Mateusz Rakowski

„Nowe wojny" – wybrane aspekty asymetrycznych konfliktów w cyberprzestrzeni[1]

Technologiczny postęp, który obserwujemy od czasów II wojny światowej, przyczynił się między innymi do rozwoju radiotelekomunikacji. Jednym z głównych wydarzeń było stworzenie rozległej sieci ARPANET[2], która została zaprezentowana przez Donalda Daviesa[3] 5 sierpnia 1968 r.[4] Dała ona początek erze Internetu, tworząc tym samym nową przestrzeń cybernetyczną. Pomimo prowadzenia prac już od końca lat 70. XX w., za początek Internetu w Polsce uznaje się 17 sierpnia 1991 r., kiedy po raz pierwszy nawiązano łączność przez protokół TCP/IP[5] z Centrum Komputerowym Uniwersytetu w Kopenhadze[6]. Nowa sieć gwałtownie rozszerzała się, obejmując swym zasięgiem cały glob. Szacuje się, że współcześnie 46,1 proc. światowej populacji korzysta z Internetu[7], włączając w to pojedynczych użytkowników, podmioty sektora prywatnego oraz instytucje państwowe.

1. Cyberprzestrzeń jako przestrzeń nieograniczona i ekspansywna oraz jej podstawowe elementy

Analizę problemu cyberwojen należy poprzedzić próbą zdefiniowania cyberprzestrzeni. *Polska Polityka Ochrony Cyberprzestrzeni* z 2013 r. opisuje tę sferę jako: (…) *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinfor-*

---

[1] Fragment pracy licencjackiej pt. *„Nowe wojny" - wybrane aspekty asymetrycznych konfliktów w cyberprzestrzeni*, która została wyróżniona w konkursie Szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2015/2016). Autor jest absolwentem Akademii im. Jana Długosza w Częstochowie, Wydział Filozoficzno-Historyczny. Redakcja dokonała w tekście niezbędnych poprawek oraz zmian numeracji przypisów (przyp. red.).

[2] *Advanced Research Projects Agency Network* (Sieć Agencji Zaawansowanych Projektów Badawczych) – stworzona przez Advanced Research Projects Agency, ARPA (obecnie: Defense Advanced Research Projects Agency, DARPA) pierwsza rozległa sieć, będąca przodkiem współczesnej sieci World Wide Web. Na jej podstawie stworzono wykorzystywany dziś protokół TCP/IP.

[3] Donald Davies (7 czerwca 1924 r. – 28 maja 2000 r.) – walijski naukowiec, od 1947 r. związany z National Physical Laboratory (Wielka Brytania), twórca konceptu komutacji pakietów, stanowiących podstawę działania Internetu w formie, która jest obecnie wykorzystywana, http://www.npl.co.uk/people/donald-davies [dostęp: 10 XII 2015].

[4] http://news.bbc.co.uk/2/hi/ technology/7541123.stm [dostęp: 10 XII 2015].

[5] TCP/IP (*Transmission Control Protocol/Internet Protocol*) – warstwowy model struktury protokołów komunikacyjnych, na których jest oparty dzisiejszy Internet. Został stworzony w latach 70. XX w. przez DARPA. Obecnie TCP/IP ma skomplikowaną strukturę, gdyż w rzeczywistości stanowi całą rodzinę protokołów komunikacyjnych, funkcjonujących w odrębnych warstwach modelu, http://www.garykessler.net/ library/tcpip.html [dostęp: 10 XII 2015].

[6] http://www.nask.pl/run/n/Historia [dostęp: 20 I 2016].

[7] http://internetworldstats.com/stats.htm [dostęp: 10 XII 2015].

matyczne, (...) *wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*[8]. Ustawodawca ujmuje niniejsze pojęcie w rozumieniu informacyjno-technicznym, zaznaczając, że przedmiotem środowiska sieciocentrycznego są dane oraz towarzyszące im procesy – nie tylko przesyłu, lecz także szeroko pojętego przetwarzania informacji. Takie rozumienie cyberprzestrzeni czyni z niej jednolity, logicznie wydzielony obszar, jednak nie precyzuje aspektów społecznych.

Podobne ujęcie środowiska sieciocentrycznego wyraża jedna z najbardziej rozpowszechnionych na świecie definicji, opracowana przez Departament Obrony Stanów Zjednoczonych Ameryki, zgodnie z którą cyberprzestrzeń (*cyberspace*) to: (…) *globalna domena składająca się z współzależnych sieci tworzonych przez struktury informatyczne oraz zawarte w nich dane, w tym: internetu, telekomunikacji, systemów komputerowych oraz zawartych weń procesorów (kontrolerów)*[9]. Również w tym przypadku jest pomijany aspekt społeczny, niezwykle ważny dla szeroko rozumianego bezpieczeństwa. Niemniej jednak w przytoczonej definicji szczególnie została podkreślona globalność całej sieci tworzonej przez infrastrukturę informatyczną, co powinno być podstawą dalszych rozważań.

Opublikowana w 2011 r. *Strategia Cyberbezpieczeństwa Zjednoczonego Królestwa* Wielkiej Brytanii stanowi, iż: (…) *cyberprzestrzeń jest interaktywną domeną stworzoną z cyfrowych sieci, wykorzystywaną do przechowywania, modyfikowania oraz przesyłania informacji. Zawiera internet, ale także pozostałe systemy informatyczne, wspierające nasz biznes, infrastrukturę oraz usługi.* (…) *Jej zasięg rozwija się z każdym podłączonym urządzeniem – naszymi telewizorami, konsolami do gier czy nawet artykułami gospodarstwa domowego*[10]. Ta definicja wskazuje, iż przestrzeń cybernetyczną tworzy nie tylko globalna sieć informacyjna, lecz także wszystkie sieci lokalne – nawet w formie współpracujących ze sobą urządzeń codziennego użytku. Pojęcie interaktywności wyróżnia szczególnie powyższe sformułowanie, gdyż podkreśla, że opisywane środowisko może być kształtowane przez użytkowników – zarówno przez aspekt logiczny (informacyjny), jak i infrastrukturalny (podłączanie oraz wykorzystywanie urządzeń).

Analizując powyższe definicje, można wnioskować, że cyberprzestrzeń to logicznie wyznaczony, wirtualny obszar o globalnym zasięgu, obejmujący równocześnie zarówno Internet, jak i wszelkiego rodzaju sieci miejscowe oraz pojedyncze

[8] *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, s. 5.

[9] Oryg.: „*A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors*" (tłum. aut.), Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms* 08 November 2010, as amended through 15 October 2015, 2015, s. 58.

[10] Oryg.: „*Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.* (...) *And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances*" (tłum. aut.), The UK Cyber Security Strategy. *Protecting and promoting the UK in a digital world,* London 2011, s. 11.

urządzenia techniczne (przechowujące dane cyfrowe)[11]. Na tę przestrzeń składa się przede wszystkim informacja będąca jej przedmiotem, podlegająca interakcji z pozostałymi elementami. Wśród nich należy wyróżnić użytkowników – jednostki lub zbiorowości modyfikujące, odbierające i przesyłające dane cyfrowe, a także relacje zachodzące między nimi. Omawiane powiązania czynią z przestrzeni cybernetycznej obszar nowych stosunków społecznych, politycznych oraz militarnych[12]. Stanowią przez to jedną ze składowych części „nowych wojen". Jednocześnie istotą nie jest suma operacji użytkowników, lecz idea wirtualnej przestrzeni, istniejącej równolegle do rzeczywistości, posiadającej też własną „fizykę", w której zamiast cząstek elementarnych istnieją bity i bajty[13]. Ponadto oprócz powszechności oraz interaktywności jedną z głównych cech omawianego środowiska jest ekspansywność zachodząca na dwóch płaszczyznach: logicznej oraz technicznej.

Pomimo globalnego charakteru cyberprzestrzeni, dostęp do jej zasobów jeszcze nie jest równomierny na całym świecie – poszczególne regiony różnią się liczbą użytkowników sieci w stosunku do miejscowej populacji ogółem (patrz wykres). Te różnice wynikają przede wszystkim z poziomu rozwoju gospodarczego, gdyż o stopniu użycia sieci decyduje liczba komputerów i innych urządzeń wykorzystywanych w danym regionie, posiadających podłączenie do sieci globalnej. Należy podkreślić, że niemożliwe jest określenie rzeczywistej liczby użytkowników, jeżeli przyjmie się, że są oni rozróżniani przez identyfikatory w formie adresu IP. Ten wyróżnik mają zarówno pojedyncze urządzenia (reprezentowane przez interfejsy), jak i ich grupy lub całe sieci. Obecnie jeden obywatel może łączyć się ze światową siecią przy użyciu licznych środków technicznych, gdzie każde z nich jest reprezentowane przez osobny adres IP. Do znacznego rozwoju tego zjawiska przyczyniła się miniaturyzacja elektroniki oraz spadek jej cen, co spowodowało wzrost sprzedaży urządzeń zdolnych do nawiązania łączności z Internetem i posiadających własny identyfikator[14]. Jednocześnie kilku użytkowników połączonych w sieci wewnętrznej może reprezentować tylko jeden adres IP w sieci globalnej. Z tego powodu liczba określana jako „liczba użytkowników", tożsama z liczbą urządzeń, jest w stanie przekroczyć liczbę ludności na świecie. To sprawia, że cyberprzestrzeń może rozprzestrzeniać się w tej strefie[15]

---

[11] A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON" 2013, nr 3, s. 9.

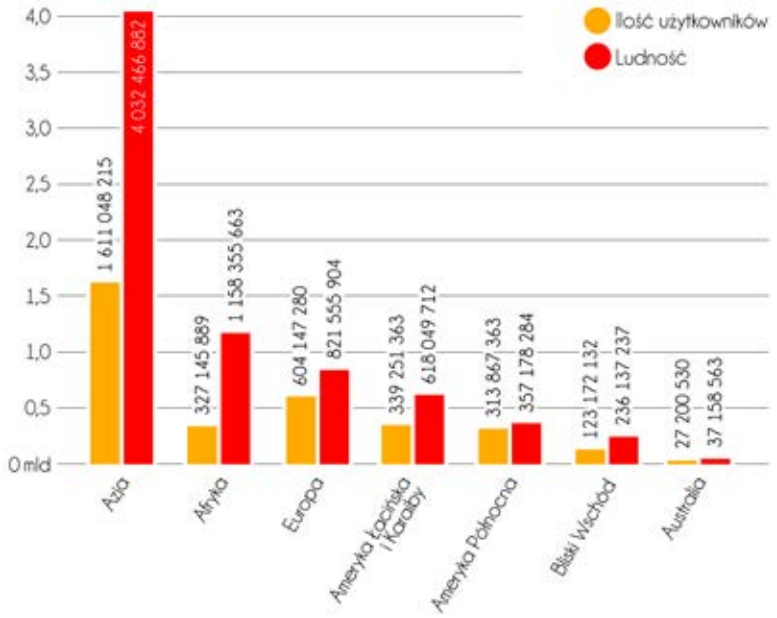
[12] A. Kańciak, *Bezpieczeństwo w cyberprzestrzeni oraz społeczeństwo informacyjne jako przedmiot analiz naukowych i debat publicznych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 310.

[13] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 231–232.

[14] Wzrost należy rozumieć przez sumaryczne zwiększenie się ilości urządzeń – proporcje między poszczególnymi ich rodzajami są różne, zmieniają się w sposób dynamiczny. I tak – wzrost popytu na urządzenia mobilne jest równoznaczny ze spadkiem sprzedaży stacjonarnych komputerów. Szersze omówienie tego problemu nie jest jednak związane z tematem pracy i wymaga osobnego opracowania, A. Garbacz, *Rynek elektroniczny w Polsce*, Warszawa 2010, s. 1.

[15] Należy przez to rozumieć ogół infrastruktury teleinformatycznej, nie tyko urządzeń podłączonych do sieci globalnej, lecz także wszystkich urządzeń z tego sektora, zdolnych do tworzenia

w sposób niemalże nieograniczony, gdyż z każdym dniem zwiększa się liczba możliwych do zidentyfikowania nadawców i odbiorców pakietów danych.



Wykres. Porównanie liczby ludności z liczbą użytkowników sieci w danym regionie w 2015 r.

Źródło: http://internetworldstats.com/stats.htm [dostęp: 10 XII 2015].

Drugim czynnikiem ekspansywności sieci są możliwości sfery logicznej, jakie niesie za sobą rozwój infrastruktury przez wspomniany wyżej wzrost liczby urządzeń. Każdy z użytkowników jest w stanie wygenerować informację o możliwej do określenia objętości. Poszczególne bajty danych mogą być zapisywane na nośnikach, choć należy też rozpatrywać je w charakterze składowej ruchu sieciowego w momencie, w którym są przesyłane pomiędzy nośnikami. Stanowią one zawartość cyberprzestrzeni możliwą, w teorii, do liczbowego wyrażenia. Niemniej jednak ruch w sieci jest nieprzerwany oraz globalny, a przez to nieprzewidywalny, gdyż pakiety danych mogą być nadawane i odbierane na różnych kontynentach, z wykorzystaniem wielu stacji pośrednich. Z tego powodu interaktywny układ przepływu oraz przechowywania informacji, tożsamy z pojęciem cyberprzestrzeni sensu stricto, cechuje się ogromną entropią (chaosem). To z kolei uniemożliwia empiryczne zmierzenie jego objętości (zawartości), pozwalając wyłącznie na szacowanie rozmiarów, które posiadał lub będzie posiadać w danym okresie. To nie podważa jednak względnej realności[16] omawianej

technicznego zaplecza logicznej sfery cyberprzestrzeni. Włącza się w to również sieci lokalne oraz odizolowaną infrastrukturę teleinformatyczną.

[16] Zbiór informacji w cyberprzestrzeni jest zapisany w formie właściwych, realnych zjawisk fizycznych w obrębie pamięci urządzeń, jednakże powszechnie nie uważa się go za obiekt fizyczny

sfery, gdyż te dane istnieją – mogą być przetwarzane, odczytywane, wysyłane oraz odbierane przez użytkowników sieci. Informacja wyraża więc rzeczywistą objętość przestrzeni cybernetycznej, mogącą ekspandować do granic, które wyznacza objętość potencjalna. Tę z kolei narzuca ograniczona pojemność nośników danych, z reguły wyrażana w możliwych do przechowania bajtach danych (i ich informatycznych lub matematycznych[17] wielokrotnościach).

Granice ekspansji cyberprzestrzeni są wytyczone przez możliwości techniczne infrastruktury działającej w ramach różnorakich sieci. Jednak ze względu na wciąż przybywającą ilość urządzeń, niemożliwe jest określenie realnego „końca" przestrzeni cyfrowej, gdyż prawdopodobnie nie będzie się w stanie zapełnić informacjami każdego istniejącego w danym czasie nośnika. Sama opisywana sytuacja również jest czysto hipotetyczna ze względu na nieustannie zwiększający się potencjał infrastruktury przechowującej i przetwarzającej dane. Można dostrzec zależność między objętością rzeczywistą (ilością obecnie wytworzonych, wirtualnych informacji) a objętością potencjalną, która limituje tę pierwszą. Niemniej jednak obie sfery nie muszą rozwijać się równomiernie, gdyż wzrost potencjału nie oznacza natychmiastowego zapełnienia nowej przestrzeni kolejnymi bajtami danych. W ostatnich latach można było zaobserwować wzrost pojemności nośników danych – obecnie dyski twarde o pojemności 1 terabajta są powszechnie dostępne w komputerach personalnych, co nie oznacza, że użytkownicy wykorzystują całą tę przestrzeń na rzecz gromadzenia osobistych danych.

Cyberprzestrzeń jest sferą niezwykle rozbudowaną, przez którą należy rozumieć nie tylko sumę urządzeń i systemów wspierających świat wirtualny. Nawet globalna sieć – Internet – mimo że stanowi większą objętość omawianej sfery, nie jest jej jedyną istotą. Przestrzeń cybernetyczna to logicznie wydzielony obszar pełen informacji reprezentujących myśl ludzką, niejednokrotnie będących jedynym składnikiem owych przedsięwzięć i idei. Tego powodem jest częste wykorzystywanie danych, które nie istnieją poza przestrzenią cybernetyczną. Nie będzie zatem nadużyciem stwierdzenie, że świat wirtualny to obecnie kolejny obszar prowadzenia operacji, obok lądu, morza, powietrza oraz przestrzeni kosmicznej[18]. Cyberprzestrzeń stała się także istotnym sektorem badań nad bezpieczeństwem, gdyż uwzględnia przedsięwzięcia prawno-organizacyjne, edukacyjne oraz techniczne, które mogą być podstawą do nowych form działań wywiadowczych i militarnych. Należy dodać, że samo wykorzystanie opisywanej sfery w taki sposób, dowodzi jej wartości dla współczesnego świata.

---

lecz logiczny, J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*... s. 229.

[17] Pomimo rozwiązania zaproponowanego w 1998 r. przez International Electrotechnical Commission (IEC), czołową organizację w standaryzacji elektrotechniki, do dziś istnieje problem w rozróżnieniu jednostek. Pojemności nośników często wyraża się przez zastosowanie przedrostków dziesiętnych (układu SI), które informują o wielokrotności tysiąca (10^n), choć tak naprawdę liczby wywodzą się z układu binarnego i powinny być wyrażane w przedrostkach dwójkowych (IEC 60027-2:1998), informujących o zwielokrotnianiu dwójek (2^n). Stąd pomimo użycia np. jednego kilobajta danych, powinno się przez to rozumieć 1024 bajty (jeden kibibajt), a nie 1000 bajtów.

[18] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 128.

2. Asymetryczność działań w cyberprzestrzeni oraz ich skutki

Jednym z praw rządzących cybernetyczną przestrzenią jest asymetria działań, która przejawia się na licznych płaszczyznach relacji pomiędzy użytkownikami oraz zawartymi weń systemami. To pojęcie można jednak rozumieć na wiele sposobów – zwłaszcza w sferze cyfrowej.

W ocenie ekspertów Sojuszu Północnoatlantyckiego niebezpieczeństwa asymetryczne przedstawiane są jako: (…) *zagrożenie wynikające z możliwości zastosowania różnych środków i metod w celu obejścia lub neutralizacji silnych punktów przeciwnika, wykorzystując jednocześnie jego słabości w celu uzyskania niewspółmiernych wyników*[19]. NATO w swojej definicji skupia się na relacji zachodzącej pomiędzy podmiotami. Podkreśla się przy tym, że każdy z nich może dysponować różnymi środkami pozwalającymi na przeprowadzenie skutecznych działań, które w sferze wirtualnej mogą przybierać nieznane do tej pory formy. Ponieważ cyberprzestrzeń należy rozumieć jako obszar logiczny[20], nie podlega ona ograniczeniom fizycznym, takim jak prawa fizyki czy przeszkody geologiczne. Bezpieczeństwo każdej informacji zawartej w sieci – globalnej lub miejscowej – staje się zagrożone w momencie, gdy wrogi podmiot uzyska dostęp do samego układu. Liczba przedsięwzięć podjętych w celu ochrony danych bywa ogromna i stanowi wyzwanie na wielką skalę (najmniejsza luka niweczy wszystko). Tworzone są platformy zarządzające cyfrowymi „dobrami", chronione[21] przez programy posługujące się często autorskimi algorytmami szyfrującymi. Złożoność takiej operacji może zostać zaprzepaszczona przez nieporównywalnie prostsze działania. Potencjalny agresor, popełniając błędy, zazwyczaj nie naraża się na to, że dotkną go konsekwencje jego działań. Często wystarczy jedna luka w systemie bezpieczeństwa, aby ten mógł zostać złamany[22]. Sprawia to, że obrońca musi podjąć znacznie więcej przedsięwzięć niż podmiot dokonujący ataku.

Skupienie uwagi wyłącznie na działaniach (operacjach) między stronami walk nie wydaje się w pełni zasadne. W kategoriach asymetrii należy rozpatrywać także istotę samych podmiotów. Niektóre z nich mogą wydawać się znacznie słabsze od reszty – w ujęciu liczebności oraz zasobu sił i środków. Jednak przy zastosowaniu metod niekonwencjonalnych z punktu widzenia oponenta mogą zagrozić jego bezpieczeństwu[23].

---

[19] *AAP-6 Słownik terminów i definicji NATO*, 2014, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf, s. 58 [dostęp: 6 XI 2017].

[20] J. Wasilewski, *Zarys definicyjny...*, s. 229.

[21] http://www.safetyandsecurity.pl/index.php/artykuly/24-numer12/128–kryptograficzne–metody–ochrony–informacji–w–systemach–i–sieciach–teleinformatycznych [dostęp: 18 XII 2015]. Zob. *Defense in Depth - A practical strategy for achieving Information Assurance in today's highly networked environments*, Fort Meade 2000; S. C. Zimmerman, *Secure Infrastructure Design*, (b.m.w.) 2002.

[22] Jako przykład może służyć włamanie na stronę internetową Białego Domu w maju 1999 r., w którym podmieniono jej zawartość (ang. *deface*). Źródło podaje, że dokonały tego zaledwie trzy osoby – dwóch przedstawicieli grupy gLobaLheLL oraz osoba kryjąca się pod pseudonimem ne0h, zob. K.D. Mitnick, W. L. Simon, *Sztuka infiltracji, czyli jak włamywać się do sieci komputerowych*, Warszawa 2006, s. 60.

[23] Z. Ciekanowski, *Działania asymetryczne jako źródło zagrożeń bezpieczeństwa*, „Bezpieczeń-

Jedną z charakterystycznych cech zagrożeń asymetrycznych w świecie realnym jest ich ponadpaństwowość – podmioty transnarodowe lub subnarodowe, takie jak ugrupowania terrorystyczne oraz organizacje przestępcze – mogą działać na obszarze wielu krajów[24]. Również i tutaj można dostrzec analogię między przestrzenią realną a cybernetyczną, gdyż w obu przypadkach asymetryczność wiąże się z trudnością wytyczenia jednoznacznych granic terytorialnych. W wirtualnej sferze logicznej jest to nawet niemożliwe, gdyż jedyną skuteczną formą unarodowienia fragmentów sieci jest infrastruktura znajdująca się na terytoriach poszczególnych państw[25]. Cyberprzestrzeń formułuje jednak szczególny charakter braku zależności od podmiotów międzynarodowych, gdyż stanowi środowisko niezwykle przyjazne tworzeniu wysoce rozproszonych, niejasnych struktur organizacyjnych, pozbawionych siedzib i punktów centralnych. Co więcej – cyfrowe środowisko oferuje też stosunkową łatwość w pozyskiwaniu trudnej do weryfikacji, fikcyjnej osobowości lub niemalże całkowite jej zatajenie, włączając w to kamuflowanie aktywności w sieci globalnej[26].

Asymetryczne konflikty w przestrzeni cybernetycznej, której bezpieczeństwo można rozpatrywać wieloaspektowo, wywierają swe piętno nie tylko na samej sferze cyfrowej, lecz także na przestrzeni realnej. Wysoce skomputeryzowany świat zamieszkany przez społeczeństwa informacyjne nierozerwalnie współdziała z cyberprzestrzenią, „żyjąc" w swoistej symbiozie. Nowoczesne rozwiązania teleinformatyczne tworzą liczne udogodnienia w życiu codziennym[27], pozwalają na niespotykany dotychczas postęp naukowy, choć niosą też zagrożenia – trudne do przewidzenia i niełatwe w przeciwdziałaniu. Brakuje norm prawnych regulujących postępowanie w przypadku wystąpienia omawianych niebezpieczeństw – także w Polsce[28]. Ponadto efekty ataku cyberterrorystycznego lub innej formy szkodliwej działalności w sieci mogą dotykać nie tylko sfery cyfrowej. Z tego względu skutki cybernetycznych walk można podzielić na trzy rodzaje:

---

stwo i Technika Pożarnicza/Safety & Fire Technique" 2009, nr 3, s. 52.

[24] Tamże, s. 54.

[25] Ten aspekt dotyczy przede wszystkim miejscowego porządku prawno-ustrojowego oraz istniejących w nim przepisów, które bezpośrednio odnoszą się do sposobu przechowywania i przesyłania informacji cyfrowych.

[26] Powszechnie stosowaną praktyką jest działanie pod pseudonimem niezwiązanym z prawdziwymi danymi osobowymi. Tożsamość w formie adresu IP jest ukrywana z kolei przez stosowanie wielu serwerów pośredniczących lub rozwiązań, takich jak sieć Tor, posiadająca sieć urządzeń rozproszonych na całym świecie. Pozwala ona na dynamiczne zmienianie adresów IP wraz z krajem pochodzenia w nieregularnych odstępach, co przy odpowiedniej złożoności operacji niemal uniemożliwia śledzenie użytkownika. Przesyłane i odbierane dane mogą być również szyfrowane, na przykład za pomocą protokołu SSL (*Secure Socket Layer*). Z tego powodu zatajanie tożsamości należy rozumieć jako ogół działań technicznych oraz społecznych, https://www.torproject.org/docs/hidden-services.html.en [dostęp: 19 XII 2015].

[27] Ł. Lysik, P. Machura, *Rola i znaczenie technologii mobilnych w codziennym życiu człowieka XXI wieku*, „Media i Społeczeństwo" 2014, nr 4, s. 21.

[28] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni...*, s. 130–132.

- skutki wirtualne – dotyczące stricte cyberprzestrzeni;
- skutki rzeczywiste – obejmujące świat realny w wymiarze:
- materialnym – powodującym straty w infrastrukturze oraz dobrach fizycznych lub wśród żywych organizmów,
- polityczno-społecznym – stwarzającym zagrożenie dla relacji podmiotów;
- skutki mieszane – związane ze stratami w obu sferach.

Wymienione wyżej konsekwencje należy odnieść do dwóch grup przedmiotów i podmiotów: występujących w cyberprzestrzeni oraz (lub) w świecie realnym. Najistotniejszymi uczestnikami wydają się organizacje rządowe oraz służby specjalne, a także podmioty międzynarodowe w ujęciu ogólnym, w tym transnarodowe grupy przestępcze oraz ugrupowania terrorystyczne. Stronami konfliktu mogą być laboratoria zajmujące się cyberbezpieczeństwem, prawne zrzeszenia, grupy hakerskie czy nawet pojedyncze osoby[29]. Wymienione strony potencjalnych konfliktów mają wspólną cechę: są w stanie zagrozić danym i systemom chroniącym informacje (zasoby)[30]. Jak wcześniej zaznaczono, ze względu na asymetrię działań często nieistotne są wielkość lub liczebność danego podmiotu, lecz stosowane przez niego metody. Warto podkreślić, że temu zjawisku sprzyja niekontrolowany postęp technologiczny prowadzący do nierównego rozwoju poszczególnych uczestników.

Precyzyjne przewidywanie konsekwencji zaprezentowanych niebezpieczeństw jest niezwykle trudne. Cyberprzestrzeń cechuje się ogromnym dynamizmem i entropią, co może stanowić problem przy ustalaniu potencjalnych efektów działań prowadzonych w środowisku sieciocentrycznym. Ponadto pojawianie się nowych zagrożeń informacyjnych jest uzależnione od tempa ekspansji przestrzeni cybernetycznej. Z tego powodu nie należy tworzyć wykazu skutków sensu stricto, gdyż uległby on szybkiej dezaktualizacji. Zamiast tego należałoby ustalić kategorie konsekwencji, porządkujące konkretne skutki w mniejszych zbiorach. Takie rozwiązanie pozwala na znacznie szybszą i precyzyjniejszą analizę negatywnych rezultatów działalności w środowisku sieciocentrycznym.

Złożone konsekwencje logiczne (wirtualne) i rzeczywiste tworzą skomplikowaną, trudną w przewidywaniu[31] strukturę ciągów przyczynowo-skutkowych. Stworzenie swoistej typologii zagrożeń w postaci precyzyjnego i komplementarnego aparatu pojęciowego wydaje się zadaniem, którego wykonanie jest mało prawdopodobne. Środowisko sieciocentryczne stanowi obszar wielowymiarowy i skomplikowany, a przede wszystkim dynamiczny. Wskazanie konieczności podziału cyfrowej sfery na mniejsze sektory wydaje się najrozsądniejszym rozwiązaniem dostępnym „na dzień dzisiejszy". Po ustaleniu podstawowych kategorii zagrożeń i ich skutków, należałoby podjąć przedsięwzięcia legislacyjne. Pozwoliłyby one na modyfikację istniejących

[29] M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, „e-Politikon" 2013, nr 6, s. 108–109

[30] http://zabezpieczenia.com.pl/ochrona-informacji/zagro%C5%BCenia-bezpiecze%C5%84stwa-informacji-w-przedsi%C4%99biorstwie-cz-1 [dostęp: 21 XII 2015].

[31] M. Grzelak. K, Liedel, *Bezpieczeństwo w cyberprzestrzeni...*, s. 129.

wykładni prawa międzynarodowego, które obecnie cechują się brakiem spójności w interpretacji incydentów cybernetycznych[32]. Brak procedur dotyczących reagowania w przypadku wystąpienia zagrożeń komputerowych może stanowić zagrożenie dla żywotnych interesów państw i organizacji transnarodowych. Z tego powodu synergiczna współpraca na płaszczyźnie naukowo-prawodawczej powinna być priorytetem dla podmiotów zaangażowanych w budowę bezpieczeństwa cybernetycznego.

3. Cyberbroń Stuxnet – geneza, struktura oraz sposób działania

Dynamizm zjawisk zachodzących w cyberprzestrzeni determinują podmioty istniejące w jej ramach oraz ich działania. Tak jak w świecie realnym wojna i zbrojenia powodowały postęp technologiczny, tak i w środowisku sieciocentrycznym można zaobserwować ciągły rozwój cyfrowych metod walki. Momentem przełomowym było odkrycie w czerwcu 2010 r. oprogramowania Stuxnet[33], które szybko zostało okrzyknięte pierwszą cyberbronią[34]. Rozsądne wydaje się jednak zbadanie słuszności użycia takiego sformułowania.

Omawiany cyberatak na infrastrukturę krytyczną jest kamieniem milowym walk w cyfrowej sferze. Uważa się, że powodem stworzenia Stuxnet był irański program nuklearny, który jest jednym z najważniejszych problemów w obszarze szeroko rozumianego bezpieczeństwa Zatoki Perskiej i całego świata. Badania nad wzbogacaniem uranu budziły obawy związane z jego militarnym wykorzystaniem, gdyż arsenał Iranu obejmował między innymi rakiety balistyczne, zdolne razić cele na Bliskim Wschodzie[35]. Sytuacja uległa zaognieniu po objęciu władzy przez Mahmuda Ahmadineżada[36], który podał do publicznej wiadomości, że jego zamiarem jest dołączenie do grupy mocarstw nuklearnych.

Wydarzenia z 2010 r. dowiodły, że zbrojne metody walki nie są już jedynym rozwiązaniem. W lipcu pojawiły się doniesienia mówiące, że przeprowadzono niekonwencjonalny atak na irańskie instalacje nuklearne[37]. Miał on doprowadzić do uszkodzenia wirówek służących do wzbogacania uranu przez zainfekowanie wirusem oprogramowania komputerowego. Spekulacje zostały potwierdzone w listopadzie przez

---

[32] M. Lakomy, *Zagrożenia dla bezpieczeństwa*..., s. 137.

[33] N. Falliere, L.O. Murchu, E. Chien, *W32.Stuxnet Dossier*, Cupertino 2011, s. 4.

[34] http://wyborcza.pl/ 1,76842,8455622,Stuxneli_Iran.html?disableRedirects=true [dostęp: 18 IV 2016]; http://www.rp.pl/artykul/890403-Kto-stworzyl-najgrozniejsza-cyberbron-.html [dostęp: 18 IV 2016]; R. Bania, *Wojny w cyberprzestrzeni – przypadek Iranu*, w: *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, R. Bania, K. Zdulski (red.), Łódź 2012, s. 195.

[35] Tamże, s. 191.

[36] Mahmud Ahmadineżad – szósty Prezydent Islamskiej Republiki Iranu w okresie od 3 sierpnia 2005 r. do 3 sierpnia 2013 r., wcześniej burmistrz Teheranu w latach 2003–2005, S. Rajabi, *Political Memory and Social Media: The case of Neda,* w: D.M. Faris, B. Rahimi, *Social media in Iran. Politics and Society after 2009*, Albany 2015.

[37] http://venturebeat.com/2011/01/15/evidence-builds-that-stuxnet-worm-was-aimed-at-averting-war-over-irans-nuclear-weapons/ [dostęp: 18 IV 2016].

samego prezydenta Ahmadineżada[38]. Nie był to pionierski cyberatak na infrastrukturę krytyczną, lecz – jak się później okazało – po raz pierwszy o tak wielkiej skali.

Istotnym elementem Stuxnetu jest jego struktura i sposób działania – głównym założeniem oprogramowania jest skanowanie komputera (środowisko Windows[39]) w poszukiwaniu sterowników PLC firmy Siemens (SIMATIC WinC[40]), które obsługiwały oprogramowanie wspomnianych wirówek. Przy negatywnym wyniku robak nie podejmuje żadnych działań, próbując jedynie replikować się na pozostałe nośniki. Dzięki temu kod pozostaje niewykryty i może być łatwo przenoszony między urządzeniami dopóty, dopóki nie natrafi na swój cel. Całość odbywa się w czterech etapach – infekcji, wykonania, przeszukiwania-replikacji, a także kamuflażu[41].

Infekcja następuje w podobny sposób, jak przy typowych robakach – pliki z zainfekowanego nośnika danych są zgrywane na twardy dysk komputera. W przeciwieństwie do innych wirusów Stuxnet nie wymusza ekstrakcji swych komponentów bezpośrednio przez plik AUTORUN.INF[42]. Zamiast tego wykorzystuje lukę parsera skrótów (.LNK[43]). Kod zostaje wprowadzony przez spreparowany plik .LNK, który prowadzi do odpowiednio przygotowanego, fałszywego panelu sterowania[44], będącego w rzeczywistości elementem wirusa (*malware*). Kiedy system próbuje przywrócić odpowiednią ikonę skrótu z pliku, uruchamia go i tym samym inicjuje moduł Stuxnet (podszywający się pod panel sterowania). Należy dodać, że użytkownik nie musi klikać na wspomnianą ikonę – całość dokonuje się samoczynnie. Szkodliwe oprogramowanie instaluje następujące pliki w systemie[45]:

- dwa pliki (*mrxcls.sys* i *mrxnet.sys*[46]) – umieszczane w katalogu sterowników %Windir%\System32\Drivers,

[38] *Wirus w wirówkach*, „Polska Zbrojna" 2011, nr 5, s. 10.

[39] Problem dotyczy luki bezpieczeństwa CVE-2010-2568 w powłoce licznych wydań Windows NT, od Windows 2000 oraz Windows Server 2003 do Windows 7 wraz z Windows Server 2008 R2. Sam Microsoft opatrzył ten problem krytycznym wskaźnikiem ważności ze względu na umożliwienie zdalnego wykonywania kodu (szczególnie W32.Stuxnet). Pełna lista zagrożonych systemów została opublikowana w „Biuletynie zabezpieczeń firmy Microsoft MS10-046", zob. *Luka w zabezpieczeniach powłoki systemu Windows umożliwia zdalne wykonanie kodu (2286198)*, https://technet.microsoft.com/pl-pl/library/security/ms10-046.aspx [dostęp: 21 IV 2016].

[40] https://www.f-secure.com/v-descs/trojan-dropper_w32_ stuxnet.shtml [dostęp: 22 IV 2016].

[41] Jest to duże uproszczenie. Ze względu na rodzaj i objętość pracy niemożliwe jest szczegółowe opisanie struktury oraz funkcjonowania Stuxnet. Dokładniejszą analizę można znaleźć w dostępnej literaturze, zob. N.Falliere, L.O. Murchu. E. Chien, *W32.Stuxnet*..., s. 8–11, 15–52.

[42] AUTORUN.INF – plik tekstowy wykorzystywany przez system Windows. Umieszczany w głównym katalogu przenośnych nośników danych, służący do automatycznego wykonywania odpowiednich komend, tuż po podłączeniu dysku. Może zawierać informacje między innymi o tym, jaki plik ma zostać automatycznie uruchomiony lub która ikona ma zastąpić wariant systemowy.

[43] .LNK – rozszerzenie skrótów w systemie Windows (zwanych też skrótami powłoki (ang. *shell links*), będących sposobem pośredniego uruchamiania plików za pośrednictwem zastosowanej w skrócie ścieżki, a nie przez fizyczne kliknięcie docelowego pliku.

[44] Jeden z podstawowych komponentów systemów z rodziny Windows NT.

[45] https://www.f-secure.com/v-descs/trojan-dropper_w32_ stuxnet.shtml [dostęp: 22 IV 2016].

[46] Oba pliki stanowią *rootkit*, czyli narzędzia wykorzystywane do ukrywania niebezpiecznych plików i procesów, pozwalając na włamywanie się do struktur systemów i utrzymywanie kontroli nad nimi.

- zaszyfrowana biblioteka DLL[47] (*oem7a.PNF*), stanowiąca główny komponent instalatora-trojana, umieszczona w: %Windir%\inf,
- zaszyfrowany plik z danymi konfiguracyjnymi (*mdmcpq3.PNF*) w: %Windir%\inf,
- zaszyfrowany 90-bitowy plik z danymi (*mdmeric3.PNF*) w: %Windir%\inf,
- zaszyfrowany plik z logami (*oem6c.PNF*) w: C%Windir%\inf[48],
- Stuxnet modyfikuje także rejestr systemu, tworząc następujące wpisy, powiązane z dwoma wyżej wymienionymi plikami, instalowanymi wśród sterowników:
- HKLM\System\CurrentControlSet\Services\Services\MRxNet,
- HKLM\System\CurrentControlSet\Services\Services\MRxCls[49].

Kolejnym etapem jest wykonanie (ang. *execution*) będące uruchomieniem wgranego wcześniej złośliwego kodu. Wykorzystując plik *mrxcls.sys*, dokonywana jest podstawowa iniekcja zaszyfrowanej biblioteki DLL z pliku *oem7a.PNF* do docelowych procesów. Reszta procedury „zarażania" obszarów funkcjonowania systemu jest kontynuowana przez dwa komponenty zawarte w *mrxcls.sys*. Zmiany w procedowaniu elementów Windows dokonywano także przez procesy services.exe, svchost.exe oraz lsass.exe. Dzięki temu opisywany robak opanowywał system i uzyskiwał możliwość przeprowadzania działań właściwych dla założonych celów.

Całość omówionego przygotowania skupia się na najważniejszym elemencie opisywanego, złośliwego kodu: jego zdolności do przeszukiwania oraz replikacji. Stuxnet, wykorzystując plik *mrxnet.sys*, poszukuje w systemie plików z nazwą ~WTR [ciąg czterech cyfr].TMP oraz o rozszerzeniach: .LNK. Jeżeli program odkryje właściwą konotację, plik zostaje ukryty przez modyfikację struktury FileInfo. Jednocześnie spreparowane biblioteki DLL próbują łączyć się z aplikacjami Siemens >SIMATIC WinCC, używając przy tym poświadczeń administracyjnych zakodowanych bezpośrednio w kodzie źródłowym. Jeżeli połączenie powiedzie się, program poszukuje pliku \GraCS\cc_tlg7.sav we wszystkich bazach danych, które zaczynają się od znaków „CC", aby wyekstrahować w tym samym miejscu *cc_tlg7.savx*[50]. Stuxnet zbiera także podstawowe informacje o systemie i wysyła je do dedykowanego centrum dowodzenia i kontroli (ang. *command and control* – C&C) za pośrednictwem HTTP. Znane są między innymi dwa adresy: www.mypremierfutbol.com oraz www.todaysfutbol.com, zlokalizowane na serwerach w Malezji i Danii[51]. W przypadku braku odnalezienia pożądanych plików (sterowników PLC Siemens), program tworzy kopię siebie same-

[47] *Dynamic-Link Library* – fragment binarnego kodu skompilowanego programu, umieszczonego poza jego plikiem wykonywalnym. Istotą bibliotek DLL jest to, że jeden kod może być wykorzystywany jednocześnie przez wiele programów, co pozwala ograniczyć objętość zbioru poleceń każdego z nich.

[48] N. Falliere, L.O. Murchu. E. Chien, *W32.Stuxnet*..., s. 18; https://blogs.technet.microsoft.com/markrussinovich/2011/04/17/analyzing-a-stuxnet-infection-with-the-sysinternals-tools-part-3/ [dostęp: 23 IV 2016].

[49] HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services – fragment „drzewa" rejestru, w którym przechowywane są wpisy dotyczące wszystkich usług funkcjonujących w systemie, w tym dane i ścieżki sterowników.

[50] https://www.f-secure.com/v-descs/trojan-dropper_w32_ stuxnet.shtml [dostęp: 22 IV 2016].

[51] N. Falliere, L.O. Murchu. E. Chien, *W32.Stuxnet*..., s. 21.

go na dostępnych dyskach przenośnych, podpinanych do zainfekowanego urządzenia wraz z dodatkowymi plikami:

- *~WTR4132.TMP* – główny instalator z dysku USB,
- *~WTR4141.TMP* – instalator sterownika w dysku USB,
- Copy of Copy of Copy of Copy of Shortcut to.lnk,
- Copy of Copy of Copy of Shortcut to.lnk,
- Copy of Copy of Shortcut to.lnk,
- Copy of Shortcut to.lnk[52].

Wymienione skróty (kolejne kopie Shortcut to.lnk) są odpowiedzialne za załadowanie *~WTR4141.TMP*, gdy dysk przenośny zostanie wpięty do nowego systemu. Następnie (za pośrednictwem zainicjowanego już *~WTR4141.TMP*), ładowany jest plik *~WTR4132.TMP*. Nim to jednak nastąpi, *~WTR4141.TMP* podejmuje próbę ukrycia swej działalności przez wykorzystanie mechanizmu przechwytywania komunikatów w *kernel32.dll* (FindFirstFileW, FindNextFileW, FindFirstFileExW) oraz *Ntdll.dll* (NtQueryDirectoryFile, ZwQueryDirectoryFile)[53].

Mimo że Stuxnet był w swoim czasie uznawany za najbardziej zaawansowany, złośliwy kod[54], to firma Root Labs twierdzi, że ten robak był napisany w sposób żenujący[55]. Oprogramowaniu zarzuca się liczne uproszczenia, zwłaszcza w omijaniu zabezpieczeń antywirusowych. Rozsądne wydaje się postawienie hipotezy o słuszność takiego działania. Dodatkowy czas i koszty poświęcone na implementowanie złożonych, „wyrafinowanych" systemów, mogłyby zaowocować niewystarczającym efektem. Zamiast tego, agresorzy mogli kierować się względami praktycznymi. Co więcej – uniknięto w ten sposób tworzenia cyfrowego „odcisku palca". Można zakładać, że liczba osób kompetentnych w niemalże doskonałym „zaciemnianiu" kodu komputerowego, jest ograniczona. Stosowanie prostych, lecz skutecznych form, pozwoliło z powodzeniem ukryć tożsamość twórców[56]. W przypadku złośliwego oprogramowania to właśnie efekty działań, a nie metoda, dzięki której osiągnięto założone cele, stanowią główny determinant ostatecznej jego oceny.

Trudno jednoznacznie wskazać autorów opisywanego złośliwego oprogramowania. Brak dowodów sprawia, że ten problem stał się przedmiotem burzliwych dyskusji medialnych. Wśród licznych spekulacji najczęściej pojawiającym się agresorem są Izrael i Stany Zjednoczone. David E. Sagner, autor książki *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, wskazał na łamach czasopisma „The New York Times" właśnie te dwa państwa[57]. Swą ocenę uzasadniał

[52] Tamże, s. 24.

[53] Tamże, s. 30.

[54] R. Bania, *Wojny w cyberprzestrzeni – przypadek Iranu*, w: *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, R. Bania, K. Zdulski (red.), Łódź 2012, s. 195.

[55] https://rdist.root.org/2011/01/17/stuxnet-is-embarrassing-not-amazing/ [dostęp: 26 IV 2016].

[56] https://niebezpiecznik.pl/post/stuxnet/ [dostęp: 26 IV 2016].

[57] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran .html?_r=3&pagewanted=2&seid=auto&smid=tw-nytimespolitics&page wanted=all

chęcią spowolnienia rozwoju irańskiego programu nuklearnego, co korzystnie wpłynęło na sytuację w rejonie Zatoki Perskiej i pozwoliło uniknąć potencjalnej agresji Izraela. Ze stanowiskiem polemizuje jednak „Forbes", według którego to Finowie oraz Chińczycy stworzyli Stuxnet. Za tą hipotezą miałyby przemawiać interesy Chińskiej Republiki Ludowej, znajdującej w Iranie ekonomicznego partnera. Potencjalne sankcje dotyczące programu atomowego mogłyby poważnie osłabić pozycję Iranu i tym samym wpłynąć na interesy azjatyckiego mocarstwa. Wykorzystanie cyberbroni do sabotażu miało być „prostym i eleganckim sposobem" na ochronę własnych kontraktów, gdyż w razie wykrycia robaka, oskarżone o jego użycie miały zostać Stany Zjednoczone wraz z Izraelem[58].

4. Infekcja Stuxnet oraz jej skutki – atak na irański program atomowy

Podstawowym założeniem stworzenia Stuxnet był sabotaż procesów technologicznych, wykorzystywanych we wzbogacaniu uranu. Całość miała być dokonana przez wprowadzenie złośliwego kodu do komputerów sterujących procesami wzbogacania uranu (SCADA[59]). Interesujące jest to, że infrastruktura teleinformatyczna wykorzystywana w irańskim programie atomowym była całkowicie odłączona od ogólnoświatowej sieci, fizycznie uniemożliwiając zdalny cyberatak. Omawiany przykład wskazuje jednak, że nawet tego typu środki bezpieczeństwa nie są w stanie zapewnić pełnej ochrony systemów. Istnieją spekulacje, że wprowadzenie wirusa nastąpiło przez podpięcie zainfekowanego dysku przenośnego przez jednego z pracowników lub techników rosyjskich[60].

Ze względu na zdolność robaka do replikacji i samodzielnego przenoszenia się zainfekował on komputery także poza Iranem. W lipcu 2010 r. Symantec – we współpracy z zespołami CERT z całego świata – stworzył system monitorujący serwery dowodzenia i kontroli Stuxnet (C&C). Kontrolowano ruch tworzony przez komputery, które były zdolne do nawiązania połączenia z C&C. Uzyskano w ten sposób możliwość identyfikowania pakietów danych, zawierających zaszyfrowane dane, takie jak wewnętrzne treści, adresy IP, a także dane o oprogramowaniu i osprzęcie komputera (szczególnie gromadzono informacje, czy wykorzystuje on sterowniki Siemens)[61].

[dostęp: 26 IV 2016].

[58] http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/#1751a80c268d [dostęp: 26 IV 2016].

[59] *Supervisory Control And Data Acquisition* – system komputerowy, nadzorujący procesy technologiczne, nadrzędny wobec PLC (ang. *Programmable Logic Controller* – Programowalny Sterownik Logiczny), sterujących bezpośrednio urządzeniami technicznymi, wykorzystywanymi w danym procesie. W przypadku Stuxnet uzyskanie dostępu do SCADA umożliwiło przejęcie kontroli nad wszystkimi wirówkami przez ich sterowniki PLC, zob. K. Stouffer, J. Falco, K. Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, Gaithersburg 2006.

[60] http://swiat.newsweek.pl/stuxnet—najgrozniejszy-wirus-swiata--czy-to-dzielo-izraelskiego-wywiadu, 65632,1,1.html [dostęp: 30 IV 2016].

[61] N. Falliere, L.O. Murchu. E. Chien, *W32.Stuxnet*..., s. 5.

Z około 100 000 zaobserwowanych hostów wyekstrahowano 40 000 unikatowych adresów IP, dowodzących zaatakowania jednego, konkretnego urządzenia. Jak się okazało, 58,31 proc. infekcji dotyczyło infrastruktury atomowej w Iranie. Pozostałe 41,69 proc. objęło ponad 155 państw świata, dowodząc tym samym skali problemu[62].

Sama agresja nie była jednostkowym wydarzeniem możliwym do przeprowadzenia w krótkim okresie. Towarzyszyły jej stosowne przygotowania, takie jak infiltracja sieci wewnętrznej przed docelowym uszkodzeniem wirówek do wzbogacania uranu. Z tego powodu wyróżnia się trzy fazy ataku z użyciem różnych wariantów Stuxnet:

- 22 czerwca 2009 r. – 3 proc. ogólnej liczby infekcji,
- 1 marca 2010 r. – 69 proc.,
- 14 kwietnia 2010 r. – 28 proc.

Te daty pochodzą z informacji przesyłanych przez robaka do C&C. Z tego powodu mogą istnieć niemożliwe do zweryfikowania rozbieżności, wynikające z różnic w strefach czasowych lub z potencjalnie błędnie ustawionej dacie w komputerze[63]. Poszczególne wersje, wykorzystane w wyżej podanych okresach, wskazują różnice strukturalne między programami. Te najbardziej widoczne dotyczą wersji z 2009 r.[64], cechującej się:

- brakiem wykorzystania luki związanej z plikami .LNK,
- posłużeniem się tylko jednym sterownikiem na pamięci przenośnej (kolejne warianty używały dwóch sterowników, ze względu na wspomnianą lukę),
- infekowaniem z bezpośrednim użyciem pliku AUTORUN.INF[65].

Największa rozbieżność kompilacji z 2009 r. w stosunku do nowszych wersji dotyczy „zasobu 207"[66], implementującego platformę Flame (później oddzieloną od Stuxnet i wykorzystywaną niezależnie). Ten komponent był istotny dla omawianego wariantu, gdyż pozwalał używać robaka przed wykorzystaniem luki plików .LNK. Jak pokazują statystyki, ta metoda nie zapewniła jednak pożądanej skuteczności. Różnice dotyczyły raczej metod wykonywania poszczególnych zadań, a nie koncepcji infekcji jako całości, która była jednakowa dla wszystkich wersji (patrz schemat).

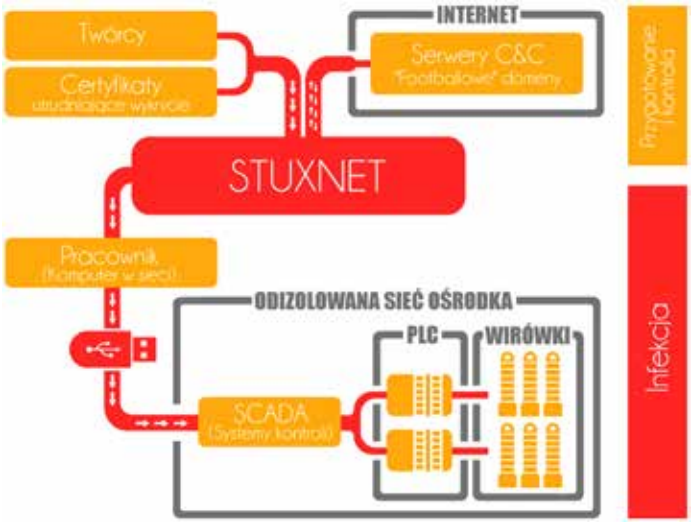
[62] Tamże, s. 6.

[63] Tamże, s. 8, 10.

[64] https://securelist.com/blog /incidents/33174/back-to-stuxnet-the-missing-link-64/ [dostęp: 2 IV 2016].

[65] Tamże.

[66] http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_ Stuxnet_and_Flame_Developers_are_Connected [dostęp: 2 V 2016].



Schemat. Sposób działania[67] programu Stuxnet.

Źródło: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/ report.pdf [dostęp: 3 V 2016].

Omawiane mechanizmy wyróżniają Stuxnet spośród innych robaków. Poza skomplikowaną strukturą kodu, tym co charakteryzuje opisywane oprogramowanie, jest precyzja działania. Ta – jak się powszechnie uważa – pierwsza na świecie cyberbroń, realizowała powierzone jej zadanie w „cieniu", ukrywając swą obecność. Bez zwątpienia pomogły temu nie tylko wspomniane już zaimplementowane systemy, lecz także odpowiednie certyfikowanie komponentów Stuxnet. Większość wirusów korzysta z preparowanych poświadczeń – w tym wypadku posłużono się kradzionymi, cyfrowymi podpisami firm JMicron Technology oraz Realtek Semiconductor[68], co utrudniło identyfikowanie robaka jako zagrożenia.

Jak już wspomniano, celem agresji były wirówki IR-1 służące do wzbogacania uranu. W celu poprawnego przeprowadzania tego procesu, musiały one pracować w zakresie od 807 do 1210 Hz. Robak przechwytywał kody PLC i modyfikował je, powodując spowalnianie (2 Hz) lub przyspieszanie (1410 Hz) pracy rotorów. Zmiana trybu pracy nie była długa, wynosiła kolejno 50 i 15 minut. Między opisanymi czynnościami przywracano standardową prędkość wirówek wynoszącą 1064 Hz[69] na 26,6 dni[70]. Jednocześnie były wyłączane protokoły bezpieczeństwa, które mogłyby

[67] Schemat stanowi uproszczone zobrazowanie sposobu działania Stuxnet. Żeby był on bardziej czytelny, nie uwzględniono między innymi sposobu przesyłu informacji z sieci odizolowanej do serwerów *command and control*. Informacje szczegółowe na ten temat zawierają raporty dotyczące robaka, N. Falliere, L.O. Murchu. E. Chien, *W32.Stuxnet*..., s. 8–11, 14–52.

[68] http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf [dostęp: 4 V 2016].

[69] Tamże.

[70] N. Falliere, L.O. Murchu. E. Chien, *W32.Stuxnet*..., s. 43.

podejmować próby przywrócenia właściwej częstotliwości. Tuż przed atakiem złośliwe oprogramowanie nagrywało bezpieczne parametry pracy urządzeń. W momencie uruchomienia separowanych sekwencji robak transferował do programów WinCC[71] wcześniej pozyskane dane, tym samym zatajając swą działalność przed operatorami, którzy obserwowali standardowe z pozoru odczyty[72]. Długie, niemalże miesięczne przerwy, pozwalały ukryć obecność Stuxnet pod pozorami jednostkowych awarii osprzętu[73]. Świadczy to o tym, że intencją twórców było działanie w ukryciu tak długo, jak to tylko możliwe.

Skutki działań omawianego oprogramowania wydają się być dwojakie. Przede wszystkim należy zwrócić uwagę na zniszczenia wywołane bezpośrednio przez robaka. Jak podaje Instytut Nauki i Bezpieczeństwa Narodowego (ISIS), Stuxnet mógł przyczynić się do zniszczenia tysiąca wirówek IR-1 w ośrodku w Natanz[74]. Potwierdził to częściowo sam prezydent Mahmud Ahmadineżad[75]. Jednocześnie zadeklarował, że problemy programu atomowego szybko zostały rozwiązane. Takie stanowisko znalazło się w przytaczanym już raporcie Symantec. Po przeanalizowaniu liczby nowo infekowanych adresów IP w skali każdego dnia, 22 sierpnia 2010 r. dostrzeżono brak kolejnych raportów z terytorium Iranu. Obecnie uważa się jednak, że wynikało to raczej z zablokowania połączeń między zaatakowaną infrastrukturą oraz serwerami C&C niż z rzeczywistego rozwiązania problemu[76]. Stuxnet mógłby prawdopodobnie spowodować znacznie większe szkody, gdyby nie został tak szybko dostrzeżony przez specjalistów do spraw bezpieczeństwa cybernetycznego[77]. Ostatecznie irański program atomowy został opóźniony, lecz nie w takim zakresie, jak zakładali twórcy robaka[78]. Uważa się, że jest to wciąż problemem, gdyż sytuacja w regionie Zatoki nie uległa zakładanym zmianom.

Innym skutkiem użycia tak zaawansowanego, złośliwego kodu, jest zwiększenie powszechnej świadomości bezpieczeństwa teleinformatycznego. Dotyczy to zarówno placówek, organizacji czy laboratoriów zajmujących się cyfrowymi zabezpieczeniami, jak i pojedynczych użytkowników sieci. Należy skupić uwagę między innymi na me-

---

[71] Program odpowiedzialny za zbieranie odczytów z urządzeń biorących udział w procesie technologicznym, w celu ich analizy, wyświetlania (prezentowania) i dystrybucji odpowiednich komend z powrotem do reszty infrastruktury. W omawianym przypadku monitory WinCC mogły być jedynym sposobem na wychwycenie nieprawidłowości w pracy wirówek.

[72] http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/ report.pdf [dostęp: 3 V 2016].

[73] Tamże.

[74] http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant [dostęp: 5 V 2016].

[75] http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129 [dostęp: 5 V 2016].

[76] N. Falliere, L.O. Murchu. E. Chien, *W32.Stuxnet*..., s. 7.

[77] Zob. tamże; http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf [dostęp: 4 V 2016].

[78] http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/ report.pdf [dostęp: 3 V 2016].

dialnym rozgłosie sprawy. Hasło c y b e r b r o ń bez zwątpienia przyczyniło się do uzyskania takiego oddźwięku, zwracając uwagę społeczeństwa na zagrożenia środowiska sieciocentrycznego. Opisywany robak dowiódł słabości współczesnych systemów sterowania, wykorzystywanych między innymi w infrastrukturach krytycznych[79]. Z tego powodu mogłoby się wydawać, że dokonanie podobnego aktu agresji w przyszłości może okazać się znacznie trudniejsze. Należy jednak wspomnieć, że kod źródłowy Stuxnet został ujawniony i wyjaśniony. Proces mający z założenia zlikwidować problem, jednocześnie zrodził inny, przez oddanie wyników studiów naukowych w ręce przestępców[80]. Świadczy to o tym, że zastosowanie nowego rodzaju broni daje tylko krótkotrwałą przewagę, a w dłuższej perspektywie stanowi obosieczne ostrze.

Zakończenie

Walka w środowisku sieciocentrycznym już trwa i cechuje się niespotykanym do tej pory w klasycznych formach prowadzenia działań wykorzystaniem cyberbroni przeciwko obcemu podmiotowi. Należy jednak pamiętać, że jest ona też swoistą bronią obosieczną, która może posłużyć do odwetu. Przyszłe starcia mogą zatem przypominać rzut bumerangiem z długofalowymi, trudnymi do przewidzenia skutkami. Dlatego też państwa oraz inne podmioty w celu sprostania tym wyzwaniom muszą tworzyć specjalistyczne jednostki, wirtualne systemy ochrony informacji oraz środki walki cybernetycznej. Niemożliwe jest jednak udzielenie odpowiedzi na pytanie, jak wirtualny konflikt wpłynie na stosunki międzynarodowe w skali globalnej. Pomimo realności zagrożenia wynikającego z cyberprzestrzeni, skutki konfliktu pozostają trudne do oceniania. Formy i metody walki, ich „kształt" oraz „zasięg rażenia" pozostają nieokreślone, gdyż cyberbroń znajduje się dopiero na początku procesu ewolucji. Zasadne wydaje się również skupienie się nie na poszukiwaniach jej autora, lecz osoby, która ją przeprojektuje. Ze względu na zaawansowaną komputeryzację współczesnego świata niemal każda infrastruktura krytyczna wydaje się zagrożona – niezależnie od jej przeznaczenia. Przykład użycia Stuxnetu ukazał, że nawet fizyczne odcięcie od globalnej sieci nie gwarantuje bezpieczeństwa. Dowiedziono także, że nazywanie robaka „cyberbronią" może być nadużyciem, gdyż program stanowił raczej prototyp tego rodzaju narzędzia. Nie oznacza to jednak, że należy bagatelizować ten rodzaj „oręża".

Wskazuje się również na brak spójnego systemu pojęciowego, który pozwoliłby skuteczniej opisywać zjawiska zachodzące w środowisku sieciocentrycznym, a tym samym tworzyć podstawy procesów legislacyjnych. Z tego powodu można dostrzec istnienie luk w prawie międzynarodowym, które w przyszłości mogą doprowadzić do zwiększenia częstotliwości występowania aktów cyberterroryzmu lub wirtualnej agresji.

[79] Tamże.

[80] R. Bania, *Wojny w cyberprzestrzeni...*, s. 197.