**aut. Szymon Palczewski** 30.09.2020

# „SZTUKA (CYBER)WOJNY" WEDŁUG KOREI PÓŁNOCNEJ. NIKT NIE JEST BEZPIECZNY W SIECI?

**Korea Północna dąży do rozbudowy potencjału w cyberprzestrzeni, aby w ten sposób realizować cele strategiczne rządu, w tym wywierać wpływ na przeciwników reżimu. Dla Zachodu rozwój „cyberzdolności" Pjongajngu to sygnał alarmowy, wymuszający konieczność podjęcia odpowiednich środków zaradczych. Problem wzrostu siły Korei Północnej dotyczy również Polski.**

Korea Północna regularnie rozwija cyberzdolności, aby zwiększyć skuteczność operacji w cyberprzestrzeni. Na przestrzeni lat reżim rozbudował swoje cyberwojsko oraz opracował narzędzia hakerskie, które wielokrotnie sprawdziły się na polu walki. Równolegle władza pamięta o redefinicji założeń operacji w cyberprzestrzeni w celu dostosowania strategii do zmieniającej się rzeczywistości oraz posiadanych możliwości. Cyberataki stały się nieodłącznym elementem polityki Korei Północnej, co jedynie pokazuje skalę jej zaangażowania w ramach wirtualnej domeny. Ostatnie wydarzenia oraz działania reżimu w cyberprzestrzeni są dowodem wzrostu jego siły na drodze ku zbudowania „cyberpotęgi"?

**Źródło bogactwa**

Cyberprzestrzeń jest dla Pjongjangu wymiarem, który daje możliwość generowania zysków finansowych i skutecznego obchodzenie międzynarodowych sankcji. Cyberataki są efektywnym narzędziem reżimu do pozyskiwania środków przeznaczanych między innymi na rozwój armii czy programu nuklearnego. Nielegalne działania w wirtualnej domenie pomagają władzy generować zysk, który staje się motorem napędowym całego państwa. Co miało wpływ na taki stan rzeczy?

Po pierwsze, umożliwił to wzrost popularności internetu w Korei Północnej. Globalna sieć staje się coraz bardziej powszechna, co pomaga reżimowi w wykorzystaniu cyberprzestępczości dla własnych celów. Odwołując się do danych liczbowych należy wskazać, że od 2017 roku posługiwanie się internetem w tym kraju wzrosło o około 300%! Niemal połowa ruchu sieciowego odbywa się dzięki połączeniu z Rosją, co pozwala na uniezależnienie się kraju od infrastruktury biegnącej przez Chiny.

Wielu ekspertów, w tym specjalistów firmy Recorded Future, wskazuje, że rozwój internetu w Korei Północnej jest realizowany wyłącznie w celu obchodzenia sankcji i innych obostrzeń nakładanych przez Zachód. Dla Pjongjangu sieć zapewnia narzędzia pozyskiwania środków finansowych w tani, ale jednocześnie bardzo skuteczny sposób.

W ciągu ostatnich lat reżim znacząco poprawił swoje zdolności i umiejętności niezbędne na przykład do nielegalnego pozyskiwania kryptowalut oraz kradzieży środków z instytucji finansowych. Północnokoreańscy hakerzy udoskonalili również sposób zacierania śladów tak, aby zminimalizować ryzyko potencjalnego wykrycia prowadzonej operacji. Cyberataki stały się codziennym narzędziem władzy.

Działalność Pjongjangu w cyberprzestrzeni jest obecna na całym świecie. O incydentach z udziałem państwowych hakerów wielokrotnie alarmowały agencje bezpieczeństwa wielu państw, w tym Stanów Zjednoczonych – jednego z głównych przeciwników reżimu. Przykładem może być poradnik „Guidance on the North Korean Cyber Threat" wydany przez FBI, w którym jednoznacznie podkreślono, że „szkodliwe działania cyberprzestępcze Korei Północnej zagrażają Stanom Zjednoczonym i krajom na całym świecie, a w szczególności stanowią poważne zagrożenie dla integralności i stabilności międzynarodowego systemu finansowego".

Amerykanie scharakteryzowali podstawowe cele Pjongjangu w cyberprzestrzeni, wskazując, że są to przede wszystkim cyberataki wymierzone w banki, wyłudzenia środków od pojedynczych użytkowników, przejmowanie kryptowalut, a także pozyskiwanie z bankomatów dziesiątek milionów dolarów w gotówce.

Globalne kampanie kradzieży środków finansowych przez Koreę Północną są przedmiotem zainteresowania społeczności międzynarodowej, która stara się zjednoczyć wysiłki na rzecz neutralizacji nielegalnych działań reżimu. Według danych ONZ pochodzących z ubiegłego roku, Pjongjang wygenerował około 2 miliardy dolarów na rozwój broni masowego rażenia, wykorzystując szeroko rozpowszechnione i coraz bardziej wyrafinowane operacje hakerskie. Dla władzy cyberprzestrzeń jest istną „kopalnią złota".

**Krok w stronę doskonałości**

Północnokoreańscy hakerzy od lat stosują różne taktyki działania w ramach kampanii. Z biegiem czasu modyfikują jednak swoje narzędzia, ulepszając je w celu podniesienia skuteczności prowadzonych operacji. Kluczowe znaczenie w tym obszarze ma również minimalizacja możliwości wykrycia cyberataku i identyfikacji hakerów.

Przykładem może być działalność grupy Lazarus, która w ciągu ostatnich dwóch lat znacznie zmieniła swoją taktykę działania. Cyberprzestępcy zaczęli między innymi wykorzystywać fikcyjne firmy do przesyłania skradzionych funduszy do kraju. Hakerzy tworzą również fałszywe strony internetowe, służące jako jedno z narzędzi używanych do realizacji kampanii.

Ewolucja dotyczy nie tylko taktyki działania, ale także samej cyberbroni. Specjaliści Kaspersky Lab wskazali, że instrumenty Lazarus zostały znacznie ulepszone, zwłaszcza w odniesieniu do narzędzi przeznaczonych do cyberataków na urządzenia z systemem Windows oraz macOS. Cyberprzestępcy starają się również skutecznie wykorzystać rozwój komunikatorów internetowych, takich jak Telegram. Służą one jako platformy rozpowszechniania złośliwego oprogramowania. Prosty i skuteczny sposób na generowanie dużej liczby ofiar.

Interesujący wydaje się być przykład operacji hakerskiej, którą Pjongjang przeprowadził przy wykorzystaniu popularnej witryny LinkedIn. Posłużyła ona jako kanał rozpowszechniania kampanii phishingowej, gdzie celem byli przedstawiciele uznanych firm z całego świata. W ramach operacji cyberprzestępcy grupy Lazarus rozsyłali spreparowane oferty pracy wraz z załącznikiem zawierającym złośliwe oprogramowanie.

Kampania została wymierzona w 14 firm z całego świata, w tym z Wielkiej Brytanii oraz Stanów Zjednoczonych. Jedną z jej ofiar było przedsiębiorstwo zajmujące się kryptowalutami. Główną motywacją hakerów stanowiło zbieranie danych uwierzytelniających z zainfekowanego urządzenia, które zabezpieczały dostęp do środków finansowych (kont bankowych oraz kryptowalutowych).

Opisana powyżej operacja jest idealnym przykładem potwierdzającym kreatywność i świadomość hakerów. W czasie pandemii, gdzie wiele osób traci pracę ze względu na pogłębiający się kryzys,

cyberprzestępcy dostrzegli swoją szansę i starają się wykorzystać problemy na rynku zatrudnienia. Dodatkowo posługują się popularną platformą, aby w ten sposób dotrzeć do konkretnej grupy użytkowników i tym samym zwiększyć skuteczność swojej kampanii. Działania hakerów Pjongjangu nie są przypadkowe, lecz ewoluują wraz ze zmieniającą się rzeczywistością.

**Z upływem lat główny cel pozostaje ten zmian**

Rozwój narzędzi, taktyki, zdolności oraz całego zaplecza hakerów przyczynił się do podniesienia skuteczności prowadzonych operacji, których kluczowym celem jest sektor finansowy. Reżim nie zmienia swojego nastawienia i stale koncentruje się na generowaniu środków, aby móc rozwijać się jako państwo, zwłaszcza w obszarze wojskowym. W tym miejscu warto podkreślić, że operacje prowadzone przez państwowych hakerów mają zwykle charakter globalny. Wydaje się, że motywuje to prosty mechanizm: im więcej ofiar, tym większy zysk.

Najnowsze kampanie są tego potwierdzeniem. Jako przykład można przytoczyć serię cyberataków wymierzonych w prywatne firmy z wielu branż, w tym przede wszystkim z sektora handlu elektronicznego i usług internetowych. Wśród ofiar znalazły się podmioty z Niemiec, Turcji, Japonii, Indii, Korei czy nawet Polski. O operacji poinformowali specjaliści Kaspersky Lab w lipcu bieżącego roku.

Co więcej, od lutego trwała inna kampania prowadzona przez hakerów Korei Północnej. Operacja polegała na włamywaniu się do banków na całym świecie w celu dokonania nielegalnych przelewów pieniędzy oraz uszkodzenia bankomatów, tak aby „wypluwały pieniądze". Amerykanie przypisali cyberataki północnokoreańskiej agencji szpiegowskiej Reconnaissance General Bureau. Tego typu incydenty zaobserwowano już w 2016 roku, lecz po początkowym wzroście przypadków kampania została wstrzymana. Kilka miesięcy temu hakerzy wznowili działania, które trwają do dziś, nękając sieci oraz systemy instytucji finansowych z całego świata.

Pozornie wydawać by się mogło, że Polska nie powinna zwracać uwagi na potencjał hakerów Korei Północnej, ponieważ ani nie jest głównym wrogiem Pjongjangu ani też mocarstwem „rozdającym karty" na arenie międzynarodowej. Jednak biorąc pod uwagę cyberbezpieczeństwo oraz cyberataki, należy wskazać, że to kwestie globalne, których nie można lekceważyć. Ryzyka płynące ze strony reżimu musi być uwzględnione również nad Wisłą, aby jak najlepiej chronić państwo i obywateli przed zaawansowanymi kampaniami płynącymi ze Wschodu.

**Chińskie wsparcie**

Działania prowadzone przez hakerów bardzo często są skomplikowane i charakteryzują się wysokim poziomem zaawansowania. Wynika to między innymi z faktu realizacji operacji w skali światowej. W związku z czym cyberprzestępczy poszukują wsparcia u podmiotów zewnętrznych, aby usprawnić cały proces przy równoczesnym podniesieniu wydajności podejmowanych czynności.

Hakerzy Pjongjangu nie są wyjątkiem. Współpracują oni z przedstawicielami środowiska przestępczego z innych państw, czego odzwierciedleniem może być na przykład sprawa nałożenia sankcji na dwóch chińskich obywateli przez Stany Zjednoczone. Zdaniem Amerykanów mężczyźni wspierali działania północnokoreańskich cyberprzestępców podczas cyberataków na branżę kryptowalut w lipcu i wrześniu 2019 roku.

Wówczas hakerzy Pjongjangu mieli wykraść odpowiednio 272 tys. (lipiec) oraz 2,5 mln (wrzesień) dolarów w kryptowalutach w ramach operacji wymierzonych w sektor finansowy, w tym giełdy bitcoinów. Współpraca z Chińczykami pozwoliła im „wyprać" pozyskane środki za pośrednictwem ponad 100 kont na innej giełdzie wirtualnych walut.

Departament Skarbu USA nie ma wątpliwości, że wpływy z kampanii hakerskich Korei Północnej często trafiają do chińskich instytucji finansowych. Z drugiej jednak strony reżim regularnie szkoli swoich cyberprzestępców, aby potrafili samodzielnie „prać skradzione pieniądze". Jednak współpraca z wyspecjalizowaną w tej dziedzinie siatką jest szybsza i bardziej efektywna.

**Kradzież środków to jedna strona medalu**

Rozbudowa cyberzdolności Pjongjangu przyczyniła się również do redefinicji celów reżimu w odniesieniu do wirtualnej domeny. Do tej pory hakerzy koncentrowali się na sektorze finansowym, aby za pomocą cyberataków wspierać dążenia państwa do rozbudowy potencjału militarnego, w tym nuklearnego. W ostatnim czasie zaobserwowano również zdecydowany wzrost aktywności Korei Północnej w innych sektorach. Świadczy to o tym, że Pjongjang rozszerza swoją strategię w cyberprzestrzeni i chce podejmować zdecydowanie bardziej aktywne działania w jej ramach. Reżim poza kradzieżą środków finansowych, przywiązuje coraz większą wagę do cyberszpiegostwa oraz ingerencji w sprawy wewnętrzne państw uznawanych za wrogie.

Ponadprzeciętne możliwości reżimu pozwalają mu na przeprowadzanie zaawansowanych kampanii wymierzonych w kluczowe sektory innych państw. Przekonały się o tym same Stany Zjednoczone, których służby zidentyfikowały cyberataki na amerykański sektor obronny, lotniczy, a także inne istotne z punktu widzenia państwa branże.

Reżim starał się wykorzystać kryzys gospodarczy związany z Covid-19 dla swoich celów, angażując w specjalną misję hakerów ugrupowania Hidden Cobra. Cyberprzestępcy wykazali się sprytem i kreatywnością, podszywając się pod pracodawców, rozsyłając oferty pracy, które w rzeczywistości były nośnikiem złośliwego oprogramowania. Ich głównym zadaniem było gromadzenie danych na temat nie tylko samych ofiar, ale również sektorów, w jakich pracują. Kampania według różnych szacunków trwała od 31 marca do 18 maja bieżącego roku.

Hakerzy Korei Północnej są elastyczni i starają się wykorzystać globalne wydarzenia do realizacji własnych celów. Wybuch pandemii Covid-19 jest tego doskonałym przykładem. Rozprzestrzenianie się wirusa spowodował lock down w wielu państwach, co pociągnęło za sobą „cięcia" w licznych zakładach pracy. Duża grupa bezrobotnych, którzy często desperacko szukają zatrudnienia w trudnych czasach, jest bardzo łatwym celem dla hakerów.

Niemalże identyczną strategię przyjęto podczas serii cyberataków wymierzonych w przemysł obronny Izraela, które również miały miejsce w 2020 roku. Była to kampania o charakterze cyberszpiegowskim, podczas której hakerzy podszywali się pod pracodawców popularnych firm oferujących atrakcyjne warunki zatrudnienia, aby nakłonić użytkowników do dalszej interakcji.

Operacja polegała na wykorzystaniu popularnej platformy LinkedIn (nie pierwszy raz), gdzie hakerzy stworzyli fikcyjne profile w celu nawiązania kontaktu ze swoimi ofiarami. Co warto podkreślić, cyberżołnierze reżimu sprawnie posługują się technikami socjotechniki, aby podnieść skuteczność swoich działań.

Izraelski Directorate of Security for the Defense Establishment we współpracy z instytucjami ds. bezpieczeństwa skutecznie zneutralizował operację ze strony grupy Lazarus. Jej podstawowym zadaniem zleconym przez reżim było włamanie się na komputery starannie wyselekcjonowanych ofiar, a następnie infiltracja ich systemów oraz kradzież poufnych danych.

Warto jednak pamiętać, że celem kampanii hakerskich Pjongjangu są nie tylko państwa, ale także organizacje międzynarodowe o kluczowym znaczeniu. Jako przykład można wskazać cyberataki na 11 przedstawicieli z 6 państw członkowskich Rady Bezpieczeństwa ONZ. Celem operacji

spearphisingowej było wyłudzenie istotnych informacji i danych.

Hakerzy, zgodnie z dostosowanym do współczesnego kształtu cyberprzestrzeni podejściem, wykorzystali w swoich działaniach Gmaila i WhatsAppa, podszywając się pod różne ważne osobistości. Kto tym razem przeprowadził złośliwą operację? Zdaniem specjalistów misję realizowały służby wywiadowcze Pjongjangu.

Oczywiście cyberprzestrzeń jest również wymiarem, który doskonale nadaje się do prowadzenia operacji wpływu lub innych kampanii, mających na celu ingerencję w scenę polityczną wrogich państw. Reżim jest tego świadomy i również w tym zakresie stara się realizować swoje interesy.

Posiadane przez Koreę Północną zasoby oraz możliwości budzą niepokój w Stanach Zjednoczonych w kontekście zbliżających się wyborów prezydenckich. Amerykanie opublikowali listę państw, które zdaniem krajowych służb stanowią największe zagrożenie dla przebiegu kampanii. Początkowo znajdowały się na niej jedynie Chiny, Rosja oraz Iran. Obecnie katalog ten został rozszerzony o kolejne trzy kraje – Kubę, Arabię Saudyjską oraz… Koreę Północną.

Zamieszczenie Pjongjangu na liście największych zagrożeń dla amerykańskich procesów demokratycznych nie jest przypadkowe. Stany Zjednoczone widzą, że reżim stale podnosi swoje cyberzdolności oraz rozwija cyberbroń, która staje się coraz bardziej skutecznym środkiem walki w wirtualnej domenie. Dodatkowo Korea Północna nieustannie prowadzi agresywną politykę w cyberprzestrzeni, nękając kolejnymi atakami inne państwa. W opinii Amerykanów Pjongjang rośnie w siłę i staje się bardzo wymagającym przeciwnikiem w sieci, który dodatkowo jest nieobliczalny w swoich działaniach.

Należy jednak pamiętać, że kampanie dezinformacyjne podejmowane przez reżim nie są jeszcze aż tak zaawansowane jak te prowadzone ze strony Rosji, Iranu czy Chin. Pomimo to na uwagę zasługuje operacja realizowana  przez północnokoreańskich hakerów na początku bieżącego roku, której celem były amerykańskie organizacje informacyjne. W ten sposób cyberprzestępcy chcieli uzyskać dostęp do danych, niezbędnych do szerzenia dalszej dezinformacji w sieci.

**Bogaty arsenał i rozwój cyberwojsk**

O sile danego państwa w cyberprzestrzeni decyduje między innymi poziom rozwoju jego cyberwojsk oraz ich zaawansowanie. W związku z tym Korea Północna od lat regularnie szkoli „cyberżołnierzy”, którzy są odpowiedzialni za prowadzenie najbardziej zaawansowanych misji w wirtualnej domenie.

Obecnie szacuje się, że reżim posiada co najmniej 6000 hakerów oraz specjalistów od szeroko rozumianej wojny technologicznej. W ciągu ostatniej dekady Pjongjang zatrudnił oraz wyszkolił łącznie kilka tysięcy osób, zdolnych do prowadzenia działań w cyberprzestrzeni. Co więcej, wiele z nich zostało rozmieszczonych poza granicami kraju. Dzięki temu „cyberżołnierze” Korei Północnej mogą prowadzić operacje z różnych stron świata, dezorientując tym samym zagraniczne służby. Hakerzy stacjonują między innymi na Białorusi, w Chinach, Indiach, Malezji czy nawet Rosji. Taka sytuacja jest możliwa dzięki luźnej strukturze organizacyjnej podmiotów tworzących cyberwojsko reżimu.

Kluczową jednostką odpowiedzialną za działania w cyberprzestrzeni jest Biuro 121. Jego skład osobowy znacznie się rozszerzył, co wiąże się z podejmowaniem bardziej zaawansowanych operacji. Według danych amerykańskich służb w ciągu ostatnich 10 lat zatrudniono ponad 5000 tysięcy hakerów i specjalistów ds. wojny elektronicznej. W 2010 roku Biuro 121 posiadało co najmniej 1000 cyberżołnierzy. Reżim inwestuje równie w rozwój Mirim College, która kształtuje dla armii około 100 hakerów rocznie.

Biuro 121 składa się z czterech głównych pododziałów – zespół Andariel (ok. 1600 osób), Bluenoroff

(ok. 1700), Lazarus (trudno określić szacunkową liczbę członków), Electronic Warfare Jamming Regiment (od 2000 do 3000 cyberżołnierzy). Trzy pierwsze zespoły odpowiedzialne są za prowadzenie działań stricte związanych z „cyberwojną", ostatni zaś jest dedykowany do operacji w zakresie „wojny elektronicznej".

Skuteczność działań prowadzonych w cyberprzestrzeni jest uzależniona nie tylko od poziomu zdolności „cyberżołnierzy", ale także zaawansowania „cyberbroni". W tym zakresie reżim również kładzie nacisk na rozwój nowych, innowacyjnych narzędzi hakerskich, które mają podnieść skuteczność prowadzonych operacji.

Przykładem może być nieznany do tej pory wariant złośliwego oprogramowania, będący odmianą trojana zdalnego dostępu (RAT). Wirus został nazwany przez Amerykanów „Blindingcan" i jest wykorzystywany przez hakerów grupy Hidden Cobra. Użyto go między innymi podczas ostatniej kampanii wymierzonej w sektor obronny USA. Narzędzie pozwoliło cyberprzestępcom na pozyskanie informacji dotyczących kluczowych amerykańskich technologii wojskowych oraz energetycznych.

**Korea Północna specyficznym przypadkiem**

Zauważalny rozwój cyberzdolności Pjongjangu, wzrost liczebności cyberwojsk oraz podniesienie poziomu jakości ich wyposażenia przekłada się na prowadzenie bardziej wyrafinowanych kampanii hakerskich w skali globalnej. Agresywna polityka reżimu w wirtualnej domenie sprawia, że wiele krajów oraz aktorów niepaństwowych obawia się cyberataków ze strony Korei Północnej. Jednak jaka jest prawda na temat obecnej siły i potencjału reżimu w cyberprzestrzeni?

Zgodnie z National Cyber Power Index 2020 (NCPI), opracowanym przez ekspertów Belfer Center for Science and International Affairs z Harvard Kennedy School, Stany Zjednoczone zostały określone liderem w rankingu „cyberpotęg" tuż przed Chinami, Wielką Brytanią Rosją oraz Holandią.

Indeks bierze pod uwagę wiele elementów, które przekładają się na możliwości i zdolności danego państwa. W ten sposób otrzymane wyniki są miarą rzeczywiście udowodnionej siły oraz potencjału, jakim dysponuje dany rząd. Jak w porównaniu z innymi krajami wypadła Korea Północna?

Autorzy rankingu nie bez powodu nazwali reżim „szczególnym przypadkiem". Pomimo wielu prób uzyskania konkretnych, a zarazem wiarygodnych informacji na temat zdolności i wirtualnego arsenału Korei Północnej, nie udało im się zgromadzić odpowiedniej jakości danych, które posłużyłyby jako podstawa racjonalnej oceny potencjały Pjongjangu. Specjaliści wskazali jednak, że reżim posiada cyberzdolności na wysokim poziomie, lecz skutecznie próbuje je utrzymać w „tajemnicy".

Z drugiej strony Pjongjang napotyka wiele trudności w zakresie prowadzenia operacji w cyberprzestrzeni. Zdaniem specjalistów CrowdStrike kampanie podejmowane przez północnokoreańskich hakerów, pomimo globalnego charakteru, są skierowane do ograniczonej liczby sektorów w porównaniu chociażby do chińskich czy irańskich podmiotów.

Z analizy ekspertów jasno wynika, że reżim stale buduje swoje cyberzdolności, lecz nie osiągnął jeszcze takiego poziomu jak inne państwa, uznawane za agresywne w cyberprzestrzeni (np. Iran, Chiny). Nie zmienia to jednak faktu, że ugrupowania działające na zlecenie Pjongjangu nie stanowią poważnego zagrożenia – wręcz przeciwnie. Cyberataki ze strony reżimu zostały uznane przez CrowdStrike za szczególnie niebezpieczne, stąd też stały się przedmiotem szerszego badania ekspertów.

**Co z Polską?**

Pozornie wydawać by się mogło, że Polska nie powinna zwracać uwagi na potencjał hakerów Korei

Północnej, ponieważ ani nie jest głównym wrogiem Pjongjangu ani też mocarstwem „rozdającym karty” na arenie międzynarodowej. Jednak biorąc pod uwagę cyberbezpieczeństwo oraz cyberataki, należy wskazać, że to kwestie globalne, których nie można lekceważyć. Ryzyko płynące ze strony reżimu musi być uwzględnione również nad Wisłą, aby jak najlepiej chronić państwo oraz obywateli przed zaawansowanymi kampaniami płynącymi ze Wschodu.

Zaniedbania w dziedzinie cyberbezpieczeństwa mogą być skutecznie wykorzystane przez północnokoreańskich hakerów, zwłaszcza w sektorze finansowym. Polska doświadczyła już tego typu poważnego incydentu w przeszłości. W tym miejscu można wskazać chociażby na cyberatak wymierzony w Komisję Nadzoru Finansowego, jaki miał miejsce w 2017 roku.

Operacja była zaawansowana i doskonale skoordynowana. Istnieje duże prawdopodobieństwo, że hakerzy prowadzili ją przez długi okres czasu. Cel cyberataku najprawdopodobniej stanowiły dane osobowe lub finansowe, które na czarnym rynku osiągają wysokie ceny.

Wspomniany wyżej incydent pokazuje, że zagrożenie dla polskiej branży finansowej, ale również innych sektorów działalności państwa jest realne. Dla hakerów Pjongjangu przeprowadzenie zaawansowanej operacji wymierzonej w centrum finansowe innego państwa nie jest niczym nowym. Odpowiednie środki oraz zdolności pozwalają reżimowi na swobodne prowadzenie kampanii hakerskiej w różnych częściach świata. Czy Polska jest obecnie na to gotowa?

Północnokoreański rząd posiada jasno wyznaczone cele w odniesieniu do cyberprzestrzeni, które stara się skutecznie realizować. Czyni to za pomocą cyberatków przeprowadzanych przez ugrupowania hakerskie oraz „cyberżołnierzy”, których zdolności są regularnie podnoszone, na przykład w specjalnie do tego celu utworzonych placówkach. Efektywność kampanii mają zagwarantować również innowacyjne narzędzia, w tym cyberbroń, stanowiące przejaw siły Pjongjangu w cyberprzestrzeni.

Pomimo początkowego skoncentrowania się na kwestii pozyskiwania środków finansowych na rzecz obejścia sankcji i zagwarantowania źródeł finansowania dla państwa, reżim stale rozszerza swój katalog celów w wirtualnej domenie. Dzięki rozwojowi cyberwojsk możliwe staje się prowadzenie operacji, których zadaniem jest na przykład cyberszpiegostwo czy sparaliżowanie działań adwersarza. To z kolei pozwala władzy na kreowanie bardziej agresywnej polityki i budowanie pozycji na arenie międzynarodowej.

Należy jednak pamiętać, że Pjongjang nie jest jeszcze na tyle silny w cyberprzestrzeni, aby móc równać się z innymi państwami, w tym wiodącymi „cyberpotęgami” jak Stany Zjednoczone, Chiny, Rosja czy Iran. Niemniej jednak reżim kładzie duży nacisk na rozwój swoich cyberzdolności i potencjału, aby z czasem dorównać najlepszym w tej dziedzinie. Korea Północna już teraz stanowi poważne zagrożenie, a w przyszłości zostanie ono jeszcze dodatkowo wzmocnione.

**Czytaj też:** Czeka nas era chińskiej dominacji? Ranking „cyberpotęg” 2020