Komentarz Ośrodka Badań Azji
Centrum Badań nad Bezpieczeństwem
Akademii Sztuki Wojennej

Komentarz nr 4/2021; data złożenia: 20 stycznia 2021

Japonia obawia się cyberataku podczas igrzysk

Japonia obawia się, że mogłaby stać się ofiarą ataku cybernetycznego ze strony Rosji bądź innego państwa (Chiny lub Korea Północna) podczas przełożonych Igrzysk Olimpijskich w Tokio. Obawa ta z jednej strony wynika z doświadczenia – cyberatak wydarzył się podczas otwarcia Zimowych Igrzysk Olimpijskich w Pyoengchangu w 2018, ale również z percepcji własnych możliwości w dziedzinie cyberbezpieczeństwa, które Japonia ocenia jako niedostateczne. Główne bolączki japońskiego systemu cyberbezpieczeństwa to jego fragmentaryczność i utrudniona koordynacja między siecią zaangażowanych podmiotów. Pewien wpływ mają również cechy wypływające z tradycyjnego japońskiego modelu gospodarczego oraz starzenie się społeczeństwa, które powoduje duże braki kadrowe.

Dokonane w ostatnich latach cyberataki obnażają niedostatki japońskiego przygotowania w dziedzinie cyberbezpieczeństwa. Oprócz ataków obliczonych na wyłudzenia pieniędzy od przedsiębiorstw, ośmieszenie państwa lub szpiegostwo, dokonywano w Japonii również cyberprzestępstw na międzynarodową skalę, jak na przykład ataki na giełdy kryptowalut, w wyniku których jednorazowo kradziono setki milionów dolarów. Nawet w ostatnich miesiącach zaobserwowano ślady podejrzanej aktywności, która może świadczyć o tym, że infrastruktura japońska była penetrowana pod kątem możliwości uzyskania nieuprawnionego dostępu.

Do niektórych z powodów narażenia Japonii na tego typu działania należą: sąsiedztwo Chin, Rosji i Korei Północnej, sojusz ze Stanami Zjednoczonymi oraz jej pozycja

gospodarcza. Radykalne zwiększenie potencjału Japonii w tej dziedzinie będzie wymagać napływu specjalistów i know-how z zewnątrz. W kontekście japońskich obaw luźno związanych z Rosją warto tu dostrzec niemały potencjał państw Europy Środkowej i Wschodniej (Czechy, Estonia, Litwa, Polska, Ukraina) i podjąć próby współpracy z Japonią.

Przełożone z powodu pandemii COVID-19 najpóźniej na lato tego roku Igrzyska Olimpijskie w Tokio, jeśli odbędą się, będą bardzo istotnym wydarzeniem dla Japonii[1]. Jedynym ze znaków zapytania dotyczącym bezpieczeństwa imprezy jest przygotowanie państwa do odparcia ewentualnego ataku cybernetycznego podczas zawodów, podobnego do tego, jaki miał miejsce podczas ceremonii otwarcia Zimowych Igrzysk Olimpijskich w Pyeongchangu w 2018 roku (najczęściej przypisywano go Rosji)[2]. Japońscy specjaliści do spraw bezpieczeństwa cybernetycznego oraz niektóre media już wiele miesięcy temu ostrzegali przed ryzykiem takiego zdarzenia[3]. Zaobserwowano również ślady podejrzanej aktywności, która może świadczyć o tym, że infrastruktura japońska była penetrowana pod kątem możliwości uzyskania nieuprawnionego dostępu. O chęć ingerencji Japonia najbardziej podejrzewa Rosję, której reprezentacja została wykluczona z udziału po skandalu dopingowym, ale również Chiny lub Koreę Północną[4]. Z powodu zaobserwowanego poważnego ryzyka cybernetycznego podjęto wysiłek zatrudnienia specjalistów, którzy w czasie Igrzysk Olimpijskich mieliby bronić japońskiej cyberprzestrzeni przed wrogim działaniem[5]. Chodzi na przykład o udaremnienie możliwości przejęcia nadawania telewizyjnego i zdyskredytowanie wizerunku Japonii przed całym światem (to na gospodarzu spoczywa obowiązek dostarczenia transmisji za granicę), ale potencjalnym celem ataku mogłaby stać się przecież również infrastruktura telekomunikacyjna, transportowa, czy energetyczna. Japończycy obawiają się także potencjalnego sabotowania pracy zdalnej, którą planuje się szerzej wykorzystać, by oddać turystom do dyspozycji więcej miejsc w środkach transportu zbiorowego (pomimo pandemii znakomita większość Japończyków nie pracuje obecnie z domu). W związku z tymi obawami Japonii warto przyjrzeć się bliżej statusowi tego państwa w dziedzinie bezpieczeństwa cybernetycznego oraz, przy okazji, przypomnieć kilka głośnych cyberataków, jakie wydarzyły się w tym kraju i przeanalizować widoczne trendy.

Według estońskiego rankingu National Cyber Security Index (NCSI)[6], który mierzy ogólny poziom cyberbezpieczeństwa, stopień przygotowania do walki z zagrożeniami w cyberprzestrzeni oraz gotowość do zarządzania dużymi incydentami i kryzysami na dużą skalę, Japonia jest na 31 miejscu w świecie (dane na listopad 2018 r.)[7]. Najwięcej punktów przyznano Japonii za rozwijanie polityki dotyczącej cyberbezpieczeństwa, ochronę podstawowych usług, ochronę danych osobowych oraz legislację dotyczącą cyberprzestępczości. Najsłabiej oceniono przygotowanie cybernetyczne Japońskich Sił Samoobrony. Warto porównać miejsce Japonii ze Stanami Zjednoczonymi (miejsce 16), a przede wszystkim bezpośrednimi rywalami Japonii w cyberprzestrzeni – Rosją (miejsce 28) i Chinami (miejsce 80). Mimo że ranking analizuje 160 państw, nie ma danych dla Korei Północnej. Korea Południowa znalazła się na miejscu 34. Bardzo zaskakujące miejsca w rankingu przyznano państwom z Europy Środkowej i Wschodniej. Czechy, Estonia i Litwa zdobyły kolejno 2, 3 i 4 miejsce. Polska znalazła się na szóstej pozycji.

W innym rankingu, National Cyber Power Index 2020 (NCPI), opracowanym przez Belfer Center for Science and International Affairs na Uniwersytecie Harvarda i uwzględniającym 30 państw, Japonia znalazła się w pierwszej dziesiątce największych cyberpotęg świata, przed Australią (na 9 miejscu)[8]. Pierwsze miejsce zajęły Stany Zjednoczone, Chiny drugie, a Rosja czwarte. Estonia została umieszczona na czternastym miejscu, a Polska nie została w ogóle ujęta. Ranking Belfer Center opiera się na idei holistycznego pomiaru siły oddziaływania danego państwa w cyberprzestrzeni, analizując rozdźwięk między założeniami a realnymi możliwościami. Na ocenę składają się takie elementy jak: nadzór i obserwacja aktywności krajowej, podnoszenie poziomu cyberbezpieczeństwa w kraju, kontrola nad przestrzenią informacyjną, zbieranie danych wywiadowczych o państwach trzecich w cyberprzestrzeni, ekosystem biznesowy wokół cyberbezpieczeństwa, zdolności niszczenia albo blokowania infrastruktury cybernetycznej nieprzyjaciela oraz wyznaczanie międzynarodowych norm i standardów cyberbezpieczeństwa. Do tego zestawienia planowano również dodać element dotyczący wykorzystania kryptowalut (na przykład do finansowania operacji wywiadowczych albo obchodzenia sankcji), ale zrezygnowano z tego z powodu braku możliwości zebrania danych[9].

Pełniejszy obraz japońskiej sytuacji cyberbezpieczeństwa przedstawia obszerny i bardzo szczegółowy raport opracowany w 2020 roku w ETH w Zurychu[10] (który wart jest

zarekomendowania). Analizuje on drogę, jaką przeszła Japonia od 2000 roku, kiedy po raz pierwszy cyberbezpieczeństwo znalazło się w obszarze zainteresowania państwa. Raport wylicza kamienie milowe japońskiej drogi do bezpieczeństwa w cyberprzestrzeni, między innymi ustawę z 2000 roku, strategię bezpieczeństwa informacyjnego, trzy kolejne strategie dotyczące cyberbezpieczeństwa, a także szczegółowo analizuje jednostki i podmioty odpowiedzialne za cyberbezpieczeństwo w różnych działach administracji rządowej. Ogólne wnioski tej pracy są następujące: japoński system cyberbezpieczeństwa jest niespójny i fragmentaryczny, przede wszystkim brakuje współpracy między poszczególnymi agencjami i aktorami oraz międzyinstytucjonalnej koordynacji, co bardzo utrudnia sterowanie i ocenę skuteczności całego systemu z zewnątrz. Widoczna jest natomiast tendencja do tworzenia nowych ciał i struktur w ramach istniejących organizacji. Mimo wczesnego dostrzeżenia konieczności rozwijania potencjału w dziedzinie cyberbezpieczeństwa, systematycznych postępów oraz ożywionego dialogu i współpracy z innymi państwami, wydaje się, że Japonia nieco odstaje od wiodących graczy w tej dziedzinie. Ta obserwacja pokrywa się z odpowiedziami aż blisko 90 procent respondentów w 1794 japońskich firmach, którzy w ankiecie z sierpnia 2019 roku ocenili środki bezpieczeństwa cybernetycznego w swoim otoczeniu pracy jako niewystarczające[11].

Warto dodać, że nie bez wpływu na średnią efektywność japońskich działań w dziedzinie cyberbezpieczeństwa mogą być czynniki takie jak: stosunkowo duży poziom zbiurokratyzowania struktur państwowych i firm prywatnych, starzenie się społeczeństwa (brakuje specjalistów w każdej branży i cyberbezpieczeństwo nie jest tu wyjątkiem; japońskie siły cybernetyczne do marca 2021 będą liczyć w sumie 290 osób[12], podczas gdy Chiny mają nawet o dwa rzędy wielkości więcej). Problemem jest również niedostateczna znajomość języka angielskiego wśród osób z wykształceniem technicznym oraz kadry urzędniczej[13]. Pewne znaczenie mogą mieć tutaj także kwestie bezpośrednio wynikające z tzw. japońskiego modelu gospodarczego. Przede wszystkim są to: skoncentrowanie większości innowacji w dużych firmach, preferowanie kształtowania sylwetki pracownika od początku do końca (unikanie specjalizacji) i niedostatek silnego w porównaniu do całości gospodarki ekosystemu start-upów[14], charakterystycznego dla państw takich jak Stany Zjednoczone, Izrael czy Estonia, a rosnącego przede wszystkim dzięki nieskrępowanemu działaniu ambitnych jednostek i ponoszeniu osobistego ryzyka na wolnym rynku. Wciąż

mocno oparta na zasadach starszeństwa i formalnej dyscypliny japońska kultura biznesowa i organizacyjna zwyczajnie nie sprzyja takim innowacjom[15], chociaż i w tym obszarze sytuacja powoli się zmienia.

Niedostatki japońskiego przygotowania w dziedzinie cyberbezpieczeństwa (zarówno na poziomie sektora publicznego jak i prywatnego) obnażają cyberataki. W czerwcu 2015 roku zaatakowano serwery JPS (Japan Pension Service; odpowiednik ZUS) i wykradziono dane dotyczące 1,25 mln obywateli (zmusiło to instytucję do wymiany wszystkich numerów identyfikacyjnych dotyczących poszkodowanych osób)[16]. W listopadzie 2016 roku prawdopodobnie chińscy hakerzy uzyskali nieuprawniony dostęp do sieci Japońskiej Federacji Biznesu (Keidanren; organizacja skupiająca kilkaset największych firm, pełniąca funkcje nieoficjalnego ministerstwa gospodarki), w wyniku którego wyciekły niejawne informacje[17]. W grudniu 2018 japońskie Ministerstwo Spraw Zagranicznych podało, że wykryto ataki na firmy prywatne i instytucje akademickie[18]. O ich dokonanie podejrzewa się chińskich hakerów z grupy APT10. Ataki spotkały się z potępieniem społeczności międzynarodowej, czyli przyniosły Japonii straty wizerunkowe. Oprócz tego w maju 2020 podano do wiadomości publicznej, że japońskie Ministerstwo Obrony bada kwestię cyberataku na Mitsubishi Electric Corporation, który doprowadził do zdobycia tajnych informacji prawdopodobnie na temat zasięgu, napędu i wytrzymałości cieplnej ponaddźwiękowego pocisku nowej generacji[19]. Ofiarami ataków padały również setki innych przedsiębiorstw, zmuszone do płacenia okupów na łączną kwotę kilkudziesięciu milionów dolarów. Najgłośniejszy taki przypadek z zeszłego roku dotyczy jeden z firm z branży gier wideo, od której (nieskutecznie) próbowano wymusić haracz około 10 mln dolarów za zwrot 350 tysięcy skradzionych, poufnych dokumentów (o przestępstwo podejrzewana jest grupa hakerów z Rosji)[20]. Ponadto, tylko w zeszłym roku kilkanaście dużych japońskich firm zostało zainfekowanych złośliwym oprogramowaniem i ransomware.

Oprócz ataków obliczonych na ośmieszenie państwa lub szpiegostwo albo zwykłych wyłudzeń od firm prywatnych, dokonywano w Japonii również cyberprzestępstw o znaczeniu międzynarodowym. Przede wszystkim chodzi tutaj o zhakowanie jednej z pierwszych i największej ówcześnie giełdy kryptowalutowej Mt. Gox w lutym 2014 roku (jeszcze przed pierwszą bańką kryptowalut), przez co skradziono Bitcoiny wyceniane w tym

czasie na 460 mln dolarów[21]. Podobny atak w 2018, na inną japońską giełdę – Coincheck – doprowadził do kradzieży kryptowalut o wartości przekraczającej 500 mln dolarów[22]. Kwestia kryptowalut jest tutaj istotna, ponieważ to, co w przeszłości dotyczyło jedynie właścicieli giełd kryptowalut (w 2014 roku jeszcze nieuregulowanych w Japonii) i stosunkowo niewielkiego grona ich użytkowników, w niedalekiej przyszłości mogłoby przytrafić się największym japońskim bankom, gdyż przynajmniej jeden z nich planował i być może nadal planuje wejść na rynek z własną kryptowalutą[23]. Można więc wyobrazić sobie sytuację, że straty wywołane kradzieżą kryptowaluty wywołałyby run na bank i wyprowadzenie depozytów w walucie państwowej.

Wnioski

Niezależnie od tego, czy Japonia powinna obawiać się cyberataku podczas Igrzysk Olimpijskich, znaczenie cyberbezpieczeństwa w tym państwie (podobnie jak na całym świecie) będzie bardzo szybko rosło. Japonia ze względu na sąsiedztwo Chin i Korei Północnej, a także Rosji oraz sojusz ze Stanami Zjednoczonymi i swoją pozycję gospodarczą, jest częstym celem cyberataków. Pod wieloma względami (kwestie instytucjonalne i organizacyjne oraz braki kadrowe) nie jest ona w stanie dostatecznie zapobiegać wszystkim próbom nieuprawnionego dostępu. Częściowo może to wynikać jednak nie ze słabości jako takiej, ale faktu, że musi mierzyć się z najsilniejszymi przeciwnikami. Radykalne zwiększenie potencjału Japonii w tej dziedzinie będzie wymagać napływu specjalistów i know-how z zewnątrz. W kontekście japońskich obaw związanych z Rosją, warto tu dostrzec własny, niemały potencjał państw Europy Środkowej i Wschodniej (Czechy, Estonia, Litwa, Polska, Ukraina) i podjąć próby współpracy z Japonią, na przykład przeprowadzając wspólne ćwiczenia. Od kilku lat Japonia blisko współpracuje w dziedzinie cyberbezpieczeństwa i technologii informatycznych z Estonią, co może oznaczać, że będzie otwarta na wymianę doświadczeń również z innymi zaprzyjaźnionymi państwami o podobnym do Estonii potencjale.

Konrad Rumiński – analityk ds. Japonii w Ośrodku Badań Azji

[1] Ze względu na pandemię igrzyska zostały przełożone z 2020 na 2021 r.
Olympic Games postponed to 2021, Tokyo 2020, 24.03.2020, https://tokyo2020.org/en/news/joint-statement-from-international-olympic-committee-and-tokyo2020 [dostęp: 24.01.2021].
[2] Nicole Perlroth, *Cyberattack Caused Olympic Opening Ceremony Disruption*, The New York Times, 02.12.2018, https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html [dostęp: 24.01.2021].
[3] Naveen Goud, *Japan issues Cyber Threat warning to Tokyo 2020 Olympics and Paralympics*, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/japan-issues-cyber-threat-warning-to-tokyo-2020-olympics-and-paralympics/ [dostęp: 24.01.2021].
[4] Patrick Wintour, Julian Borger, Justin McCurry, *Russia planned cyber-attack on Tokyo Olympics, says UK*, The Guardian, 20.10.2020, https://www.theguardian.com/world/2020/oct/19/russia-planned-cyber-attack-on-tokyo-olympics-says-uk [dostęp: 24.01.2021].
[5] *Hackers trained by Tokyo Olympics organizers to fight cyberattacks*, Kyodo News, 04.01.2021, https://english.kyodonews.net/news/2021/01/f7bff5ba1369-hackers-trained-by-tokyo-olympics-organizers-to-fight-cyberattacks.html [dostęp: 24.01.2021].
[6] *The National Cyber Security Index ranks 160 countries' cyber security status*, E-Estonia, maj 2020, https://e-estonia.com/the-national-cyber-security-index-ranks-160-countries-cyber-security-status/ [dostęp: 24.01.2021].
[7] *NCSI - Japan*, e-Governance Academy Foundation Company, https://ncsi.ega.ee/country/jp/ [dostęp: 24.01.2021].
[8] Bruce Sussman, *Top 10 Most Powerful Countries in Cyberspace*, Secureworld, 10.09.2020, https://www.secureworldexpo.com/industry-news/top-10-most-powerful-countries-in-cyberspace [dostęp: 24.01.2021]
[9] Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, Anina Schwarzenbach, *National Cyber Power Index 2020*, Harvard Kennedy School Belfer Center for Science and International Affairs, wrzesień 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf [dostęp: 24.01.2021].
[10] Stefan Soesanto, *Japan's National Cybersecurity and Defense Posture*, CSS ETH Zurich, wrzesień 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf [dostęp: 24.01.2021].
[11] Yasuhiro Nabei, *Information Security as a Management Strategy in the DX Era*, NRI, 21.08.2019, https://www.nri.com/en/journal/2019/0821 [dostęp: 24.01.2021].
[12] Daishi Abe, *Lagging China and the US, Japan to beef up cyberdefense*, Nikkei Asia, 20.06.2020, https://asia.nikkei.com/Politics/Lagging-China-and-the-US-Japan-to-beef-up-cyberdefense [dostęp: 24.01.2021].
[13] *Engineers must have English skills to succeed*, Japan Times Forum on English Education/ Laurence Anthony's Website, 05.10.2009,https://www.laurenceanthony.net/research/japan_times/japan_times_disc_20091005.pdf [dostęp: 24.01.2021].
[14] Anthony Joh, *Tokyo-based podcaster explains Japan's declining startup scene and its future*, Tech in Asia, 21.07.2017, https://www.techinasia.com/talk/japan-declining-startup-scene-future [dostęp: 24.01.2021].
[15] *The big reason Japanese companies can't innovate*, Disrupting Japan, 12.11.2019, https://www.disruptingjapan.com/the-big-reason-japanese-companies-cant-innovate/ [dostęp: 24.01.2021].
[16] Tomoko Otake, *1.25 million affected by Japan Pension Service hack*, The Japan Times, 01.06.2015, https://www.japantimes.co.jp/news/2015/06/01/national/crime-legal/japan-pension-system-hacked-1-25-million-cases-personal-data-leaked/ [dostęp: 24.01.2021].
[17] *China hackers likely attacked Japan business lobby in 2016*: experts, Kyodo News, 13.01.2019, https://english.kyodonews.net/news/2019/01/4354ae41b20d-china-hackers-likely-attacked-japan-business-lobby-in-2016-experts.html [dostęp: 24.01.2021].
[18] *Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga*), Ministerstwo Spraw Zagranicznych Japonii, 21.12.2018, https://www.mofa.go.jp/press/release/press4e_002281.html [dostęp: 24.01.2021].
[19] Kevin Buckland, Christopher Cushing, *Japan defence ministry investigating potential hack of next-gen missile details: Asahi*, Reuters, 20.05.2020, https://www.reuters.com/article/us-mitsubishi-elec-cyber/japan-defence-ministry-investigating-potential-hack-of-next-gen-missile-details-asahi [dostęp: 24.01.2021].

[20] Thisanka Siripala, *Japanese Companies Fall Victim To Unprecedented Wave of Cyber Attacks*, The Diplomat, 23.12.2020, https://thediplomat.com/2020/12/japanese-companies-fall-victim-to-unprecedented-wave-of-cyber-attacks/ [dostęp: 24.01.2021].
[21] Andy Greenberg, *Bitcoin's Price Plummets As Mt. Gox Goes Dark, With Massive Hack Rumored*, Forbes, 25.02.2014, https://www.forbes.com/sites/andygreenberg/2014/02/25/bitcoins-price-plummets-as-mt-gox-goes-dark-with-massive-hack-rumored/ [dostęp: 24.01.2021].
[22] *How to Steal $500 Million in Cryptocurrency*, Fortune/Bloomberg, 31.01.2018, https://fortune.com/2018/01/31/coincheck-hack-how/ [dostęp: 24.01.2021].
[23] David Pan, *Japan's Banking Giant MUFG Plans to Launch Blockchain Payment Network in 2021*, Coindesk, 20.11.2020, https://www.coindesk.com/japans-banking-giant-mufg-plans-to-launch-blockchain-payment-network-in-2021 [dostęp: 24.01.2021].

Asia Research Centre Commentary
Centre for Security Studies
War Studies University
January 20, 2021

Japan fears cyberattack during the Olympic Games

Konrad Rumiński

Japan fears that it could become a victim of a cyberattack that would come from Russia or another country (such as China or North Korea) during the postponed Tokyo Olympics. This fear stems not only from experiences of other nations (such as the cyberattack that occurred during the opening of the 2018 Winter Olympics in Pyoengchang), but also from Japan's own perception of its cybersecurity capabilities which Tokyo considers insufficient. Inefficient coordination and fragmentation within the network of actors involved protecting Japan's cyberspace are some of main problems of the country's cybersecurity system. Other factors related to its traditional economic model as well as aging population, which causes staff shortages, also have an impact on the cybersecurity situation in the country. Cyberattacks conducted in recent years have revealed the shortcomings of Japan's preparedness in this regard. Millions of dollars were lost because of major attacks targeting companies, these have also affected the country's international image. Even in recent months, suspicious activities have been observed, which may indicate that the Japanese infrastructure has been penetrated by third parties in an effort to gain unauthorised access. Some of the factors affecting Japan's exposure to this type of activities include its geographical proximity to China, Russia and North Korea, Tokyo's alliance with the US and Japan's economic position. If Japan wants to seriously improve its cybersecurity standing, such an effort will require an influx of foreign specialists and know-how. Moreover, because Japan and Central and Eastern European states share some Russia-related fears, it might be beneficial for them to boost cooperation in the field of cybersecurity.