Security, Economy & Law
Nr 3/2017 (XVI), (100–108)
DOI 10.24356/SEL/16/6

RELACJE CHIN I STANÓW ZJEDNOCZONYCH W CYBERPRZESTRZENI

CHINA-UNITED STATES RELATIONS IN CYBERSPACE

Robert WYDRA
Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego
„Apeiron" w Krakowie

Abstract

The governments of China and United States of America have varying views about the internet. This also includes the way society shout have access to it. These differences are fundamental and rooted in different cultural and political systems. The internet is also a place where those countries can – not always in a legal manner – gain advantage on the world stage. The article's author tries to present China-U.S. relations in the cyberspace.

Key words: Cybersecurity, USA, China, cyberspace, cyberespionage

Abstrakt

Rządy Chin i Stanów zjednoczonych cechują odmienne podejścia do kwestii sieci Internet, w tym dostępu społeczeństwa do niej. Różnice te są fundamentalne i wynikają z zupełnie różnych systemów kulturalnych i politycznych. Sieć jest też dla obu krajów miejscem, gdzie mogą, nie zawsze w sposób legalny, uzyskać informacje pozwalające zdobyć przewagę na arenie międzynarodowej. Autor artykułu stara się przestawić wzajemne relacje Chin i Stanów Zjednoczonych w cyberprzestrzeni.

Słowa kluczowe: Cyberbezpieczeństwo, Stany Zjednoczone, Chiny, cyberprzestrzeń, cyberszpiegostwo

Sieć internetowa stała się nieodłączną częścią życia większości mieszkańców cywilizowanego świata. Zgodnie z informacjami opublikowanymi przez Międzynarodowy Związek Telekomunikacyjny, w roku 2015 korzystało z niego 3,2 miliarda ludzi. Nawet w najmniej rozwiniętych krajach świata, takich jak Somalia czy Nepal korzysta z niego ponad 9% populacji[1]. Wraz z popularyzacją takich urządzeń jak smartfony czy tablety, urządzenia podłączone do Internetu stają się częścią życia coraz większej liczby ludzi.

Krajem z największą liczbą użytkowników Internetu są Chiny – jest ich tam ponad 710 milionów[2]. Stanowi to 53,2% populacji tego kraju. Stany zjednoczone plasują się w tym rankingu dopiero na trzecim miejscu (za Indiami) z 245 milionami użytkowników, co jednak stanowi aż 76% ich populacji[3].

Rządy Chin i Stanów zjednoczonych cechują odmienne podejścia do kwestii samej sieci internetowej i dostępu społeczeństwa do niego. Różnice te są fundamentalne i wynikają z zupełnie innych systemów kulturalnych i politycznych. Stany zjednoczone opowiadają się za otwartym, interoperacyjnym, bezpiecznym i niezawodnym Internetem[4]. Są przeciwne oddaniu go pod kontrolę państw lub organizacji międzynarodowych, zamiast tego promują ideę globalnej sieci jako miejsca, gdzie nie ma miejsca na cenzurę lub inne formy ograniczania wolności słowa. Kraj ten jest najstarszą nowożytną demokracją świata i wartości, które leżą u jego fundamentów próbuje też przenieść do cyberprzestrzeni. W Chinach, których ustrój jest daleki od standardów demokratycznych państwo stara się ściśle kontrolować treści do jakich dostęp mają jego obywatele. Zgodnie z obowiązującym tam prawem tzw. „great firewall" dba o to, aby obywatele korzystający z sieci internetowej pozostali na ścieżce ściśle wytyczonej przez rząd[5]. System filtrów i routerów uniemożliwia dostęp do treści, które ten uznał za niewłaściwe.

[1] Internet used by 3.2 billion people in 2015, http://www.bbc.com/news/technology-32884867 (dostęp 10.09.2017).

[2] China's internet users total 710 million, http://www.chinadaily.com.cn/business/tech/2016-08/04/content_26345610.htm (dostęp 10.09.2017).

[3] Individuals using the Internet (% of population), https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2016&locations=CN-US&start=1995 (dostęp 10.09.2017).

[4] International Strategy for Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (dostęp 10.09.2017).

[5] I. Bremmer, *Democracy in Cybespace. What Information Technology Can and Cannot Do*, "Foreign Affairs" 2010, Vol. 89, nr 6, s. 93

Różnice między oboma krajami sięgają głębiej i dotyczą także kwestii tego kto ma sprawować kontrolę nad infrastrukturą sieci Internet oraz procesami standaryzacji jego elementów. Rząd w Waszyngtonie należy do jednego z największych promotorów podejścia, że Internet i jego zasoby powinny być kontrolowane przez prywatne przedsiębiorstwa oraz podmioty niepaństwowe – tak jak ma to miejsce obecnie. Każda z prób oddania kontroli nad Internetem organizacjom międzynarodowym, jak np. Międzynarodowy Związek Telekomunikacyjny, wywołuje sprzeciw Stanów Zjednoczonych[6]. Chińczycy podchodzą do kwestii kontroli nad siecią w sposób odmienny. W roku 2011 rząd Chin podjął próbę przeforsowania na forum ONZ *Międzynarodowego kodeksu postępowania w zakresie bezpieczeństwa informacji*[7]. W dokumencie tym znalazły się kontrowersyjne zapisy, takie jak ten mówiący o ochronie cyberprzestrzeni przed napływem informacji, które mogły by zostać uznane za potencjalnie szkodliwe.

Pierwszy poważny przypadek konfrontacji w cyberprzestrzeni na linii Chiny-USA ma związek z incydentem do jakiego doszło 1 kwietnia 2001 roku w pobliżu wysp Paracelskich. Operujący w tym regionie samolot rozpoznania radioelektronicznego EP-3 zderzył się z chińskim samolotem myśliwskim J-8II. W wyniku zdarzenia śmierć poniósł pilot myśliwca a załoga samolotu rozpoznawczego została zmuszona do awaryjnego lądowania na wyspie Hainan. 24-osobowa załoga amerykańskiego samolotu została aresztowana i zwolniona dopiero po 10 dniach[8]. W trakcie incydentu i krótko po nim ponad 100 stron rządowych (w domenie .gov) oraz komercyjnych (w domenie .com) padło ofiarą ataku DoS[9] [10]. Źródło ataku znajdowało się w Chinach i przy stopniu kontroli jaki Państwo Środka sprawuje nad swoją infrastrukturą sieciową trudno, aby taka akcja odbyła się bez wiedzy rządzących. Ataki te miały najprawdopodobniej na celu

[6] A. Segal, *Chinese Computer Games: Keeping Safe in Cyberspace*, "Foreign Affairs" 2012, Vol. 91, nr 2, s.70

[7] *China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations*, http://nz.chineseembassy.org/eng/zgyw/t858978.htm (dostęp 11.09.2017).

[8] *US: it was the Chinese pilot's fault*, https://www.theguardian.com/world/2001/apr/13/china (dostęp 11.09.2017).

[9] DoS czyli Denial of Service – atak polegający na przeciążeniu serwera dużą ilością zapytań aż ten przestanie odpowiadać.

[10] *Cyber Protests: The Threat to the U.S. Information Infrastructure*, http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.pdf, s. 3 (dostęp 11.09.2017).

przetestowanie ważnych sieci komputerowych w USA i ich ochrony oraz zbadanie reakcji rządu amerykańskiego na podobny atak. Zaatakowane systemy komputerowe wykazały marną odporność na atak, skutkował on uniemożliwieniem dostępu do prawie wszystkich zaatakowanych stron internetowych. Administracja George'a W. Busha nie zareagowała w żaden sposób na ataki przeprowadzone przez chińskich hakerów[11]. Świadczy to o jej nieprzygotowaniu na podobny rodzaj zagrożenia.

Kolejny poważny incydent miał miejsce w latach 2003 – 2005. W tym czasie chińscy informatycy przeprowadzili operację o nazwie „Titan Rain". W odróżnieniu od ataków DoS przeprowadzonych w roku 2001 jest ona przykładem zorganizowanej akcji szpiegostwa w cyberprzestrzeni. Przez dwa lata na komputerach m.in. amerykańskich agencji rządowych, przedsiębiorstw z sektora obronnego i kosmicznego oraz laboratoriów badań jądrowych aktywne było złośliwe oprogramowanie przekazujące wrażliwe dane do Chin. W trakcie tego ataku wykraść udało się m.in. plany myśliwca V generacji Lockheed Martin F-35 Lightning II czy plany systemów obrony przeciwrakietowej[12].

Już rok później rozpoczęła się kolejna operacja szpiegowska w Internecie, określona kryptonimem „Shady RAT". Trwała ona aż do roku 2011. Celem tych cyberataków były amerykańskie firmy zbrojeniowe, Organizacja Narodów Zjednoczonych, Międzynarodowy Komitet Olimpijski oraz międzynarodowe korporacje[13]. Złośliwe oprogramowanie umieszczone przez hakerów w zaatakowanych systemach komputerowych pozostawało więc niewykryte przez wiele lat.

Barack Obama po objęciu urzędu Prezydenta Stanów Zjednoczonych uczynił z cyberbezpieczeństwa priorytet dla bezpieczeństwa narodowego swojego kraju[14]. Mimo podjętych działań, nie udało się powstrzymać działań Chińskich hakerów w sieci Internet. Aby przeciwdziałać wynikającym z tego zagrożeniom powołane zostało U.S. Cyber Command podległe Dowództwu Sił Strategicznych. Jednym z celów tej instytucji jest podniesienie poziomu bezpieczeństwa amerykańskich sieci wojskowych.

[11] R. Stiennon, *Surviving Cyberwar,* The Scarecrow Press, Toronto 2010, s. 14

[12] Ibidem, s. 2

[13] *Revealed: Operation Shady RAT*, http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf (dostęp 12.09.2017).

[14] *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (dostęp 12.09.2017).

Działania kolejnego prezydenta Stanów Zjednoczonych zdały się przynieść czasowy skutek, lecz już w 2011 roku dokonane zostało włamanie do amerykańskiego przedsiębiorstwa RSA. Firma ta zajmuje się dostarczaniem rozwiązań z zakresu cyberbezpieczeństwa a jej generatory kodów (tokeny) są de facto standardem w zakresie autentykacji użytkowników w sieciach korporacyjnych, bankowości internetowej i sieciach organizacji rządowych. Dane uzyskane w czasie tego ataku nie umożliwiły uzyskania haseł dostępu do systemów klientów firmy RSA, ale mogły zawierać informacje na temat sposobów zabezpieczeń stosowanych w kluczowych amerykańskich instytucjach[15].

Amerykańska firma Madiant, zajmująca się cyberbezpieczeństwem, opublikowała w 2013 roku raport zatytułowany *Exposing One of China's Cyber Espionage Unit*. Dokument ten stanowił zwieńczenie sześciu lat badań ataków dokonanych na sieci amerykańskich firm i agencji rządowych. Stwierdza on, że za znaczną liczbę ataków odpowiada jednostka nr 61398 Chińskiej Armii Ludowo-Wyzwoleńczej. Ma ona być głównym organem armii chińskiej odpowiedzialnym za działania szpiegowskie w sieci Internet[16]. Dokument ten był pierwszym bezpośrednim oskarżeniem władz Chin o działania z zakresu szpiegostwa internetowego.

W maju tego samego roku „The Washington Post" ujawnił fakt, że doszło do kolejnego skutecznego ataku na firmy zbrojeniowe i instytucje rządowe. Hakerzy, zgodnie z raportem Defence Science Board – organu doradczego amerykańskiego Departamentu Obrony, uzyskali dostęp do informacji na temat myśliwców Lockheed Martin F-35, McDonnell Douglas F/A-18, śmigłowców Sikorsky UH-60 Black Hawk, samolotu pionowego startu i lądowania Bell Boeing V-22 Osprey, systemów walki radioelektronicznej oraz systemów obrony przeciwrakietowej Patriot PAC-3, THAAD i Aegis[17]. Raport nie wskazuje wprost na Chińczyków, jednak w kontekście wcześniejszych ataków mających na celu wykradzenie danych dotyczących nowoczesnych systemów wojskowych oraz zasobów wymaganych do przeprowadzenia podobnego ataku, udział Państwa Środka w tym incydencie

[15] *Anatomy of an Attack*, https://blogs.rsa.com/anatomy-of-an-attack/ (dostęp 12.09.2017).

[16] *APT1 Exposing One of China's Cyber Espionage Units*, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (dostęp 12.09.2017).

[17] E. Nakashima, *Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies*, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html (dostęp 12.09.2017).

wydaje się być wysoce prawdopodobny. Szczególnie interesujące dla strony chińskiej wydają się być informacje na temat współczesnych i przyszłych myśliwców pokładowych (F/A-18, F-35), samolotów V-22 wykorzystywanych przez U.S. Navy i U.S. Marine Corps oraz morskiego systemu walki Aegis, wykorzystywanego do osłony m.in. lotniskowcowych grup uderzeniowych. Są to systemy uzbrojenia, które zostałyby wykorzystane w potencjalnym konflikcie między Stanami zjednoczonymi a Chinami. Marynarka wojenna Stanów Zjednoczonych kładzie szczególny nacisk na obronę swoich okrętów przed pociskami typu cruise oraz pociskami balistycznymi[18]. Uzyskane informacje pozwalają jednak na opracowanie skutecznych sposobów przełamywania takiej obrony. Stanowi to duże zagrożenie dla amerykańskich okrętów operujących w rejonie Pacyfiku.

Administracja Baracka Obamy opublikowała w 2013 roku dokument opisujący strategię walki ze szpiegostwem internetowym – *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*[19]. Kładzie on nacisk na szpiegostwo przemysłowe, także to dokonywane za pomocą narzędzi informatycznych. Wśród sposobów walki z kradzieżą własności intelektualnej wymienia się w nim:

– Zwiększenie współpracy z partnerami współdzielącymi interesy handlowe ze Stanami Zjednoczonymi, w celu promocji ochrony tajemnicy handlowej oraz powstrzymania handlu dobrami i usługami zwierającymi wykradzione tajemnice handlowe.
– Lokalizowanie i usuwanie luk w mechanizmach ochrony tajemnicy handlowej za pomocą dostępnych narzędzi.
– W ramach negocjowanych umów handlowych, takich jak *Trans Pacific Partnership*, inne kraje zostaną zobowiązane do wdrożenia mechanizmów ochrony tajemnicy handlowej podobnych do tych obecnych w prawie amerykańskim.
– Położenie nacisku na ochronę tajemnicy handlowej w ramach dwustronnych, regionalnych i wielostronnych dyskusji na temat handlu.

W marcu 2013 roku amerykański Kongres uchwalił ustawę mającą na celu ograniczenie ryzyka związanego z zakupami chińskiego sprzętu

[18] *AIR–SEA BATTLE Service Collaboration to Address Anti-Access & Area Denial Challenges*, http://navylive.dodlive.mil/files/2013/06/ASB-26-June-2013.pdf, s. 3 (dostęp 13.09.2017).

[19] *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, https://www.justice.gov/criminal-ccips/file/938321/download (dostęp 13.09.2017).*

i oprogramowania, mogącego zawierać złośliwe oprogramowanie lub backdoory[20]. Ustawa ta zabrania NASA oraz departamentom Handlu i Sprawiedliwości zakupów w.w. dóbr bez uzyskania stosownego zezwolenia ze strony FBI[21]. Ustawa ta mówi wprost o sprzęcie, który został wyprodukowany lub złożony przez przedsiębiorstwa zarządzane lub subsydiowane przez Chiny. Fakt ten stanowi o zmianie sposobu myślenia o cyberbezpieczeństwie w administracji amerykańskiej. Wcześniej skupiano się głównie na oprogramowaniu, jednak od tego czasu zaczęto też interesować się sprzętem, na którym to oprogramowanie jest uruchamiane.

Do kolejnego spektakularnego ataku na instytucje rządu Stanów Zjednoczonych doszło w roku 2015. W czerwcu tego roku administracja Baracka Obamy ujawniła, że z *Office of Personal Management*, agencji posiadającej informacje na temat każdego pracownika zatrudnionego przez rząd Stanów Zjednoczonych wykradziono dane o 4 milionach osób[22]. Amerykanie oskarżyli o te działania Chiny, które stanowczo temu zaprzeczyły. Według oficjalnych komentarzy pracowników administracji amerykańskiej, działanie to miało na celu zdobycie bazy danych osób, które następnie będą inwigilowane w tradycyjny sposób.

Nie tylko Chiny są agresorem w przypadku ujawnionych cyberataków. Często to chińskie instytucje i przedsiębiorstwa padają ofiarą hakerów. Władze w Pekinie wielokrotnie oskarżały amerykańskich hakerów o działalność na szkodę chińskich firm i instytucji. Doszło do tego, że chińskie Ministerstwo Obrony przedstawiło dane mające świadczyć o tym, że 2/3 cyberataków na cele w tym kraju pochodzi z terenu Stanów Zjednoczonych[23].

Władze w Chinach wyraziły też swoje oburzenie faktem, że zgodnie z publikacją dziennika „The Guardian", prezydent Brack Obama podpi-

[20] Backdoor – luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania.

[21] A. Selyukh, *U.S. law to restrict government purchases of Chinese IT equipment*, http://www.reuters.com/article/us-usa-cybersecurity-espionage/u-s-law-to-restrict-government-purchases-of-chinese-it-equipment-idUSBRE92Q18O20130328 (dostęp 13.09.2017).

[22] A. Griffin, *OPM hack: as China blames US for huge cyberattack, new era of cyberwarfare and internet terrorism arrives*, http://www.independent.co.uk/life-style/gadgets-and-tech/news/opm-hack-as-china-blames-us-for-huge-cyberattack-new-era-of-cyber warfare-and-internet-terrorism-10299003.html (dostęp 14.09.2017)

[23] A. Toor, *China blames US for majority of cyberattacks on military websites,* https://www.theverge.com/2013/2/28/4039300/china-says-us-is-responsible-for-hacks-on-defense-websites (dostęp 13.09.2017).

sał tajną dyrektywę nakazującą utworzenie niejawnej listy celów na całym świecie wobec których można by było przeprowadzić cyberataki. Ataki te miały by służyć promowaniu interesów Stanów Zjednoczonych poza granicami swego kraju[24]. Zgodnie z informacjami ujawnionymi przez dziennik, ataki te nie zostały przeprowadzone, lecz sam fakt przygotowań do nich wzbudził zaniepokojenie rządu w Pekinie.

Mimo zasadniczych różnic w kwestii Internetu – od kontroli treści po próby oddania go pod kontrolę państwową i mimo wzajemnych oskarżeń o cyberszpiegostwo czy ataki DoS, Stany Zjednoczone i Chiny starają się nawiązać nić porozumienia w kwestii współpracy w cyberprzestrzeni. Pierwszym przykładem poważnego działania w tym zakresie było wspólne zobowiązanie prezydentów Stanów Zjednoczonych Baracka Obamy i Chin Hu Jintao do poprawienia relacji między oboma krajami, w tym w sferze sieci Internet. Deklaracja ta padła po rozmowach, które obaj prezydenci odbyli w roku 2011.

Bibliografia

1. Bremmer I., *Democracy in Cybespace*. What Information Technology Can and Cannot Do, "Foreign Affairs" 2010, Vol. 89, nr 6.
2. Segal A., *Chinese Computer Games: Keeping Safe in Cyberspace*, "Foreign Affairs" 2012, Vol. 91, nr 2.
3. Stiennon R., *Surviving Cyberwar*, The Scarecrow Press, Toronto 2010.
4. http://www.bbc.com/news/technology-32884867 (dostęp 10.09.2017).
5. http://www.chinadaily.com.cn/business/tech/2016-08/04/content_26345610.htm (dostęp 10.09.2017).
6. https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2016&locations=CN-US&start=1995 (dostęp 10.09.2017).
7. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (dostęp 10.09.2017).
8. http://nz.chineseembassy.org/eng/zgyw/t858978.htm (dostęp 11.09.2017).
9. https://www.theguardian.com/world/2001/apr/13/china (dostęp 11.09.2017).
10. http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.pdf, s. 3 (dostęp 11.09.2017).
11. http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf (dostęp 12.09.2017).

[24] *Obama orders US to draw up overseas target list for cyber-attacks*, https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas (dostęp 13.09.2017)

12. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (dostęp 12.09.2017).
13. https://blogs.rsa.com/anatomy-of-an-attack/ (dostęp 12.09.2017).
14. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (dostęp 12.09.2017).
15. https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html (dostęp 12.09.2017).
16. http://navylive.dodlive.mil/files/2013/06/ASB-26-June-2013.pdf, s. 3 (dostęp 13.09.2017).
17. https://www.justice.gov/criminal-ccips/file/938321/download (dostęp 13.09.2017).
18. http://www.reuters.com/article/us-usa-cybersecurity-espionage/u-s-law-to-restrict-government-purchases-of-chinese-it-equipment-idUSBRE92Q18O20130328 (dostęp 13.09.2017).
19. https://www.theverge.com/2013/2/28/4039300/china-says-us-is-responsible-for-hacks-on-defense-websites (dostęp 13.09.2017).
20. http://www.independent.co.uk/life-style/gadgets-and-tech/news/opm-hack-as-china-blames-us-for-huge-cyberattack-new-era-of-cyber warfare-and-internet-terrorism-10299003.html (dostęp 14.09.2017).
21. https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas (dostęp 13.09.2017).

mgr Robert Wydra – student Wyższej Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, absolwent Wyższej Szkoły Bankowej w Poznaniu oraz Polsko-Japońskiej Akademii Technik Komputerowych, pracuje na stanowisku Demo Solutions Specialist w firmie SAP Polska.