# Wojna i konflikt w cyberprzestrzeni. Piąty teatr wojny[1]

War and conflict in cyberspace. The fifth theatre of war

MACIEJ HEROMIŃSKI

Autor niezależny

https://orcid.org/0009-0007-4137-5326

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 185–211



https://doi.org/10.4467/20801335PBW.24.008.19610

ARTYKUŁ

Abstrakt

Celem artykułu jest przedstawienie genezy cyberprzestrzeni oraz typologii zagrożeń związanych z działaniami prowadzonymi w tej sferze zarówno przez podmioty państwowe, jak i pozapaństwowe. Dokonano systematyzacji pojęć z zakresu cyberbezpieczeństwa, zwłaszcza cyberprzestrzeni, która jest traktowana jako nowy teatr wojny, oraz zaprezentowano, jakie właściwości omawianego zjawiska mogą zostać wykorzystane do prowadzenia działań destrukcyjnych w przestrzeni cyfrowej oraz w świecie rzeczywistym. Cyberprzestrzeń staje się dogodnym obszarem do realizacji efektywnych działań, które służą unieszkodliwieniu przeciwnika w krótkim czasie i przy niewielkim nakładzie sił. Autor omówił przykłady realizacji takich działań z pierwszych dwóch dekad XXI w.: cyberwojnę w Estonii, izraelsko-amerykańskie operacje przeciwko irańskim systemom teleinformatycznym oraz cyberstarcia Stanów Zjednoczonych Ameryki z Chinami.

Słowa kluczowe

cyberprzestrzeń, cyberwojna, teatr wojny, cyberataki, Estonia, Federacja Rosyjska, USA, Izrael, Iran, Chiny

[1] Artykuł powstał na podstawie pracy licencjackiej pt. *Wojna i konflikt w cyberprzestrzeni. Piąty teatr wojny* obronionej na Wydziale Nauk Społecznych Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie (obecnie Uniwersytet Jana Długosza w Częstochowie). Praca została wyróżniona w XII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Abstract

The aim of this article is to present the genesis and typology of cyberspace and the threats that result from activities carried out in this area by state and non-state entities. The basic concepts, especially cyberspace, which is treated as a potential new theater of war, have been systematized. It was also presented the characteristics of the studied phenomenon from the point of view of using it to carry out destructive activities in the digital space and in the real world. Cyberspace is becoming an area for carrying out effective activities that serve to neutralize the enemy in a short time and with little effort. To prove his theses, the author uses numerous examples from the actual international relations, such as: the cyberwarfare in Estonia, the Israeli-American operations against Iranian ICT systems and the cyber-clashes between the United States of America and China.

Keywords

cyberspace, cyberwarfare, theater of war, cyberattacks, Estonia, Russian Federation, US, Israel, Iran, China

## Wprowadzenie

Wojny towarzyszą ludzkości od początku jej istnienia. Są one wynikiem przede wszystkim ludzkiej skłonności do przemocy, chciwości oraz chęci zdobycia bogactw czy sławy. Oblicze działań wojennych na przestrzeni dziejów się zmieniało, na co miało wpływ kilka czynników, ale do najważniejszych z nich można zaliczyć rozwój technologiczny, społeczny oraz ideologiczny.

Dzięki osiągnięciom technologicznym człowiek tworzył nowe wynalazki i systemy uzbrojenia. Miały się one przyczynić do skuteczniejszego prowadzenia działań militarnych oraz umożliwić najtańszą i najbardziej skuteczną likwidację przeciwników. W ten sposób stworzono m.in. proch strzelniczy, następnie telegram, kolej, radio, telefon, silniki parowe, a później spalinowe, komputery oraz Internet. Rozwój technologiczny przyczynił się również do powstania nowych teatrów wojny. Najstarszym z nich jest przestrzeń lądowa. Wraz z rozwojem żeglugi kolejnym miejscem starć stron konfliktu stała się przestrzeń morska. W związku ze skonstruowaniem pierwszego samolotu i praktycznym wykorzystaniem go w locie powstała następna przestrzeń wojenna – obszar powietrzny. W czasie zimnej wojny człowiek rozpoczął ekspansję w kosmosie, który stał się nowym obszarem rywalizacji państw. Za kolejny teatr wojny uważa się cyberprzestrzeń. Celem artykułu jest przedstawienie jej genezy oraz typologii zagrożeń związanych z prowadzeniem działań przy jej wykorzystaniu.

Zagadnienie zostało omówione na przykładach działań na terenie Estonii, Syrii, Iranu oraz Stanów Zjednoczonych.

Początkowo pojęcie cyberprzestrzeni istniało jedynie w literaturze. Przedstawiono ją np. w publikacjach *Neuromancer* Williama Gibsona (1984 r.), *True Names* Vernora Vinge'a (1981 r.) czy *Web of Angels* Johna M. Forda (1980 r.). Naukowcy z całego świata postawili sobie za cel urzeczywistnienie tychże wizji. Popularność zyskał głównie obraz wykreowany przez Gibsona. Zakładał on, że cyberprzestrzeń to niematerialny, nierealny obszar, który jest wypełniony mnóstwem danych w postaci cyfrowej, a także strefa potencjalnego konfliktu interesów wielkich koncernów. Duży wpływ na pojmowanie tego pojęcia miał Neal Stephenson, autor powieści *Snow Crash* (1989 r.). W swojej twórczości głosił koncepcję, która wskazywała, że cyberprzestrzeń może zostać ukazana w postaci graficznej (takie przedstawienie jest widoczne w filmie *Matrix* w postaci ciągu liczb pojawiających się z góry do dołu ekranu).

Współcześnie to pojęcie jest definiowane jako nieograniczony (pod względem zasięgu i swobody korzystania) środek komunikacji międzyludzkiej. Zaczęto je również utożsamiać z Internetem, jest to jednak uproszczenie, gdyż cyberprzestrzeń składa się z elementów fizycznych (takich jak komputery) oraz niefizycznych (nie mają one granic geograficznych czy fizycznych; można zaliczyć do nich wszelkie oprogramowania lub wspomniany Internet).

Rozwój fizycznych środków teleinformatycznych rozpoczął się już w drugiej połowie XIX w., kiedy wynaleziono telegrafię i telefonię. Wydarzenia te dały początek myśli technologicznej nakierowanej na przesyłanie informacji w nieograniczony sposób. Kolejnym krokiem w tworzeniu cyberprzestrzeni było wynalezienie radiotelefonu oraz zwiększenie efektywności druku na początku XX w. Największy przełom naukowy, nazywany komputeryzacją, dokonał się w trakcie i po zakończeniu zimnej wojny. Trudno jednak wskazać dokładny czas rozpoczęcia tego procesu. Przyjmuje się, że nastąpiło to w drugiej połowie XX w. wraz z początkiem rewolucji informatycznej, której efekty są szczególnie widoczne w XXI w. Wpłynęła ona na większość sfer życia człowieka – kulturową, społeczną, gospodarczą czy polityczną.

Pierwotnie technologia teleinformatyczna była wykorzystywana głównie przez wojsko, jednak z czasem stała się bardziej dostępna i została rozpowszechniona również w sektorze cywilnym. Postawiło to nowe wyzwania przed władzami państw i organizacji międzynarodowych, które przeniosły część swojej działalności do cyberprzestrzeni. Tym samym pojawiły się nowe zagrożenia związane z tą sferą. Dzielą się one na dwie podstawowe kategorie: zagrożenia ustrukturalizowane i nieustrukturalizowane. Pierwsze z nich są związane z działalnością zorganizowanych grup, które dysponują wyspecjalizowanym sprzętem technicznym. Grupy te najczęściej motywują swoje działania celami politycznymi, wojskowymi, religijnymi i gospodarczymi. Do zagrożeń ustrukturalizowanych należą: cyberterroryzm,

cyberszpiegostwo, operacje zbrojne w cyberprzestrzeni oraz cyberwojna. Zagrożenia nieustrukturalizowane natomiast cechują się niskim stopniem zorganizowania. Prowadzone są z zamiarem osiągnięcia celów politycznych, społecznych lub indywidualnych. Do tego typu zagrożeń zalicza się: haking, haktywizm, zwłaszcza haktywizm patriotyczny, oraz cyberprzestępczość. Warto jednak podkreślić, że granice między tymi kategoriami są płynne i mogą się dynamicznie zmieniać. To znaczy, że zagrożenia nieustrukturalizowane mogą się przerodzić w ustrukturalizowane, np. w momencie, gdy kilku samotnych hakerów zdecyduje się współpracować w ramach organizacji terrorystycznej.

## Rosyjska dezinformacja w cyberprzestrzeni

Dezinformacja stanowi jedno z najbardziej efektywnych narzędzi realizowania polityki. Polega na przeprowadzaniu różnego rodzaju operacji psychologicznych w celu wymuszenia na ofierze (odbiorcy) określonego zachowania, ukrycia swoich prawdziwych zamiarów i stworzenia fałszywej rzeczywistości, m.in. na wykorzystywaniu fałszywych lub na wpół prawdziwych informacji. Podmiot będący celem ataku często nie jest świadomy skali zagrożenia z racji deficytu swojej wiedzy, stąd też jego potencjalna reakcja może okazać się nieskuteczna. Dezinformacja sprowadza się również do manipulowania prawdziwymi informacjami przez nieujawnianie lub zmianę ich treści. W ten sposób stwarza się częściowo fałszywą wiadomość, która może ułatwić wpłynięcie na decyzję albo opinię odbiorcy lub całych grup społecznych. Istotnym elementem odróżniającym dezinformację od wprowadzania w błąd jest czas oddziaływania. Pierwsza z nich przewiduje, że fałszywe informacje mają wpływać na ofiarę i jej decyzję w dłuższej perspektywie czasowej[2].

Współcześnie przestrzenią najczęściej wykorzystywaną do szerzenia dezinformacji jest cyberprzestrzeń. Wynika to z jej ogólnodostępności. Fałszywe dane mogą zostać szybko rozpowszechnione na całym świecie, bez generowania nadmiernych kosztów[3]. Metody wprowadzania tych fałszywych danych zmieniały się na przestrzeni lat. Na początkowym etapie stosowania dezinformacji wykorzystywano czynnik ludzki. Wraz z postępem technologicznym środkami manipulacji stawały się prasa, radio, telewizja, a obecnie również technologie teleinformatyczne[4].

[2] T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2, s. 51. https://doi.org/10.15804/ppk.2015.02.03.

[3] J. Gerlach, *Wpływ prasy, radia, telewizji i internetu na współczesne zachowania nabywcze*, „Współczesne Problemy Ekonomiczne" 2018, nr 2, s. 10. https://doi.org/10.18276/wpe.2018.18-01.

[4] V. Volkoff, *Dezinformacja – oręż wojny*, Warszawa 1991, s. 119.

Jednym z krajów stosujących dezinformację na wielką skalę jest Federacja Rosyjska (FR). Rozwój rosyjskiej dezinformacji przypadł na okres rewolucji bolszewickiej, ale jej początki sięgają czasów carskich. Początkowo służyła ona wprowadzaniu w błąd za pomocą spreparowanych informacji. Z czasem stała się narzędziem prowadzenia walki informacyjnej z blokiem zachodnim (szczególnie w okresie zimnej wojny).

Federacja Rosyjska wykorzystuje przestrzeń teleinformatyczną do szerzenia dezinformacji na skalę globalną. Nie postrzega jednak cyberprzestrzeni jako odrębnego teatru wojny. Przedstawiciele władz Rosji w oficjalnym przekazie nie używają określenia „cyberprzestrzeń", lecz „przestrzeń informacyjna". Jest ona eksploatowana do prowadzenia walki informacyjnej, która według FR polega na oddziaływaniu na świadomość danej populacji[5]. Realizowanie rosyjskich operacji w przestrzeni informacyjnej spoczywa na Federalnej Służbie Bezpieczeństwa FR (Федеральная служба безопасности Российской Федерации, FSB), Służbie Wywiadu Zagranicznego FR (Служба Внешней Разведки Российской Федерации, SWR), Głównym Zarządzie Wywiadowczym Sztabu Generalnego Sił Zbrojnych FR (Главное разведывательное управление Генерального штаба Вооружённых сил Российской Федерации, GRU FR) oraz Agencji Badań nad Internetem (Агентство интернет-исследований, do 2023 r. tzw. fabryka Prigożyna). Podlegają im różne rosyjskie agencje prasowe, takie jak Sputnik czy Baltnews, odpowiedzialne za rozpowszechnianie dezinformacji. Niektóre z nich przekazują wiadomości w wielu wersjach językowych[6]. Działania dezinformacyjne są prowadzone również za pomocą mediów społecznościowych, takich jak Facebook, X (dawniej Twitter), i serwisu YouTube oraz fałszywych kont zakładanych na forach lub w mediach społecznościowych przez tzw. trolle[7] czy boty[8].

---

[5] O. Bieniek, *Cyberprzestrzeń w rosyjskiej przestrzeni informacyjnej*, „Wiedza Obronna" 2017, nr 3–4, s. 42–43.

[6] T. Chłoń, K. Kozłowski, *Wybrane studia przypadku systemowych działań dezinformacyjnych: Rosja i Chiny*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 36-37.

[7] Słowo „troll" wywodzi się z mitologii greckiej i oznacza 'potwora'. W skandynawskich bajkach trollami są stworzenia psotne i podstępne. Współcześnie słowo to odnosi się do zjawiska trollowania (ang. *trolling*). Polega ono na działaniu mającym na celu wywołanie sporu między członkami grupy internetowej. Takie osoby często stosują agresywną i wulgarną retorykę. W swojej aktywności wykorzystują również elementy dezinformacji. Trolle najczęściej działają na forach i w grupach dyskusyjnych. Zob. D. Jachyra, *Trollowanie – antyspołeczne zachowania w Internecie, sposoby wykrywania i obrony*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2011, nr 28, s. 253.

[8] Boty to programy lub aplikacje, które po zaprogramowaniu wykonują określone czynności. Obecnie są wykorzystywane na wiele sposobów. Mogą służyć do publikowania określonych informacji na danej stronie internetowej bez ingerencji człowieka. Boty często są programowane tak, aby ich działania przypominały ludzkie zachowania. W ramach dezinformacji tego typu programy mogą być

Jednym z przykładów wpływu rosyjskiej dezinformacji w cyberprzestrzeni na określone grupy społeczne jest pierwsza cyberwojna w Estonii w 2007 r. Cyberwojna to skomplikowane zjawisko, polegające na wykorzystywaniu sprzętu teleinformatycznego do dokonywania ataków na systemy potencjalnych ofiar. Zasadniczymi celami prowadzenia tego typu działań są: pozyskanie informacji, które przechowuje się (gromadzi) w danej sieci, dokonanie zniszczeń w sieciach, modyfikacja danych lub przejęcie kontroli nad niektórymi funkcjami. Ustalenie granic cyberprzestrzeni jest niemożliwe, a co za tym idzie – nie sposób określić granic danego obszaru oddziaływania (zainteresowania) państwa, które prowadzi w niej działalność. Z tego powodu bardzo trudno rozstrzygnąć, kiedy zwykły atak na daną sieć informatyczną staje się działaniem wojennym.

Estonia po 1991 r. dążyła do odcięcia się od związków z Rosją. W tym celu ukierunkowała swoją politykę na zbliżenie z Zachodem. Rząd w Tallinie podjął starania o akces do NATO i Unii Europejskiej, które miały stanowić gwarancję bezpieczeństwa dla tego kraju w związku z jego niekorzystnym położeniem geopolitycznym[9]. Federacja Rosyjska, mimo że ostatecznie zaakceptowała niepodległość Estonii, nie pogodziła się z utratą wpływów w tej republice[10].

Estońska przestrzeń teleinformatyczna od początku lat 90. XX w. jest jedną z najbardziej rozwiniętych wśród państw europejskich. Obywatele za pośrednictwem internetu mogą np. brać udział w głosowaniach czy składać deklaracje podatkowe. Cyberprzestrzeń tego państwa była pierwszą wykorzystaną jako teatr wojny[11]. Jedną z przyczyn ataku w tej cyberprzestrzeni była decyzja rządu w Tallinie z 2007 r. o przeniesieniu pomnika radzieckiego żołnierza (znanego także jako Brązowy Żołnierz, pomnik Armii Czerwonej)[12] znajdującego się w centrum stolicy. Relokacja tego

stosowane do masowego, automatycznego wysyłania określonych informacji do wielu użytkowników internetu. Zob. A. Grycuk, *Fake news, trolle, boty i cyborgi w mediach społecznościowych*, „Analizy BAS" 2021, nr 1, s. 4–5; F. Bryjka, *Wykrywanie i zwalczanie dezinformacji – zarys skryptu. Materiał pomocniczy do sylabusa zajęć akademickich*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 114.

[9] Estonia graniczy z Litwą i Rosją, ma dostęp do Morza Bałtyckiego, a także bogatą linię brzegową. Jest zaliczana do państw znajdujących się w rosyjskiej strefie wpływów, a FR dąży do ich zwiększenia w regionie bałtyckim. Zob. P. Bryczek-Wróbel, *Sytuacja geopolityczna Estonii w polityce zagranicznej Federacji Rosyjskiej*, „Polityka i Społeczeństwo" 2021, t. 19, nr 3, s. 32. https://doi.org/10.15584/polispol.2021.3.2.

[10] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 184.

[11] S. Wierzbicki, *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, t. 2, nr 1, s. 140–141.

[12] Pomnik upamiętniający poległych w II wojnie światowej powstał w 1947 r., w okresie gdy Estonia była republiką związkową ZSRR. Przedstawia on bezimiennego żołnierza Armii Czerwonej, który

obiektu na podmiejski cmentarz wojenny spotkała się ze sprzeciwem mniejszości rosyjskiej zamieszkującej Estonię[13] oraz społeczeństwa Rosji[14], przez które pomnik Brązowego Żołnierza jest postrzegany jako symbol walki Związku Radzieckiego z nazistami. Społeczeństwo Estonii uznaje go natomiast za symbol okupacji radzieckiej, która trwała od 1940 r. do 6 września 1991 r. W odwecie FR przeprowadziła kampanię dezinformacyjną – forsowano tezę, że władze Estonii dążą do zlikwidowania pomnika. Spowodowało to zwiększenie napięcia na ulicach Tallina i doprowadziło do licznych demonstracji. W zamieszkach przeciwko decyzji estońskiego rządu wzięło udział ok. 1500 osób[15].

W związku z tym, że za potencjalnego inspiratora wydarzeń została uznana Rosja, konflikt ten nazywa się „rosyjsko-estońską wojną o historię"[16]. Wśród ekspertów nie brakuje opinii, że za częścią ataków mogli stać również haktywiści, działający niezależnie od rosyjskich władz, ale sympatyzujący z ich decyzjami[17]. Przeciwko estońskim systemom zastosowano liczne ataki typu DDoS[18]. Doszło do naruszenia infrastruktury krytycznej tego państwa. Strony rządowe oraz sektor prywatny, w tym serwisy informacyjne, oświatowe, strony bankowe oraz handlowe, zostały zablokowane na trzy tygodnie. Pierwszego z ataków dokonano 28 kwietnia 2007 r. przy użyciu sieci botnet. Szczytowy moment rosyjskiej ofensywy na estońską sieć nastąpił w obchodzonym przez Rosję Dniu Zwycięstwa, tj. 9 maja[19]. Trwał aż do 19 maja. Do prowadzenia działań wykorzystano w tym czasie ok. 85 000 zainfekowanych

w lewej ręce trzyma hełm. Mowa ciała (lekko pochylona głowa) może wskazywać na żałobę bohatera po poległych towarzyszach. Zob. A. Schmidt, *The Estonian Cyberattacks*, w: *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, J. Healey (red.), Vienna 2013, s. 2.

13 Na przełomie pierwszej i drugiej dekady XXI w. stanowiła ona ok. 24,8% ludności Estonii (ok. 320 000 osób). Zob. M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 186.

14 A. Schmidt, *The Estonian Cyberattacks*…, s. 1–2.

15 I. Juurvee, M. Mattiisen, *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*, International Centre for Defence and Security, sierpień 2020 r., https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf, s. 16–18 [dostęp: 8 IV 2024].

16 S. Wierzbicki, *Wojny cybernetyczne*…, s. 141.

17 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 149.

18 Atak DDoS (ang. *distributed denial of service*) – atak na system komputerowy lub usługę sieciową przeprowadzony równocześnie z wielu komputerów w celu uniemożliwienia działania przez zajęcie wszystkich wolnych zasobów. Za: Wikipedia, https://pl.wikipedia.org/wiki/DDoS [dostęp: 8 IV 2024] – przyp. red.

19 W tym dniu każdego roku dochodziło do demonstracji przed usuniętym pomnikiem radzieckiego żołnierza. Po przeciwnych stronach stawała mniejszość rosyjska oraz Estończycy. Starcia ograniczały się jednak do potyczek słownych. W 2006 r. manifestacje zaczęły się nasilać. Zob. A. Schmidt, *The Estonian Cyberattacks*…, s. 2.

komputerów[20]. Wśród zaatakowanych systemów należy wskazać sieci dwóch największych banków w Estonii – Hansapanku i SEB Ühispanku, które były zmuszone do wstrzymania transakcji zagranicznych oraz zawieszenia wszystkich usług świadczonych w internecie. Estońskie banki oszacowały straty na kwotę ok. miliona dolarów[21]. Ofiarą padły również strony internetowe serwisów informacyjnych. Wśród nich znalazł się jeden z największych dzienników –„Postimees"[22].

W odpowiedzi na agresję na estońską cyberprzestrzeń państwa członkowskie NATO podjęły decyzję o wsparciu estońskiej obrony. W tym celu do Tallina wysłano grupę ekspertów w dziedzinie cyberbezpieczeństwa, którzy mieli wspomóc lokalnych informatyków w zneutralizowaniu skutków ataków. Niestety, pomoc ta okazała się niedostateczna i ujawniła bezsilność Sojuszu wobec tego typu zagrożeń[23]. Należy dodać, że incydentu związanego z rosyjskim atakiem nie uznano za wystarczający do uruchomienia art. 5 traktatu północnoatlantyckiego, ponieważ agresji na przestrzeń teleinformatyczną państwa członkowskiego NATO nie można było wówczas nazwać operacją militarną[24].

Sytuacja zmieniła się dopiero w 2016 r., kiedy podczas szczytu NATO w Warszawie więcej uwagi poświęcono cyberprzestrzeni. Uznano wtedy, że wrogie działania prowadzone w tym teatrze wojny wobec państw członkowskich Sojuszu będą stanowiły podstawę do uruchomienia art. 5. Sekretarz generalny Jens Stoltenberg zapowiedział, że cyberprzestrzeń będzie traktowana na równi z powietrzem, ziemią i morzem[25].

W konsekwencji wojny w estońskiej cyberprzestrzeni w 2011 r. podjęto decyzję o powołaniu specjalnej jednostki obrony cybernetycznej w Estońskiej Lidze Obrony (Cyber Defence Unit of the Estonian Defence League)[26]. W jej skład wchodzą

---

[20] A. Małecka, *Nation-State Cyber Operations Legal Considerations: An Estonian Case Study*, „Safety & Defense" 2021, t. 7, s. 101. https://doi.org/10.37105/sd.139.

[21] S. Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, „Journal of Strategic Security" 2011, t. 4, nr 2, s. 52. http://dx.doi.org/10.5038/1944-0472.4.2.3.

[22] S. Wierzbicki, *Wojny cybernetyczne*…, s. 141.

[23] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, rozprawa doktorska, Białystok 2017, s. 271 (rozprawa jest dostępna w wersji elektronicznej: https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/5875/1/J_Worona_%20Cyberprzestrzen_a_%20prawo_miedzynarodowe_Status_quo_i_perspektywy.pdf).

[24] S. Wierzbicki, *Wojny cybernetyczne*…, s. 141–142.

[25] N. Bochyńska, *Art. 5 Traktatu NATO a działania w cyberprzestrzeni. Czy istnieją „granice" dla cyberwojny?*, CyberDefence24, 17 III 2022 r., https://cyberdefence24.pl/cyberbezpieczenstwo/art-5-traktatu-o-nato-a-dzialania-w-cyberprzestrzeni-czy-istnieja-granice-dla-cyberwojny [dostęp: 7 V 2022].

[26] K. Kaska, A.M. Osula, J. Stinissen, *The Cyber Defence Unit of the Estonian Defence League. Legal, Policy and Organisational Analysis*, Tallinn 2013, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf, s. 13–14 [dostęp: 8 IV 2024].

ochotnicy, inżynierowie, pracownicy banków, korporacji i ministerstw. W razie ataku na przestrzeń teleinformatyczną jednostka ta ma podlegać dowództwu wojskowemu[27].

Ataki na estońską cyberprzestrzeń nie były szczególnie groźne dla obywateli Estonii, nie wpłynęły nawet w znaczącym stopniu na infrastrukturę krytyczną. Rosyjska agresja spowodowała głównie ograniczenia w sprawnym funkcjonowaniu państwa i społeczeństwa. Utrudniono bowiem komunikację i korzystanie ze środków finansowych, a dostęp do informacji ograniczono lub zablokowano. To, że skala oraz metody działań użyte przez agresora w tej cyberwojnie nie wyrządziły większych szkód, nie oznacza, że kolejny atak nie okaże się dużo poważniejszy i nie doprowadzi do większego paraliżu funkcjonowania struktur państwa i społeczeństwa[28].

## Walka w cyberteatrze: Izrael–USA–Iran. Stuxnet, Duqu i Flame

Izrael, który powstał po zakończeniu II wojny światowej, znalazł się w niezwykle trudnej sytuacji geopolitycznej. Otaczały go państwa arabskie, których zamiarem była likwidacja państwa żydowskiego. Konflikt zainicjowany pod koniec lat 40. XX w. nieprzerwanie trwa do dziś. Izrael, chociaż walczący w osamotnieniu, nie tylko nie dał się pokonać, lecz także powiększył swoje terytorium kosztem sąsiadów.

Szczególnym zagrożeniem dla Tel Awiwu był irański program nuklearny. Projekt zakładał utworzenie w Iranie sieci 23 elektrowni atomowych[29]. Kraj ten był gotowy do jego realizacji już w 1959 r. Wtedy to Stany Zjednoczone sprzedały władzom w Teheranie pierwszy reaktor jądrowy. Z uwagi na wybuch rewolucji w 1979 r. plan został odroczony[30]. Po przejęciu władzy reżim Chomeiniego[31]

---

[27] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17, s. 25.

[28] S. Wierzbicki, *Wojny cybernetyczne*…, s. 142.

[29] M. Sahimi, *Iran's Nuclear Program. Part I: Its History*, 2 X 2003 r., https://www.iranwatch.org/library/sahimi-irans-nuclear-program-part-i-its-history-10-2-03 [dostęp: 7 V 2022].

[30] Pierwsze sprzeciwy wyrażano już w 1977 r., kiedy władza pod presją administracji amerykańskiego prezydenta Jimmy'ego Cartera nieco uelastyczniła swoje restrykcyjne rządy. Studenci i intelektualiści masowo kierowali petycje, w których domagali się przestrzegania zasad konstytucyjnych i liberalizacji życia społecznego, a podczas spotkań w Instytucie Goethego w Teheranie elity intelektualne po raz pierwszy publicznie skrytykowały legitymizację władzy Mohammada Rezy Pahlawiego. Zob. S. Mazurek, *Rewolucja islamska w Iranie – przyczyny, przebieg, konsekwencje*, „Nurt SVD" 2017, nr 1, s. 48.

[31] Ruhollah Chomeini (1902–1989) – ortodoksyjny wyznawca islamu, duchowny i polityk irański. Po 16-letnim wygnaniu powrócił do Iranu. W 1979 r. przeprowadził rewolucję i obalił monarchię. Doprowadził do ustanowienia państwa religijnego, czyli Islamskiej Republiki Iranu. Pozostał zagorzałym przeciwnikiem USA i innych państw Zachodu. Kierował licznymi przedsięwzięciami wspierającymi

podjął decyzję o wznowieniu prac nad programem nuklearnym. Miał on stać się czynnikiem rozwoju Iranu jako mocarstwa regionalnego. Podstawą koncepcji była działalność następujących ośrodków: stacji wzbogacania uranu w Komie, elektrowni atomowej w Buszehrze, stacji przetwarzania uranu w Isfahanie, centrum wzbogacania uranu w Natanz, fabryki ciężkiej wody w Araku oraz ośrodków badań atomowych (wśród wielu z nich można wskazać centra badań w Teheranie i w Bonabie)[32].

Pod koniec lat 90. XX w. wywiad Stanów Zjednoczonych i Izraela uzyskał dane, które wskazywały na istnienie tajnych planów rozwoju broni nuklearnej Iranu[33]. Irańska opozycja przedstawiła dowody świadczące o pracach prowadzonych nad rozwojem tego typu broni. Pod koniec 2002 r. podobne oskarżenia wobec teherańskiego reżimu wysunęły Stany Zjednoczone. Niepokój wśród elit politycznych USA i ich europejskich sojuszników wynikał z obawy przed rosnącym zagrożeniem dla Izraela, wojsk amerykańskich, z niepewnego status quo na Bliskim Wschodzie, a także możliwości rozpowszechnienia się broni masowego rażenia wśród ugrupowań terrorystycznych.

W celu udaremnienia dalszych prac nad produkcją broni jądrowej przez Iran zrealizowano wiele przedsięwzięć dyplomatycznych. Zabiegi te nie przyniosły jednak oczekiwanych rezultatów. Brak porozumienia z władzami Iranu zmusił państwa członkowskie oraz Radę Bezpieczeństwa ONZ do nałożenia na to państwo dotkliwych sankcji[34]. Irański reżim pomimo tych działań kontynuował rozwój technologii broni atomowej. Spowodowało to załamanie relacji na linii Tel Awiw––Teheran, które do 1979 r. opierały się na bliskiej współpracy. Iran podejrzewał Izrael o chęć ingerowania w jego sytuację wewnętrzną, strona izraelska zaś widziała w irańskim reżimie zagrożenie własnego bezpieczeństwa narodowego. Izrael zakładał w związku z tym przeprowadzenie uderzenia prewencyjnego, które miałoby na celu zatrzymanie rozwoju programu atomowego. Poglądy zbliżone do Tel Awiwu miały Stany Zjednoczone, ponieważ Iran stanowił zagrożenie amerykańskiej

rozwój radykalizmu islamskiego. Zob. J. Kukułka, *Historia współczesna stosunków międzynarodowych 1945–2000*, Warszawa 2007, s. 232–233; S. Jones, *The Islamic Republic of Iran: An introduction*, House of Commons Library, 11 XII 2009 r., https://researchbriefings.files.parliament.uk/documents/RP09-92/RP09-92.pdf, s. 8 [dostęp: 8 IV 2024].

[32] K. Szymczyk, *Irański program nuklearny jako czynnik warunkujący stosunki międzynarodowe w obszarze i poza obszarem MENA*, w: *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, R. Bania, K. Zdulski (red. nauk.), Łódź 2012, s. 148.

[33] Informacja na ten temat została przekazana opinii publicznej dopiero w 2002 r. Zob. M. Kaniewska, *Między kijem a marchewką – Organizacja Narodów Zjednoczonych wobec programu nuklearnego Iranu*, w: *Stabilizacja czy destabilizacja? Społeczność międzynarodowa wobec programu nuklearnego Iranu*, A. Malantowicz, Ł. Smalec (red. nauk.), Warszawa 2014, s. 56.

[34] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar…*, s. 254.

pozycji na Bliskim Wschodzie[35]. W przeciwieństwie do Izraela jednak amerykański rząd nie dopuszczał możliwości przeprowadzenia operacji militarnej. Waszyngton starał się także zahamować izraelskie dążenia do uderzenia wyprzedzającego. Dokonywał tego przez redukcję wsparcia militarnego wysyłanego władzom w Tel Awiwie. Ponadto rozmieszczenie ośrodków atomowych wymagałoby przeprowadzenia jednoczesnego bombardowania odległych od siebie celów. Realizacja operacji wojskowej, która miałaby zniszczyć irański przemysł atomowy, równałaby się ze stanowczą odpowiedzią militarną ze strony Teheranu. Izraelska agresja mogłaby się również spotkać z poważną reakcją świata arabskiego, w tym ugrupowań terrorystycznych (np. Hezbollahu). Obawiano się także zablokowania przez stronę irańską cieśniny Ormuz[36], która stanowi główny punkt transportu surowców energetycznych. Użycie broni konwencjonalnej nie gwarantowało przerwania prac nad programem atomowym, mogło jedynie doprowadzić do jego opóźnienia[37].

Przedstawiony bilans ryzyka, ewentualnych zysków i strat zmusił Izrael oraz Stany Zjednoczone do podjęcia innych kroków. Półśrodkiem w rozwiązaniu tego problemu było zaangażowanie służb specjalnych w dokonywanie zabójstw naukowców odgrywających najważniejszą rolę w realizacji programu atomowego. W wyniku tych pozamilitarnych działań w latach 2007–2012 zlikwidowano pięciu irańskich specjalistów, ale nie miało to istotnego wpływu na rozwój programu[38].

Kolejnym sposobem na zatrzymanie irańskich aspiracji było wykorzystanie cyberprzestrzeni. Izrael już na początku XXI w. dysponował rozwiniętą infrastrukturą teleinformatyczną. Ponadto miał doświadczenie w prowadzeniu działań ofensywnych w tym obszarze w związku ze zrealizowaną przez niego operacją „Orchard"[39].

---

[35] J. Dobbins i in., *Coping with a Nuclearizing Iran*, Santa Monica 2011, s. 11.

[36] H. Ajili, N. Rezaee, *Iranian Military Capabilities and Possibility of Blocking Hormuz Strait by Iran*, „Cywilizacja i Polityka" 2020, nr 18, s. 61. https://doi.org/10.15804/cip202005.

[37] J. Zanotti i in., *Israel: Possible Military Strike Against Iran's Nuclear Facilities*, Congressional Research Service, 28 IX 2012 r., https://sgp.fas.org/crs/mideast/R42443.pdf, s. 41–43 [dostęp: 7 V 2022].

[38] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 254.

[39] Operacja ta została przeprowadzona w 2007 r. na terytorium Syryjskiej Republiki Arabskiej i miała na celu zatrzymanie syryjskich aspiracji do zwiększenia wpływów w regionie. Syria dążyła do stworzenia broni jądrowej. Pierwszą elektrownię atomową zbudowała we współpracy z Koreańską Republiką Ludowo-Demokratyczną na początku XXI w. Izraelski wywiad uzyskał jednak informację, że jest ona wykorzystywana również w celach militarnych. Stanowiło to zagrożenie bezpieczeństwa Izraela. Rząd w Tel Awiwie podjął decyzję o interwencji zbrojnej na terenie tego państwa. W celu zabezpieczenia swojego lotnictwa przed systemami przeciwlotniczymi przeciwnika zastosowano ataki w cyberprzestrzeni. Izrael we współpracy z amerykańskimi agencjami opracował program SUTER. Powstał on w trzech generacjach. Pierwsza dawała możliwość śledzenia informacji pokazywanych na syryjskich radarach. Druga była bardziej agresywna – pozwalała na przejęcie kontroli nad siecią i sensorami ofiary ataku. Trzecia umożliwiała sterowanie systemami w zainfekowanej sieci

Rozwój zdolności w przestrzeni wirtualnej został wymuszony na Izraelu z powodu rosnącego zagrożenia cyberterroryzmem ze strony lokalnych grup terrorystycznych. Wewnątrz struktur izraelskich służb specjalnych zostały utworzone wyspecjalizowane zespoły do walki w przestrzeni teleinformatycznej.

Izraelskie możliwości oddziaływania w sieci przesądziły o formie działań, jakie zamierzano podjąć, aby powstrzymać irański program nuklearny. Za cel obrano zakłady produkujące wzbogacony uran. Uznano, że obiektem, którego uszkodzenie najskuteczniej wpłynie na rozwój broni jądrowej, będą wirówki służące do wytwarzania wzbogaconego uranu. Dlatego, aby je zniszczyć, postanowiono wprowadzić do oprogramowania sterującego pracą tych urządzeń wirus komputerowy o nazwie W32.Stuxnet (początkowo nazwany W32.Temphid)[40]. Ten akt sabotażu nie tylko nie pozwolił na oddzielenie uranu, lecz także doprowadził do trwałego uszkodzenia części zaatakowanych urządzeń[41].

Fora specjalistyczne zaczęły udostępniać informacje o tym złośliwym oprogramowaniu w czerwcu 2010 r. Pierwszy kontakt z wirusem miała białoruska firma VirusBlokAda[42] w dniu 17 czerwca. Stworzony przez nią raport na temat nowego zagrożenia wskazywał, że oprogramowanie powinno zostać zaliczone do kategorii najbardziej niebezpiecznych. Po zainfekowaniu komputera program rozpoczynał proces ukrywania swojej obecności w systemie. Wykorzystywał do tego luki oraz błędy systemu operacyjnego. Dodatkowo wirus dezorientował programy antywirusowe, co również wpływało na zdolność ukrycia swojej obecności na danym nośniku. W lipcu 2010 r. Siemens zaobserwował, że Stuxnet atakuje stworzone przez tę firmę systemy przemysłowe SCADA. W dniu 20 lipca przedsiębiorstwo Symantec wykryło łączność tego wirusa ze zdalnymi serwerami dowodzenia i kontroli. Ślady infekcji Stuxnetem odkryto w wielu państwach świata. Według przeprowadzonych badań zaatakowano ok. 100 000 komputerów, m.in. w Indiach, Indonezji, Chinach,

(w tym systemami rakietowymi lub radarami). SUTER sprawia, że operatorzy zaatakowanej sieci mają wrażenie, że system działa prawidłowo. W wyniku paraliżu systemów obrony przeciwlotniczej siły powietrzne Izraela dokonały skutecznego zniszczenia reaktora w okolicach miasta Dajr az-Zaur. Zob. S. Dygnatowski, P. Dygnatowski, Ł. Domżał-Drzewicki, *Analiza wykorzystania rozwiązań strukturalnych w obszarze cyberbezpieczeństwa na przykładzie operacji Orchard*, „Journal of KONBiN" 2019, t. 49, nr 1, s. 293–296. http://dx.doi.org/10.2478/jok-2019-0014.

[40] *Wirus Stuxnet (robak Stuxnet)*, w: *Vademecum bezpieczeństwa informacyjnego*, t. 2, O. Wasiuta, R. Klepka (red.), Kraków 2019, s. 514.

[41] J.P. Farwell, R. Rohozinski, *Stuxnet and the Future of Cyber War*, „Survival. Global Politics and Strategy" 2011, t. 53, nr 1, s. 28. https://doi.org/10.1080/00396338.2011.555586.

[42] Przedsiębiorstwo to zajmuje się dystrybucją oprogramowania antywirusowego. Zob. https://www.anti-virus.by/ [dostęp: 9 IV 2024].

Korei Południowej i Australii, przy czym 60 000 zainfekowanych systemów znajdowało się na terenie Iranu[43].

W 2010 r. irański prezydent Mahmoud Ahmedinejad potwierdził szkody wyrządzone przez robaka Stuxnet w infrastrukturze krytycznej. Przyjmuje się, że w wyniku serii ataków zostało uszkodzonych ok. 1000 wirówek działających w zakładach w miejscowości Natanz. Irańskie władze, manipulując danymi, nie podały dokładnych informacji na temat poniesionych strat[44]. W tym samym roku 30 września opracowano interesujący i precyzyjny raport na temat sposobu działania tego wirusa oraz jego specyfiki. W tym okresie wzrosło też zainteresowanie społeczności międzynarodowej problemem ataków w cyberprzestrzeni oraz pochodzeniem tego robaka. Eksperci zaznaczali, że poziom zaawansowania Stuxnetu wskazuje na to, że mógł on powstać tylko w wyspecjalizowanym ośrodku rządowym.

Władze Iranu od początku twierdziły, że inicjatorem tych ataków były Stany Zjednoczone, które współpracowały z Izraelem. Przy czym ograniczenie wysiłków Iranu ukierunkowanych na stworzenie broni jądrowej poparły również państwa arabskie, m.in. Arabia Saudyjska, Egipt czy Jordania, które obawiały się zbyt dużego wpływu reżimu ajatollahów na Bliskim Wschodzie. Obecnie jednak przyjmuje się, że za atakiem na irańską cyberprzestrzeń stały izraelskie służby specjalne, które współpracowały ze Stanami Zjednoczonymi. Państwa te uchodzą za jedne z najlepiej przygotowanych do działań militarnych w omawianym teatrze wojny[45].

Stuxnet nie był jedynym złośliwym robakiem wykorzystywanym w tym konflikcie. W październiku 2011 r. grupa informatyków z Uniwersytetu Technologii i Ekonomii w Budapeszcie odkryła złośliwe oprogramowanie Duqu. Jego nazwa pochodzi od pliku, który tworzył się na zainfekowanym systemie .DQ. Ustalono, że został on oparty na technologii oraz kodzie wykorzystanych do stworzenia Stuxnetu. Zasady jego działania były podobne do pierwowzoru, ale używano go do innych celów[46]. Zdolności keyloggera[47] pozwalały mu na rejestrowanie aktywności użytkownika komputera. Podobnie jak Stuxnet, Duqu cechował się wysokim poziomem skomplikowania, ale jego szczególnym atrybutem był trudny do zidentyfikowania język programowania. Zdolności Duqu były jednak znacznie ograniczone

[43] S. Wierzbicki, *Wojny cybernetyczne*…, s. 145.

[44] K. Kowalczewska, *Wpływ nowoczesnych technologii na współczesne konflikty zbrojne*, Warszawa 2022, s. 24.

[45] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 256–258.

[46] B. Bencsáth i in., *Duqu: A Stuxnet-like malware found in the wild. Technical Report by Laboratory of Cryptography and System Security (CrySys)*, 14 X 2011 r., https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf, s. 5 [dostęp: 8 IV 2024].

[47] Keylogger – rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika. Za: Wikipedia, https://pl.wikipedia.org/wiki/Keylogger [dostęp: 8 IV 2024] – przyp. red.

w porównaniu z możliwościami poprzednika. Ślad jego działalności wykryto w kwietniu 2011 r. (prawdopodobnie pierwszy atak z użyciem Duqu przeprowadzono pod koniec 2010 r.) i, jak się wydaje, mógł zostać wykorzystany do zainfekowania komputerów w ośmiu krajach, m.in. w Iranie, we Francji oraz w Indiach[48].

Duqu został zaliczony do grupy trojanów. Nie służył do ingerowania w integralność zainfekowanego systemu, lecz był stosowany jako program szpiegowski. Za jego pomocą cyberżołnierz mógł pozyskać dane zawarte na zaatakowanym komputerze, w tym informacje na temat używanych klawiszy, specyfikacje zainfekowanego sprzętu teleinformatycznego oraz innych urządzeń znajdujących się w jednej sieci, a ponadto mógł dokonywać zrzutów z ekranu danego komputera. Ten złośliwy program stanowi wręcz idealne narzędzie służące do rozpoznania infrastruktury informatycznej, nad którą można przejąć kontrolę przez uzupełnienie programu o komponenty Stuxnetu[49].

W listopadzie 2011 r. Iran potwierdził obecność Duqu w sieciach komputerowych związanych z programem atomowym. Strona irańska informowała, że skutecznie zwalcza ataki we własnej cyberprzestrzeni. Trudno jednak ocenić wiarygodność tego przekazu, ponieważ nie są znane ani konsekwencje ataków przeprowadzonych za pomocą tego złośliwego programu, ani szczegóły kontrakcji irańskich specjalistów[50].

W maju 2012 r. wykryto kolejny złośliwy program, który miał kilka cech wspólnych ze Stuxnetem i Duqu. Był to Worm.W32.Flame (ang. *flame* oznacza 'płomień', 'ogień')[51]. Grupy badawcze podjęły pracę nad analizą tego wirusa po ataku na systemy teleinformatyczne irańskiego Ministerstwa ds. Ropy Naftowej oraz inne podmioty związane z infrastrukturą energetyczną. Hakerzy za pomocą tego programu usuwali dane z twardych dysków komputerów znajdujących się w irańskim ministerstwie. Flame był bardziej skomplikowany niż oba wirusy przedstawione wcześniej. Prawdopodobnie został wykorzystany już kilka lat przed jego wykryciem, ale ustalenie dokładnej daty jego pierwszego użycia jest niemożliwe, gdyż w celu ukrycia tej informacji cyberżołnierze modyfikowali daty utworzenia zainfekowanych plików[52]. Na podstawie niektórych analiz wskazuje się, że być może

[48] S. Wierzbicki, *Wojny cybernetyczne*…, s. 143–145.

[49] B. Bencsáth i in., *The Cousins of Stuxnet: Duqu, Flame and Gauss*, „Future Internet" 2012, nr 4, s. 979–980. https://doi.org/10.3390/fi4040971.

[50] E. Chein, L. OMurchu, N. Falliere, *W32.Duqu. The precursor to the next Stuxnet*, https://www.usenix.org/system/files/conference/leet12/leet12-final11.pdf, s. 1–2 [dostęp: 7 V 2022].

[51] K. Majdan, *Wykryto nowe „cyberzagrożenie". „Z czymś takim jeszcze się nie spotkaliśmy"*, na Temat, 29 V 2012 r., https://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czyms-takim-jeszcze-sie-nie-spotkalismy [dostęp: 7 V 2022].

[52] B. Bencsáth i in., *The Cousins of Stuxnet*…, s. 980.

powstał on w 2008 r.[53] Został opracowany w celu pozyskiwania informacji z zaatakowanych komputerów. Podobnie jak Duqu wykorzystywał do tego keyloggery, ale miał także szeroki wachlarz innych narzędzi[54]. Przy ich użyciu haker mógł uzyskać kontrolę nad kamerą lub mikrofonem komputerowym i nagrywać obraz oraz dźwięki z otoczenia, uzyskiwać dostęp do podłączonych nośników danych czy też wykorzystać technologię Bluetooth do wyszukiwania telefonów w pobliżu zainfekowanego sprzętu[55].

Rozpowszechnienie Flame'a następowało w momencie podłączenia nośnika pamięci (za pomocą USB) do komputera stanowiącego cel ataku lub za pomocą lokalnej sieci. Program ten przez śledzenie ruchów w sieci tworzył listę haseł, a także pozyskiwał inne dane wrażliwe. Następnie przesyłał je do serwerów dowodzenia i kontroli. Po osiągnięciu zamierzonych celów wirus samoczynnie usuwał się z twardego dysku[56].

## Chińsko-amerykańskie cyberstarcie

Współpraca chińsko-amerykańska o szczególnym charakterze została nawiązana po zakończeniu II wojny światowej. Relacje załamały się jednak po wojnie domowej wygranej w 1949 r. przez komunistów pod przywództwem Mao Tse-tunga. Doszło również do walk pomiędzy tymi państwami podczas wojny koreańskiej w latach 1950–1953. Unormowanie stosunków nastąpiło pod koniec lat 70. XX w., kiedy władze USA oficjalnie uznały Chińską Republikę Ludową (ChRL) za państwo. Relacje te jednak wciąż były napięte. Wynikało to z odmiennych stanowisk odnośnie do niezależności Tajwanu, nieakceptowania przez Waszyngton autorytarnego systemu politycznego Chin oraz braku poszanowania praw człowieka w tym państwie[57].

Po rozpadzie Związku Radzieckiego w 1991 r. rola USA na arenie międzynarodowej wzrosła. Wpisywało się to w ideę nowego ładu światowego, proklamowaną przez prezydenta George'a Busha. Zakładała ona wykorzystanie potencjału militarnego i ekonomicznego oraz instrumentów wpływu politycznego do kreowania

[53] A. Zakrzewski, *Jak to jest z tym Stuxnetem, Flamem, Duqu?*, „DLP Expert" 2013, nr 1, s. 9–13.

[54] *First Stuxnet – Now the Flame Virus*, The Availability Digest, czerwiec 2012 r., www.availabilitydigest.com/public_articles/0706/flame_virus.pdf, s. 2 [dostęp: 10 V 2022].

[55] J.P. Farwell, R. Rohozinski, *The New Reality of Cyber War*, „Survival. Global Politics and Strategy" 2012, t. 54, nr 4, s. 109. https://doi.org/10.1080/00396338.2012.709391.

[56] K. Zetter, *Odliczając do dnia zero. Stuxnet, czyli prawdziwa historia cyfrowej broni*, Gliwice 2014, s. 285–287.

[57] *1949–2023 U.S.-China Relations*, Council on Foreign Relations, https://www.cfr.org/timeline/us-relations-china [dostęp: 10 V 2022].

pozycji lidera w skali globalnej. Cele te zostały doprecyzowane przez prezydenta Billa Clintona, który jako priorytety polityki zagranicznej wskazał także wzmacnianie bezpieczeństwa, rozwijanie dobrobytu Stanów Zjednoczonych oraz promowanie demokracji[58]. Przedstawione założenia stanowiły przeszkodę w utrzymaniu stabilnych relacji z Chinami. Również dynamiczny rozwój ChRL i jej rosnące możliwości oddziaływania na politykę Azji Wschodniej oraz w przestrzeni globalnej wywoływały konflikt interesów między oboma państwami. Dlatego Stany Zjednoczone dążyły do działań mających na celu ograniczenie wzrostu chińskiej potęgi oraz wpływów w różnych rejonach świata (m.in. w Afryce, gdzie dochodziło do rywalizacji o surowce energetyczne). Kursy polityczne kolejnych amerykańskich prezydentów zakładały zmianę polityki zagranicznej, która miała obejmować sprawy dotyczące Azji Wschodniej[59].

Polityka Pekinu była ukierunkowana dwutorowo. Po pierwsze, skupiała się na utrzymaniu niepodległości, suwerenności oraz integralności terytorialnej ChRL, a po drugie, dążono do wprowadzania odpowiednich reform oraz wywierania wpływu w środowisku międzynarodowym. Warto podkreślić, że według oficjalnego stanowiska Pekinu te założenia miały być realizowane w sposób pokojowy. Wraz ze wzrostem chińskiego potencjału i wpływów władze ChRL zaczęły jednak ingerować w stosunki międzynarodowe z wykorzystaniem różnych narzędzi[60].

Wśród czynników, które miały wpływ na powstanie i narastanie napięcia między USA a ChRL, należy wskazać:

- brak wspólnego wroga – po upadku ZSRR nie pojawiły się zagrożenia, które wymagałyby wspólnego działania,
- wyrównanie poziomów rozwoju – wskazywana była rywalizacja między potęgą „wschodzącą", jaką były Chiny, a potęgą „schodzącą", reprezentowaną przez Stany Zjednoczone,
- różnice ideologiczne, czyli klasyczny konflikt pomiędzy ustrojem komunistycznym a demokratycznym[61].

Otwarte działania zbrojne między tymi państwami są jednak mało prawdopodobne. Wynika to głównie z tego, że zarówno Chiny, jak i Stany Zjednoczone

[58] J. Zając, *Polityka zagraniczna USA*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, Warszawa 2011, s. 61–64.

[59] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 297–298.

[60] J. Marszałek-Kawa, *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, T. Łoś-Nowak (red.), Warszawa 2011, s. 115.

[61] J.K. Park, *A Report of the CSIS Korea Chair. China–U.S. Relations in East Asia. Strategic Rivalry and Korea's Choice*, Center for Strategic and International Studies, kwiecień 2013 r., https://ciaotest.cc.columbia.edu/wps/csis/0028481/f_0028481_23160.pdf, s. 7–9 [dostęp: 8 IV 2024].

dysponują arsenałem broni atomowej[62]. Dlatego Pekin rozpoczął rozwijanie wielu projektów oraz programów, które można wykorzystać w ramach działań asymetrycznych i hybrydowych z zastosowaniem systemów zdolnych do niszczenia amerykańskich satelitów oraz realizacji operacji ofensywnych w cyberprzestrzeni[63].

Chińska Republika Ludowa w zakresie rozwoju nowoczesnych technologii informatycznych przez długi okres pozostawała daleko za stroną amerykańską. Ten stan rzeczy należy już jednak do przeszłości. Obecnie to właśnie Chiny nadają ton w obszarze nowych technologii, zwłaszcza tych wykorzystywanych w cyberprzestrzeni[64].

Rewolucja informatyczna w Chinach nastąpiła bardzo szybko, świadczy o tym m.in. ogromna liczba internautów w tym kraju. Powstało także wiele bardzo dużych korporacji, takich jak Baidu (która stworzyła wyszukiwarkę internetową), DXY.cn (media społecznościowe) czy Huawei (zajmujący się produkcją sprzętu komputerowego i telekomunikacyjnego)[65]. Ponadto w ChRL wyprodukowano komputery obliczeniowe, będące najprawdopodobniej najpotężniejszym sprzętem tego rodzaju na skalę światową. Są one wykorzystywane m.in. do łamania szyfrów oraz prowadzenia operacji militarnych w cyberprzestrzeni. W wyniku zaostrzającej się rywalizacji między ChRL a Stanami Zjednoczonymi oraz dynamicznego rozwoju technologii informatycznych konflikt między tymi państwami przeniósł się do cyberprzestrzeni[66].

Do pierwszego incydentu wynikającego z tej rywalizacji doszło w 1999 r. W związku ze zbombardowaniem przez lotnictwo NATO ambasady ChRL w Belgradzie – w ramach operacji militarnej prowadzonej przeciwko tzw. trzeciej Jugosławii – Chińczycy przeprowadzili w odpowiedzi serię masowych cyberataków[67]. Jednym z nich był atak typu DDoS, za pomocą którego na trzy dni zablokowano strony Białego Domu. Drugim modelowym działaniem chińskiego cyberwojska stało się masowe wysyłanie spamu na pocztę elektroniczną amerykańskiej administracji. W ten sposób zamierzano ją przeciążyć i sparaliżować. Ostatnim rodzajem ataku były włamania na strony internetowe Departamentu Energii oraz Departamentu Spraw Wewnętrznych, na których zamieszczono hasła sprzeciwu

---

62 Tamże.

63 S. Kumar, *Asymmetric Capabilities of China's Military*, Institute of Peace and Conflict Studies, 19 XI 2008 r., https://www.ipcs.org/comm_select.php?articleNo=2735 [dostęp: 10 V 2022].

64 F.S. Reeder i in., *Updating U.S. Federal Cybersecurity Policy and Guidance. Spending scarce taxpayer dollars on security programs that work*, Center for Strategic and International Studies, październik 2012 r., https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121019_Reeder_A130_Web.pdf, s. 1–2 [dostęp: 8 IV 2024].

65 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 307.

66 J. Carr, *Inside Cyber Warfare*: *Mapping the Cyber Underworld*, Beijing–Cambridge–Farnham–Köln–Sewastopol–Taipei–Tokyo 2010, s. 2.

67 Tamże.

wobec interwencji zbrojnej USA i państw NATO na obszarze Kosowa. Oficjalnie do przeprowadzonych ataków przyznały się grupy chińskich haktywistów. Ich działalność spotkała się z aprobatą władz[68].

Kolejne starcie w cyberprzestrzeni pomiędzy ChRL i USA nastąpiło w kwietniu i maju 2001 r. Operacje w tym przypadku były prowadzone przez obie strony. Ich przyczyną było zderzenie się w przestrzeni powietrznej nad Morzem Południowochińskim chińskiego myśliwca J-8 z amerykańskim samolotem zwiadowczym EP-3[69]. Incydent spowodował wzrost napięcia na linii Pekin–Waszyngton. W wyniku tego zdarzenia haktywiści ze Stanów Zjednoczonych dokonali włamań do ok. 1000 chińskich witryn internetowych. W odpowiedzi chińskie środowiska hakerów w maju przeprowadziły serię ataków na podobną liczbę amerykańskich stron. Tym razem jednak władze ChRL uznały działania własnych hakerów za sprzeczne z prawem i zakwalifikowały je jako cyberterroryzm[70].

W wyniku utraty poparcia władz część chińskich grup hakerskich przekształciła się w firmy zajmujące się bezpieczeństwem teleinformatycznym. W związku z pełną kontrolą przestrzeni teleinformatycznej w Chinach opisywane przedsiębiorstwa zostały jednak zmuszone do współpracy ze służbami specjalnymi Państwa Środka. Oficjalnie Pekin nigdy nie potwierdził kooperacji z sektorem prywatnych firm z branży bezpieczeństwa IT, ale większość ekspertów uważa, że chińskie władze korzystały ze złośliwego oprogramowania i technik stworzonych przez wspomniane grupy hakerskie[71].

Zmiana stanowiska Pekinu w związku z działalnością haktywistów w operacjach przeciwko Stanom Zjednoczonym była spowodowana koniecznością dokonania zmian w taktyce prowadzenia chińskich operacji w cyberprzestrzeni. Chińska Republika Ludowa skupiła się bowiem na skrytym działaniu na amerykańskich serwerach w celu pozyskiwania informacji niejawnych.

W latach 2002–2003 w ramach kampanii „Titan Rain"[72] Chińczycy włamali się za pomocą programów typu trojan m.in. do amerykańskich systemów Departamentu Obrony, Departamentu Stanu, Departamentu Energii, Departamentu Bezpieczeństwa Krajowego, komputerów struktur wchodzących w skład amerykańskiej

[68] B. Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, The US-China Economic and Security Review Commission, 9 X 2009 r., https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf, s. 36–37 [dostęp: 8 IV 2024].

[69] S. Wierzbicki, *Wojny cybernetyczne*…, s. 139.

[70] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 311–312.

[71] B. Krekel, *Capability of the People's Republic of China*…, s. 37–38.

[72] J. Andress, S. Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham 2011, s. 11.

armii oraz NASA, a także do systemów informatycznych największych amerykańskich koncernów[73]. W wyniku tych działań ChRL uzyskała informacje dotyczące: systemów informatycznych wykorzystywanych w amerykańskich myśliwcach, danych technicznych napędów kosmicznych oraz planów paneli słonecznych wykorzystywanych w sprzęcie kosmicznym. Po ujawnieniu w 2005 r. tych ataków władze w Pekinie stanowczo zaprzeczyły, że są ich sprawcami[74].

W sierpniu 2006 r. ofiarą chińskiego cyberataku padł Pentagon. W wyniku włamania do wojskowej sieci NIPRNET grupy hakerskie z terytorium ChRL wykradły około 20 terabajtów danych[75]. W 2008 r. wykryto ingerencję w bazy danych prezydenckich kampanii wyborczych obu stron – Partii Republikańskiej i Partii Demokratycznej. Ślady pozostawione przez hakerów wskazywały, że ataki były przeprowadzone z terytorium Państwa Środka[76].

Do ponownego ataku na Pentagon doszło w 2009 r. Według oficjalnego przekazu w wyniku włamania pochodzącego z terytorium Chin pozyskano dane na temat amerykańskiego programu zbrojeniowego Joint Strike Fighter (zakładającego modernizację lotnictwa oraz systemów obrony przeciwlotniczej). Podczas neutralizacji skutków tego cyberataku odkryto, że program zbrojeniowy był inwigilowany od 2007 r., przy czym metody szyfrowania plików wykorzystane przez hakerów uniemożliwiły określenie, jakie informacje zostały utracone. Chińska Republika Ludowa za pośrednictwem swojej ambasady w USA zaprzeczyła, jakoby władze w Pekinie prowadziły działania cyberprzestępcze, a oskarżenia uznano za fałszywe i mające na celu szerzenie poczucia zagrożenia rzekomo wynikającego z chińskiej działalności w cyberprzestrzeni[77].

Największa wykryta chińska kampania przeciwko amerykańskiej przestrzeni teleinformatycznej także rozpoczęła się w 2009 r. Operacja „Aurora" miała na celu przeprowadzenie ataków na serwery ponad 30 korporacji Stanów Zjednoczonych. Do stycznia 2010 r. stwierdzono naruszenie integralności sieci takich firm, jak: Google, Adobe Systems, Yahoo!, Morgan Stanley (zajmującej się obsługą finansową) oraz Dow Chemical Company (działającej w przemyśle chemicznym). Atak

[73] R. Wydra, *Relacje Chin i Stanów Zjednoczonych w cyberprzestrzeni*, „Security, Economy & Law" 2017, nr 3, s. 103. https://doi.org/10.24356/SEL/16/6.

[74] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 312–313.

[75] J.C. Mulvenon, *Chinese Cyber Espionage. Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law*, Washington 2013, s. 29.

[76] L. Glendinning, *Obama, McCain computer 'hacked' during election campaign*, The Guardian, 7 XI 2008 r., https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa [dostęp: 10 V 2022].

[77] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 316–317.

zagroził również systemom informatycznym instytucji innych państw świata, w tym Niemiec, Wielkiej Brytanii i Tajwanu[78].

Jednym ze złośliwych programów użytych podczas operacji „Aurora" był trojan Hydraq. Jego instalacja na komputerze następowała w momencie wejścia na zainfekowaną stronę internetową. Następnie program przeszukiwał zawartość dysków twardych, po czym kopiował zamieszczone na nich dane. Po zaszyfrowaniu przechwyconej zawartości wysyłał ją do Chin[79]. Skala przeprowadzonych ataków spowodowała ostrą reakcję ze strony Stanów Zjednoczonych, wzywających ChRL do przeprowadzenia transparentnego śledztwa. Strona chińska zlekceważyła jednak żądania USA[80].

W lipcu 2011 r. doszło do kolejnego poważnego ataku na amerykańskie korporacje z sektora obronnego. W wyniku cyberwłamań wykradziono ok. 24 000 plików. Oficjalne stanowisko USA jednoznacznie nie wskazywało sprawcy, lecz sugerowało, że hakerzy przeprowadzili operacje z terytorium Chin[81].

Na początku 2013 r. ofiarami chińskich cyberataków padły największe amerykańskie media, takie jak „The New York Times", „The Wall Street Journal" i „The Washington Post". W przypadku pierwszego z nich włamania na komputery dziennikarzy tej gazety trwały przez cztery miesiące. Jedną z prawdopodobnych przyczyn przeprowadzenia tych działań była publikacja artykułu, w którym opisano majątek chińskiego premiera Wena Jiabao[82]. Hakerzy poszukiwali również materiałów, które miały posłużyć do opracowania kolejnych tekstów o członkach chińskiego rządu.

W lutym 2013 r. Departament Bezpieczeństwa Krajowego ujawnił, że w czasie sześciu miesięcy została przeprowadzona seria cyberataków na infrastrukturę krytyczną Stanów Zjednoczonych. Podczas włamań do sieci 23 przedsiębiorstw gazowych hakerzy uzyskali dane dostępu administracji sieci, ich specyfikację oraz informacje na temat dostępu do systemów kontroli gazociągów[83].

Raport opublikowany w 2013 r. przez korporację Mandiant potwierdził większość opinii ekspertów na temat źródeł cyberataków w przestrzeni teleinformatycznej Stanów Zjednoczonych. Ponadto wskazywał, że część grup hakerskich

---

78 Tamże.

79 Tamże, s. 317.

80 B. Johnson, *US asks China to explain Google hacking claims*, The Guardian, 13 I 2010 r., https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us [dostęp: 10 V 2022].

81 C. Lefkow, *24,000 files stolen from defense contractor: Pentagon*, phys.org, 15 VII 2011 r., https://phys.org/news/2011-07-stolen-defense-contractor-pentagon.html [dostęp: 10 V 2022].

82 *New York Times 'hit by hackers from China'*, BBC News, 31 I 2013 r., https://www.bbc.com/news/world-asia-china-21271849 [dostęp: 10 V 2022].

83 M. Clayton, *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*, The Christian Science Monitor, 27 II 2013 r., https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage [dostęp: 10 V 2022].

rzeczywiście jest komponentem Biura II w Departamencie III Sztabu Generalnego Chińskiej Armii Ludowo-Wyzwoleńczej, która to jednostka zajmuje się prowadzeniem działań w cyberprzestrzeni[84].

Stany Zjednoczone nie tylko są ofiarą chińskich ataków. Według danych ujawnionych przez amerykańską Agencję Bezpieczeństwa Narodowego (National Security Agency) w 2011 r. USA przeprowadziły w odwecie 231 cyberataków na systemy Chin, Rosji, Iranu i Korei Północnej[85].

## Podsumowanie

Wzrost popularności technologii teleinformatycznych, wynikający z kilku czynników (głównie z dostępności, niskich kosztów pozyskania, utrzymania oraz naprawy narzędzi teleinformatycznych w przypadku awarii lub ataku oraz ich stosunkowo prostej obsługi), sprawił, że cyberprzestrzeń stała się również elementem życia codziennego. Dzięki niej można komunikować się w czasie rzeczywistym z odbiorcą, który znajduje się w odległym miejscu, przy niewielkim nakładzie finansowym. Internet (jeden z głównych elementów, na które składa się cyberprzestrzeń) jest również ogromną bazą danych.

Zwiększający się wpływ cyberprzestrzeni na życie jednostek i państw był widoczny także w czasie pandemii COVID-19. Przestrzeń teleinformatyczna umożliwiła podtrzymanie ciągłości pracy niektórych elementów państwa, takich jak oświata czy służba zdrowia. Wraz ze wzrostem powszechności dostępu do tej przestrzeni powstają także różnego typu zagrożenia. Największe z nich to działalność cyberprzestępców. Dysponując wieloma narzędziami, najczęściej dążą oni do kradzieży środków finansowych z kont bankowych oraz tożsamości. Z tego rodzaju zagrożeniami muszą się mierzyć również instytucje państwowe. Źródłem niebezpieczeństwa jest także aktywność w cyberprzestrzeni grup i organizacji terrorystycznych. Świat rzeczywistości wirtualnej stał się wręcz idealnym miejscem do szerzenia ekstremizmu religijnego i islamistycznej propagandy.

Przedstawione w artykule przypadki stanowią dowód na to, że cyberprzestrzeń może się stać niebezpiecznym teatrem działań. Jeśli podmiot podejmujący wrogą aktywność dysponuje umiejętnościami oraz odpowiednimi narzędziami, jest w stanie sparaliżować państwo bez użycia siły militarnej. Działania w sieci nie przypominają konwencjonalnych operacji wojennych. Szkody wywołane udanym,

[84] *APT1: Exposing One of China's Cyber Espionage Units*, https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf [dostęp: 10 V 2022].

[85] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 325.

zwłaszcza masowym atakiem mogą być jednak większe niż te będące skutkiem walki zbrojnej pomiędzy dwoma lub więcej podmiotami stosunków międzynarodowych. Zakłada się, że ataki hakerskie nie przyniosą raczej bezpośrednich ofiar w ludziach. Nie można jednak wykluczyć celowego uderzenia w większe skupiska ludzkie, np. w przypadku ataku na elektrownię jądrową, zakłady chemiczne czy sieci transportowe.

Ataki na infrastrukturę krytyczną polegające na włamaniu się do jej systemów zazwyczaj wiążą się z zakłóceniem jej pracy, a w niektórych przypadkach również z jej zniszczeniem. Tak się stało w wyniku zainfekowania przez izraelskich hakerów irańskich ośrodków wzbogacających uran. Ponadto na skutek tej operacji Stuxnet uderzył w systemy informatyczne wielu innych państw, co wskazuje na to, że tego rodzaju oprogramowanie może się stać bronią obosieczną.

Cyberataki mogą służyć również jako wsparcie podczas konwencjonalnych działań militarnych. Przykładem takiego wykorzystania przestrzeni teleinformatycznej jest operacja „Orchard". W pierwszej fazie polegała ona na wprowadzeniu w błąd systemów informatycznych sterujących siecią radarową sił zbrojnych Syrii. W kolejnej fazie izraelskie lotnictwo wykonało skuteczne uderzenie na ośrodek prowadzący badania nad bronią jądrową. Cyberprzestrzeń jest wykorzystywana także przez podmioty stosunków międzynarodowych do pozyskiwania nowoczesnych technologii oraz systemów uzbrojenia. Szczególnie aktywne działania tego typu prowadzi ChRL. Dokonując włamań do systemów teleinformatycznych innych państw, pozyskuje dane, które służą jej do rozwijania swojej gospodarki, sił zbrojnych czy też do prowadzenia polityki.

Przestrzeń wirtualna jest też obszarem oddziaływania na opinię społeczną w szerszym, globalnym ujęciu. Dzięki swobodnej wymianie informacji zarówno pojedynczy hakerzy, jak i instytucje państwowe mogą w dowolny sposób kreować zachowania jednostek i zbiorowości ludzkich, skłaniając je do określonych działań lub zaniechania aktywności. Ten stan rzeczy budzi uzasadnione zaniepokojenie, zwłaszcza w instytucjach odpowiedzialnych za bezpieczeństwo państwa. Aby skutecznie przeciwdziałać zagrożeniom występującym w przestrzeni wirtualnej i reagować na nie, należy budować i rozwijać własne systemy obronne i ofensywne.

Wzrost zainteresowania przeniesieniem działalności do przestrzeni wirtualnej ze strony różnych graczy, a przede wszystkim aktorów państwowych, spowodował powstanie zjawiska cyberwojny, której pierwszą ofiarą była Estonia w 2007 r. W przyszłości cyberwojownicy, zorganizowani w ramach określonych grup czy jednostek wojskowych danego kraju, będą prawdopodobnie prowadzić cyberoperacje przeciwko zasobom strategicznym oraz infrastrukturze krytycznej kraju obranego za cel. Działania te mają lub będą miały na celu sparaliżowanie funkcjonowania państwa, a więc nie tylko infrastruktury rządowej, lecz także całego systemu

infrastruktury krytycznej, od której działania w szerokim zakresie jest uzależnione bezpieczeństwo społeczne.

Rozwój przestrzeni wirtualnej sprawia, że zjawisko cyberwojny może odgrywać coraz większą rolę. Przykład operacji „Orchard" pokazuje, jak istotnymi narzędziami prowadzenia działań wojennych są technologie teleinformatyczne. Izraelskie służby włamały się na syryjskie systemy komputerowe i „oślepiły" radary. Tym samym nadały operacjom w rzeczywistości wirtualnej nowy wymiar. Najprawdopodobniej kolejny konflikt na poziomie globalnym rozpocznie się w cyberprzestrzeni i tam też może się zakończyć.

## Bibliografia

Ajili H., Rezaee N., *Iranian Military Capabilities and Possibility of Blocking Hormuz Strait by Iran*, „Cywilizacja i Polityka" 2020, nr 18, s. 59–80. https://doi.org/10.15804/cip202005.

Andress J., Winterfeld S., *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham 2011.

Bencsáth B. i in., *The Cousins of Stuxnet: Duqu, Flame and Gauss,* „Future Internet" 2012, nr 4, s. 971–1003. https://doi.org/10.3390/fi4040971.

Bieniek O., *Cyberprzestrzeń w rosyjskiej przestrzeni informacyjnej*, „Wiedza Obronna" 2017, nr 3–4, s. 35–48.

Bryczek-Wróbel P., *Sytuacja geopolityczna Estonii w polityce zagranicznej Federacji Rosyjskiej*, „Polityka i Społeczeństwo" 2021, t. 19, nr 3, s. 23–35. https://doi.org/10.15584/polispol.2021.3.2.

Bryjka F., *Wykrywanie i zwalczanie dezinformacji – zarys skryptu. Materiał pomocniczy do sylabusa zajęć akademickich*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 113–136.

Carr J., *Inside Cyber Warfare: Mapping the Cyber Underworld*, Beijing-Cambridge-Farnham-Köln-Sewastopol-Taipei-Tokyo 2010.

Chłoń T., Kozłowski K., *Wybrane studia przypadku systemowych działań dezinformacyjnych: Rosja i Chiny*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 33–60.

Dobbins J. i in., *Coping with a Nuclearizing Iran*, Santa Monica 2011.

Dygnatowski S., Dygnatowski P., Domżał-Drzewicki Ł., *Analiza wykorzystania rozwiązań strukturalnych w obszarze cyberbezpieczeństwa na przykładzie operacji Orchard*, „Journal of KONBiN" 2019, t. 49, nr 1, s. 290–298. http://dx.doi.org/10.2478/jok-2019-0014.

Farwell J.P., Rohozinski R., *Stuxnet and the Future of Cyber War*, „Survival. Global Politics and Strategy" 2011, t. 53, nr 1, s. 23–40. https://doi.org/10.1080/00396338.2011.555586.

Farwell J.P., Rohozinski R., *The New Reality of Cyber War*, „Survival. Global Politics and Strategy" 2012, t. 54, nr 4, s. 107–120. https://doi.org/10.1080/00396338.2012.709391.

Gerlach J., *Wpływ prasy, radia, telewizji i Internetu na współczesne zachowania nabywcze*, „Współczesne Problemy Ekonomiczne" 2018, nr 2, s. 5–12. https://doi.org/10.18276/wpe.2018.18-01.

Grycuk A., *Fake news, trolle, boty i cyborgi w mediach społecznościowych,* „Analizy BAS", 2021, nr 1, s. 1–12.

Herzog S., *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,* „Journal of Strategic Security" 2011, t. 4, nr 2, s. 49–60. http://dx.doi.org/10.5038/1944-0472.4.2.3.

Jachyra D., *Trollowanie – antyspołeczne zachowania w Internecie, sposoby wykrywania i obrony*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2011, nr 28, s. 253–261.

Kacała T., *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2, s. 49–65. https://doi.org/10.15804/ppk.2015.02.03.

Kaniewska M., *Między kijem a marchewką – Organizacja Narodów Zjednoczonych wobec programu nuklearnego Iranu*, w: *Stabilizacja czy destabilizacja? Społeczność międzynarodowa wobec programu nuklearnego Iranu*, A. Malantowicz, Ł. Smalec (red.), Warszawa 2014, s. 55–66.

Kowalczewska K., *Wpływ nowoczesnych technologii na współczesne konflikty zbrojne*, Warszawa 2022.

Kukułka J., *Historia współczesna stosunków międzynarodowych 1945–2000*, Warszawa 2007.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku,* „Bezpieczeństwo Narodowe" 2011, nr 17, s. 15–28.

Małecka A., *Nation-State Cyber Operations Legal Considerations: An Estonian Case Study*, „Safety & Defense" 2021, t. 7, s. 99–108. https://doi.org/10.37105/sd.139.

Marszałek-Kawa J., *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, T. Łoś-Nowak (red.), Warszawa 2011, s. 104–127.

Mazurek S., *Rewolucja islamska w Iranie – przyczyny, przebieg, konsekwencje*, „Nurt SVD" 2017, nr 1, s. 38–55.

Mulvenon C.J., *Chinese Cyber Espionage. Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law*, Washington 2013.

Schmidt A., *The Estonian Cyberattacks*, w: *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, J. Healey (red.), Vienna 2013.

Szymczyk K., *Irański program nuklearny jako czynnik warunkujący stosunki międzynarodowe w obszarze i poza obszarem MENA*, w: *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, R. Bania, K. Zdulski (red. nauk.), Łódź 2012, s. 145–155.

*Vademecum bezpieczeństwa informacyjnego*, t. 2, O. Wasiuta, R. Klepka (red.), Kraków 2019.

Volkoff V., *Dezinformacja – oręż wojny*, Warszawa 1991.

Wierzbicki S., *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, t. 2, nr 1, s. 134–148.

Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017.

Wydra R., *Relacje Chin i Stanów Zjednoczonych w cyberprzestrzeni*, „Security, Economy & Law" 2017, nr 3, s. 100–108. https://doi.org/10.24356/SEL/16/6.

Zając J., *Polityka zagraniczna USA*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, T. Łoś-Nowak (red.), Warszawa 2011, s. 61–80.

Zakrzewski A., *Jak to jest z tym Stuxnetem, Flamem, Duqu?*, „DLP Expert" 2013, nr 1.

Zetter K., *Odliczając do dnia zero. Stuxnet czyli prawdziwa historia cyfrowej broni*, Gliwice 2014.

### Źródła internetowe

*1949–2023 U.S.-China Relations*, Council on Foreign Relations, https://www.cfr.org/timeline/us-relations-china [dostęp: 10 V 2022].

*About Company,* http://anti-virus.by/en/index.shtml.

*APT1: Exposing One of China's Cyber Espionage Units,* https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf [dostęp: 8 IV 2024].

Bencsáth B. i in., *Duqu: A Stuxnet-like malware found in the wild. Technical Report by Laboratory of Cryptography and System Security (CrySys)*, 14 X 2011 r., https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf [dostęp: 8 IV 2024].

Bochyńska N., *Art. 5 Traktatu NATO a działania w cyberprzestrzeni. Czy istnieją „granice" dla cyberwojny?*, CyberDefence24, 17 III 2022 r., https://cyberdefence24.pl/cyberbezpieczenstwo/art-5-traktatu-o-nato-a-dzialania-w-cyberprzestrzeni-czy-istnieja-granice-dla-cyberwojny [dostęp: 7 V 2022].

Chein E., OMurchu L., Falliere N., *W32.Duqu. The precursor to the next Stuxnet*, https://www. usenix.org/system/files/conference/leet12/leet12-final11.pdf [dostęp: 7 V 2022].

Clayton M., *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*, The Christian Science Monitor, 27 II 2013 r., https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage [dostęp: 10 V 2022].

*First Stuxnet – Now the Flame Virus*, The Availability Digest, czerwiec 2012 r., www.availabilitydigest.com/public_articles/0706/flame_virus.pdf [dostęp: 10 V 2022].

Glendinning L., *Obama, McCain computer 'hacked' during election campaign*, The Guardian, 7 XI 2008 r., https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa [dostęp: 10 V 2022].

Johnson B., *US asks China to explain Google hacking claims*, The Guardian, 13 I 2010 r., https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us [dostęp: 10 V 2022].

Jones S., *The Islamic Republic of Iran: An introduction*, House of Commons Library, 11 XII 2009 r., https://researchbriefings.files.parliament.uk/documents/RP09-92/RP09-92.pdf [dostęp: 8 IV 2024].

Juurvee I., Mattiisen M., *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*, International Centre for Defence and Security, sierpień 2020 r., https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf [dostęp: 8 IV 2024].

Kaska K., Osula A.M., Stinissen J., *The Cyber Defence Unit of the Estonian Defence League. Legal, Policy and Organisational Analysis*, Tallinn 2013, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf [dostęp: 8 IV 2024].

Krekel B., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* The US-China Economic and Security Review Commission, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf [dostęp: 8 IV 2024].

Kumar S., *Asymmetric Capabilities of China's Military*, Institute of Peace and Conflict Studies, 19 XI 2008 r., https://www.ipcs.org/comm_select.php?articleNo=2735 [dostęp: 10 V 2022].

Lefkow C., *24,000 files stolen from defense contractor: Pentagon*, phys.org, 15 VII 2011 r., https://phys.org/news/2011-07-stolen-defense-contractor-pentagon.html [dostęp: 10 V 2022].

Majdan K., *Wykryto nowe „cyberzagrożenie". „Z czymś takim jeszcze się nie spotkaliśmy"*, na Temat, 29 V 2012 r., https://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czym-s-takim-jeszcze-sie-nie-spotkalismy [dostęp: 7 V 2022].

*New York Times 'hit by hackers from China'*, BBC News, 31 I 2013 r., https://www.bbc.com/news/world-asia-china-21271849 [dostęp: 10 V 2022].

Park J.K., *A Report of the CSIS Korea Chair. China – U.S. Relations in East Asia. Strategic Rivalry and Korea's Choice*, Center for Strategic and International Studies, kwiecień 2013 r., https://ciaotest.cc.columbia.edu/wps/csis/0028481/f_0028481_23160.pdf [dostęp: 8 IV 2024].

Reeder F.S. i in., *Updating U.S. Federal Cybersecurity Policy and Guidance. Spending scarce taxpayer dollars on security programs that work*, Center for Strategic and International Studies, październik 2012 r., https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121019_Reeder_A130_Web.pdf [dostęp: 8 IV 2024].

Sahimi M., *Iran's Nuclear Program. Part I: Its History*, 10 II 2003 r., https://www.iranwatch.org/library/sahimi-irans-nuclear-program-part-i-its-history-10-2-03 [dostęp: 8 IV 2024].

Zanotti J. i in., *Israel: Possible Military Strike Against Iran's Nuclear Facilities*, Congressional Research Service, 28 IX 2012 r., https://sgp.fas.org/crs/mideast/R42443.pdf [dostęp: 7 V 2022].

Maciej Heromiński

Absolwent Wydziału Nauk Społecznych Uniwersytetu Jana Długosza w Częstochowie na kierunku bezpieczeństwo narodowe, ze specjalizacją bezpieczeństwo państwa. Interesuje się zagadnieniami związanymi z cyberprzestrzenią oraz polemologią.

**Kontakt:** m.herominski21@gmail.com