obszarze na automatyzacji, lecz jako główne narzędzie realizacji operacji informacyjnych wykorzystuje zasoby ludzkie[23].

Struktura północnokoreańskich grup cybernetycznych cechuje się wysokim stopniem specjalizacji oraz ścisłym podporządkowaniem państwowym organom

[22] Tamże.

[23] S. Bradshaw, P.N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Oxford Internet Institute, 2017, s. 13.

bezpieczeństwa. Wśród tych podmiotów szczególne znaczenie ma grupa APT37, prawdopodobnie podlegająca Ministerstwu Bezpieczeństwa Państwowego. Jej działalność skupia się na pozyskiwaniu informacji wywiadowczych służących interesom wojskowym, politycznym i gospodarczym Korei Północnej. Grupa działa co najmniej od 2012 r., początkowo koncentrowała się na sektorze publicznym i prywatnym w Korei Południowej. Od 2017 r. odnotowano rozszerzenie jej aktywności na Japonię, Wietnam oraz region Bliskiego Wschodu. Grupa APT37 interesuje się sektorami strategicznymi, takimi jak przemysł chemiczny, elektroniczny, lotniczy, motoryzacyjny oraz ochrona zdrowia. W ostatnich latach jej aktywność wyraźnie się zmniejszyła, co – według specjalistów z firmy Mandiant – może świadczyć o konsolidacji jej struktur w ramach GBZ[24].

Najważniejszym organem prowadzącym operacje ofensywne pozostaje Jednostka 121, funkcjonująca w ramach GBZ. Jest to elitarna struktura, której członkowie są starannie selekcjonowani, a sama jednostka składa się z wyspecjalizowanych podgrup odpowiedzialnych za różne działania. Jedna z tych podgrup to Laboratorium 110, które bywa utożsamiane z nazwą Lazarus. Warto jednak podkreślić, że w źródłach otwartych nazwa ta jest często używana zbiorczo i obejmuje różne klastry działalności cybernetycznej powiązanej z Koreą Północną[25]. Nie istnieje pełny konsensus co do granic pomiędzy poszczególnymi grupami, co wynika zarówno ze złożonej i rozproszonej natury tych struktur, jak i świadomej polityki reżimu, polegającej na utrzymywaniu wysokiego poziomu tajności działań[26].

W ramach Laboratorium 110 funkcjonują mniejsze zespoły operacyjne, spośród których wyróżniają się TEMP.Hermit, APT38 oraz Andariel[27]. TEMP.Hermit, aktywny od 2013 r., odgrywa kluczową rolę w pozyskiwaniu danych strategicznych i koncentruje swoje działania na administracji publicznej, sektorze obronnym, telekomunikacyjnym oraz finansowym[28]. APT38 specjalizuje się w działaniach mających na celu generowanie środków finansowych. Odpowiada za jedne z najpoważniejszych ataków na instytucje finansowe na świecie, w tym skoordynowane działania wymierzone w system przelewów międzybankowych SWIFT, banki, giełdy kryptowalut oraz kasyna. Straty spowodowane przez tę formację sięgają

[24] M. Barnhart i in., *Not So Lazarus…*

[25] Pojęcie grupy Lazarus jest odmiennie rozumiane przez różne ośrodki i źródła. Autor używa tego pojęcia w artykule w różnych kontekstach znaczeniowych, w zależności od źródeł, na które się powołuje.

[26] K. Chung, K. Lee, *Advancement of Science and Technology…*, s. 23–26.

[27] *Lazarus Group*, MITRE ATT&CK, https://attack.mitre.org/groups/G0032/ [dostęp: 17 XII 2024].

[28] M. Barnhart i in., *Not So Lazarus…*

setek milionów dolarów[29]. Z kolei Andariel kieruje swoją aktywność na zagraniczne przedsiębiorstwa, agencje rządowe, infrastrukturę finansową i sektor obronny. Oprócz działań szpiegowskich formacja angażuje się w operacje nastawione na generowanie środków finansowych[30].

Istotnym elementem północnokoreańskiego krajobrazu cybernetycznego pozostaje również grupa Kimsuky, funkcjonująca prawdopodobnie w strukturach Ministerstwa Bezpieczeństwa Państwowego. Grupa ta, aktywna co najmniej od 2012 r., początkowo koncentrowała swoje działania na celach w Korei Południowej, takich jak instytucje rządowe, organizacje badawcze i eksperci z zakresu polityki oraz bezpieczeństwa. W późniejszych latach jej działalność objęła również Stany Zjednoczone, Rosję, Europę oraz instytucje Organizacji Narodów Zjednoczonych. Kimsuky specjalizuje się w cyberwywiadzie skupiającym się na gromadzeniu informacji dotyczących polityki zagranicznej, bezpieczeństwa narodowego, sankcji oraz programu nuklearnego, z ukierunkowaniem na osoby mające dostęp do wrażliwych danych w tych obszarach[31].

Całość północnokoreańskiego systemu operacji cybernetycznych tworzy wysoce zorganizowaną, wielopoziomową strukturę, w której poszczególne grupy realizują cele wywiadowcze, propagandowe, destrukcyjne oraz finansowe. Wspierają tym samym strategiczne interesy reżimu i jego zdolność do globalnej projekcji siły.

## Przegląd najbardziej dochodowych kampanii – sektor bankowy

W 2016 r. świat obiegły wiadomości o ataku na Bank Centralny Bangladeszu, który zakończył się kradzieżą 81 mln dolarów[32]. Nie udało się ich odzyskać, ponieważ zostały wyprane przez zaangażowanych w proceder pracowników jednego z filipińskich banków[33]. Ten atak stanowił punkt kulminacyjny w procesie kształtowania się celów operacyjnych KRLD w cyberprzestrzeni. Do tej pory jej działalność ograniczała się głównie do operacji infiltracyjnych, zakłócających, sabotażowych

[29] *APT38*, MITRE ATT&CK, https://attack.mitre.org/groups/G0082/ [dostęp: 16 XII 2024].

[30] *Andariel*, MITRE ATT&CK, https://attack.mitre.org/groups/G0138/ [dostęp: 16 XII 2024].

[31] M. Barnhart i in., *Not So Lazarus…*; *Kimsuky*, MITRE ATT&CK, https://attack.mitre.org/groups/G0094/ [dostęp: 17 XII 2024].

[32] A. Haertle, *Jak zniknęło 81 milionów dolarów – historia prawdziwa*, Zaufana Trzecia Strona, 20 III 2016 r., https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/ [dostęp: 19 XII 2024].

[33] M. Kabir, *Lessons Learned From the Bangladesh Bank Heist*, ISACA, 6 XII 2023 r., https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist [dostęp: 18 XII 2024].

i wywiadowczych. W wyniku przeprowadzonego ataku spektrum celów grupy zostało rozszerzone o operacje finansowe na dużą skalę, które umożliwiły generowanie znaczących wpływów finansowych na rzecz budżetu reżimu[34].

Charakter działań tego agresora wyróżniał się wśród innych grup przestępczych. Badania wykazały, że hakerzy z Korei Północnej w niektórych przypadkach poświęcali nawet kilka miesięcy na dogłębną analizę docelowego środowiska. Wiele czasu przeznaczano na poznawanie wewnętrznych polityk i procedur stosowanych przez ofiary, co miało na celu ograniczenie ryzyka wykrycia przez systemy identyfikujące anomalie[35]. Jednym z końcowych etapów rekonesansu było zlokalizowanie serwera odpowiedzialnego za komunikację z systemem SWIFT. Atakujący musieli nawiązać połączenie z licznymi systemami działającymi w ramach złożonej topologii sieci. Cel został osiągnięty za sprawą zastosowanych środków i dużej skali operacji. Północnokoreańscy cyberprzestępcy dążyli do kradzieży w łącznej kwocie niemal miliarda dolarów. Zgodnie z doniesieniami Banku Rezerwy Federalnej w Nowym Jorku (Federal Reserve Bank of New York) instytucja ta skontaktowała się z Bankiem Centralnym Bangladeszu po wykryciu nietypowo wysokiej liczby transakcji kierowanych do podmiotów prywatnych i organizacji pozarządowych. W wyniku podjętych działań podejrzane transakcje zostały zatrzymane, a bankom udało się zablokować fałszywe przelewy o wartości od 850 mln do 870 mln dolarów, co uniemożliwiło ich transfer na konta przestępców[36].

Po przeprowadzeniu wstępnego dochodzenia Bank Rezerwy Federalnej zrekonstruował szczegółowy przebieg transakcji. Z przedstawionych relacji wynika, że podczas akceptacji pierwszej puli transakcji kilka z 30 poleceń skierowano do dalszej weryfikacji pod kątem zgodności z obowiązującymi sankcjami. Następnie w wyniku analizy ręcznej Bank Rezerwy Federalnej w Nowym Jorku ustalił, że działalność była potencjalnie podejrzana i polecenia płatnicze nie powinny być realizowane bez uprzedniego zapytania do banku centralnego[37].

Sam atak rozpoczął się od ukierunkowanej kampanii phishingowej, w ramach której rozesłano 25 wiadomości e-mail. Analiza powłamaniowa wykazała, że na co najmniej trzech urządzeniach pobrano złośliwe oprogramowanie. Złośliwy kod rejestrował się jako usługa systemowa w środowisku operacyjnym opartym

[34] *Dark Web Profile: Lazarus Group*, SOCRadar, https://socradar.io/apt-profile-who-is-lazarus-group/ [dostęp: 13 IV 2024].

[35] J. DiMaggio, *Sztuka wojny cyfrowej*…, s. 68–75.

[36] *Dark Web Profile: Lazarus Group*…

[37] Federal Reserve Bank of New York, Responses to Rep. Maloney Letter of March 22, 2016, https://www.newyorkfed.org/medialibrary/media/newsevents/statements/2016/Maloneyletter.pdf [dostęp: 11 XII 2024].

na SWIFT Alliance[38], wspieranym przez bazę danych Oracle. Oprogramowanie monitorowało komunikaty finansowe przesyłane przez sieć SWIFT i wydobywało kluczowe dane, takie jak numery referencyjne transakcji i numery kont, co umożliwiało manipulację danymi w bazie. Istotnym elementem ataku było modyfikowanie lokalnych instalacji SWIFT Alliance Access przez patchowanie modułu *liboradb.dll* – atakujący zastąpili instrukcję skoku warunkowego dwiema instrukcjami NOP[39]. To pozwoliło na ominięcie mechanizmów weryfikacji zabezpieczeń. Dodatkowo złośliwe oprogramowanie umożliwiało ciągłe monitorowanie i modyfikację komunikatów SWIFT przez parsowanie plików w wyznaczonych katalogach systemowych oraz generowanie poprawnych poleceń SQL. W rezultacie były usuwane lub modyfikowane rekordy w lokalnej bazie danych. Proces patchowania polegał na skanowaniu aktywnych procesów w poszukiwaniu pliku *liboradb.dll* oraz modyfikacji jego pamięci, co umożliwiało obejście krytycznych kontroli bezpieczeństwa i manipulację danymi transakcyjnymi[40]. Późniejsze analizy incydentu dowiodły, że Bank Centralny Bangladeszu dopuścił się wielu zaniedbań związanych zarówno z bezpośrednim zabezpieczeniem samej infrastruktury wrażliwego systemu, jak i ze zdolnościami wykrywania zagrożeń w odpowiednim czasie.

Po tym incydencie pociągnięto do odpowiedzialności osoby prywatne oraz organizacje, wpłynął on także na nałożenie bezpośrednich sankcji na reżim Korei Północnej. Dnia 8 czerwca 2018 r. Departament Sprawiedliwości Stanów Zjednoczonych (U.S. Department of Justice) opublikował zawiadomienie o popełnieniu przestępstwa przez obywatela KRLD, Parka Jin Hyoka. W zawiadomieniu przedstawiono zarzuty związane z kilkoma przestępstwami natury cybernetycznej[41]. Objęły one również atak na Komisję Nadzoru Finansowego z 2016 r., który poważnie zagroził polskiemu sektorowi bankowemu[42]. Zidentyfikowanie Korei Północnej jako sprawcy ataku na Bank Centralny Bangladeszu zostało wykorzystane jako podstawa

[38] SWIFT Alliance to główny serwer komunikacyjny umożliwiający połączenie z siecią SWIFT. Umożliwia on zarządzanie przepływem danych finansowych, integruje różne formaty wiadomości i obsługuje protokoły wymiany informacji finansowych.

[39] Instrukcja NOP to instrukcja procesora, która nie powoduje żadnych zmian w stanie maszyny, z wyjątkiem zwiększenia licznika operacji o jeden, aby wskazywać na kolejną operację.

[40] S. Shevchenko, *Two Bytes to $951M*, BAE Systems, 25 IV 2016 r., https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html [dostęp: 26 IV 2024].

[41] United States of America v. Park Jin Hyok, United States District Court for the Central District of California, MJ18-1479, 2018, s. 23–125.

[42] *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 5 IV 2024].

dowodowa również podczas pierwszego w historii nałożenia sankcji za cyberataki przez Radę UE[43].

## Przegląd najbardziej dochodowych kampanii – kryptowaluty

W marcu 2022 r. doszło do jednego z najpoważniejszych ataków hakerskich w środowisku kryptowalut. Celem cyberprzestępców stała się infrastruktura bocznego łańcucha Ethereum[44], będącego częścią ekosystemu blockchainowej[45] gry *Axie Infinity*. Technologia blockchain zyskała ogromną popularność – przyciąga miliony użytkowników możliwością swobodnego transferowania aktywów cyfrowych. Za atakiem stała grupa Lazarus, znana z działalności wymierzonej w sektor kryptowalut. Hakerzy wykorzystali najsłabszy punkt sieci, czyli jej walidatorów, łącząc techniki socjotechniczne z lukami w zabezpieczeniach protokołów. Udało im się w ten sposób przejąć kontrolę nad pięcioma z dziewięciu prywatnych kluczy należących do sieci Ronin. Uzyskany nieautoryzowany dostęp pozwolił im na autoryzowanie transakcji jako zaufany podmiot. Następnie przystąpili oni do transakcji, w ramach której wyprowadzili równowartość 600 mln dolarów w kryptowalutach ether i USDC. Kradzież ta została uznana za jedną z największych w historii zdecentralizowanych finansów[46].

Po udanej kradzieży grupa Lazarus rozpoczęła złożony proces prania skradzionych środków, aby utrudnić ich śledzenie. W tym celu fundusze przenoszono między wieloma adresami, konwertowano na inne kryptowaluty oraz przepuszczano przez zdecentralizowane giełdy i miksery, które zwiększają anonimowość transakcji. Początkowo część środków trafiła na scentralizowane giełdy, lecz gdy te zaczęły współpracować z organami ścigania, hakerzy zmienili strategię i zaczęli korzystać

[43] *Rozporządzenie wykonawcze Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim*.

[44] Ethereum to zdecentralizowana platforma blockchain, która umożliwia tworzenie i działanie inteligentnych kontraktów oraz zdecentralizowanych aplikacji. Oprócz pełnienia funkcji platformy Ethereum ma również swoją kryptowalutę, znaną jako ether (ETH).

[45] Blockchain to zdecentralizowana technologia rejestrów, która umożliwia zapisywanie transakcji w formie ciągu bloków danych połączonych za pomocą kryptografii. Każdy blok zawiera kryptograficzny skrót poprzedniego bloku, znacznik czasu oraz transakcje i tworzy w ten sposób łańcuch bloków.

[46] *Back to Building: Ronin Security Breach Postmortem*, Roninchain, 27 IV 2022 r., https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364 [dostęp: 13 XII 2024].

z narzędzi pozwalających na ukrycie przepływu środków. W efekcie znaczna część skradzionych aktywów została rozproszona, co utrudniło ich odzyskanie[47].

Właśnie ten incydent bezpieczeństwa w znacznym stopniu przyczynił się do zaostrzenia działań Departamentu Skarbu Stanów Zjednoczonych (U.S. Department of the Treasury) przeciwko narzędziom wykorzystywanym do prania skradzionych środków. Biuro Kontroli Aktywów Zagranicznych (Office of Foreign Assets Control) systematycznie nakładało sankcje na miksery walut wirtualnych, takie jak Blender.io[48], Sinbad.io[49] i Tornado Cash[50], które odegrały kluczową rolę w ukrywaniu dochodów z działalności cyberprzestępczej.

Pod koniec lutego 2025 r. pojawiły się pierwsze doniesienia o nowej kradzieży wymierzonej w giełdę Bybit. Wyniosła ona niemal równowartość 1,5 mld dolarów[51], co stanowi kwotę przewyższającą łączną wartość strat związanych z kryptowalutami przypisywanych północnokoreańskim grupom hakerskim w całym 2024 r. (równowartość 1,34 mld dolarów)[52]. Po kilku miesiącach od zdarzenia zarówno amerykańskie Federalne Biuro Śledcze (Federal Bureau of Investigation, FBI)[53], jak i niezależne podmioty zajmujące się analizą blockchain, w tym Chainalysis, stwierdziły, że za atakiem na giełdę Bybit stała grupa hakerska powiązana z KRLD[54]. Wstępne ustalenia śledczych wskazywały na grupę TraderTraitor, znaną również

---

47 *North Korea's Lazarus Group identified as exploiters behind $540 million Ronin bridge heist*, Elliptic, 14 IV 2022 r., https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge [dostęp: 11 IV 2024].

48 *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, U.S. Department of the Treasury, 6 V 2022 r., https://home.treasury.gov/news/press-releases/jy0768 [dostęp: 11 IV 2024].

49 *Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency*, U.S. Department of the Treasury, 29 XI 2023 r., https://home.treasury.gov/news/press-releases/jy1933 [dostęp: 11 IV 2024].

50 *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. Department of the Treasury, 8 VIII 2022 r., https://home.treasury.gov/news/press-releases/jy0916 [dostęp: 13 XI 2024].

51 *Bybit Hack: Leveraging Transparency for Collaboration in the Wake of Record-Breaking Theft*, Chainalysis, 24 II 2025 r., https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/ [dostęp: 10 III 2025].

52 Tamże.

53 Federal Bureau of Investigation, *North Korea Responsible for $1.5 Billion Bybit Hack*, Internet Crime Complaint Center, 26 II 2025 r., https://www.ic3.gov/PSA/2025/PSA250226 [dostęp: 15 III 2025].

54 *2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Records*, Chainalysis, 17 VII 2025 r., https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/ [dostęp: 10 X 2025].

jako UNC4899, którą FBI oficjalnie powiązało z tym incydentem[55]. Wcześniej grupa była odpowiedzialna za atak na japońską giełdę DMM Bitcoin, w której skradziono 308 mln dolarów[56], co stanowiło jedną z największych pojedynczych operacji cyberprzestępczych w 2024 r. Reakcja Bybit również wskazuje na Koreę Północną jako sprawcę ataku. Dyrektor generalny Ben Zhou zapowiedział zdecydowane działania przeciwko grupie Lazarus i podkreślił konieczność globalnej współpracy w zwalczaniu cyberprzestępczości sponsorowanej przez państwo[57]. Giełda uruchomiła program działań naprawczych „Lazarus Bounty", którego nazwa wskazuje na sprawców ataku[58].

Raport Sygnia oraz analiza NCC Group pokazują, że atak na giełdę Bybit był wieloetapowy i rozpoczął się od kompromitacji środowiska deweloperskiego powiązanego z portfelem Safe{Wallet}, najprawdopodobniej w wyniku zastosowania technik socjotechnicznych. Napastnicy uzyskali dostęp do infrastruktury i zmodyfikowali elementy interfejsu użytkownika przez wprowadzenie złośliwego kodu JavaScript, który w momencie autoryzacji transakcji przez uprawnionych pracowników Bybit podmieniał jej treść. W rezultacie zatwierdzono transakcję skutkującą przejęciem kontroli nad portfelem przez atakujących i kradzieżą ok. 400 000 tokenów ether[59]. Obie analizy odnotowały także, że po wykonaniu kradzieży złośliwy kod został usunięty z frontendu, co utrudniło śledztwo, oraz że skradzione środki zostały szybko rozproszone pomiędzy liczne portfele i przesłane przez zdecentralizowane giełdy i miksery, co w połączeniu z technikami maskowania transakcji uwidacznia wysoki stopień zaawansowania atakujących[60].

Przytoczony materiał dowodowy z relatywnie wysokim prawdopodobieństwem wskazuje na udział podmiotów powiązanych z Koreą Północną, chociaż

---

55 Federal Bureau of Investigation, *North Korea Responsible for $1.5 Billion Bybit Hack…*

56 Federal Bureau of Investigation, *FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com*, 23 XII 2024 r., https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-usd-from-bitcoindmmcom [dostęp: 10 X 2025].

57 B. Zhou (@benbybit), *Join us on war against Lazarus*, wpis na portalu X, 25 II 2025 r., https://x.com/benbybit/status/1894397098323579333 [dostęp: 13 III 2025].

58 *ByBit*, Lazarus Bounty, https://www.lazarusbounty.com/en/ [dostęp: 13 III 2025].

59 *Bybit – What We Know So Far*, Sygnia, 16 III 2025 r., https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/ [dostęp: 10 X 2025]; M. Rivas, R. Santos, J. Sanz, *In-Depth Technical Analysis of the Bybit Hack*, NCC Group, 10 III 2025 r., https://www.nccgroup.com/research-blog/in-depth-technical-analysis-of-the-bybit-hack/ [dostęp: 10 X 2025].

60 Tamże.

w momencie pisania tego artykułu procesy atrybucji nie zostały jeszcze definitywnie zakończone.

## Przychody z działalności cyberprzestępczej na tle reżimu sankcyjnego

W odpowiedzi na pierwsze próby nuklearne przeprowadzone w 2006 r. przez KRLD na reżim nałożono sankcje, mające na celu ograniczenie proliferacji broni jądrowej oraz zahamowanie rozwoju programów zbrojeniowych. Rada Bezpieczeństwa ONZ wprowadziła wówczas m.in. embargo na handel bronią, zamrożenie aktywów podmiotów zaangażowanych w północnokoreański program nuklearny oraz częściowe ograniczenia w imporcie i eksporcie towarów mogących wspierać rozwój broni masowego rażenia[61].

Równolegle do regulacji ONZ niezależne sankcje wdrożyła UE[62], a m.in. Stany Zjednoczone, Korea Południowa, Japonia i Australia zastosowały środki jednostronne[63]. Od 2016 r. sankcje wobec Korei Północnej były systematycznie zaostrzane zarówno przez ONZ, jak i UE w odpowiedzi na kolejne testy nuklearne i próby balistyczne reżimu. Oprócz wcześniejszych ograniczeń w handlu, sektorze finansowym i energetycznym rozszerzono restrykcje dotyczące eksportu i importu, zamrażania aktywów oraz zakazu współpracy gospodarczej. Wprowadzono także sankcje personalne wobec osób i podmiotów powiązanych z północnokoreańskim programem zbrojeniowym[64].

W 2022 r. Chiny i Rosja sprzeciwiły się zaostrzeniu sankcji wobec Korei Północnej, argumentując, że dotychczasowe restrykcje nie przyniosły oczekiwanych rezultatów. Oba państwa określiły projekt rezolucji jako kontrproduktywny i niehumanitarny. W związku z tym Rada Bezpieczeństwa ONZ nie była w stanie przyjąć rezolucji wzmacniającej sankcje w odpowiedzi na próby balistyczne reżimu. Mimo

---

[61] *UN Documents for DPRK (North Korea): Security Council Resolutions*, Security Council Report, https://www.securitycouncilreport.org/un_documents_type/security-council-resolutions/page/2?ctype=DPRK+%28North+Korea%29&cbtype=dprk-north-korea#038;cbtype=dprk-north-korea [dostęp: 10 II 2025].

[62] *Unijne sankcje wobec Korei Północnej – kalendarium*, Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/policies/sanctions-against-north-korea/timeline-eu-sanctions-against-north-korea/ [dostęp: 10 II 2025].

[63] *Democratic People's Republic of Korea Sanctions*, U.S. Department of State, https://www.state.gov/democratic-peoples-republic-of-korea-sanctions/ [dostęp: 11 II 2025].

[64] O. Pietrewicz, *Ograniczenia polityki sankcji wobec Korei Północnej*, Polski Instytut Spraw Międzynarodowych, 27 II 2018 r., https://pism.pl/publikacje/Ograniczenia_polityki_sankcji_wobec_Korei_P__nocnej [dostęp: 19 XI 2024].

poparcia 13 członków Rady propozycja złożona przez Stany Zjednoczone została zawetowana. Sprzeciw Chin i Rosji, oparty na przekonaniu o nieskuteczności sankcji i konieczności prowadzenia dialogu, kontrastuje z postawą pozostałych członków Rady, dążących do bardziej zdecydowanych działań wobec naruszeń ze strony Korei Północnej. Ten impas w Radzie Bezpieczeństwa ONZ nie tylko uwydatnia trudności w osiągnięciu konsensusu w kwestiach najważniejszych dla stabilności międzynarodowej, lecz także podkreśla konieczność poszukiwania nowych, skuteczniejszych rozwiązań dyplomatycznych w celu ograniczenia napięć na Półwyspie Koreańskim[65].

Osłabienie mechanizmów egzekwowania sankcji znalazło swoją kulminację w zakończeniu działalności Panelu Ekspertów ONZ ds. sankcji wobec Korei Północnej. Panel ten, funkcjonujący od 2009 r. na mocy rezolucji Rady Bezpieczeństwa ONZ nr 1874, odgrywał kluczową rolę w monitorowaniu i raportowaniu naruszeń sankcji nałożonych na KRLD. Jego działalność została oficjalnie zakończona w marcu 2024 r. w wyniku weta Federacji Rosyjskiej, co jest kolejnym przykładem rosnącego podziału w Radzie Bezpieczeństwa ONZ i osłabienia mechanizmów nadzoru nad egzekwowaniem sankcji. Brak niezależnego organu monitorującego wprowadzanie restrykcji i analizującego metody ich obchodzenia przez KRLD znacznie utrudni kontrolę przestrzegania sankcji. Oznacza to potencjalne osłabienie mechanizmów nacisku na Pjongjang, który wielokrotnie wykazywał zdolność do unikania restrykcji przez sieci pośredników i nielegalnych transakcji, często przy cichym wsparciu niektórych państw[66].

Równolegle z impasem dyplomatycznym narasta aktywność cyberprzestępcza Korei Północnej. Według raportu Panelu Ekspertów ONZ ds. sankcji wobec Korei Północnej z marca 2023 r. północnokoreańscy hakerzy ukradli w 2022 r. równowartość od 630 mln do ponad miliarda dolarów w atakach obejmujących kryptowaluty[67]. Najnowszy raport z marca 2024 r. wskazuje kwotę 750 mln w 2023 r. oraz informuje o prowadzeniu śledztwa dotyczącego prawie 60 cyberataków przeprowadzonych w latach 2017–2023, które były powiązane z kryptowalutami wycenionymi na ok. 3 mld dolarów[68].

---

[65] *Security Council Fails to Adopt Resolution Tightening Sanctions Regime in Democratic People's Republic of Korea, as Two Members Wield Veto*, United Nations, 26 V 2022 r., https://press.un.org/en/2022/sc14911.doc.htm [dostęp: 3 VIII 2024].

[66] *Update: DPRK (North Korea): Vote on Panel of Experts Mandate Renewal*, Security Council Report, 22 III 2024 r., https://www.securitycouncilreport.org/whatsinblue/2024/03/dprk-north-korea-vote-on-panel-of-experts-mandate-renewal.php [dostęp: 3 II 2025].

[67] *Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2023/171)*, UN Documents for DPRK (North Korea), 2023, s. 74–78.

[68] *Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2024/215)*, UN Documents for DPRK (North Korea), 2024, s. 60–65.

Raport Chainalysis z 2025 r. potwierdza, że Korea Północna utrzymuje dominującą pozycję w cyberprzestępczości związanej z kryptowalutami. Według tego raportu północnokoreańscy hakerzy przeprowadzili w 2023 r. 20 ataków na giełdy i platformy kryptowalutowe, kradnąc w ten sposób równowartość ok. 660 mln dolarów. W 2024 r. liczba incydentów wzrosła ponaddwukrotnie do 47, a łączna wartość skradzionych środków osiągnęła, jak wspomniano, 1,34 mld dolarów, co oznacza dwukrotny wzrost w porównaniu z rokiem poprzednim. Hakerzy powiązani z reżimem Kim Dzong Una odpowiadali za 61% całkowitej wartości kryptowalut skradzionych w 2024 r., co jednoznacznie potwierdza ich wiodącą rolę w globalnej cyberprzestępczości[69].

Biorąc pod uwagę wartość środków pozyskiwanych przez północnokoreańskich hakerów, zasadne wydaje się ich zestawienie z dostępnymi szacunkami budżetowymi kraju – wydatków na obronność oraz PKB. Należy jednak podkreślić, że te dane powinny być interpretowane z ostrożnością – ze względu na zarówno ograniczony dostęp do źródeł, jak i ryzyko błędów w zakresie atrybucji, w tym operacji pod fałszywą flagą. Z powodu hermetyczności reżimu KRLD dokładne oszacowanie wydatków zbrojeniowych nie jest możliwe, jednak dostępne dane pozwalają na ustalenie przybliżonych kwot. Według szacunków Departamentu Stanu USA Korea Północna mogła przeznaczyć na obronność ok. 4 mld dolarów w 2019 r., co stanowiło 26% jej szacowanego PKB. Był to najwyższy odsetek spośród 170 przeanalizowanych państw[70]. Niższe szacunki przedstawił Sztokholmski Międzynarodowy Instytut Badań Pokojowych. Wskazał on, że w 2018 r. wydatki zbrojeniowe Korei Północnej wyniosły ok. 1,6 mld dolarów[71].

Dla pełniejszego zobrazowania znaczenia środków pozyskiwanych z działalności cyberprzestępczej warto również przywołać szacunkowe dane dotyczące całkowitej wielkości gospodarki Korei Północnej. Według raportu Banku Korei rzeczywisty PKB Korei Północnej w 2023 r. wyniósł ok. 32 bln wonów południowokoreańskich, co przy kursie walutowym aktualnym na czas pisania artykułu odpowiadało ok. 28 mld dolarów[72].

---

[69] *The 2025 Crypto Crime Report*, Chainalysis, https://www.chainalysis.com/wp-content/uploads/2025/02/the-2025-crypto-crime-report-release.pdf [dostęp: 8 III 2025].

[70] *World Military Expenditures and Arms Transfers 2021 Edition*, U.S. Department of State, 30 XII 2021 r., https://www.state.gov/world-military-expenditures-and-arms-transfers-2021-edition/ [dostęp: 13 XII 2024].

[71] *SIPRI Military Expenditure Database*, Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1949-2022.xlsx [dostęp: 15 XII 2024].

[72] *Gross Domestic Product Estimates for North Korea in 2023*, Bank of Korea, 26 VII 2024 r., https://www.bok.or.kr/eng/bbs/E0000634/view.do?nttId=10086116&menuNo=400423&relate=Y&depth=400423&programType=newsDataEng [dostęp: 11 II 2025].

Zgromadzone dane wskazują, że cyberprzestępczość stanowi obecnie nie tylko trwały komponent systemu finansowego KRLD, lecz prawdopodobnie także narzędzie coraz głębiej osadzone w instytucjonalnej strukturze gospodarki państwa.

## Reakcja międzynarodowa i jej wpływ na aktywność cybernetyczną Korei Północnej

Publiczna atrybucja w przestrzeni cybernetycznej, często utożsamiana z publicznym piętnowaniem (ang. *naming and shaming*[73]), bywa postrzegana jako narzędzie odstraszania, pokazujące, że identyfikacja sprawców ataków jest możliwa. Jednak, jak wynika z analizy przedstawionej w pracy Michaela Poznansky'ego i Evana Perkoskiego, dyskusyjna okazuje się skuteczność tego narzędzia, szczególnie wobec podmiotów traktujących działania cybernetyczne jako sposób projekcji siły. Autorzy podkreślają, że decyzja sprawcy cyberataku o ujawnieniu swojej tożsamości jest ściśle powiązana z celami, jakie pragnie on osiągnąć. Państwa najczęściej działają w ukryciu, gdy ich celem jest szpiegostwo bądź sabotaż – wówczas sukces operacji nie wymaga współpracy ofiary, a anonimowość minimalizuje ryzyko eskalacji konfliktu i odwetu. Ujawnienie swojej roli staje się natomiast istotne w przypadku operacji o charakterze przymuszającym (ang. *cyber coercion*), kiedy to osiągnięcie zamierzonego rezultatu wymaga, aby cel znał tożsamość agresora i zrozumiał groźby dalszych działań stojące za atakiem[74].

W świetle tego rozróżnienia publiczna atrybucja działań cybernetycznych jako samodzielne narzędzie napotyka istotne ograniczenia w odniesieniu do państw, których priorytetem jest globalna projekcja siły – takich jak Korea Północna. Reżim ten wielokrotnie angażował się w operacje wymierzone w państwa zachodnie, w tym atak na Bank Centralny Bangladeszu oraz kampanie ransomware, takie jak WannaCry w 2017 r. W obu przypadkach Stany Zjednoczone zdecydowały się na publiczne przypisanie odpowiedzialności za ataki, co można interpretować jako próbę osłabienia międzynarodowej pozycji Pjongjangu oraz wywarcia wpływu na jego przyszłe decyzje strategiczne. Dotychczasowa praktyka nie potwierdziła jednak wyraźnej skuteczności takiego podejścia, co skłania do pytań o rzeczywistą efektywność publicznych atrybucji w odniesieniu do izolowanych reżimów.

[73] *Naming and shaming* to termin oznaczający strategię egzekwowania norm i praw człowieka przez publiczne piętnowanie państw dopuszczających się naruszeń.

[74] M. Poznansky, E. Perkoski, *Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution*, „Journal of Global Security Studies" 2018, t. 3, nr 4, s. 402–416. https://doi.org/10.1093/jogss/ogy022.

Efektywność publicznej atrybucji jako narzędzia odstraszania może być znacznie ograniczona w przypadku Korei Północnej z kilku powodów. Po pierwsze, reżimy totalitarne, takie jak północnokoreański, charakteryzują się niską podatnością na presję ze strony społeczności międzynarodowej, a ujawnienie ich aktywności w cyberprzestrzeni rzadko przekłada się na realne koszty polityczne wewnątrz systemu władzy. Po drugie, ograniczona integracja Korei Północnej z globalną infrastrukturą cyfrową oraz jej peryferyjna pozycja w międzynarodowym systemie gospodarczym sprawiają, że działania odwetowe, zarówno o charakterze cybernetycznym, jak i ekonomicznym, nie wywierają na ten podmiot odpowiednio silnego wpływu. Asymetria stopnia cyfryzacji oraz uzależnienia od światowych sieci technologicznych między Koreą Północną a wysoko rozwiniętymi państwami Zachodu redukuje potencjalną skuteczność retorsji. Po trzecie, publiczna atrybucja ataków może generować niezamierzone efekty wzmacniające reżim i sprzyjać budowie jego pozycji jako podmiotu dysponującego zaawansowanymi zdolnościami cybernetycznymi oraz zdolnego do projekcji siły w wymiarze globalnym, co może wpisywać się w szerszą strategię polityki odstraszania realizowaną przez Pjongjang.

Atrybucja służy również do legitymizacji działań odwetowych, w tym sankcji gospodarczych bądź operacji defensywnych. Na przykład zidentyfikowanie Korei Północnej jako sprawcy ataku na Bank Centralny Bangladeszu, jak wskazano, zostało wykorzystane podczas pierwszego w historii nałożenia przez Radę UE sankcji za cyberataki[75].

Zdaniem części badaczy można przekonująco dowodzić, że zgodnie z prawem międzynarodowym państwa powinny przeprowadzać poprawną i rzetelną atrybucję przed podjęciem działań odwetowych w odpowiedzi na cyberatak, szczególnie jeśli te działania w innych okolicznościach mogłyby naruszać normy międzynarodowe[76]. Proces wymaga przedstawienia wiarygodnych i jasnych dowodów, które jednoznacznie identyfikują sprawcę i potwierdzają jego odpowiedzialność za konkretny atak. Ten wymóg jest zgodny z zasadami proporcjonalności i konieczności, które są fundamentalnymi elementami prawa międzynarodowego. Rzetelna atrybucja nie tylko legitymizuje działania państwa, lecz także minimalizuje ryzyko eskalacji konfliktu i wspiera stabilność w relacjach międzynarodowych, a jednocześnie ogranicza arbitralność podejmowanych decyzji[77].

---

[75] *Rozporządzenie wykonawcze Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim.*

[76] M. Finnemore, D.B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, „European Journal of International Law" 2020, t. 31, nr 3, s. 975–1003. https://doi.org/10.1093/ejil/chaa056.

[77] Tamże.

Za najintensywniejsze działania jednostronne względem cyberataków Korei Północnej można uznać te podejmowane przez Stany Zjednoczone, m.in. wspomniane wcześniej zawiadomienie o popełnieniu przestępstwa przez obywatela KRLD, Parka Jin Hyoka. Od tego czasu Stany Zjednoczone konsekwentnie stosują akty oskarżenia jako narzędzie służące przypisywaniu cyberataków Korei Północnej[78]. Przykładem jest akt oskarżenia dotyczący Rima Jong Hyoka, który dokonał ataków głównie na szpitale i firmy prywatne sektora ochrony zdrowia Stanów Zjednoczonych oraz Korei Południowej przy użyciu złośliwego oprogramowania typu ransomware[79].

Nie ulega wątpliwości, że KRLD w istotny sposób przyczyniła się do dynamicznego rozwoju podejścia państw zachodnich do zjawiska atrybucji cyberataków. Chociaż działalność przestępcza prowadzona w cyberprzestrzeni o charakterze zarobkowym nie wydaje się występować w przypadku Korei Północnej z mniejszą częstotliwością niż kilka lat wcześniej (najnowsze dane wskazują trend wzrostowy), to należy pamiętać, że sama praktyka działalności przestępczej tego typu w wykonaniu reżimów państwowych jest stosunkowo nowa. Trwa bowiem nieco ponad dekadę. Coraz więcej państw oraz organizacji międzynarodowych decyduje się temu przeciwdziałać, stosując m.in. publiczną atrybucję czy sankcje. Mimo że środki te nie mają wystarczającego oparcia w prawie międzynarodowym, to ich częstsze stosowanie zdaje się obiecujące, ponieważ stopniowo podnosi koszty polityczne i operacyjne dla KRLD.

## Wnioski

Działalność cybernetyczna o charakterze przestępczym stanowi jedno z najważniejszych źródeł finansowania reżimu Korei Północnej. W kontekście sankcji międzynarodowych nałożonych na KRLD skala środków pozyskiwanych w ten sposób nie powinna być lekceważona, szczególnie w świetle rosnącego prawdopodobieństwa, że przyczyniają się one do finansowania programów zbrojeniowych.

Analiza dostępnych danych wskazuje na konsekwentny wzrost skuteczności działań cybernetycznych prowadzonych przez Koreę Północną. Zarówno analiza danych liczbowych pochodzących z publicznie dostępnych raportów, jak i zauważalny

[78] United States of America v. Park Jin Hyok, United States District Court for the Central District of California, CR 2:18-cr-00759, 2018; United States of America v. J. Chang Hyok, K. Il, and P. Jin Hyok, United States District Court for the Central District of California, CR 2:20-cr-00614-DMG, 2020.

[79] United States of America v. Rim Jong Hyok, United States District Court for the District of Kansas, 24-20061-HLT-ADM, 2024, s. 1–17.

spadek efektywności mechanizmów monitorujących przestrzeganie sankcji nie wskazują, aby ten proceder miał się radykalnie zmienić. Przeciwnie, operacje hakerskie KRLD od ok. 2013 r. wykazują rosnącą efektywność, co stanowi istotne wyzwanie dla międzynarodowych wysiłków na rzecz egzekwowania restrykcji.

Niepokojącym sygnałem jest rozwiązanie jednego z kluczowych organów monitorujących działalność KRLD – Panelu Ekspertów ONZ ds. sankcji wobec Korei Północnej. Ta decyzja znacznie osłabiła międzynarodowy system nadzoru nad północnokoreańskimi naruszeniami sankcji oraz możliwości raportowania tych działań na forum ONZ. Może to skutkować dalszą intensyfikacją aktywności przestępczej reżimu w cyberprzestrzeni, zwłaszcza że rozwiązanie panelu zdaje się pokrywać czasowo z nasileniem współpracy militarnej i gospodarczej między Koreą Północną a Federacją Rosyjską[80].

Pomimo trudnych uwarunkowań są dostrzegalne oznaki rosnącego zainteresowania rozwojem zdolności dotyczących przypisywania odpowiedzialności za ataki cybernetyczne konkretnym podmiotom państwowym. Początkowo te działania były inicjowane głównie przez Stany Zjednoczone, ale od początku trzeciej dekady XXI w. zauważalnie wzrasta liczba międzynarodowych koalicji atrybucyjnych oraz jest widoczne większe zaangażowanie aktorów takich jak UE (organizacja o charakterze ponadnarodowym). Rośnie także aktywność naukowa ukierunkowana na usprawnienie mechanizmów odpowiedzialności państw za działalność cybernetyczną. Mimo że tendencje te stanowią krok w stronę większej transparentności i egzekwowania odpowiedzialności za operacje cybernetyczne, ich dynamika nie wydaje się na tyle intensywna, by w perspektywie najbliższych lat skutecznie ograniczyć proceder cyberprzestępczy. Możliwe efekty tych działań należy raczej rozpatrywać w kategoriach długoterminowych.

Warto podkreślić, że skuteczność publicznych atrybucji w odniesieniu do Korei Północnej pozostaje ograniczona, ponieważ reżim o wysokim stopniu izolacji na arenie międzynarodowej niekoniecznie reaguje w konwencjonalny sposób na przypisywanie mu odpowiedzialności. Funkcja odstraszająca publicznych atrybucji może mieć drugorzędne znaczenie wobec ich wiodącej roli w kształtowaniu narracji politycznych oraz mobilizowaniu poparcia dla określonych działań państw w obszarze bezpieczeństwa. W tym kontekście ważne jest wzmacnianie międzynarodowych mechanizmów współpracy oraz kontynuowanie starań na rzecz odpowiedniego dokumentowania naruszeń sankcji. Wysiłki koalicji atrybucyjnych mogą

[80] O. Guseinova, *Unequal Partnership: North Korea's Uneven Bargain with Russia*, Friedrich Naumann Foundation for Freedom Korea, 2024, https://shop.freiheit.org/#!/Publikation/1997 [dostęp: 10 X 2025]; O. Pietrewicz, *Wzmocnienie wsparcia Korei Północnej dla rosyjskiej wojny przeciwko Ukrainie*, Polski Instytut Spraw Międzynarodowych, 18 XI 2024 r., https://www.pism.pl/publikacje/wzmocnienie-wsparcia-korei-polnocnej-dla-rosyjskiej-wojny-przeciwko-ukrainie [dostęp: 10 X 2025].

częściowo wypełnić lukę powstałą po likwidacji Panelu Ekspertów ONZ ds. sankcji wobec Korei Północnej, jednak ich skuteczność będzie uzależniona od poziomu zaangażowania społeczności międzynarodowej oraz zdolności do wypracowania szerokiego konsensusu w kwestii odpowiedzialności za operacje cybernetyczne.

## Bibliografia

Banks W., *Cyber Attribution and State Responsibility*, „International Law Studies" 2021, t. 97, s. 1039–1072.

Baszkiewicz J., *Władza*, Wrocław 1999.

Bradshaw S., Howard P.N., *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Oxford Internet Institute, 2017.

Chung K., Lee K., *Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle*, Seoul 2017.

DiMaggio J., *Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej*, Warszawa 2023.

Eichensehr K.E., *The Law and Politics of Cyberattack Attribution*, „UCLA Law Review" 2020, t. 67, s. 520–598.

Finnemore M., Hollis D.B., *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, „European Journal of International Law" 2020, t. 31, nr 3, s. 969–1003. https://doi.org/10.1093/ejil/chaa056.

Guerrero-Saade J.A., Raiu C., *Walking in your enemy's shadow: when fourth-party collection become attribution hell*, Virus Bulletin, 2017.

Ji Young K., Jong In L., Kyoung Gon K., *The All-Purpose Sword: North Korea's Cyber Operations and Strategies*, w: *2019 11th International Conference on Cyber Conflict: Silent Battle*, T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (red.), Tallinn 2019.

Jun J., LaFoy S., Sohn E., *North Korea's Cyber Operations: Strategy and Responses*, Center for Strategic & International Studies, 2023.

Lin H., *Attribution of Malicious Cyber Incidents*, „Aegis Paper Series" 2016, nr 1607, s. 1–55.

Mueller M., Grindal K., Kuerbis B., Badiei F., *Cyber Attribution: Can a New Institution Achieve Transnational Credibility?*, „The Cyber Defense Review" 2019, t. 4, nr 1, s. 107–122.

Poznansky M., Perkoski E., *Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution*, „Journal of Global Security Studies" 2018, t. 3, nr 4, s. 402–416. https://doi.org/10.1093/jogss/ogy022.

Rid T., Buchanan B., *Attributing Cyber Attacks*, „Journal of Strategic Studies" 2015, t. 38, nr 1–2, s. 4–37. http://dx.doi.org/10.1080/01402390.2014.977382.

Skopik F., Pahi T., *Under false flag: using technical artifacts for cyber attack attribution,* „Cybersecurity" 2020, t. 3, s. 1–20. https://doi.org/10.1186/s42400-020-00048-4.

Stewart S.R., *DPRK Overseas Financial Networks*, w: *People for Profit: North Korean Forced Labour on a Global Scale*, R.E. Breuker, I.B.L.H. van Gardingen (red.), Leiden 2018, s. 120–125.

Yin R.K., *Studium przypadku w badaniach naukowych. Projektowanie i metody*, Kraków 2015.

### Źródła internetowe

*2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Records*, Chainalysis, 17 VII 2025 r., https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/ [dostęp: 10 X 2025].

*Andariel*, MITRE ATT&CK, https://attack.mitre.org/groups/G0138/ [dostęp: 16 XII 2024].

*APT38*, MITRE ATT&CK, https://attack.mitre.org/groups/G0082/ [dostęp: 16 XII 2024].

*Atak teleinformatyczny na polski sektor finansowy,* Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 5 IV 2024].

*Back to Building: Ronin Security Breach Postmortem*, Roninchain, 27 IV 2022 r., https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364 [dostęp: 13 XII 2024].

Barnhart M., Cantos M., Johnson J., Fox E., Freas G., Scott D., *Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations*, Mandiant, 23 III 2022 r., https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government#intelligence-submenu [dostęp: 19 XII 2024].

*Bybit – What We Know So Far*, Sygnia, 16 III 2025 r., https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/ [dostęp: 10 X 2025].

*Bybit Hack: Leveraging Transparency for Collaboration in the Wake of Record-Breaking Theft*, Chainalysis, 24 II 2025 r., https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk/ [dostęp: 10 III 2025].

*ByBit*, Lazarus Bounty, https://www.lazarusbounty.com/en/ [dostęp: 13 III 2025].

*Dark Web Profile: Lazarus Group*, SOCRadar, https://socradar.io/apt-profile-who-is-lazarus-group/ [dostęp: 13 IV 2024].

*Democratic People's Republic of Korea Sanctions*, U.S. Department of State, https://www.state.gov/democratic-peoples-republic-of-korea-sanctions/ [dostęp: 11 II 2025].

Federal Bureau of Investigation, *FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin. DMM.com*, 23 XII 2024 r., https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-usd-from-bitcoindmmcom [dostęp: 10 X 2025].

Federal Bureau of Investigation, *North Korea Responsible for $1.5 Billion Bybit Hack*, Internet Crime Complaint Center, 26 II 2025 r., https://www.ic3.gov/PSA/2025/PSA250226 [dostęp: 15 III 2025].

Federal Reserve Bank of New York, Responses to Rep. Maloney Letter of March 22, 2016, https://www.newyorkfed.org/Maloneyletter.pdf [dostęp: 11 XII 2024].

Garamone J., *Pentagon Says 10K North Korean Troops in Kursk Oblast*, U.S. Department of War, 4 XI 2024 r., https://www.defense.gov/News/News-Stories/Article/Article/3955757/pentagon-says-10k-north-korean-troops-in-kursk-oblast/ [dostęp: 18 III 2025].

*Gross Domestic Product Estimates for North Korea in 2023*, Bank of Korea, 26 VII 2024 r., https://www.bok.or.kr/eng/bbs/E0000634/view.do?nttId=10086116&menuNo=400423&relate=Y&depth=400423&programType=newsDataEng [dostęp: 11 II 2025].

Guseinova O., *Unequal Partnership: North Korea's Uneven Bargain with Russia*, Friedrich Naumann Foundation for Freedom Korea, 2024 r., https://shop.freiheit.org/#!/Publikation/1997 [dostęp: 10 X 2025].

Haertle A., *Jak zniknęło 81 milionów dolarów – historia prawdziwa*, Zaufana Trzecia Strona, 20 III 2016 r., https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/ [dostęp: 19 XII 2024].

Kabir M., *Lessons Learned From the Bangladesh Bank Heist*, ISACA, 6 XII 2023 r., https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist [dostęp: 18 XII 2024].

*Kimsuky*, MITRE ATT&CK, https://attack.mitre.org/groups/G0094/ [dostęp: 17 XII 2024].

*Lazarus Group*, MITRE ATT&CK, https://attack.mitre.org/groups/G0032/ [dostęp: 17 XII 2024].

*North Korea's Lazarus Group identified as exploiters behind $540 million Ronin bridge heist*, Elliptic, 14 IV 2022 r., https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge [dostęp: 11 IV 2024].

Pietrewicz O., *Ograniczenia polityki sankcji wobec Korei Północnej*, Polski Instytut Spraw Międzynarodowych, 27 II 2018 r., https://pism.pl/publikacje/Ograniczenia_polityki_sankcji_wobec_Korei_P__nocnej [dostęp: 19 XI 2024].

Pietrewicz O., *Wzmocnienie wsparcia Korei Północnej dla rosyjskiej wojny przeciwko Ukrainie*, Polski Instytut Spraw Międzynarodowych, 18 XI 2024 r., https://www.pism.pl/publikacje/wzmocnienie-wsparcia-korei-polnocnej-dla-rosyjskiej-wojny-przeciwko-ukrainie [dostęp: 10 X 2025].

Rivas M., Santos R., Sanz J., *In-Depth Technical Analysis of the Bybit Hack*, NCC Group, 10 III 2025 r., https://www.nccgroup.com/research-blog/in-depth-technical-analysis-of-the-bybit-hack/ [dostęp: 10 X 2025].

*Security Council Fails To Adopt Resolution Tightening Sanctions Regime In Democratic People's Republic Of Korea, As Two Members Wield Veto*, United Nations, 26 V 2022 r., https://press.un.org/en/2022/sc14911.doc.htm [dostęp: 3 VIII 2024].

Shevchenko S., *Two Bytes to $951M*, BAE Systems, 25 IV 2016 r., https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html [dostęp: 26 IV 2024].

*SIPRI Military Expenditure Database*, Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1949-2022.xlsx [dostęp: 15 XII 2024].

Starks C., Barnhart M., Long T., Lombardi M., Pisano J., Revelli A., *Staying a Step Ahead: Mitigating the DPRK IT Worker Threat*, Mandiant, 23 IX 2024 r., https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat [dostęp: 8 III 2025].

*The 2025 Crypto Crime Report*, Chainalysis, https://www.chainalysis.com/wp-content/uploads/2025/02/the-2025-crypto-crime-report-release.pdf [dostęp: 8 III 2025].

*Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency*, U.S. Department of the Treasury, 29 XI 2023 r., https://home.treasury.gov/news/press-releases/jy1933 [dostęp: 11 IV 2024].

*UN Documents for DPRK (North Korea): Security Council Resolutions*, Security Council Report, https://www.securitycouncilreport.org/un_documents_type/security-council-resolutions/page/2?ctype=DPRK+%28North+Korea%29&cbtype=dprk-north-korea#038;cbtype=dprk-north-korea [dostęp: 10 II 2025].

*Unijne sankcje wobec Korei Północnej – kalendarium*, Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/policies/sanctions-against-north-korea/timeline-eu-sanctions-against-north-korea/ [dostęp: 10 II 2025].

*Update: DPRK (North Korea): Vote on Panel of Experts Mandate Renewal*, Security Council Report, 22 III 2024 r., https://www.securitycouncilreport.org/whatsinblue/2024/03/dprk-north-korea-vote-on-panel-of-experts-mandate-renewal.php [dostęp: 3 II 2025].

*U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, U.S. Department of the Treasury, 6 V 2022 r., https://home.treasury.gov/news/press-releases/jy0768 [dostęp: 11 IV 2024].

*U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. Department of the Treasury, 8 VIII 2022 r., https://home.treasury.gov/news/press-releases/jy0916 [dostęp: 13 XI 2024].

*World Military Expenditures and Arms Transfers 2021 Edition*, U.S. Department of State, 30 XII 2021 r., https://www.state.gov/world-military-expenditures-and-arms-transfers-2021-edition/ [dostęp: 13 XII 2024].

Zhou B. (@benbybit), *Join us on war against Lazarus*, wpis na portalu X, 25 II 2025 r., https://x.com/benbybit/status/1894397098323579333 [dostęp: 13 III 2025].

### Akty prawne

*Rozporządzenie wykonawcze Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim* (Dz. Urz. UE L 246/4 z 30 VII 2020 r.).

### Inne dokumenty

United States of America v. J. Song Hwa, R. Kyong Sik, K. Ryu Song et al., United States District Court for the Eastern District of Missouri, CR 4:24CR648 MTS/JSD, 2024.

United States of America v. Rim Jong Hyok, United States District Court for the District of Kansas, 24-20061-HLT-ADM, 2024.

United States of America v. J. Chang Hyok, K. Il, and P. Jin Hyok, United States District Court for the Central District of California, CR 2:20-cr-00614-DMG, 2020.

United States of America v. Park Jin Hyok, United States District Court for the Central District of California, MJ18-1479, 2018.

United States of America v. Park Jin Hyok, United States District Court for the Central District of California, CR 2:18-cr-00759, 2018.

*Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2023/171)*, UN Documents for DPRK (North Korea), 2023.

*Final report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (S/2024/215)*, UN Documents for DPRK (North Korea), 2024.

Sebastian Jeż

Doktorant Szkoły Doktorskiej Nauk Społecznych Uniwersytetu Warszawskiego oraz specjalista ds. cyberbezpieczeństwa. Absolwent De Montfort University i Uniwersytetu Warszawskiego. Od 2016 r. związany z obszarem technicznego cyberbezpieczeństwa, a od 2020 r. koncentruje się na jego wymiarze ofensywnym oraz interdyscyplinarnych badaniach z pogranicza technologii i nauk politycznych.

**Kontakt:** s.jez@uw.edu.pl