aut. Małgorzata Fraser 23.07.2021

#CYBERMAGAZYN: PO TRZECH LATACH WOJNY HANDLOWEJ Z USA CHINY OKOPUJĄ SIĘ NA POZYCJI CYFROWEJ POTĘGI

W 2018 roku ówczesny prezydent USA Donald Trump napisał słynnego tweeta o tym, że „wojny handlowe są dobre, bo łatwo się je wygrywa". Trzy lata później teza postawiona przez Trumpa nie sprawdza się – dowodzi prosty rachunek ekonomiczny. Chińska gospodarka nie tylko wytrzymała nakładane przez USA sankcje i cła, ale też szybko odbiła się po pandemii koronawirusa, obecnie umacniając się na pozycji cyfrowej potęgi.

Chiny bardzo szybko poradziły sobie z pandemią koronawirusa i jej gospodarczymi skutkami – również dzięki temu, że koronakryzys pokazał, jak bardzo pracujący i uczący się zdalnie świat jest zależny od chińskiej produkcji urządzeń elektronicznych i telekomunikacyjnych. Okazało się, że tylko chińskie moce produkcyjne są na tyle duże, by móc sprostać rosnącemu popytowi na nowe laptopy, ale też sprzęt medyczny, którego ceny w 2020 roku szybowały do nieznanych wcześniej poziomów.

Choć w 2019 roku Donald Trump nakazał amerykańskim firmom produkcyjnym przeniesienie swojej działalności przemysłowej do USA, bądź też znalezienie innej alternatywy wobec taniej produkcji w Państwie Środka, według agencji Bloomberga obecnie nie ma dowodów na to, że faktycznie firmy zdecydowały się masowo na taki ruch. Spółki, pytane o powody, dla których nie planują przenosić swojej produkcji do innej lokalizacji, przeważnie deklarowały, że powodem jest szybki wzrost chińskiego rynku konsumenckiego, połączony z dużymi lokalnymi możliwościami produkcyjnymi.

Jak wojna handlowa przerodziła się w rywalizację technologiczną…

Sankcje nałożone przez amerykańskie ministerstwo handlu oraz byłego prezydenta USA Donalda Trumpa przełożyły się na utrudnienia w działalności wielkich firm technologicznych z Chin, takich jak Huawei czy SMIC (Semiconductor Manufacturing International Corp.). W opublikowanym na początku tego roku artykule, dwóch badaczy zatrudnionych przez państwową uczelnię w prowincji Jiangsu napisało, że „jeśli USA będą dalej zwiększały swoją blokadę technologiczną, modernizacja Chin i ich postęp na drodze w górę globalnego łańcucha przemysłowego będą niewątpliwie negatywnie dotknięte".

Tak drastyczny wpływ sankcji USA na ChRL obecnie nie jest widoczny – Pekin zmienił strategię i z globalnej ekspansji swoich koncernów technologicznych zrezygnował na rzecz stabilizacji i konsolidacji rynku wewnętrznego. Chiny chcą być technologicznie samowystarczalne – a najlepszym potwierdzeniem tej strategii są styczniowe decyzje Pekinu o zwiększeniu mocy państwa w zakresie strategicznych badań naukowych i rozwoju technologii, które dla władz mają charakter działania ściśle związanego z gospodarką kraju.

… i w cyberwojnę

Wojna handlowa z Chinami to nie tylko cła, ograniczenia eksportowe i inne sankcje nakładane na firmy z Państwa Środka. To również konflikt w cyberprzestrzeni, który trwa co najmniej od kilkunastu lat.

W 2009 roku wszystkie 16 amerykańskich agencji wywiadowczych sklasyfikowało Chiny (zaraz obok Rosji) jako najpoważniejszego adwersarza w cyberprzestrzeni.

Cyberprzestępcy działający na rzecz ChRL wyspecjalizowali się przede wszystkim w atakach, których celem są kradzieże własności intelektualnej – dzięki dużym operacjom skierowanym przeciwko amerykańskim firmom i uniwersytetom, Chiny zdołały wykraść mnóstwo informacji napędzających rozwój gospodarczy i technologiczny Państwa Środka. W 2014 roku - w związku z tymi incydentami - skazano pięć osób, odpowiedzialnych m.in. za cyberataki na firmy Westinghouse Electric i United States Steel Corporation. Oskarżeni to żołnierze cyberjednostki chińskiej armii – tzw. Unit 61398, grupa znana w sieci jako „UglyGorilla" czy „KandyGoo". Na swoim koncie mają setki, a według niektórych analityków – tysiące cyberataków sprofilowanych na pozyskiwanie informacji gospodarczych.

Sprawcy od 2006 roku mieli dokonywać wtargnięć do sieci amerykańskich korporacji, kopiować wymieniane maile, a niejednokrotnie – infekować komputery firm złośliwym oprogramowaniem. Nie jest jasne, jak bardzo chińska gospodarka skorzystała na wykradzionych w ten sposób danych.

Jak czytamy w akcie oskarżenia sformułowanym przez amerykańskie ministerstwo sprawiedliwości - na potrzeby wynikające z tego rodzaju działalności - chińskie służby miały jednak zbudować specjalną bazę danych przechowującą informacje związane z wywiadem gospodarczym i biznesowym.

Cyberataki powstrzymała dyplomacja prezydenta Baracka Obamy, który w 2015 roku ustami swoich urzędników zagroził prezydentowi ChRL Xi Jinpingowi, że obłoży Chiny sankcjami, jeśli te nie zaprzestaną swojej działalności. Punktem zapalnym był atak na biuro personelu Białego Domu, w wyniku którego chińscy cyberprzestępcy pozyskali ponad 20 mln odcisków palców Amerykanów wcześniej poddawanych procedurom weryfikacji pod kątem bezpieczeństwa.

Przez 18 miesięcy po zawarciu umowy z Xi Jinpingiem, która obejmowała powstrzymanie się Chin od cyberataków motywowanych gospodarczo, badacze specjalizujący się w cyberbezpieczeństwie obserwowali znaczący spadek aktywności tego typu.

Wojna handlowa, którą Trump wypowiedział Chinom, ożywiła uśpionych chińskich cyberprzestępców – tym razem działających już nie z inspiracji wojska, lecz Ministerstwa Bezpieczeństwa Państwa, kontrolującego chińskie siły wywiadowcze, służby bezpieczeństwa i tajną policję.

Nasiliły się cyberataki ukierunkowane na wykradanie tajemnic handlowych – jednak znów, nie brało już w nich udziału wojsko i jego jednostki, a sieć powiązanych z administracją państwową firm, w tym – zatrudniających topowych inżynierów oprogramowania w ChRL.

Według niektórych, inżynierowie ci za dokonywanie cyberataków otrzymują dodatkowe wynagrodzenie. Według innych – nie mają wyboru i muszą być w pełni posłuszni odgórnym rozkazom swoich zależnych od państwa przełożonych.

W miniony poniedziałek, Biały Dom oficjalnie oskarżył Ministerstwo Bezpieczeństwa Państwa ChRL o cyberatak na system Microsoft Exchange. W koordynowaniu cyberataków miały brać udział nie tylko firmy i ich współpracownicy, ale również i chińskie wyższe uczelnie, które zarządzają operacjami w

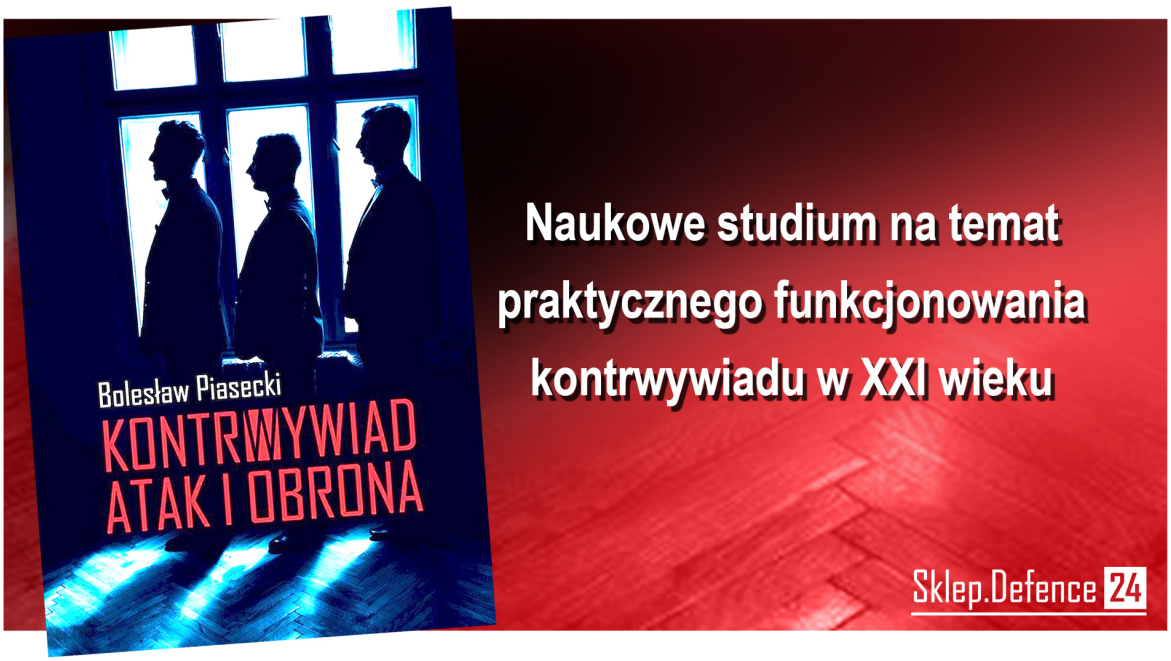
cyberprzestrzeni zlecanymi swoim studentom.

Cyberataki nowym narzędziem gospodarczej „dyplomacji”

Wcześniej w lipcu tego roku Pekin ogłosił wprowadzenie nowych regulacji prawnych, które zobowiążą badaczy cyberbezpieczeństwa do informowania rządu o wszelkich wykrywanych podatnościach typu zero-day, zanim przekażą wiedzę na ich temat firmom dostarczającym usługi cyfrowe.

Wykorzystanie ofensywnych działań z zakresu cyberbezpieczeństwa to nie tylko sposób na budowanie przewagi militarnej, z czego świat zachodni w kontekście Chin zdał sobie sprawę relatywnie niedawno – to dziś przede wszystkim sposób na obchodzenie sankcji gospodarczych, jakie Zachód nakłada na swoich adwersarzy mając nadzieję, że reguły gry na geopolitycznej arenie mimo wszystko są trwałe. Jak pokazuje doświadczenie – ich trwałość nie odbiega znacząco od tej, jaką wykazują się publiczne deklaracje przedstawicieli chińskiej dyplomacji, co rusz zaprzeczających jakiejkolwiek ofensywie w cyberprzestrzeni przeciwko celom na Zachodzie.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.



Fot. Reklama