GLOBALNIE · ANALIZA

RYWALIZACJA CHIŃSKO-AMERYKAŃSKA W CYBERPRZESTRZENI

Paweł Lizoń · 19 lutego 2024



Przemysł wysokich technologii odgrywa kluczową rolę w amerykańskiej gospodarce, będąc bardzo ważnym składnikiem potęgi Stanów Zjednoczonych. Przyciąga on uwagę nie tylko partnerów handlowych, lecz także państw, które chcą uzyskać przewagę konkurencyjną poprzez nielegalne pozyskiwanie wrażliwych informacji. Chiny powtarzają historyczny schemat państw pretendujących do roli mocarstw, goniących czołówkę technologiczną. Do zniwelowania swoich zapóźnień technologicznych używają szerokiego zakresu narzędzi, w tym narzędzi szpiegowskich.

Chińska działalność szpiegowska w cyberprzestrzeni

Jak można przeczytać w opublikowanym w 2018 r. raporcie Narodowego Centrum Kontrwywiadu i Bezpieczeństwa USA, zagraniczne szpiegostwo gospodarcze i przemysłowe skierowane przeciwko Stanom Zjednoczonym stanowi znaczące zagrożenie dla dobrobytu, bezpieczeństwa i przewagi konkurencyjnej USA. Cyberprzestrzeń jest preferowaną domeną operacyjną dla szerokiej gamy podmiotów zaangażowanych w szpiegostwo gospodarcze. To w niej swoje działania prowadzą zarówno konkurencyjne państwa, przedsiębiorstwa komercyjne i sponsorowane grupy wyspecjalizowanych hakerów.

Ponadto, na co zwraca uwagę The National Counterintelligence and Security Center, technologie nowej generacji, takie jak sztuczna inteligencja i internet rzeczy, tworzą w zabezpieczeniach amerykańskich sie-

ci nowe luki, na które instytucje odpowiedzialne za bezpieczeństwo cyberprzestrzeni nie są w stanie znaleźć skutecznej odpowiedzi. Skuteczna reakcja wymaga zrozumienia szpiegostwa gospodarczego jako ponadnarodowego, wielowektorowego zagrożenia dla integralności gospodarek krajowych oraz światowego handlu.

Należy podkreślić, że zaawansowane zdolności w cyberprzestrzeni posiadają głównie państwa narodowe. Sponsorowana przez państwo wroga działalność w tym obszarze zazwyczaj obejmuje wsparcie dla operacji szpiegowskich, rozpoznanie sieci wojskowych do późniejszego wykorzystania podczas konfliktu, kradzież danych handlowych lub własności intelektualnej, a czasem demonstrowanie zdolności, które mają na celu odstraszenie rywalizującego państwa.

Przykładów działalności szpiegowskiej w cyberprzestrzeni skierowanej przeciwko amerykańskiemu przemysłowi wysokiej technologii jest naprawdę wiele. Jak podaje Ellen Nakashima, korespondentka ds. bezpieczeństwa narodowego, w swym opracowaniu dla „The Washington Post", poprzez działalność wywiadowczą w cyberprzestrzeni Chiny pozyskały niezwykle wrażliwe dane z ponad dwóch tuzinów programów zbrojeniowych USA. Co istotne, nie były to programy o drugorzędnym znaczeniu, lecz priorytetowe inicjatywy amerykańskiego przemysłu obronnego, w tym dotyczące systemu rakietowego Patriot, F-35 Joint Strike Fighter oraz nowego okrętu bojowego marynarki wojennej.

Jak podkreślono w raporcie National Counterintelligence and Security Center z 2018 r., Chińska Republika Ludowa podjęła szeroko zakrojone wysiłki w celu pozyskania amerykańskiej technologii, w tym wrażliwych tajemnic handlowych i zastrzeżonych informacji.

> ChRL wykorzystuje cyberszpiegostwo do wspierania swoich strategicznych celów rozwojowych, takich jak: rozwój nauki i technologii, modernizacja wojskowa i obszar polityki gospodarczej. Ponadto chińskie operacje w cyberprzestrzeni są częścią złożonej, wielopłaszczyznowej strategii rozwoju technologii, która wykorzystuje zarówno te legalne, jak i nielegalne metody do osiągnięcia określonych celów.

Zarówno chińskie firmy, jak i osoby fizyczne często nabywają amerykańską technologię do celów komercyjnych i naukowych. Według autorów ww. raportu chiński rząd stara się zwiększyć swoje zasoby amerykańskiej technologii, pozyskując wsparcie szerokiego grona podmiotów z całego świata. Ma być to możliwe dzięki zaawansowanym działaniom ChRL w obszarze wywiadowczym, polegającym na szerokim wykorzystywaniu prywatnych przedsiębiorstw do pozyskiwania istotnych danych z amerykańskich firm.

Chiński cybersmok

Raport amerykańskiej firmy FireEye, zajmującej się cyberbezpieczeństwem, z czerwca 2016 r. opisuje wzajemne przenikanie się chińskich państwowych i niepaństwowych operacji w cyberprzestrzeni. Pracownicy FireEye przeanalizowali incydenty naruszenia bezpieczeństwa sieci przez siedemdziesiąt dwie grupy, co do których firma „podejrzewa, że działają w Chinach lub w inny sposób wspierają chińskie interesy państwowe". Skrupulatny proces analizy przeprowadzonej przez FireEye obejmował gromadzenie różnych form dowodów, w tym zakres i sposób realizacji operacji. Firma FireEye skupiła się na zbadaniu szeregu elementów, takich jak: konkretne taktyki, techniki i procedury oraz szczegóły operacyjne, np. wy-

siłki na rzecz ukrycia i anonimowości. Jednak nawet przy tych zaawansowanych metodach śledzenia źródeł chińskich operacji twórcy raportu przyznają, że spektrum zaangażowanych podmiotów – od personelu wojskowego po cyberaktywistów działających z pobudek patriotycznych – praktycznie uniemożliwia precyzyjne określenie stopnia kierownictwa lub kontroli państwa.

CZYTAJ TAKŻE: Półprzewodniki rodem z Chin. Czy Zachód ma kłopoty? Cz. 1

Chiny w cyberprzestrzeni

Chiński potencjał w cyberprzestrzeni składa się z wielu podmiotów wojskowych i niewojskowych z sektora publicznego i prywatnego. Biorąc pod uwagę skomplikowaną strukturę biurokratyczną KPCh, a także częste wzajemne przenikanie się chińskich podmiotów publicznych i prywatnych, trudno jest dokładnie ocenić, w jaki sposób zorganizowane są chińskie zdolności w obszarze cyberprzestrzeni. Pewne wskazówki można jednak uzyskać z publikacji doktrynalnych wydanych przez ChRL. Według Science of Military Strategy chińskie siły z obszaru cyber dzielą się na trzy kategorie:

- Wyspecjalizowane siły wojny sieciowej – siły te składają się głównie z jednostek Chińskiej Armii Ludowo-Wyzwoleńczej, które są przeszkolone do prowadzenia ofensywnych i obronnych operacji w cyberprzestrzeni.
- Autoryzowane siły niewojskowe – obejmują one nieumundurowanych operatorów, takich jak Ministerstwo Bezpieczeństwa Państwowego i Ministerstwo Bezpieczeństwa Publicznego.
- Siły cywilne – mogą one obejmować cybermilicję/ siły pomocnicze, które są osadzone w instytucjach cywilnych, takich jak uniwersytety i firmy telekomunikacyjne.

Poniżej zostaną przedstawione wybrane chińskie operacje cyberszpiegowskie. Mnogość takich przedsięwzięć uniemożliwia przytoczenie ich wszystkich, dlatego poniżej są zaprezentowane jedne z istotniejszych.

- Operation Aurora: W grudniu 2009 r. firma Google odkryła, że jej sieć korporacyjna została spenetrowana poprzez wykorzystanie luki w oprogramowaniu Internet Explorer. Ataki zostały następnie zidentyfikowane jako część wyrafinowanej operacji wymierzonej w co najmniej trzydzieści cztery firmy z sektora technologicznego, finansowego i obronnego – w tym Yahoo, Symantec, Adobe, Morgan Stanley, Northrop Grumman i Dow Chemical. Ataki były przeprowadzone poprzez różne luki w zabezpieczeniach. Doniesienia medialne, depesze dyplomatyczne, których treści wyciekły, oraz oświadczenia Google w sprawie włamania sugerowały, że ataki były operacją kierowaną przez ChRL mającą na celu infiltrację amerykańskich korporacji w celu uzyskania politycznie wrażliwych informacji na temat działaczy na rzecz praw człowieka i cennych ekonomicznie danych na temat strategicznych sektorów wysokiej technologii.
- Night Dragon: w lutym 2011 r. firma McAfee opublikowała białą księgę identyfikującą serię ataków APT na globalne firmy energetyczne, które rozpoczęły się w listopadzie 2009 r. i które nazwała Operation Night Dragon. Podobnie jak w przypadku wyżej opisanej Operacji Aurora, ataki wykorzystywały różne środki do penetracji sieci firmowych, gdzie przejęły wrażliwe, zastrzeżone operacje i informacje o finansowaniu projektów w odniesieniu do ofert na pola naftowe i gazowe. Ataki pochodziły z kilku lokalizacji w Chinach. McAfee zidentyfikowało chińską firmę, która świadczyła usługi hostingowe dla hakerów, ale w raporcie nie powiązano ich z żadnym konkretnym podmiotem państwowym lub niepaństwowym.

- Nitro: w październiku 2011 r. firma Symantec opublikowała swoją białą księgę, która identyfikowała operację spear phishingu pochodzącą z amerykańskiego wirtualnego serwera prywatnego (VPS) należącego do obywateli ChRL z siedzibą w Hebei. Operacja rozpoczęła się od ataków na organizacje zajmujące się prawami człowieka, ale później przeniosła się na kradzież własności intelektualnej firm z branży chemicznej i zaawansowanych materiałów. Żaden z zebranych dowodów nie powiązał operacji z chińskim rządem.
- Sykipot: w styczniu 2012 r. AlienVault zidentyfikował atak typu spear phishing skierowany na karty mikroprocesowe używane przez wielu pracowników rządowych USA, w tym w Departamencie Obrony. AlienVault powiązał ataki z wariantem złośliwego oprogramowania z rodziny Sykipot, z serwerami w Chińskiej Republice Ludowej. Niemniej nie zgłoszono dalszych dowodów łączących ataki z chińskim rządem lub z podmiotami związanymi z ChRL.

Problemy kontrwywiadowcze w USA

Według analityków The Heritage Foundation jednym z największych problemów w osłonie kontrwywiadowczej przemysłu wysokich technologii jest fakt, że amerykańskie elity rządzące oraz społeczność uniwersytecka nie dostrzegają powagi zagrożenia, jakie stanowi cyberszpiegostwo.

Dobrym przykładem ww. problemu są uniwersytety, które mocno zabiegają o międzynarodowych studentów, głównie dlatego, że płacą oni pełne czesne. Fakt ten wykorzystują Chińczycy, opłacając swoim obywatelom studia w USA. Przed pandemią COVID-19 35% wszystkich zagranicznych studentów w USA stanowili obywatele Chińskiej Republiki Ludowej. Od tego czasu odsetek ten zdecydowanie spadł, ale chińscy studenci nadal zajmują nieproporcjonalnie dużą część miejsc – zwłaszcza na podyplomowych kierunkach z obszaru STEM (science, technology, engineering and mathematics). Jak podkreśla amerykański instytut, innowacje i postępy techniczne generowane przez badania uniwersyteckie (wraz z badaniami i rozwojem sektora prywatnego) miały ogromny wkład w bezpieczeństwo USA, a także amerykańskiej gospodarki. Jednak dążący do stania się globalną potęgą Pekin stosuje różne taktyki – zarówno nielegalne, jak i legalne – w celu pozyskania najnowocześniejszych technologii i własności intelektualnej z uniwersyteckich systemów badawczych, międzynarodowych laboratoriów i korporacyjnych obiektów badawczo-rozwojowych. W rezultacie Chiny szybko nadrabiają zaległości technologiczne względem swojego największego konkurenta.

Narodowe Centrum Kontrwywiadu i Bezpieczeństwa USA nieustannie ostrzega, że uniwersytety, prezesi dużych firm high-tech oraz urzędnicy państwowi muszą lepiej chronić swoją własność intelektualną. W przeciwnym razie, jak donosi Associated Press, „mogłoby to dać Pekinowi decydującą przewagę militarną i możliwą dominację nad opieką zdrowotną i innymi istotnymi sektorami w Ameryce". Samo FBI szacuje, że amerykańska gospodarka traci rocznie od 225 do 600 miliardów dolarów z powodu pirackiego oprogramowania, kradzieży tajemnic handlowych i podrabianych towarów. Dodatkowo, aby podkreślić wagę problemu, warto przytoczyć analizę Cybereason, firmy technologicznej zajmującej się cyberbezpieczeństwem. Firma szacuje, że jedna chińska państwowa operacja w cyberprzestrzeni ukradła „setki gigabajtów własności intelektualnej i wrażliwych danych" o wartości miliardów dolarów z trzydziestu międzynarodowych firm. Należy podkreślić, że takich operacji w skali roku jest naprawdę wiele. Jednak, jak podkreśla Dustin Carmack, pracownik naukowy ds. cyberbezpieczeństwa, wywiadu i nowych technologii w The Heritage Foundation, niewielu ustawodawców zwraca należytą uwagę na to zagrożenie.

Aby zilustrować problem nieszczelności amerykańskiego kontrwywiadu, warto przytoczyć tutaj przykład

Texas A&M University, który w maju 2020 r. zdobył wiele nagród federalnych i ponad 400 milionów dolarów dotacji federalnych na prowadzenie wrażliwych badań. Był także jednym z pięciu podmiotów, które otrzymały prestiżową nagrodę Defense Counterintelligence & Security Agency Award for Excellence in Counterintelligence za 2021 r. Jest to wyróżnienie przyznawane przez rząd USA w ramach uznania dla wysoce dojrzałych i skutecznych programów branżowych kontrwywiadu, zwiększających bezpieczeństwo narodowe i promujących bezkompromisowe dostarczanie wrażliwych i niejawnych usług Departamentowi Obrony i innym agencjom rządowym. Według komunikatu prasowego Uniwersytetu w konkursie wzięło udział ponad 10 000 organizacji korporacyjnych i akademickich. Trzy miesiące później tamtejszy profesor, będący również badaczem NASA, został aresztowany pod zarzutem spisku, składania fałszywych oświadczeń i oszustw finansowych. Rzekomo ukrywał swoje powiązania z chińskim programem rządowym mającym na celu rozwój zaawansowanych technologii w tym kraju.

Właśnie z takich powodów amerykańskie think tanki z obszaru bezpieczeństwa apelują o podjęcie konkretnych kroków przez amerykańskie uniwersytety, aby lepiej współpracować z organami ścigania i agencjami wywiadowczymi w celu ochrony owoców swoich badań. Brak działań mających na celu zapobieganie kradzieży własności intelektualnej i nielegalnemu transferowi technologii uderza w amerykańskie interesy gospodarcze i stanowi istotne wyzwanie dla bezpieczeństwa narodowego.

CZYTAJ TAKŻE: Czy możliwy jest technologiczny skok przez demograficzną przepaść?

Co dalej?

Jak zauważono w dokumencie NATO Cooperative Cyber Defence Centre of Excellence – *China and Cyber: Attitudes, Strategies, Organisation* z 2016 r., różne postrzeganie zarządzania cyberprzestrzenią może wpisywać się jako część ogólnej geopolitycznej rywalizacji między ChRL a Zachodem. Mimo że do tej pory udało się uniknąć fizycznej konfrontacji pomiędzy USA i ChRL, sytuacja zaostrza się w cyberprzestrzeni, którą zarówno Departament Obrony USA, jak i jego chiński odpowiednik postrzegają jako nową domenę konfliktu.

Należy się spodziewać kontynuacji rywalizacji w cyberprzestrzeni pomiędzy dwoma mocarstwami. Co zrozumiałe, wraz ze wzrostem znaczenia cyberprzestrzeni w życiu codziennym rywalizacja ta będzie generować większe napięcia w sferze gospodarczej i politycznej.

Mimo że na potrzeby niniejszego artykułu przeanalizowane zostały chińskie operacje w domenie cyber, należy podkreślić, że USA również dysponuje ogromnym potencjałem w tym obszarze, który niejednokrotnie był już wykorzystywany przeciwko chińskiemu rywalowi. Ich zakres pokazał między innymi Edward Snowden, który w 2013 r. ujawnił blisko 200 tys. tajnych dokumentów NSA, co stanowiło jeden z największych wycieków tajnych informacji w dziejach Stanów Zjednoczonych. Snowden twierdził wtedy, że hakerska aktywność NSA przeciwko Chinom sięga 2009 r., a wśród celów inwigilowanych przez systemy komputerowe amerykańskiego wywiadu w Chinach wymienił urzędników, uczelnie, firmy i studentów. Chińskie cele, według Snowdena, miały być elementem ponad 61 tys. globalnych operacji hakerskich amerykańskich służb specjalnych.

Zbliżony potencjał w cyberprzestrzeni obu państw, który obserwujemy dzisiaj, nie musi się długo utrzymywać. Sprawne wdrożenie rozwiązań związanych z rewolucją w dziedzinie sztucznej inteligencji czy technologii kwantowej może przechylić szalę zwycięstwa na korzyść któregoś z rywalizujących mocarstw. Chiny, pretendujące do roli globalnego mocarstwa, będą wykorzystywały coraz to bardziej za-

awansowane rozwiązania, aby gonić czołówkę technologiczną, którą dziś stanowią Stany Zjednoczone.

D. Boawn, *Cyber counterintelligence, defending the United States' information technology and communications critical infrastructure from Chinese threats*, Utica College; ProQuest Dissertations Publishing, 2014.

D. Carmack, *Do More to Prevent Chinese Espionage* [online], 1.09.2022, https://www.heritage.org/asia/commentary/do-more-prevent-chinese-espionage [data dostępu: 7.01.2024].

E. Chien, G. O'Gorman, *The Nitro Attacks: Stealing Secrets from the Chemical Industry*, Symantec Security Response, 2011.

B. Krekel, P. Adams, G. Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*,U.S.-China Economic and Security Review Commission, 2011.

W. Lynn, *Remarks on the Department of Defense Cyber Strategy*,Biuro asystenta sekretarza obrony ds. publicznych, National Defense University, Waszyngton 2011.

McAfee, *Global Energy Cyberattacks: Night Dragon*, 2011.

R. Morgus, B. Fonseca, K. Green, *Are China and Russia on the Cyber Offensive in Latin America and the Caribbean?* A Review of Their Cyber Capabilities and Implications for the U.S. and its Partners in the Region,„New America", 2019.

E. Nakashima, *Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies*, „The Washington Post" 2013.

National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*, 2018.

K. Pollpeter i in., *The PLA as an Organization 2.0*,Defense Technical Information Center, 2012.

M. Raud, *China and Cyber: Attitudes, Strategies, Organisation*, NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Red Line Drawn: China Recalculates Its Use of Cyber Espionage, FireEye Special Report, 2016.

R. Williams, *The 'China, Inc.+' Challenge to Cyberspace Norms*, A Hoover Institution Essay, „Aegis Series Paper" No. 1803, 2018.

Oryginał: https://nlad-kopia1113.instawp.site/rywalizacja-chinsko-amerykanska-w-cyberprzestrzeni/

DOBRA ANALIZA WYMAGA CZASU

Rzetelny tekst to dni pracy: źródła, dane, redakcja. Każda wpłata pozwala nam przygotować kolejny. Nawet niewielka kwota ma znaczenie.

WSPIERAM ANALIZY

wspieram.nlad.pl



Zeskanuj, aby wesprzeć