# Wpływ szpiegostwa internetowego na stosunki między USA a Chinami

Michał Grzelak

Bezpieczeństwo cyberprzestrzeni od pewnego czasu dominuje dyskusję na temat współczesnych zagrożeń. Wśród metod przeciwdziałania cyberzagrożeniom wymienia się konieczność międzynarodowej współpracy, która w praktyce pozostaje ograniczona. Wydarzenia ostatnich miesięcy – liczne doniesienia dotyczące inwigilacji i szpiegostwa – podsyciły dyskusję nad koniecznością uregulowania działalności państw w cyberprzestrzeni. Głównymi aktorami tego teatru działań są Stany Zjednoczone i Chiny. USA stosują kontrowersyjne metody gromadzenia poufnych danych, jednak otwarcie oskarżają ChRL o infiltrowanie amerykańskich sieci i kradzież własności intelektualnej. Chiny odpierają oskarżenia i nawołują do współpracy utrzymując, że też są ofiarą zagranicznych hakerów.

Bezpieczeństwo cyberprzestrzeni jest w ostatnich latach jedną z najczęściej dyskutowanych dziedzin bezpieczeństwa. Ochroną infrastruktury sieciowej, danych i użytkowników zajmują się prywatne przedsiębiorstwa, państwowe i międzynarodowe instytucje, organizacje non-profit i wiele innych podmiotów. Cyberprzestrzeń trafia do oficjalnych dokumentów – rezolucji, doktryn, strategii bezpieczeństwa oraz porozumień, a przedrostek „cyber" dołączany jest do wszelkich możliwych pojęć związanych z bezpieczeństwem. Zagrożeniem dla cyberprzestrzeni i jej użytkowników są cyberprzestępcy i cyberterroryści. Cyberaktywiści organizują cyberprotesty czy cyberdemonstracje[1], dzięki czemu udaje im się wpływać na realną politykę (co pokazały m.in. wydarzenia „arabskiej wiosny" oraz protesty związane z planami podpisania ACTA), a państwa tworzą oddziały cyberwojska[2] i cy-

[1] Cyberdemonstracja – nowe zjawisko będące wirtualnym odpowiednikiem aktu obywatelskiego nieposłuszeństwa. Rozmowa z szefem BBN Stanisławem Koziejem na temat kontrowersji w sprawie ACTA. 26 stycznia 2012 r. http://www.bbn.gov.pl/portal/pl/2/3650/Szef_BBN_dla_Super_Expressu_quotPrezydent_nie_wprowadzi_stanu_wojennegoquot.html (dostęp: 19 lipca 2013 r.).

[2] Niektóre państwa tworzą wojska obrony cybernetycznej, jako osobny rodzaj wojsk, obok sił lądowych, sił powietrznych czy marynarki wojennej.

berbronie, gotowe do użycia w cyberwojnach. Część wymienianych zagrożeń stanowi codzienność użytkowników globalnej sieci, którzy padają ofiarą coraz bardziej wymyślnych ataków przestępców działających w cyberprzestrzeni. Inne są na razie zagrożeniami teoretycznymi (z uwagi na problemy z ich dokładnym zdefiniowaniem), prowadzone są punktowo i na niewielką skalę (np. ataki na irańskie instalacje nuklearne) czy też zwyczajnie nie miały miejsca, czego przykładem jest cyberwojna. Część komentatorów terminem tym określa zajścia z Estonii w 2007 r. czy Gruzji w 2008 r. Faktem jest, że w obu przypadkach doszło do zmasowanych ataków (aktów cyberagresji) na infrastrukturę teleinformatyczną Estonii i Gruzji, w żadnym z nich nie udało się jednak zebrać dowodów potwierdzających bezpośrednie zaangażowanie rosyjskich władz w incydenty komputerowe[3].

Osobnym tematem są działania szpiegowskie prowadzone z wykorzystaniem cyberprzestrzeni. Naturalną funkcją tego środowiska jest przetwarzanie i wymiana informacji[4]. To właśnie dane zorganizowane w informacje są najcenniejszym zasobem cyberprzestrzeni. Zdecydowana większość przechowywanych informacji jest jawna, możliwa do odnalezienia, a także – w różnym zakresie – dozwolona do skopiowania i dalszego przetwarzania (używana np. na potrzeby białego wywiadu). Jednak z różnych powodów część informacji została sklasyfikowana jako wrażliwa (cywilne i wojskowe informacje niejawne, dane osobowe, tajemnice handlowe itp.), stąd dąży się do ograniczenia dostępu do nich. Dotarcie do tajemnic przechowywanych w cyfrowej postaci na dyskach komputerów jest celem cyberszpiegów, działających na zlecenie władz państwowych, prywatnych przedsiębiorstw, bądź organizacji[5].

Większość szkodliwych działań w cyberprzestrzeni ma charakter destrukcyjny – ich celem jest uszkodzenie, modyfikacja, całkowite zniszczenie lub ograniczenie dostępu do infrastruktury bądź przechowywanych informacji. Cele cyberprzestępców są zazwyczaj materialne, polegają na oszustwach i kradzieży pieniędzy. W związku z tym, nawet jeśli trudno

[3] *Estonia has no evidence of Kremlin involvement in cyber attacks*, RIA Novosti, 6 września 2007 r., http://en.rian.ru/world/20070906/76959190.html (dostęp: 11 czerwca 2013 r.).

[4] Ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, http://www.bbn.gov.pl/download/1/8238/Ustawa_o_zmianie_ustawy_o_stanie_wojennym____30_08_2011.pdf (dostęp: 10 czerwca 2013 r.).

[5] Financial Times Lexicon – *cyber espionage*, http://lexicon.ft.com/Term?term=cyber-espionage (dostęp: 10 czerwca 2013 r.).

ustalić rzeczywistych sprawców incydentu komputerowego, to jego skutki są zazwyczaj szybko widoczne i odczuwalne. Jest to jedna z głównych cech odróżniających pospolite przestępstwa w cyberprzestrzeni od incydentów związanych ze szpiegostwem. Dobrze zorganizowane i sprawnie przeprowadzone mogą pozostać nigdy nieodkryte, skutki związane z utratą poufnych informacji są trudne do zmierzenia, a internetowym szpiegom niezwykle trudno udowodnić winę, a jeszcze trudniej wskazać ich mocodawców.

Zdobywanie niejawnych informacji dotyczących zarówno wrogów, jak i sojuszników jest jednym z zadań realizowanych przez służby specjalne. Również prywatne przedsiębiorstwa dążą do uzyskania informacji o konkurencji, co jest jednym ze sposobów (nie zawsze legalnych) zdobycia przewagi na rynku. Niemal od początku istnienia cyberprzestrzeni dochodziło do przypadków kradzieży danych przez hakerów działających na zlecenie państw[6]. Informacje dotyczące cyberszpiegowskiej kampanii wymierzonej w USA i amerykańskie przedsiębiorstwa przedostawały się do opinii publicznej od wielu lat. Zawsze pozostawały jednak w sferze spekulacji, plotek lub dziennikarskich śledztw, niepotwierdzonych oficjalnie przez władze Stanów Zjednoczonych. Ataki internetowych szpiegów kierowane były głównie w stronę firm działających w sektorach energetycznym, finansowym, teleinformatycznym, lotniczym, samochodowym oraz obronnym. Skala problemu narastała, a straty ponoszone przez amerykańską gospodarkę stawały się coraz większe, według różnych szacunków sięgając poziomu 25–100 mld dolarów rocznie. Wśród państw szukających sposobów na zdobycie użytecznych danych znajdujących się w systemach komputerowych amerykańskich firm wymieniano zarówno konkurentów, jak i sojuszników USA, m.in. Rosję, Izrael i Francję, jednak skala aktywności tych państw pozostawała stosunkowo niewielka w porównaniu z agresywnymi operacjami prowadzonymi przez Chiny[7].

[6] *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, M. Łapczyński, Komentarz Międzynarodowy Pułaskiego, http://www.stosunkimiedzynarodowe.info/artykul,393,Zagrozenie_cyberterroryzmem_a_polska_strategia_obrony_przed_tym_zjawiskiem (dostęp: 10 czerwca 2013 r.).

[7] *U.S. said to be target of massive cyber-espionage campaign*, The Washington Post, 11 lutego 2013 r., http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html (dostęp: 11 czerwca 2013 r.).

## Jednostka PLA 61398

W lutym 2013 r. opublikowano raport *Exposing One of China's Cyber Espionage Units*[8], przygotowany przez firmę Mandiant, zajmującą się bezpieczeństwem teleinformatycznym. Jak wynikać ma z dowodów zgromadzonych przez autorów raportu w trakcie trwającego sześć lat śledztwa, wchodząca w skład Chińskiej Armii Ludowo-Wyzwoleńczej jednostka 61398, będąca centralnym ogniwem chińskiego systemu wywiadu komputerowego, ma być odpowiedzialna za znaczną liczbę ataków na amerykańskie firmy i rządowe agencje. Jak napisano w raporcie, atakujący amerykańskie komputery hakerzy należący do grupy nazwanej APT.1, działają z rejonu geograficznego, w którym zlokalizowana jest jednostka 61398, co ustalono na podstawie analizy adresów IP, którymi posługiwali się napastnicy. Zdaniem Mandiant, biorąc pod uwagę wysoki poziom kontroli internetu przez chińskie władze, jest niemożliwe, aby były one nieświadome działalności grupy – wręcz przeciwnie, prawdopodobne jest, że wysoką skuteczność w wykradaniu amerykańskich tajemnic hakerzy uzyskują dzięki ścisłej współpracy z jednostką 61398 lub po prostu są jej częścią. Publikacja raportu stanowiła pierwsze publiczne i bezpośrednie oskarżenie pod adresem władz Chin o zaangażowanie w proceder ataków i kradzieży własności intelektualnej należącej do amerykańskich przedsiębiorstw, organizacji oraz instytucji państwowych, a także uzyskiwanie zdolności do sterowania elementami amerykańskiej infrastruktury krytycznej, m.in. siecią energetyczną[9].

Również raport[10] przygotowany przez rządową instytucję zajmującą się polityką handlową USA (*Office of the United States Trade Representative*, USTR) wyraża obawy dotyczące bezpieczeństwa tajemnic handlowych i własności intelektualnej w kontaktach z Chinami. Jego autorzy podkreślają, że kwestie te już od lat stanowiły jedno z głównych zagrożeń, jednak sytuację znacznie pogorszyły incydenty cyberszpiegostwa prowadzone przez aktorów działających z terytorium Chin. Raport USTR wyróżnia się na tle innych dokumentów z tego zakresu tym, że zauważa zaangażowanie i pozytywną rolę państwa chińskiego w zakresie prowadzonych reform mających

[8] *Exposing One of China's Cyber Espionage Units*, lutego 2013 r., http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (dostęp: 11 czerwca 2013 r.).

[9] *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, The New York Times, 18 lutego 2013 r., http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=1&_r=1& (dostęp: 18 lutego 2013 r.).

[10] *2013 Special 301 Report*, http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf (dostęp: 31 maja 2013 r.).

na celu poprawę ustawodawstwa dotyczącego ochrony własności intelektualnej. Zmiany legislacyjne oceniono pozytywnie, zaznacza się jednak problemy z egzekwowaniem przyjętego prawa.

Pod koniec maja 2013 r., powołując się na niejawny raport przygotowany przez grupę doradczą Departamentu Obrony USA – Defense Science Board[11] – media poinformowały o nieuprawnionym uzyskaniu dostępu przez chińskich hakerów do danych dotyczących najbardziej kluczowych i zaawansowanych systemów uzbrojenia znajdujących się na wyposażeniu sił zbrojnych Stanów Zjednoczonych. Na liście znalazło się ponad 20 projektów, m.in. myśliwce F/A-18 i F-35; wielozadaniowy samolot pionowego startu i lądowania V-22 Osprey; śmigłowiec UH-60 Black Hawk; systemy przeciwrakietowe Patriot PAC-3, THAAD, Aegis oraz systemy walki elektronicznej i rozpoznania[12]. Doniesienia nie precyzują jednak kiedy, ani gdzie miało dojść do incydentu lub incydentów. Warto zauważyć, że autorzy nie mówią wprost o „kradzieży danych", ale o uzyskaniu przez Chiny „dostępu do zaawansowanych technologii, mogących przyspieszyć rozwój ich systemów uzbrojenia oraz osłabić w przyszłości przewagę militarną USA".

W innym raporcie, przygotowanym w maju br. przez Pentagon dla Kongresu USA, zwraca się uwagę m.in. na fakt, że Chiny, realizując długoterminową strategię modernizacji sił zbrojnych, wykorzystują działania szpiegowskie – również w cyberprzestrzeni – jako jedno z kluczowych narzędzi niwelowania przewagi militarnej Stanów Zjednoczonych przy znacznej redukcji czasu (liczonego w dziesiątkach lat) i wydatków (liczonych w miliardach dolarów) przeznaczanych na badania i rozwój[13].

Mimo potężnych strat – materialnych i wizerunkowych – ponoszonych przez amerykańskie przedsiębiorstwa, korzyści płynące ze współpracy z Chinami wciąż pozostają zbyt duże, aby z niej zrezygnować. Nie zmienia to faktu, że USA zamierzają działać i nie pozostają pasywne w obliczu problemu, jakie dla amerykańskiej gospodarki stanowi szpiegostwo w cyberprzestrzeni. Departament Stanu USA postanowił, że problem ten będzie intensywnie podejmowany na forum dyplomatycznym i stanie się jednym

[11] W styczniu 2013 r. opublikowano jawną wersję raportu – *Resilient Military Systems and the Advanced Cyber Threat*, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

[12] *Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies*, The New York Times, 28 maja 2013 r., http://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: 11 czerwca 2013 r.).

[13] *Military and Security Developments Involving the People's Republic of China 2013*, http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf (dostęp: 31 maja 2013 r.).

z tematów strategicznego dialogu bezpieczeństwa z Chinami. Wśród rozważanych wariantów działania wymienia się także formalne protesty, wydalenie personelu dyplomatycznego, restrykcje w polityce wizowej oraz skargi do Światowej Organizacji Handlu[14].

Konkretne propozycje dotyczące walki z procederem kradzieży amerykańskich tajemnic zostały zawarte w dokumencie Białego Domu *Administration Strategy On Mitigating The Theft Of U.S. Trade Secrets*[15]. Zaprezentowano go dwa dni po publikacji firmy Mandiant, jest więc mało prawdopodobne, aby stanowił bezpośrednią odpowiedź na tezy zawarte w raporcie. Biorąc pod uwagę objętość nowej strategii oraz liczbę zaangażowanych w jego przygotowanie agencji rządowych (m.in. departamenty handlu, obrony, bezpieczeństwa wewnętrznego, sprawiedliwości, stanu, skarbu), zasadne jest aby uznać, że przygotowywano ją znacznie dłużej. Zgodnie z zapowiedzią, strategia ma na celu ochronę amerykańskiej innowacyjności, konkurencyjności, gospodarki i miejsc pracy. Dokument zwraca uwagę na rosnącą skalę zjawiska cyberszpiegostwa, w tym działań prowadzonych przez osoby sponsorowane przez państwa. Opisuje jednak nie tylko szpiegostwo w cyberprzestrzeni, ale również „tradycyjne" techniki szpiegowskie, np. werbowanie agentów. W dokumencie podane są przykłady sytuacji, w których obce państwo było zaangażowane w kradzież danych należących do amerykańskich przedsiębiorstw. Niemal wszystkie z nich dotyczą Chin. Strategia wymienia pięć obszarów działań amerykańskiej administracji, mających pomóc w ochronie tajemnic handlowych:

1. Wzmocnienie działań dyplomatycznych – również na najwyższym szczeblu – zwłaszcza w kontaktach z państwami szczególnie zaangażowanymi w działalność szpiegowską. Amerykanie chcą też współpracować w tym zakresie z organizacjami międzynarodowymi, a także tworzyć koalicje z państwami podzielającymi ich obawy.
2. Rozwój współpracy i wymiana informacji z sektorem prywatnym, a także tworzenie oraz promowanie „dobrych praktyk" i wytycznych służących ochronie tajemnic gospodarczych.

[14] *U.S. said to be target of massive cyber-espionage campaign*, The Washington Post, 11 lutego 2013 r., http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story_1.html (dostęp: 11 czerwca 2013 r.).

[15] *Administration Strategy On Mitigating The Theft Of U.S. Trade Secrets*, luty 2013 r., http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (dostęp: 11 czerwca 2013 r.).

3. Kontynuacja działań wymiaru sprawiedliwości – w tym działań śledczych, mających na celu wykrycie i postawienie przed sądem osób czy firm odpowiedzialnych za kradzież tajemnic. Amerykańskie służby mają również przekazywać firmom opracowane analizy ryzyka i ostrzeżenia w sytuacjach zagrożenia.
4. Przegląd ustawodawstwa i ewentualne zmiany legislacyjne w celu zapewnienia prawa pozwalającego na skuteczną ochronę tajemnic należących do amerykańskich przedsiębiorstw.
5. Zwiększenie świadomości społecznej w zakresie ochrony tajemnic handlowych i szkodliwego wpływu tego procederu na amerykańską gospodarkę.

Propozycje zawarte w strategii są już wcielane w życie, co szczególnie widać w wymiarze współpracy publiczno-prywatnej, działaniach legislacyjnych oraz dyplomatycznych. Niespełna miesiąc po prezentacji strategii prezydent USA Barack Obama spotkał się z przedstawicielami najważniejszych amerykańskich korporacji w celu omówienia działań w zakresie poprawy cyberbezpieczeństwa w sektorze prywatnym[16].

Krótko potem pojawiła się informacja o nowych przepisach dotyczących wydatkowania funduszy przez amerykańskie instytucje rządowe do końca bieżącego roku fiskalnego, który upływa 30 września 2013 r. Znalazł się tam zapis zabraniający wybranym rządowym agencjom kupowania sprzętu komputerowego produkowanego bądź składanego przez firmy będące własnością, zarządzanych lub subsydiowanych przez Chiny. Instytucje mogą dokonać takich zakupów wyłącznie po konsultacjach z Federalnym Biurem Śledczym (FBI) i uzyskaniu potwierdzenia, że zakup nie spowoduje ryzyka szpiegostwa lub sabotażu[17]. W wydanym wcześniej raporcie skierowanym do amerykańskich instytucji i przedsiębiorstw znalazło się zalecenie, aby nie prowadzić interesów z chińskimi gigantami teleinformatycznymi – Huawei oraz ZTE – z uwagi na zagrożenia bezpieczeństwa teleinformatycznego mogące wynikać z takiej współpracy[18].

[16] *Obama to meet CEOs on cyber security*, Reuters, 12 marca 2013 r., http://www.reuters.com/article/2013/03/13/us-usa-obama-cyber-idUSBRE92B17Y20130313 (dostęp: 11 czerwca 2013 r.).

[17] *Obama BANS U.S. government from buying Chinese-made computer technology over cyber-attack fears*, Daily Mail, 28 marca 2013 r., http://www.dailymail.co.uk/news/article-2300518/Obama-BANS-U-S-government-buying-Chinese-technology-cyber-attack-fears.html (dostep: 11 czerwca 2013 r.).

[18] *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, Permanent Select Committee on Intelligence, 8 października 2012 r., http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf (dostep: 3 lipca 2013 r.).

Fakty te są łączone z doniesieniami o możliwości wycofania koncernu Huawei ze Stanów Zjednoczonych[19]. W jednej z wypowiedzi przedstawiciel korporacji zadeklarował, że nie jest już ona zainteresowana obecnością na amerykańskim rynku, stanowisko to było jednak później łagodzone przez chińskie media[20].

Niektóre amerykańskie firmy zaczęły także stosować taktykę polegającą na umieszczeniu fałszywych danych na serwerach. Taka praktyka ma przede wszystkim dezinformować przeciwnika. Wystawianie fałszywych danych „na przynętę" ma także umożliwić identyfikację cyberszpiegów oraz poznanie ich metod działania[21].

## Chiny odpowiadają

Chiny – podobnie jak i w innych przypadkach – zaprzeczyły amerykańskim oskarżeniom, nazywając je „nieprofesjonalnymi". Władze podkreślają, że na terenie Chińskiej Republiki Ludowej hakerstwo jest niezgodne z prawem, państwo nie utrzymuje związków z osobami czy grupami prowadzącymi tego typu działalność, a właściwe służby walczą z tym procederem. Co więcej, Chiny postrzegają siebie jako ofiarę hakerów i wskazują, że wiele ataków na chińskie systemy komputerowe przeprowadzanych jest z terytorium Stanów Zjednoczonych. Zdaniem Chin, amerykańskie panowanie nad cyberprzestrzenią jest niekwestionowane, a USA to w istocie „prawdziwe imperium hakerskie"[22]. Według chińskiego Ministerstwa Obrony, Stany Zjednoczone odpowiadają za blisko dwie trzecie (62,9 proc.) spośród ponad 140 tys. cyberataków wykrywanych co miesiąc przez władze Chin[23]. Zgodnie z informacjami podawanymi przez zajmującą się walką z incydentami w cy-

[19] *Huawei 'not interested in the US any more'*, Financial Times, 23 kwietnia 2013 r., http://www.ft.com/cms/s/0/7b212314-ac28-11e2-a063-00144feabdc0.html#axzz2VDVG6FOY (dostęp: 11 czerwca 2013 r.).

[20] *Huawei denies abandon the U.S. market*, BJ News, 25 kwietnia 2013 r., http://www.bjnews.com.cn/finance/2013/04/25/260509.html (dostęp: 11 czerwca 2013 r.).

[21] *To thwart hackers, firms salting their servers with fake data*, The Washington Post, 3 stycznia 2013 r., http://www.washingtonpost.com/world/national-security/to-thwart-hackers-firms-salting-their-servers-with-fake-data/2013/01/02/3ce00712-4afa-11e2-9a42-d1ce6d0ed278_story_1.html (dostęp: 11 czerwca 2013 r.).

[22] *China calls US the „real hacking empire" after Pentagon report*, Reuters, 7 maja 2013 r., http://www.reuters.com/article/2013/05/08/china-us-defence-idUSL3N0DP0A720130508 (dostęp: 11 czerwca 2013 r.).

[23] *China blames US for majority of cyberattacks on military websites*, The Verge, 28 lutego 2013 r., http://www.theverge.com/2013/2/28/4039300/china-says-us-is-responsible-for-hacks-on-defense-websites (dostęp: 11 czerwca 2013 r.).

berprzestrzeni instytucją National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT), Chiny dysponują olbrzymią ilością danych potwierdzających, że ataki płyną ze strony USA, jednak ich ujawnienie nie sprzyjałoby rozwiązaniu problemu[24].

Potwierdzenie tez stawianych przez Chiny nadeszło ze strony najmniej spodziewanej przez Stany Zjednoczone. Na początku czerwca 2013 r. gazety „The Washington Post"[25] oraz „The Guardian"[26], powołując się na tajne dokumenty przekazane przez Edwarda Snowdena, byłego pracownika Centralnej Agencji Wywiadowczej (*Central Intelligence Agency*, CIA) oraz Agencji Bezpieczeństwa Narodowego (*National Security Agency*, NSA) opisały amerykański program PRISM. Jego celem jest inwigilacja danych gromadzonych na serwerach dziewięciu dostawców usług internetowych: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube oraz Apple. Dzięki PRISM amerykańskie służby od 2007 r. mają dostęp m.in. do nagrań audio i wideo, czatów, zdjęć, rozmów oraz poczty użytkowników korzystających z serwisów należących do wymienionych firm, które zaprzeczyły współpracy ze służbami czy wiedzy na temat programu. W przypadku PRISM wykorzystano fakt, że większość danych w ramach światowej komunikacji elektronicznej przechodzi przez serwery należące do amerykańskich firm. Choć doniesienia dotyczące programu wywołały prawdziwą burzę i falę oskarżeń pod adresem USA, amerykańskie władze bronią PRISM. Dyrektor wywiadu amerykańskiego James Clapper powiedział, że jest on zgodny z obowiązującym prawem i nie może być użyty do umyślnego monitorowania obywateli USA lub innych osób zamieszkałych na terenie Stanów Zjednoczonych. Działanie PRISM koncentruje się bowiem na obcokrajowcach, a zebrane dane są wykorzystywane do ochrony przed różnymi zagrożeniami, np. terroryzmem. PRISM bronił również prezydent USA Barack Obama[27], który podkreślił, że mimo klauzuli tajności, program jest „przejrzysty" i zgodny

[24] *China has 'mountains of data' about U.S. cyber attacks: official*, Reuters, 5 czerwca 2013 r., http://www.reuters.com/article/2013/06/05/us-china-usa-hacking-idUSBRE95404L20130605 (dostęp: 11 czerwca 2013 r.).

[25] *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, The Washington Post, 6 czerwca 2013 r., http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (dostęp: 3 lipca 2013 r.).

[26] *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, 7 czerwca 2013 r., http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data (dostęp: 3 lipca 2013 r.).

[27] *Obama defends secret NSA surveillance programs – as it happened*, The Guardian, 7 czerwca 2013 r., http://www.guardian.co.uk/world/2013/jun/07/obama-administration-nsa-prism-revelations-live (dostęp: 3 lipca 2013 r.).

z prawem[28]. B. Obama zapewnił, że administracja szuka rozwiązania, które uspokoi społeczeństwo, a także udowodni, że ich rozmowy i korespondencja nie są inwigilowane przez „Wielkiego Brata". PRISM najmocniej bronił szef NSA gen. Keith Alexander[29], który ocenił, że ujawnienie informacji na temat programu, który pozwolił udaremnić co najmniej 50 „terrorystycznych spisków", stanowi olbrzymią, niemożliwą do naprawienia szkodę dla USA i ich sojuszników.

Zapewnienia przedstawicieli administracji Stanów Zjednoczonych pozwalają sądzić, że dane gromadzone w ramach programu PRISM (także wśród użytkowników pochodzących z Chin[30]) są wykorzystywane do zagwarantowania bezpieczeństwa amerykańskich obywateli, a nie szpiegostwa przemysłowego. Niemniej dowody dostarczone przez E. Snowdena, a także atmosfera „tajności" oraz społeczne obawy dotyczące inwigilacji na globalną skalę będą dla wrogów, konkurentów i sojuszników USA potężnym argumentem w dyskusji nad cyberszpiegostwem i inwigilacją w cyberprzestrzeni, niezależnie od tego, jak szczytne idee przyświecają Amerykanom.

Jeszcze przed początkiem sprawy związanej z programem PRISM, Chińczycy wezwali do uzgodnienia międzynarodowych „zasad i współpracy" w kwestiach szpiegostwa w internecie[31]. Propozycje rozmów i chińsko-amerykańskiej kooperacji w dziedzinie cyberbezpieczeństwa padały wielokrotnie z ust najwyższych przedstawicieli ChRL. Krótko po wyborze na stanowisko nowy premier Chin Li Keqiang zapowiedział nawiązanie nowego rodzaju relacji ze Stanami Zjednoczonymi. Zwracał on uwagę na potrzebę zachowania pokoju w regionie Azji i Pacyfiku, a także zakończenia „wojny na słowa w sprawie cyberprzestrzeni"[32].

Mimo powyższych wyzwań obie strony są świadome wzajemnych zależności, utrzymują gotowość do rozmów i chęć dalszego pogłębiania współ-

---

[28] Foreign Intelligence Surveillance Act, https://www.fas.org/irp/agency/doj/fisa/ (dostęp: 3 lipca 2013 r.).

[29] *Column: NSA and the Pandora's box of surveillance*, 24 czerwca 2013 r., http://www.reuters.com/article/2013/06/24/us-shafer-nsa-idUSBRE95N1GQ20130624 (dostęp: 3 lipca 2013 r.).

[30] *Alleged NSA snooping target is one of China's Internet hubs*, Reuters, 24 czerwca 2013 r., http://www.reuters.com/article/2013/06/24/us-usa-security-tsinghua-idUSBRE95N0M220130624 (dostęp: 3 lipca 2013 r.).

[31] *In Wake of Cyberattacks, China Seeks New Rules*, The New York Times, 10 marca 2013 r., http://www.nytimes.com/2013/03/11/world/asia/china-calls-for-global-hacking-rules.html?ref=world (dostęp: 11 czerwca 2013 r.).

[32] *China, U.S. should stop war of words on hacking, says new Chinese premier*, Reuters, 17 marca 2013 r., http://www.reuters.com/article/2013/03/17/china-parliament-hacking-idUSL3N0C902O20130317 (dostęp: 11 czerwca 2013 r.).

pracy, również wojskowej[33]. Kwestie związane z cyberbezpieczeństwem poruszane są w kontaktach dyplomatycznych na najwyższym szczeblu – m.in. szefów sztabów armii Stanów Zjednoczonych i Chin – gen. Martina Dempsey'a oraz gen. Fanga Fenghui[34], a także ówczesnego doradcę prezydenta USA do spraw bezpieczeństwa narodowego Toma Donilona i kilku czołowych przedstawicieli chińskich władz[35].

Temat cyberszpiegostwa był również poruszany w czerwcu 2013 r. podczas amerykańsko-chińskiego szczytu w Kalifornii. Co prawda nie zaowocował on żadnym formalnym porozumieniem w kwestiach cyberbezpieczeństwa, jednak prezydent Stanów Zjednoczonych Barack Obama przekazał prezydentowi Chin Xi Jinpingowi „jasną wiadomość", że jeśli kradzież amerykańskiej własności intelektualnej nie ustanie, będzie to stanowiło „bardzo poważny problem" dla stosunków gospodarczych między państwami[36].

W efekcie szybkiego rozwoju cyfrowej infrastruktury Chiny stają się coraz bardziej uzależnione od systemów funkcjonujących w cyberprzestrzeni. Tym samym chińskie instytucje i przedsiębiorstwa także będą coraz mocniej narażone na ataki hakerów i próby uzyskania nieuprawnionego dostępu do poufnych danych zgromadzonych na dyskach twardych komputerów. Niebawem Chiny mogą się przekonać, że cyberprzestrzeń jest bronią obosieczną, służącą nie tylko do walki z ekonomicznymi i militarnymi rywalami, ale także źródłem zagrożeń, przed którymi nie sposób obronić się samodzielnie[37]. Chińskie władze starają się utrzymywać ścisłą kontrolę nad cyberprzestrzenią, ale całkowite odcięcie krajowych sieci od globalnej infrastruktury jest niemożliwe. Chińczycy już teraz są podatni na ataki hakerów, niezależnie od ich motywacji, zleceniodawców czy faktycznego miejsca, w którym się znajdują. Ma to szczególne znaczenie w czasie, kiedy chińskie

[33] *Analysis: From opera to exercises, U.S. and China deepen military ties*, Reuters, 22 maja 2013 r., http://www.reuters.com/article/2013/05/22/us-usa-china-military-analysis-idUSBRE94L0X-920130522 (dostęp: 11 czerwca 2013 r.).

[34] *U.S. and China Put Focus on Cybersecurity*, The New York Times, 22 kwietnia 2013 r., http://www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html?ref=global-home&_r=1& (dostęp: 11 czerwca 2013 r.).

[35] *China says willing to discuss cyber security with the U.S.*, Reuters, 12 marca 2013 r., http://www.reuters.com/article/2013/03/12/us-usa-china-cybersecurity-idUSBRE92A0XO20130312 (dostęp: 11 czerwca 2013 r.).

[36] *Obama confronts Xi on cyber theft*, Reuters, 9 czerwca 2013 r., http://in.reuters.com/article/2013/06/09/usa-china-idINDEE95800A20130609 (dostęp: 11 czerwca 2013 r.).

[37] A. Segal, *Chinese Computer Games – Keeping Safe in Cyberspace*, Foreign Affairs, March/April 2012, s. 15.

przedsiębiorstwa nie chcą już zajmować się wyłącznie tanim wytwarzaniem zachodnich produktów, ale też dążą do tego, aby na własną rękę rozwijać nowe, innowacyjne technologie i konkurować z zagranicznymi firmami jak „równy z równym". Będzie to wymagało dostępu do globalnej sieci, wolnej od wszechogarniającej kontroli chińskich władz, a więc narażonej na zagrożenia takie jak w krajach zachodnich.

Wyzwaniem dla chińskiego przemysłu jest też tendencja polegająca na wycofywaniu produkcji z Chin przez zachodnie firmy i przenoszeniu jej do innych państw. Według danych z 2012 r., duże amerykańskie przedsiębiorstwa już teraz decydują się na budowę fabryk w Stanach Zjednoczonych[38]. Głównym powodem takiego działania są rosnące koszty produkcji w chińskich wytwórniach. Inne przyczyny takiego działania to względy wizerunkowe i ochrona rodzimych miejsc pracy, ale też bezpieczeństwo cennej wiedzy dotyczącej patentów i wytwarzania zaawansowanych technologicznie produktów[39].

## Chiny, Stany Zjednoczone i inni

Internet to globalna sieć i nie można mieć realnej nadziei, że z jakiegoś powodu pewne niebezpieczeństwa ominą systemy komputerowe należące do jakiegokolwiek państwa. Cyberszpiegostwo stanowi wyzwanie także dla Unii Europejskiej oraz NATO, a więc i państw będących członkami tych organizacji. Dotyczy to również Polski, która utrzymuje kontakty i bliską współpracę gospodarczą m.in. z największymi potęgami oskarżanymi o szpiegowanie w internecie. Można więc przypuszczać, że w nadchodzącym czasie zagrożenie to będzie rosło i dotykało coraz więcej polskich instytucji oraz przedsiębiorstw.

W ostatnich latach mocno zacieśniane są polsko-chińskie stosunki handlowe, o czym świadczą kontakty na szczeblu prezydenckim[40], rządowym[41],

[38] *Factories begin to shift back to US*, Financial Times, 20 maja 2013 r., http://www.ft.com/cms/s/0/115005c6-a225-11e1-a22e-00144feabdc0.html (dostęp: 11 czerwca 2013 r.).

[39] *Is the U.S. the Next Low-Cost Manufacturing Country?*, ThomasNet, 16 kwietnia 2013 r., http://www.news.thomasnet.com/IMT/2013/04/16/is-the-u-s-the-next-low-cost-manufacturing-country/ (dostęp: 11 czerwca 2013 r.).

[40] Wizyta prezydenta RP Bronisława Komorowskiego w Chińskiej Republice Ludowej w grudniu 2011 r.; spotkanie ambasadora ChRL w Warszawie Xu Jiana z szefem BBN Stanisławem Koziejem w grudniu 2012 r.

[41] Wizyta premiera Chińskiej Republiki Lugowej Wena Jiabao w Polsce w kwietniu 2012 r.; wizyta ministra obrony narodowej Tomasza Siemoniaka w Chinach w maju 2013 r.

a także parlamentarnym[42]. Współpraca z takim partnerem daje wiele korzyści, jednak nie można zapominać o ryzyku, jakie ze sobą niesie. Dotyczy ono nie tylko polskich służb i instytucji, ale też przedsiębiorstw, prowadzących współpracę z Chinami i firmami pochodzącymi z tego państwa.

Należy pamiętać, że celem cyberszpiegów, działających na zlecenie dowolnego państwa, mogą być nie tylko plany najnowszych typów uzbrojenia, ale również tajemnice gospodarcze czy informacje pozornie nieistotne, np. wyniki finansowe firm, strategie negocjacyjne, bazy danych, a nawet prywatna korespondencja pracowników. Doświadczenia innych państw pokazują, że w celu zdobycia informacji stosuje się także takie „niepozorne" techniki, jak np. „obdarowywanie" sprzętem elektronicznym mogącym służyć do nieuprawnionego zdobywania danych (nośniki danych, telefony, komputery itp.). Dlatego konieczne jest stosowanie zasady ograniczonego zaufania i sprawdzanie urządzeń pod kątem bezpieczeństwa informacyjnego.

Warto przypomnieć opisany przez media we wrześniu 2011 r. przypadek dotyczący przekazania sprzętu komputerowego Ministerstwu Spraw Wewnętrznych i Administracji przez jeden z chińskich koncernów. Wątpliwości dotyczące przekazania sprzętu miała Agencja Bezpieczeństwa Wewnętrznego, do której skierowano prośbę o sprawdzenie sprzętu elektronicznego pod kątem bezpieczeństwa informacji[43].

Szczególnie teraz, w okresie wzmożonej działalności cyberszpiegów, w podobnych sytuacjach należy zachowywać szczególną ostrożność, dbałość o bezpieczeństwo teleinformatyczne, ochronę systemów komputerowych, a także procedury i „dobre praktyki" służące ochronie informacji. Do tej pory na terenie Polski nie doszło do spektakularnego przypadku kradzieży wrażliwych danych za pośrednictwem cyberprzestrzeni, zagrożenie jest jednak realne.

W Niemczech funkcjonuje grupa zadaniowa zajmująca się bezpieczeństwem teleinformatycznym w gospodarce. Niemiecki minister gospodarki i technologii Rainer Brüderle przyznał, że bardziej niż o bezpieczeństwo wielkich korporacji obawia się o tajemnice małych i średnich przedsiębiorstw, które często nie zdają sobie sprawy z zagrożeń, lekceważą je lub nie

[42] Wizyta polskiej delegacji parlamentarnej pod przewodnictwem marszałek Sejmu Ewy Kopacz w Chinach w czerwcu 2013 r.

[43] *ABW sprawdza chiński prezent dla MSWiA*, Gazeta Prawna, 23 września 2011 r., http://www.gazetaprawna.pl/wiadomosci/artykuly/550082,abw_sprawdza_chinski_prezent_dla_mswia.html# (dostęp: 11 czerwca 2013 r.).

dysponują środkami pozwalającymi na właściwą ochronę[44]. Dla Niemców szpiegostwo przemysłowe i kradzież własności intelektualnej generują coraz większe problemy i wymierne straty finansowe, jednak firmy-ofiary wciąż unikają współpracy z władzami. Zdaniem zrzeszającej niemieckich producentów maszyn i urządzeń organizacji VDMA, straty tej branży z tytułu kradzieży własności intelektualnej wynoszą – według różnych szacunków – od 4 do 8 mld euro rocznie[45]. Problemem zainteresowała się już Komisja Europejska, która prowadzi konsultacje w sprawie ochrony tajemnic handlowych w Europie[46]. Warto jednak podkreślić, że problem nasilonego szpiegostwa i piractwa gospodarczego nie wiąże się wyłącznie z Chinami, a kradzieżą tajemnic handlowych coraz częściej zajmują się również przedsiębiorstwa pochodzące z innych, także europejskich państw.

Dla polskich przedsiębiorców, coraz szerzej obecnych na europejskich rynkach, cyberszpiegostwo stanowi rosnące zagrożenie. Z pewnością nie ominie ono także firm sektora obronnego, decydujących się na kooperację z zagranicznymi partnerami m.in. przy realizacji wielonarodowych projektów w ramach inicjatyw *pooling and sharing* oraz *smart defence*. Warto pamiętać, że cyberszpiegostwem zajmują się także bliscy sojusznicy i partnerzy.

Szczególnie wymowny jest międzynarodowy skandal wywołany publikacją niemieckiego tygodnika „Der Spiegel"[47]. Powołując się na ściśle tajne dokumenty z 2010 r., ujawnione przez byłego pracownika CIA oraz NSA E. Snowdena, gazeta napisała, że amerykańska Agencja Bezpieczeństwa Narodowego zajmowała się nie tylko zbieraniem danych obywateli UE w ramach programu PRISM, ale też podsłuchiwała rozmowy telefoniczne przedstawicieli UE pracujących w biurach w Waszyngtonie i Nowym Jorku. NSA miała także infiltrować sieci komputerowe w tych placówkach, uzyskując dostęp do wewnętrznych dokumentów oraz poczty elektronicznej unijnych dyplomatów. Zdaniem „Der Spiegel", NSA próbo-

[44] *Cyberwojna z hakerami*, Deutsche Welle, 1 kwietnia 2011 r., http://www.dw.de/cyberwojna-z-hakerami/a-14958016 (dostęp: 11 czerwca 2013 r.).

[45] *Szpiegostwo przemysłowe doskwiera niemieckim firmom*, Deutsche Welle, 25 kwietnia 2012 r., http://www.dw.de/szpiegostwo-przemys%C5%82owe-doskwiera-niemieckim-firmom/a-15907123 (dostęp: 11 czerwca 2013 r.).

[46] *Trade Secrets*, Verband Deutscher Maschinen- und Anlagenbau, 26 marca 2013 r., http://www.vdma.org/en_GB/article/-/articleview/1246945 (dostęp: 11 czerwca 2013 r.).

[47] *Attacks from America: NSA Spied on European Union Offices*, Der Spiegel, 29 czerwca 2013 r., http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html (dostęp: 1 lipca 2013 r.).

wała również podsłuchiwać rozmowy telefoniczne w siedzibie Rady UE w Brukseli. Dziennikarskie doniesienia wywołały gwałtowną reakcję europejskich urzędników[48] oraz przywódców państw członkowskich Unii, którzy domagali się stosownych wyjaśnień od Stanów Zjednoczonych[49], a szef Komisji Europejskiej José Manuel Barroso nakazał doraźne kontrole zabezpieczeń przed inwigilacją w budynkach instytucji oraz systemie komunikacji[50]. Brytyjski dziennik „The Guardian" sprecyzował[51], że na liście ujawnionej przez E. Snowdena znajdowało się 38 „celów", w tym ambasad należących do najbliższych sojuszników Stanów Zjednoczonych. Poza państwami członkowskimi UE lista obejmowała m.in. Japonię, Koreę Południową czy Turcję. Praktyki stosowane przez NSA i „manię zbierania informacji" porównano do metod wykorzystywanych w czasach „zimnej wojny". Pojawiły się nawet opinie, że Unia Europejska powinna skierować tę sprawę do międzynarodowych instytucji, a także zawiesić negocjacje z USA o utworzeniu strefy wolnego handlu.

Doniesienia medialne komentował amerykański sekretarz stanu John Kerry, którego zdaniem wszystkie państwa prowadzą „wiele działań" w celu ochrony swojego bezpieczeństwa narodowego i przyczyniają się do tego wszelkiego rodzaju informacje. Europejskich sojuszników uspokajał prezydent USA B. Obama, który powiedział, że jego administracja ocenia treść artykułów prasowych cytujących dokumenty dostarczone przez E. Snowdena i zapewnił, że we właściwym czasie Stany Zjednoczone dostarczą sojusznikom odpowiedzi na pytania w sprawie elektronicznej inwigilacji[52].

Niezależnie od tego, jak zakończy się skandal wywołany doniesieniami „Der Spiegel", można przyjąć, że w pewnym zakresie doszło do naruszenia zaufania między sojusznikami. Ciężko jednak sobie wyobrazić,

[48] *Spying 'Out of Control': EU Official Questions Trade Negotiations*, Der Spiegel, 30 czerwca 2013 r., http://www.spiegel.de/international/europe/eu-officials-furious-at-nsa-spying-in-brussels-and-germany-a-908614.html (dostęp: 1 lipca 2013 r.).

[49] *Europeans Voice Anger Over Reports of Spying by U.S. on Its Allies*, The New York Times, 1 lipca 2013 r., http://www.nytimes.com/2013/07/01/world/europe/europeans-voice-anger-over-reports-of-spying-by-us-on-its-allies.html (dostęp: 2 lipca 2013 r.).

[50] *Barroso orders security sweep after allegations of US spying*, The European Voice, 1 lipca 2013 r., http://www.europeanvoice.com/article/2013/july/barroso-orders-security-sweep-after-allegations-of-us-spying/77721.aspx (dostęp: 2 lipca 2013 r.).

[51] *New NSA leaks show how US is bugging its European allies*, The Guardian, 30 czerwca 2013 r., http://www.guardian.co.uk/world/2013/jun/30/nsa-leaks-us-bugging-european-allies (dostęp: 1 lipca 2013 r.).

[52] *U.S. seeks to calm European outrage over alleged spying*, Reuters, 1 lipca 2013 r., http://www.reuters.com/article/2013/07/01/us-usa-eu-spying-idUSBRE95T09C20130701 (dostęp: 2 lipca 2013 r.).

aby relacje transatlantyckie ucierpiały z tego powodu, współpraca jest bowiem zbyt istotna dla obu stron. Niemniej sytuacja w tym zakresie jest dynamiczna, gdyż E. Snowden nie ujawnił jeszcze wszystkich wykradzionych tajemnic.

Działania globalnych potęg w cyberprzestrzeni znacząco się od siebie różnią. Medialna dyskusja dotycząca cyberszpiegów z Chin koncentruje się na kwestiach gospodarczych – kradzieży tajemnic handlowych i patentów – a ich cele są bardziej materialne. Stany Zjednoczone, które w przeciwieństwie do Chińczyków nie wypierają się prowadzenia działań wywiadowczych w cyberprzestrzeni, bardziej zainteresowane są informacjami dotyczącymi polityki i działań innych państw – sojuszników i przeciwników – oraz zwykłych ludzi, co w założeniu ma służyć poprawie bezpieczeństwa. Tę globalną mozaikę uzupełniają działania innych państw, w różnym stopniu zaangażowanych lub dotkniętych problemem cyberszpiegostwa.

## Podsumowanie

Kwestie cyberszpiegostwa są jedynie niewielkim elementem złożonych stosunków między Stanami Zjednoczonymi a Chinami, państwami które mimo fundamentalnych różnic łączą silne zależności i trudne do rozerwania więzi. Obok wielu spornych kwestii – m.in. strategicznego przeniesienia uwagi Stanów Zjednoczonych w region Azji i Pacyfiku, działania na forum Rady Bezpieczeństwa ONZ, rozwiązywania międzynarodowych sporów i kwestii przestrzegania praw człowieka – cyberszpiegostwo pozostaje niezwykle wrażliwym, także politycznie, tematem, który w pewnych warunkach może stanowić zagrożenie dla amerykańsko-chińskich relacji. Obie strony prezentują różną wizję przyszłości cyberprzestrzeni, kontroli i wykorzystania tego środowiska. USA widzą internet jako zdecentralizowane, otwarte, bezpieczne i niezawodne narzędzie wspierające rozwój oraz współpracę międzynarodową. Dla Chin cyberprzestrzeń jest źródłem potencjalnego zagrożenia, dlatego razem ze znajdującymi się w niej treściami powinna podlegać kontroli władz[53]. Oba państwa są jednak świadome, że nieuregulowanie omawianej kwestii może prowadzić do „cybernetycznej zimnej wojny" oraz nakręcać spiralę wzajemnych oskarżeń i zrzucania winy. Działania tych mocarstw wywierają efekt w skali globalnej, wpływając na

[53] A. Segal, *op.cit.*, s. 15.

wszystkie państwa, korporacje i indywidualnych użytkowników obecnych w przestrzeni wirtualnej. Kradzież tajemnic jest jednym z wielu elementów cyberbezpieczeństwa, a już od pewnego czasu mówi się o potrzebie międzynarodowego uregulowania tej domeny. Dobrze byłoby, gdyby ewentualna współpraca Stanów Zjednoczonych i Chin stała się impulsem do zaangażowania innych stron i podjęcia pracy nad sformalizowaniem – politycznie lub na gruncie prawa międzynarodowego – relacji między państwami w przestrzeni wirtualnej, podobnie jak konwencje międzynarodowe pozwoliły ustanowić międzynarodowy ład w przestrzeni realnej. Najważniejsze z nich powstały po wielkich konfliktach zbrojnych. Być może doświadczenia przeszłości sprawią, że w przypadku cyberprzestrzeni będzie inaczej.