Piotr Borkowski

Koncepcja cyberbezpieczeństwa w ujęciu Chińskiej Republiki Ludowej – wybrane aspekty

W Chińskiej Republice Ludowej tematyka dostępu do Internetu, wykorzystywania technologii informacyjnych oraz prowadzenia działań ofensywnych nabiera zupełnie innego kształtu niż w krajach europejskich czy USA. Według doniesień medialnych oraz dostępnych analiz publikowanych przez specjalistów sektora bezpieczeństwa teleinformatycznego jest to kraj, który obecnie najszerzej wykorzystuje zdolności inwigilacji cyfrowej, dopuszczając się ataków na najlepiej strzeżone bazy danych. Podejście do omawianej problematyki wywodzi się z uwarunkowań społeczno-historyczno-kulturowych, które kształtowały stosunek Chin do wojny, szeroko opisywany przez stratega Sun Tzu. Pomimo upływu wieków, jego główne myśli przewodnie są wykorzystywane w polityce i w działalności międzynarodowej, w tym przy używaniu technologii informacyjnych do osiągania przewagi ekonomicznej. W wielu obszarach życia gospodarczego i politycznego środki wykorzystywane w celu osiągnięcia przewagi znacznie odbiegają od norm przyjmowanych w krajach tzw. cywilizacji zachodniej. Z założenia neguje się działanie Chin jako kraju, który nie przestrzega określonych reguł. Przestrzega, ale stworzonych na własne potrzeby.

Aspekty polityczno-strategiczne

Jedną z zasad stosowanych przez chińskich strategów, od której się nie odchodzi, jest dokładna analiza przeciwnika. Chińczycy w kontekście cyberdziałań wskazują mocne i słabe strony Stanów Zjednoczonych jako głównego oponenta w działaniach w cyberprzestrzeni. Umiejętność wyciągania przez specjalistów z USA wniosków, które wynikają z błędnych decyzji, określają na bardzo wysokim poziomie. Tak samo jak gospodarowanie budżetem na rozwój nowoczesnych technologii. Jako zdecydowaną wadę wskazują dużą zależność USA od technologii, które rozwijają, co może być przyczyną potencjalnych problemów natury technicznej w związku z możliwością zdalnego niszczenia niektórych z nich[1]. Nie zmienia to jednak podejścia przeważającego w Chinach, że rozwój technologii informacyjnych jest uważany za największą rewolucję technologiczną w historii, i wskazuje się przyszłość wojen jako nieodwracalny proces skomputeryzowania pól bitew, niezależnie od tego, czy będą one prowadzone w skali makro czy mikro. Chińscy specjaliści w zdecydowany sposób oddzielają pojęcie „wojny informacyjnej" i „bezpieczeństwa informacji" od „wojny komputerowej" i „bezpieczeństwa informatycznego"[2]. Analizując *Politykę Bezpieczeństwa Narodowego Chińskiej Republiki Ludowej* z 2008 r., można zauważyć, że terminy „informatyzacja" i „rozwój systemów informacyjnych" były terminami najczęściej używanymi w tym dokumencie[3]. Dokument opublikowany w 2013 r. na pierwszym miejscu w hierarchii

[1] Zob. T.L. Thomas, *The dragons quantum leap*, Fort Leavenworth 2009, s. 18–20.
[2] T.L. Thomas, *The dragons*..., s. 23.
[3] Tamże, s. 39.

priorytetów wyraźnie stawia informatyzowanie sił bezpieczeństwa oraz sił zbrojnych[4]. W tym celu podkreśla się potrzebę rozwoju własnych projektów badawczych oraz korzystanie z doświadczeń innych krajów. Warto zwrócić uwagę, że hasło „korzystanie z doświadczeń innych krajów" nie jest połączone ze współpracą międzynarodową. Ta pojawia się później w przedmiotowym dokumencie i opisuje współpracę (wyłącznie – przyp. aut.) z Brazylią przy projektach kosmicznych.

Nie tylko w opisywanym dokumencie realna współpraca w zakresie cyberbezpieczeństwa w Chinach nie istnieje. Skupienie wysiłków na budowie szczelnego systemu ochraniającego sieci rządowe i wojskowe powoduje, że edukacja społeczeństwa jest znikoma, tak samo jak znikome jest zabezpieczenie obywateli przed przestępstwami komputerowymi. W 2011 r. ofiarą ataków komputerowych padało codziennie prawie 9 mln komputerów, co stanowiło wzrost o 48 proc. w stosunku do 2010 r. Ponad 60 proc. z 2500 osób badanych przez Chińskie Centrum Testów Oprogramowania przyznało się, że wykradziono im prywatne dane[5].

Bezpieczeństwo teleinformatyczne i jego priorytety w sferze cywilnej określa wspominany w niektórych opracowaniach tzw. dokument „27", nazwany przez specjalistów „chińską strategią cywilnej narodowej cyberobrony". Za realizację projektów związanych z tą sferą odpowiadają cztery główne instytucje:

1) Ministerstwo Bezpieczeństwa Publicznego – odpowiada za cyberprzestępstwa oraz ochronę infrastruktury krytycznej kraju,
2) Narodowe Biuro Szyfrów, znane również jako Centralna Komisja Kryptograficzna – odpowiada za zarządzanie poufnością informacji w sieciach partii (rządowych) oraz wojskowych,
3) Narodowe Biuro Tajemnic, zwane również Biurem Ochrony Tajemnic – zarządza wszystkimi sieciami niejawnymi,
4) Sztab Generalny Wojska – bierze aktywny udział w ochronie sieci cywilnych przez takie jednostki, jak m.in. 3/PLA i 4/PLA[6].

Innymi ważnymi instytucjami są również: Ministerstwo Przemysłu i Technologii Informacyjnych, Ministerstwo Bezpieczeństwa Narodowego oraz Polityczne Biuro Propagandy.

W dokumencie „27" podkreśla się istotę tzw. aktywnej obrony, która w ujęciu chińskim przyjmuje nieco inną postać niż w przypadku krajów członkowskich NATO. Przez a k t y w n ą o b r o n ę rozumie się działania wywiadowcze, których celem jest pozyskanie jak największej liczby informacji, wśród których mogą znaleźć się również dane dotyczące potencjalnych zagrożeń sieciowych. Do priorytetów zawartych w dokumencie można zaliczyć:

– utworzenie wielowymiarowego schematu ochrony informacyjnej infrastruktury krytycznej kraju,
– utrzymanie standardu przyjmowania produktów do sieci zamkniętych przez biura certyfikacyjne znajdujące się w każdej jednostce odpowiedzialnej,
– rozwój polityki szyfrowania w kierunku podpisów elektronicznych, certyfikatów autoryzacyjnych itd.,

[4] *Defense Policy*, Ministry of National Defense The People's Republic of China [online], http://eng.mod.gov.cn/Database/DefensePolicy/index.htm [dostęp: 1 XI 2014].

[5] L. Yuxiao, *Cyberspace security and International cooperation in China*, w: *Report: China and cybersecurity – political, economic and strategic dimensions*, San Diego 2012, s. 4–5.

[6] J. Goodrich, *Chinese civilian cybersecurity: stakeholders, strategies and policy*, w: *Report: China and cybersecurity…*, s. 5–6.

- udoskonalenie przez Narodowe Centrum Informacji systemu zarządzania oraz analizy ryzyka bezpieczeństwa informacyjnego,
- standardy bezpieczeństwa teleinformatycznego Chin mają być zatwierdzane przez Chińską Narodową Komisję ds. Technicznych Standardów Ochrony Informacji zwaną również TC260 składającą się z przedstawicieli agencji bezpieczeństwa. Jest niedostępna dla obcych uczestników,
- rozwój projektów badawczych nadzorowanych przez takie instytucje jak: Fundacja Rozwoju Przemysłu lub Krajowe Laboratorium Ochrony Informacji[7].

Władze Chin określają również podstawowe zagrożenia bezpieczeństwa kraju. Wśród nich wymieniają: cyberprzestępczość i hacking, propagandę internetową oraz luki w systemach wojskowych. Ciekawe jest określenie propaganda internetowa w kontekście dostępu obywateli do treści propagowanych przez kraje zachodnie, które mają wprowadzać ich w stan niewiedzy i dezinformacji. Chiny określają siebie mianem kraju, który zajmuje pierwsze miejsce w światowym rankingu państw najczęściej atakowanych w cyberprzestrzeni. Wskazuje się również wszelkiego rodzaju treści ogólnie dostępne w Internecie oraz portale społecznościowe jako podstawowe narzędzia dezinformacji, które należy kontrolować[8]. W związku z takim podejściem wprowadzono wiele systemów cenzury internetowej, która dopuszcza tylko wybrane treści do ogólnego wglądu obywateli. Cenzura oraz kontrola zawartości treści w Internecie jest – w porównaniu do innych państw – najbardziej rozbudowanym systemem na świecie[9]. Poza uregulowaniami prawnymi, które dokładnie wskazują, jakie treści są dozwolone, zastosowano wiele rozwiązań technologicznych. Stosuje się blokowanie witryn internetowych przez wykrywanie słów już na poziomie routerów, które są tak zaprogramowane, aby na połączeniu z serwerami proxy wykrywać istotne dla władz stwierdzenia, i jeżeli zostają wykryte – odsyłać użytkownikowi wiadomość blokującą dostęp[10]. Te strony, które zostały w taki sposób skonstruowane, aby omijać zautomatyzowane formy filtrowania, są wyszukiwane przez „cyberpolicję", czyli około 30 000 zatrudnionych przez Ministerstwo Bezpieczeństwa Publicznego pracowników, którzy ręcznie przeszukują strony internetowe w poszukiwaniu nielegalnych treści[11]. Próba dokonania pełnej kontroli Internetu w Chinach przechodziła trzy fazy rozwoju: automatycznego i ręcznego blokowania treści, filtrowania treści znajdujących się w sieciach Chin na podstawie międzynarodowych umów z operatorami i dostawcami Internetu oraz model, który zawiera w sobie oba powyższe w połączeniu z trzecim – samocenzurą obywateli, którzy są nagradzani za ujawnianie nielegalnych treści w Internecie[12]. Tak wiele rozwiązań dotyczących sfery obywatelskiej w Internecie, w połączeniu z mocnymi zabezpieczeniami sieci wojskowych oraz rządowych tworzy wrażenie, że chiński Internet aspiruje do bycia strukturą zamkniętą, otwieraną tylko wyselekcjonowanym jednostkom. W literaturze używa się często określenia „Wielki Cyfrowy/CyberMur Chiński". Coś, co teoretycznie jest mało możliwe do osiągnięcia, Chiń-

[7] Tamże, s. 7.

[8] C.A. Cooper, *Chinese Perceptions of and Strategic Response to Threats in Cyberspace*, w*: Report: China and cybersecurity*…, s. 8–9.

[9] M.W. Lau, *Internet Development and Information Control in the People's Republic of China*, Report for Congres, USA 2005, s. 2 [online], www.fas.org/sgp/crs/row/ [dostęp: 3 XI 2014].

[10] Tamże, s. 5–6.

[11] Tamże, s. 6–7.

[12] W. Yang-Wang, *Who's blocking the Chinese Internet? The rise of cybercultures and the generational conflicts in China*, s. 2–3 [online], http://eprints.qut.edu.au/61096/1/Who%27s_blocking_the_Chinese_Internet_–_Hard_Copy_Chapter.pdf [dostęp: 29 X 2014].

czycy próbują zrobić w skali do tej pory niespotykanej – na ponad miliardzie użytkowników wszystkich sieci teleinformatycznych Chin. Oczywiście nigdy nie będzie możliwe osiągnięcie w stu procentach zamierzonego celu, jakim jest pełna kontrola sieci, co wynika m.in. z nonkonformizmu i indywidualizmu obywateli, prowadzona działalność propagandowa oraz wojna psychologiczna ograniczają jednak również i to potencjalne źródło zagrożenia.

Potencjał ofensywny

Analizując Państwo Środka w kontekście działań w sferze cyber, nie można pominąć zagadnień związanych z wywiadem elektronicznym i potencjałem ofensywnym Chin, który jest uznawany za jeden z największych, jeżeli nie za największy na świecie. Najbardziej znane jednostki wywiadu odpowiedzialne za tę formę działalności, to wymieniane przez niektórych autorów AL.-W3 odpowiadające za SIGINT i Wojnę Informacyjną oraz AL.-W4 realizujące zadania związane z wojną elektroniczną[13]. To jednak zaledwie dwie z wielu jednostek wywiadowczych, które zajmują się działaniami ofensywnymi. Obecnie wykorzystuje się różne metody ataków do pozyskiwania informacji i materiałów wywiadowczych o różnym charakterze lub też ukierunkowanego szpiegowania osób czy instytucji. W myśl chińskich założeń wykorzystanie tego potencjału musi być również możliwe w czasie cyberwojny, a nie tylko w czasie pokoju.

Militarna koncepcja wojny elektronicznej ewoluowała na przestrzeni lat. Obecnie stwierdza się, że możliwości technologiczne są najważniejsze dla przyszłości prowadzenia operacji wojskowych. Li Deyi, zastępca dziekana Wydziału Teorii Działań Wojennych i Strategii Wojskowej Akademii Nauk, jako najważniejsze czynniki wskazujące na taki stan rzeczy wymienia:

- zmianę sposobu myślenia, dopasowując go do bieżących i przyszłych realiów w celu osiągania zwycięstwa,
- nierozerwalność strategii i technologii w dzisiejszych czasach. „Superautostrady informacyjne" mogą stanowić źródło działań dezinformacyjnych,
- opracowywanie strategii opierających się na informacji, systemach informatycznych oraz modelach informatycznych w celu zredukowania efektywności bojowej przeciwnika,
- informacje i technologie informacyjne determinujące efektywność bojową oraz decydujące o zwycięstwie lub porażce. Są one jednym z trzech podstawowych zasobów strategicznych,
- nowy model myślenia integrujący z sobą analizę informacji i zdolności strategiczne,
- nowy model podejścia do sieci – sieci są systemami, wymagają zatem systematyzacji w myśleniu.
- Te zmiany oraz wiele innych czynników wpływających na reorganizację sytemów wewnątrz państwowych prowadzą dalej do konkluzji dotyczących wykorzystania technik informacyjnych na polu walki. Najważniejsze wnioski dotyczą następujących zagadnień:
- zastępcza destrukcja: zamiast używania ciężkiej broni do zniszczenia wrogich dowództw, można wykorzystywać technologie informacyjne, aby je unieszkodliwiać,

[13] R. Faligot, *Tajne służby chińskie. Od Mao do igrzysk olimpijskich*, Katowice 2009, s. 508.

- elektroniczne działania wojenne: za pomocą technik komputerowych, radiowych czy elektromagnetycznych można niszczyć wrogie centra wywiadowcze, radary itp.,
- wojenne oszustwa: można używać symulowanych ataków komputerowych w celu ukrycia realnych działań lub zmylenia wywiadu wroga,
- utrzymanie tajemnicy operacyjnej: za pomocą technik kryptograficznych i innych technik komputerowych można ukrywać realne zamierzenia,
- wojna psychologiczna: można skutecznie używać nowoczesnych środków przekazu w celu obniżenia morale przeciwnika[14].

Warto zauważyć, że w chińskiej literaturze wojskowej stwierdza się, iż: (…) *cyberataki w połączeniu z możliwościami unieszkodliwiania amerykańskich satelitów oraz zdalnych centrów dowodzenia stanowią specjalną broń, która może zahamować amerykańskie działania wojenne w rejonie Zachodniego Pacyfiku*[15]. Chińczycy w wyścigu cyberzbrojeń uważają Amerykanów za największego przeciwnika i wiele doktryn oraz myśli przewodnich jest konstruowanych, mając właśnie ten kraj na uwadze. Poza planami, w jaki sposób można wykorzystać udoskonalane techniki penetracyjne, jednostki chińskie na bieżąco testują te techniki, stosując działania tzw. zwiadu dalekiego zasięgu, w którym pozyskuje się niejawne informacje ekonomiczne, zbrojeniowe czy naukowe. Ćwiczenia z zakresu nielegalnego pozyskiwania informacji oraz kamuflowania działań są często regularnie przeprowadzane w wyspecjalizowanych jednostkach Chińskiej Armii Ludowo-Wyzwoleńczej[16]. W związku z tak szybkim rozwojem technologii informacyjnych, a co za tym idzie – zwiększaniem ich potencjału, chińscy stratedzy opracowali koncepcję działania o nazwie *Moulue*, co, tłumacząc z języka chińskiego, oznacza: *mou* – pomysł, podstęp; *lue* – plan, podstęp. Razem określenie *moulue* można przetłumaczyć jako taktykę podstępu oraz sztuczek[17]. Działając w myśl tej idei, systemy państw na całym świecie stają się ofiarami cyberwojny zwanej „podjazdową", w której łupem padają wrażliwe dane. Operacje wywiadowcze prowadzone przez Wydział 3 Sztabu Generalnego (AL.-W3) są często realizowane nie bezpośrednio z siedzib oficjalnych i nie przez oficerów, a przez wynajmowanych i opłacanych cywili. W ten sposób Chiny dodatkowo zabezpieczają się przed oskarżeniami o działalność szpiegowską, w momencie gdy jakaś akcja zostaje upubliczniona[18]. Do głównych obszarów inwigilowanych przez Chiny należą: systemy komputerowe Tybetu (GhostNet[19]), systemy obronne Ameryki oraz krajów europejskich, własność intelektualna znajdująca się w systemach amerykańskich oraz państw europejskich, szczegóły związane z pozycją negocjacyjną firm konkurujących z firmami chińskimi o wpływy w konkretnych sektorach[20]. W 2013 r. został opublikowany raport, w którym amerykańska firma Mandiant zajmująca się cyberbezpieczeństwem odkryła kulisy działalności jednostki APT1, która rzekomo miała być jednostką ope-

[14] M. Chanosoria, *Informationising Warfare: China Unleashes the Cyber and Space Domain*, New Delhi 2010, s. 4–6.

[15] L. Wortzel, *The Chinese Way of (Cyber) War*, w: „Defense Dossier" 2012, nr 4, s. 1 (tłumaczenie własne autora).

[16] T.L. Thomas, *The dragons…*, s. 104–106.

[17] Tamże, s. 120.

[18] N. Inkster, *Chinese Intelligence Operations and Transnational Consequences*, w: *Report: China and cybersecurity…*, s. 24.

[19] GhostNet – komputerowa sieć szpiegowska, wykryta po raz pierwszy w sieciach tybetańskich, nadzorowana z terytorium Chin. Obecnie zainfekowane są nią komputery w co najmniej 103 krajach.

[20] N. Inkster, *Chinese Intelligence Operations…*, s. 25–26.

racyjną sieciowych działań wywiadowczych. Według informacji zawartych w raporcie można się dowiedzieć, że jednostka ta (występująca pod inną nazwą: Oddział 61398) była wyposażona w zupełnie oddzielną sieć doprowadzoną przez rządowego dostawcę usług internetowych. Metodą ich działania nie były jednorazowe ataki, tylko ataki ukierunkowane i zakamuflowane typu APT. Jeżeli eksploracja systemu kończyła się sukcesem, maskowano swoją obecność i pozostawano „w środku" w celu stałego poboru informacji. Według autorów omawiana jednostka stanowi drugie biuro wspominanego już trzeciego departamentu Sztabu Generalnego (3/PLA)[21]. Pomimo wielu zbieżności z ideami i sposobem działania władz chińskich, należy zaznaczyć, że raport ten nie został zweryfikowany i potwierdzony, tak więc jest oparty na poszlakach i nie można go uznawać za pewne źródło wiedzy.

Pomijając jednak pytanie, czy ataku dokonują wyspecjalizowane jednostki rządowe, czy wynajmowane grupy, pewne jest, że taka działalność jest koordynowana przez najwyższe organy. Ta pewność wynika m.in. z wykrywania w czasie rzeczywistym niektórych takich aktywności. W styczniu 2011 r. Google ogłosiło, że padło ofiarą ataku penetrującego pochodzącego z Chin. Atak, który miał być skierowany na dane komercyjnych firm współpracujących z Google, miał być przeprowadzony z dwóch źródeł: Shanghai Jiaotong University i Lanxiang Vocational School. Oficjalnie chińskie władze wyparły się tego ataku, istnieje jednak wiele poszlak (poza technologicznymi również dobór firm był nieprzypadkowy dla interesów Chin), które wskazują na skoordynowane działanie[22]. Inne przypadki ataków władz Chin odnotowane w źródłach otwartych to: atak „tytanowego deszczu" na Departament Obrony USA oraz infiltracja 70 proc. baz danych Pentagonu[23].

Warto zwrócić uwagę, że poza działaniami „czysto" państwowymi Chińska Republika Ludowa wykorzystuje również firmy do prowadzenia działań na skalę globalną. Spośród chińskich firm wybiera się tzw. championy, których celem jest podbój rynków zagranicznych, a później rekrutowanie tamtejszych specjalistów jako wykładowców i ekspertów w celu wykorzystywania ich wiedzy i posiadanych przez nich koneksji na rynku. Przykładami tego typu firm mogą być np. Huawei czy ZTE[24].

Taka liczba, skala i powszechność ataków pochodzących z terytorium Chin jest spowodowana dużą liczbą czynników wpływających na ich skuteczność i efektywność. Najważniejsze z nich to:

- stosunkowo słabe zabezpieczenia systemów teleinformatycznych w USA,
- anonimowość cyberataków,
- możliwość wykorzystania ludzi i sprzętu jako surogatów w celu zamaskowania prawdziwego źródła ataku,
- brak regulacji oraz zapisów prawnych w prawie międzynarodowym dotyczących ataków w cyberprzestrzeni,
- długo- i krótkookresowe możliwości działań wywiadowczych,
- skłonność krajów zachodnich do dialogu zamiast konfrontacji w cyberprzestrzeni,

---

[21] *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant 2013, s. 5–8 [online], http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [dostęp: 15 X 2014].

[22] T.L. Thomas, *Google Confronts China's "Three Warfares"*, Fort Leavenworth 2010, s. 101–105; dostępne również online: http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2010summer/Thomas.pdf [dostęp: 12 VII 2014].

[23] T.L. Thomas, *The dragons…*, s. 184–185.

[24] L. Wortzel, *Assesing The Chinese Cyber Threat…*, s. 3–4.

– ponadnarodowy charakter działań w cyberprzestrzeni,
– łatwy dostęp do tajemnic gospodarczych, militarnych itp.

Rozbudowany system aparatu rządowego w połączeniu z wykorzystywaniem wielu grup hakerskich wynajmowanych przez rząd do realizacji zadań pokazuje, w jaki sposób, nawet przy rozbudowanych programach detekcyjnych, można unikać odpowiedzialności za popełnione przestępstwa w cyberprzestrzeni, jednocześnie w pełni wykorzystując zgromadzone materiały. Chiny wraz ze Stanami Zjednoczonymi jako pierwsze stworzyły uniwersalne programy szpiegowskie, wykorzystywane szeroko w sieciach teleinformatycznych różnego typu. Mogą to być sieci otwarte, jak w przypadku GhostNet, lub sieci przemysłowe, jak to było w przypadku wirusa Stuxnet i wykorzystania go pierwotnie w elektrowni jądrowej w Iranie. Jako prekursorzy innowacyjnych rozwiązań i wykorzystywania złośliwego oprogramowania oraz technik penetracyjnych kraje stojące na dwóch krańcach globu prowadzą nieoficjalny wyścig cyberzbrojeń, określany przez niektórych komentatorów mianem nowej zimnej wojny. W tym wyścigu biorą udział również inni główni aktorzy, tacy jak Rosja, Izrael oraz Iran.

Wykorzystanie grup hakerskich

Dosyć często w opracowaniach specjalistycznych pojawia się wzmianka o grupie Comment Crew, która jest chińską grupą hakerów ściśle współpracujących bądź należących do jednostki PLA 61398[25], będącej częścią drugiego biura w trzecim departamencie[26] Sztabu Generalnego Chińskich Sił Zbrojnych. Jej powiązanie z działaniami chińskiego rządu może być również potwierdzone przez rodzaje ataków, dobierane cele oraz poziom zaawansowania. To właśnie ta grupa odpowiada za jedne z najbardziej zaawansowanych, skutecznych i długotrwałych ataków typu APT[27] na najważniejsze instytucje i firmy odpowiadające za bezpieczeństwo narodowe i międzynarodowe na całym świecie.

Grupa powstała około 2006 r., a miejsce, z którego są prowadzone ataki, znajduje się na przedmieściach Szanghaju, obok siedziby PLA 61398. Comment Crew korzysta dokładnie z tej samej sieci, która została udostępniona praktycznie na wyłączność wspomnianej jednostce[28]. Z analiz wynika, że najczęstszymi celami ataków są m.in. agendy rządowe, firmy zbrojeniowe i operatorzy infrastruktury krytycznej. Powodem ataków jest zazwyczaj chęć zdobycia ściśle tajnych danych dotyczących badań nad nowymi technologiami lub poznanie planów i systemów obsługujących infrastrukturę krytyczną[29]. Według niepotwierdzonych informacji jednostka PLA 61398 może liczyć ponad tysiąc pracowników, grupa Comment Crew zaś, stanowiąca coś w rodzaju elitarnego oddziału zewnętrznego, to nawet kilkadziesiąt osób.

[25] Nie ma dowodów, które mogłyby wskazywać na prawdziwość którejś odpowiedzi. Wiadomo, że grupa realizuje większość ataków dla omawianej jednostki oraz że ataki te są przeprowadzane z lokalizacji znajdującej się w odległości kilkudziesięciu (kilkuset) metrów od głównej siedziby drugiego biura.

[26] Departament ten jest odpowiedzialny m.in. za prowadzenie operacji SIGINT.

[27] APT – Advanced Persistent Threat, ataki polegające na niezauważalnym dostępie do systemów wewnętrznych atakowanego celu i długotrwałej, niewykrywalnej kradzieży danych.

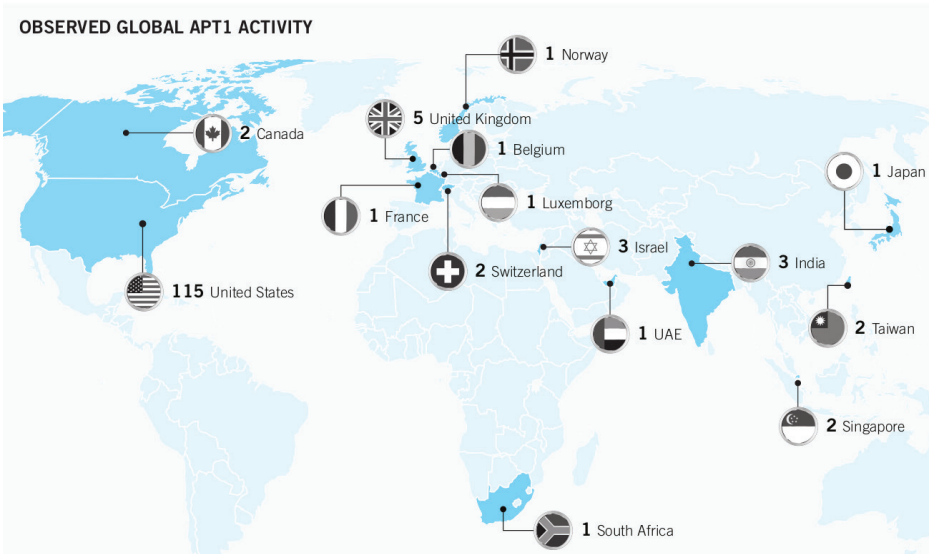
[28] Niespotykane jest, aby grupa hakerów mogła w sposób nieograniczony realizować ataki z jednego miejsca, bez potrzeby ukrywania miejsca lub dyslokacji jej członków w różnych punktach kraju.

[29] A. Martin, *Meet 'Comment Crew,' China's Military-Linked Hackers* [online], http://nymag.com/daily/intelligencer/2013/02/meet–comment–crew–chinas–military–hackers.html [dostęp: 1 XI 2014].

Według Kevina Mandii prezesa firmy Mandiant:

> (...) albo ataki Comment Crew są robione dla jednostki PLA 61398 lub będąc jej częścią, albo w kraju posiadającym jeden z najlepiej rozbudowanych systemów inwigilacji sieci wewnątrz kraju, jakaś grupa prowadzi ataki hakerskie dokładnie z tej samej dzielnicy, w której znajduje się jednostka odpowiadająca za operacje cyberszpiegowskie – co wydaje się mało prawdopodobne[30].

Warto odnotować, że poziom zaawansowania, częstotliwość ataków oraz dobór złożoności celów ciągle rosną. Poza systemami takich gigantów, jak Coca Cola, które zostały spenetrowane w momencie prowadzenia negocjacji z jedną z chińskich firm chcących współpracować z Amerykanami[31], ofiarą ataku padła również firma RSA zajmująca się budową rozwiązań dla systemów bezpieczeństwa, która stworzyła tzw. Tokeny ID, służący pracownikom wszystkich agencji wywiadowczych w USA. Straty dla firmy oraz dla kraju po tak precyzyjnie przeprowadzonym ataku bywają nie do oszacowania – zarówno pod względem spadku poziomu zabezpieczeń, jak i ekonomicznym i finansowym[32]. Co ciekawe i warte odnotowania, większość ataków APT była przeprowadzana na firmy i instytucje znajdujące się w krajach anglojęzycznych[33].



Mapa. Liczba ataków Comment Crew typu APT z podziałem na kraje, w których je przeprowadzono.

Źrodło: www.threatpost.com [dostęp: 12 X 2014].

[30] D.E. Sanger, D Barboza, N. Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.* [online], http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=1& [dostęp: 17 X 2014] – tłumaczenie własne autora.

[31] Na skutek zdobycia informacji o technikach negocjacyjnych i założonych celach Coca Cola straciła miliardy dolarów.

[32] D.E. Sanger, D. Barboza, N. Perlroth, *Chinese Army Unit Is Seen…*

[33] M. Mimoso, *Comment Crew Expose a new level of China attack attribution* [online], http://threatpost.com/comment–crew–expos–new–level–china–attack–attribution–021913/77538 [dostęp: 18 X 2014].

Warto zauważyć, że aktywność grupy współpracującej z PLA 61398 była niezmiennie intensywna do początku 2013 r. Wtedy to zaobserwowano zaprzestanie prowadzenia również tych operacji, które były w trakcie realizacji. Eksperci twierdzą, że był to czas zmiany taktyki działania oraz przebudowy infrastruktury technicznej w celu usprawnienia operacji oraz zmniejszenia wykrywalności[34]. Dzięki temu zabiegowi od tego czasu, pomimo wzrostu aktywności grupy, jej działania są dużo trudniejsze do wykrycia. Poszlaki oraz tropy, które prowadziły do Comment Crew, a zostały ujawnione w raporcie firmy Mandiant, są w dużej części nieaktualne. Według ekspertów nie jest prawdą, że zaprzestano ataków na dotychczasowe cele i rozpoczęto wyłącznie nowe kampanie. Wszystkie poprzednie operacje są prowadzone z nowej infrastruktury w zmieniony sposób[35].

Comment Crew już po zmianie taktyki działania przeprowadziła wiele skutecznych ataków. Dwa, zrealizowane jeszcze w latach 2011–2013, opublikowano już w czasie ich nowego sposobu działania. W maju 2013 r. do opinii publicznej dotarły informacje o penetracji systemów amerykańskiej firmy QinetiQ, realizującej zlecenia dla amerykańskich sił zbrojnych. Łupem hakerów miały paść gigabajty ściśle tajnych danych dotyczących technologii wykorzystywanej przy budowie śmigłowców i dronów. Model chińskiego drona zbliżony do skradzionych projektów amerykańskich zdaje się potwierdzać tę teorię[36]. Drugą serię ataków Comment Crew przeprowadziła na izraelskie firmy zbrojeniowe oraz agendy rządowe powiązane z projektem „Iron Dome" (system przeciwrakietowy chroniący Izrael)[37]. Wymieniane firmy to m.in.: Elisra Group, Israel Aerospace Industries i Rafael Advanced Defense Systems. Okazuje się, że skradziono ponad 700 dokumentów dotyczących szczegółów technicznych „Żelaznej Kopuły" oraz schematów i projektów rakiet balistycznych Arrow III, które zostały zaprojektowane przez firmę Boeing, a także pojazdów UAV. Taki wyciek informacji ma istotny wpływ na bezpieczeństwo kraju, który padł ofiarą ataku. Pociąga za sobą również stratę środków zainwestowanych w ten system, który był finansowany nie tylko przez rząd Izraela, lecz także przez Stany Zjednoczone (w wysokości jednego miliarda dolarów)[38].

Bardzo interesujące wydają się również kwestie personalne dotyczące jednostki. Pomocne w typowaniu specjalistów znajdujących się w grupie mogą być wymagania stawiane osobom chcącym dostać się do jednostki PLA 61398. Permanentna rekrutacja jest prowadzona dla: specjalistów ds. ukrywania komunikacji, anglistów, administratorów sieci, specjalistów ds. przetwarzania sygnałów cyfrowych oraz bezpieczeństwa sieci[39].

Najaktywniejszymi członkami Comment Crew jest kilka osób, z których jedna używa nicka Ugly Gorilla. Jego działania rozpoznano już w 2004 r. Jest on twórcą m.in. malware'u o nazwie MANITSME oraz WEBC2-UGX, które stworzył w 2007 r., a które to do 2013 r. były wykorzystywane przy atakach APT prowadzonych przez Comment Crew. Inny haker należący do grupy to tzw. DOTA. Według niektórych publiko-

[34] P. Paganini, *Chinese hacker group 'Comment Crew' is still active and operating under cover* [online], http://thehackernews.com/2013/06/Comment–Crew–Chinese–Hackers.html [dostęp: 12 X 2014].

[35] Tenże, *Comment Crew, China–based group of hackers is changing tactics* [online], http://securityaffairs.co/wordpress/15605/intelligence/hackers–comment–crew–i–changing–tactics.html [dostęp: 12 X 2014].

[36] J.E. Dunn, *Chinese 'Comment Crew' hackers emptied QinetiQ of top–secret military data* [online], http://news.techworld.com/security/3445282/chinese–comment–crew–hackers–emptied–qinetiq–of–top–secret–military–data/ [dostęp: 14 X 2014].

[37] P. Paganini, *Chinese Hackers Comment Crew stole plans of Iron Dome Defense System* [online], http://securityaffairs.co/wordpress/27132/cyber–crime/comment–crew–stole–plans–iron–dome.html [dostęp: 12 X 2014].

[38] B. Krebs, *Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System* [online], http://krebsonsecurity.com/tag/comment–crew/ [dostęp: 27 IX 2014].

[39] *ATP1: Exposing One of China's Cyber Espionage Units*, Washington 2013, Mandiant, s. 10.

wanych analiz odpowiada on za fazę wstępną ataku, czyli za przygotowywanie akcji phishingowych. Wiadomo, że często używał również nicków „Rodney" albo „Raith" do komunikacji mailowej w języku angielskim. Trzecim członkiem grupy opisywanym w raporcie Mandiant jest tzw. Super Hard. Jest on znany m.in. ze stworzenia dwóch wirusów: AURIGA i BANGAT[40]. Wszyscy trzej wymienieni posługiwali się adresami IP oraz numerami telefonów z okręgu szanghajskiego. W 2013 r. ujawniono również tożsamość pięciu innych osób zaangażowanych w ataki na krytyczne systemy Stanów Zjednoczonych, za którymi FBI wydało list gończy[41]. Nie jest jednak jasne, czy są oni członkami Comment Crew, czy jednostki PLA 61398, czy też ich obu.

Poza kwestiami osobowymi warto również wskazać, w ujęciu ogólnym, podstawowy model ataku wykorzystywany zarówno przez Comment Crew, jak i przez jednostkę PLA 61398. Ataki APT charakteryzują się następującymi fazami:

- wstępny rekonesans i wybór celu,
- uzyskanie wstępnego dostępu do sieci; na tym etapie najczęściej wykorzystywaną metodą jest phishing mailowy, w celu przekazania pracownikom złośliwego oprogramowania, które umożliwia dostęp do ich kont i uprawnień,
- stabilizacja dostępu, która następuje po zainstalowaniu malware'u na komputerze ofiary. Wtedy w sposób zdalny napastnik formułuje komendy oraz programuje system w taki sposób, aby pozostać niezauważonym – może się to dziać przez implementację jakichś formuł tworzących napastnikowi nieistniejący do tej pory *backdoor*,
- po stabilizacji następuje etap główny, na który składają się cztery procesy: zwiększanie uprawnień w sieci wewnętrznej, rekonesans wewnętrzny po sieci i pozyskiwanie danych, sprawdzanie bezpieczeństwa połączenia i maskowanie śladów obecności, utrzymywanie obecności przez jak najdłuższy czas,
- faza wyjścia inicjowana albo przez napastnika, jeżeli uzyskał już wszelkie niezbędne informacje i wykonał misję, albo przez dyskredytację operacji i odnalezienie błędów przez dział bezpieczeństwa IT w danej instytucji[42].

Konkluzje

Chiny są znane z dynamicznego rozwoju siatki szpiegowskiej na świecie. Również ten rodzaj szpiegostwa (cyberszpiegostwo) udoskonalają w sposób precyzyjny i szybki. Globalna forma działania, a także posługiwanie się językiem angielskim jako uniwersalnym w krajach anglojęzycznych lub w organizacjach międzynarodowych daje możliwość wpływania na dużą i ważną grupę państw, organizacji i firm. Ich główna metoda, jaką są ataki APT (przy wykorzystaniu wielu różnych narzędzi do realizacji celów), wskazuje na motywację polityczną. Brak działań o charakterze wizerunkowym, podmienianie zawartości stron czy ataki typu rozproszona odmowa usługi (DDoS) również mogą potwierdzać tę tezę. Cele są dobierane w sposób precyzyjny, a priorytetem jest pozyskanie jak największej liczby informacji, które mogą być wykorzystane do uzyskania przewagi w konkretnej dziedzinie gospodarki albo w rozwoju technologicznym sił zbrojnych. Comment Crew będąca częścią PLA 61398 lub grupą realizującą dla tej

[40] Tamże, s. 51–58.
[41] B. Krebs, *Hackers Plundered Israeli Defense Firms…*
[42] *ATP1: Exposing One of China's Cyber Espionage Units…*, s. 27–38.

jednostki misje prowadzi je przy wsparciu lub (i) akceptacji władz Chińskiej Republiki Ludowej, co z jednej strony daje grupie ochronę, z drugiej zaś pozwala na większą swobodę w działaniu.

W związku z prowadzeniem działalności globalnej również Rzeczypospolita Polska może być potencjalnym celem ataków wyprowadzanych z Chin. Zagrożonymi obszarami mogą być: sektor energetyczny, w związku z prowadzoną dywersyfikacją źródeł energii oraz środków przesyłu oraz sektor zbrojeniowy, biorący udział w realizacji programu modernizacji polskiej armii, która ma zostać zakończona do 2022 r. Nie są to jedyne sektory, które mogą paść ofiarą ataku, wydaje się jednak, że stanowią grupę podwyższonego ryzyka.

Abstrakt

W prezentowanym artykule autor porusza tematykę dotyczącą cyberbezpieczeństwa, ukazując to zjawisko z perspektywy jednego z najsilniejszych w tym aspekcie krajów – Chin. Państwo Środka uważane jest za jedno z trzech najsilniejszych cybermocarstw oprócz USA oraz Federacji Rosyjskiej. Analiza wybranych obszarów działalności ChRL jest oparta zarówno na wskazaniu metod organizacyjnych, instytucjonalnych oraz strategicznych w odniesieniu do potencjału defensywnego i ofensywnego, jak i na przedstawieniu najczęściej wykorzystywanych narzędzi technologicznych. Autor w swoim studium stara się wskazać na różnice między podejściem do omawianej problematyki realizowanym m.in. w krajach NATO a Chińską Republiką Ludową, dokonując próby określenia efektywniejszych rozwiązań. Całość analizy jest uzupełniona informacjami dotyczącymi grupy Comment Crew posądzanej o realizację zleceń dla rządu w Pekinie oraz przedstawieniem wybranych specjalistów przeprowadzających ataki o charakterze szpiegowskim.

Słowa kluczowe: cyberszpiegostwo, hakerstwo, APT, bezpieczeństwo teleinformatyczne, nowe technologie.

Abstract

In the article the author raises the subject of cybersecurity – from the perspective of one of the most advanced in this aspect countries – China. It is considered as one of three cyber powers alongside with Russian Federation and U.S. The analysis of chosen areas of activity of PRC is based on organizational, institutional and strategic methods in relation to defensive and offensive potential, as well as the most commonly used technological tools. In this study the author tries to point differences between approaches of NATO countries and PRC with attempt for identifying efficient solutions. The whole analysis is supplemented with data on hacker group Comment Crew which carries out missions for the government in Bejing but also on chosen experts, who are thought to prepare cyber espionage attacks.

Keywords: cyber espionage, hacking, APT, ITC security, new technologies.