**JAKUB SABAŁA***

# CYBERPRZESTRZEŃ JAKO TEATR DZIAŁAŃ WYWIADU

**Abstrakt**

Cyberprzestrzeń stanowi już nieodłączną część współczesnego życia. Przetwarzanie oraz przechowywanie informacji w sieciach teleinformatycznych stało się już standardem, ponieważ wiele systemów opiera swoje działanie na technologiach informacyjnych. Niezliczone ilości tych informacji są cennym źródłem dla służb wywiadowczych, dlatego wywiad w cyberprzestrzeni stanowi współcześnie nowe, sukcesywnie rozwijane pole aktywności służb. Artykuł ma za zadanie przybliżyć znaczenie tego sektora wywiadu, jakie niesie za sobą szanse i możliwości oraz postawić hipotezy, które mogą być elementem dyskursu akademickiego w tym temacie.

**Słowa kluczowe:** Cyberprzestrzeń, Internet, wywiad, cyberszpiegostwo, CYBINT.

## Wstęp

Internet oraz szerzej – cyberprzestrzeń to już immanentna część współczesnego życia. Osoby prywatne, jak i instytucje, przedsiębiorstwa coraz częściej korzystają z technologii informacyjnych, zarówno w zakresie marketingu, jaki i komunikacji. To sprawia, iż coraz więcej aktywności społeczeństwa, a co za tym idzie informacji zostaje umieszczanych w cyberprzestrzeni. Historia świata dowiodła, że służby wywiadowcze podążają za potężnymi informacji.

Problematyka wywiadu w cyberprzestrzeni jest bardzo szeroka i jest sukcesywnie rozwijana na gruncie akademickiego dyskursu. Celem artykułu jest ukazanie podstawowych zagadnień związanych z podejmowanym tematem oraz uwypuklenie krytycznych jego elementów, co powinno być preludium do dalszych rozważań na gruncie nauki i sektora bezpieczeństwa. Ponadto autor pragnie w niniejszym artykule ukazać wywiad w cyber-

* Jakub Sabała – absolwent studiów licencjackich i magisterskich na kierunku bezpieczeństwo wewnętrzne w Instytucie Nauk Politycznych UW. Doktorant Nauk o Bezpieczeństwie na Wydziale Nauk Politycznych i Studiów Międzynarodowych UW. Zawodowo związany z pozyskiwaniem informacji w sektorze finansowym.

przestrzeni nie jako zagrożenie, lecz jako możliwość i szansę na lepsze zapewnianie bezpieczeństwa.

Pragnąc zrealizować cel należy postawić kilka pytań badawczych, na które autor postara się odpowiedzieć w niniejszym artykule. Jakie znaczenie ma współcześnie cyberszpiegostwo i jakie znaczenie będzie miało w przyszłości?; Jakie są zalety i wady zastosowania wywiadu w cyberprzestrzeni we współczesnym świecie?; Co wpływa na sukcesy i porażki cyberszpiegów?; Jakie są perspektywy rozwoju wywiadu w cyberprzestrzeni?

Wywiad w cyberprzestrzeni, cyberszpiegostwo stanowić będą coraz szersze pole działania dla agencji wywiadowczych na całym świecie i wraz z rozwojem technologii informacyjnych zaangażowanie w tej dyscyplinie pozyskiwania informacji będzie rosło. Teza ta nie może dziwić, gdyż każdego roku zastosowania informatyki w różnych sektorach polityki, gospodarki, czy życia codziennego rośnie. Wraz z tym wzrostem ilość danych dostępnych w cyberprzestrzeni zwiększa się, przez co stanowić będzie proporcjonalnie istotniejsze źródło informacji dla wywiadu. Cyberszpiegostwo niesie za sobą wiele możliwości i szans, których nie niosła za sobą żadna inna dyscyplina wywiadowcza.

Celem uporządkowania rozważań należy wyjaśnić termin cyberprzestrzeni. Pojęcie cyberprzestrzeni użył po raz pierwszy w 1982 roku William Gibson na kartach swojej powieści „Burning Chrome”[1]. Na gruncie rozwoju cyberprzestrzeni powstało kilka definicji. Jedną z nich, która jest wystarczająco kompleksowa dla tematyki, jest definicja zawarta w raporcie „Zagraniczni szpiedzy wykradają gospodarcze tajemnice USA w cyberprzestrzeni” Biura Dyrektora Krajowego Kontrwywiadu USA, która określa cyberprzestrzeń jako powiązaną ze sobą sieć infrastrukturalną technologii informatycznych, obejmujące Internet, sieci telekomunikacyjne, systemy komputerowe oraz systemy kierujące procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego[2].

Z początkiem lat 90. XX wieku pojęcie cyberprzestrzeni weszło do powszechnego użytku. Technologie informacyjne w tamtym okresie były już na takim poziomie rozwoju, że Nicholas Negroponte stwierdził, iż atom przestał być podstawowym składnikiem elementarnym, a zastąpiła go cyfra binarna[3]. Świadczyć o tym może fakt, że obecnie poziom prowadzenia działań wojennych – szczególnie z zakresie wojny informacyjnej – nie jest już domeną lądu, morza czy powietrza, lecz również świata cyfrowego w sieciach teleinformatycznych. Różnicami jakie wiążą się z tym środowiskiem działań jest to, iż środowisko to zostało w sposób całkowity stworzone przez człowieka, a efektem walk prowadzonych w nim może być całkowita zmiana specyfiki, cech i topografii terenu działań[4]. Ponadto, sama geografia, geopolityka czy geolokalizacja traci na znaczeniu. Wojna informacyjna

---

1 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego”, 9/13, 2013, s. 226.

2 *Foreign Spies Stealing US Economic Secrets in Cyberspace*, [w:] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf [dostęp: 2.12.2017].

3 S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki, organizacji, państwa*, Warszawa 2016, s. 212.

4 Wpływ aktorów na środowisko walki w cyberprzestrzeni jest tak silny, iż eksperci porównując to z walką lądową w sposób konwencjonalny wskazują za przykład pojawiającą się lub znikającą górę. Zastosowanie najpotężniejszej współcześnie broni tj. bomby atomowej wg ekspertów nie niesie za sobą takich zmian w środowisku, jakie mogą nieść wpływy oponentów w środowisku cyfrowym.

w cyberprzestrzeni nie posiada jasno wytyczonych granic państwowych oraz sama odległość między państwami traci na znaczeniu. RAND Corporation w 1995 r. zbadała, na zlecenie Departamentu Obrony Stanów Zjednoczonych, możliwości jakie będzie niosła za sobą wojna informacyjna w cyberprzestrzeni. W raporcie końcowym stwierdzono, iż technologia informacyjna pozwoli zatrzeć odległości, które miały znaczenie w walce konwencjonalnej, a tym samym cele ataku w Stanach Zjednoczonych staną się tak samo narażone na ingerencję, jak cele lokalne[5].

## Znaczenie wywiadu w cyberprzestrzeni

Od samego początku istnienia cyberprzestrzeni i kolejne lata jej rozwoju zastanawiano się nad istotą tego zjawiska. Oczywiście, w zależności od sektora, w jakim ta cyberprzestrzeń jest wykorzystywana, może przynosić różne profity i ułatwienia. Dla wywiadu i cyberszpiegostwa można wytypować kilka podstawowych korzyści. Po pierwsze, sprawcy szpiegostwa cyfrowego są znacznie trudniej wykrywalni niż ci konwencjonalni. Szpiedzy mogą wykradać informacje na odległość przy jednoczesnym ukrywaniu swojej tożsamości, lokalizacji. Po drugie, sprawcami kradzieży informacji w cyberprzestrzeni mogą być zarówno pojedyncze osoby, korporacje, państwa o znacznie mniejszym potencjale ekonomicznym i technologicznym niż światowe mocarstwa. Po trzecie, cyberprzestrzeń powoduje, że trudniej jest ustalić motywy działania sprawców kradzieży informacji. W konwencjonalnej działalności wywiadowczej pozyskanie jakiegoś dokumentu czy informacji wiązało się z ujawnieniem obszaru zainteresowania służby wywiadowczej, natomiast w cyberszpiegostwie możliwe jest pobieranie ogromnych ilości informacji, które mogą być ze sobą niepowiązane, dlatego łatwiej jest ukryć prawdziwy cel kradzieży. Po czwarte, wywiad w cyberprzestrzeni redukuje zagrożenie dla sprawców i agentów wewnątrz organizacji, poprzez brak fizycznego spotkania agenta z funkcjonariuszem prowadzącym, co stanowczo zmniejsza ryzyko wykrycia. Po piąte, cyberszpiegostwo jest działalnością szybszą i tańszą w stosunku do podstawowych dyscyplin pozyskiwania informacji. Cyberprzestrzeń oferuje możliwość natychmiastowego transferu ogromnych ilości informacji[6].

Znaczenie pozyskiwania informacji w cyberprzestrzeni zauważył amerykański teoretyk badacz wywiadu Robert M. Clark, który w swoim opracowaniu *Intelligence Collection* wyróżnił pośród głównych dyscyplin wywiadowczych[7] subdyscyplinę CYBINT – Cyber Intelligence.

Wywiad w cyberprzestrzeni czy też cyberszpiegostwo są działaniami wymierzonymi w pozyskiwanie informacji, które są przetwarzane w systemach teleinformatycznych,

---

5 S. Wojciechowska-Filipek, Z. Ciekanowski, dz. cyt., s. 212–213.

6 M. Ciecierski, R. Nogacki, *Bezpieczeństwo współczesnej firmy. Wywiad, szpiegostwo, ochrona tajemnic*, Warszawa 2016, s. 204.

7 Pięć głównych dyscyplin wywiadowczych funkcjonujących w teorii wywiadu i kontrwywiadu to HUMINT (wywiad osobowy); OSINT (wywiad jawnoźródłowy); IMINT (wywiad obrazowy); SIGINT (wywiad ze źródeł elektromagnetycznych) oraz MASINT (wywiad pomiarowo-badawczy).

i nie zawsze można je kategoryzować w ramach klasycznych dyscyplin wywiadowczych. CYBINT jest subdyscypliną, w której możemy odnaleźć elementy takich dyscyplin jak OSINT, HUMINT, SIGINT[8], które to elementy odpowiadają pozyskiwaniu informacji z cyberprzestrzeni.

Wywiad w cyberprzestrzeni bez wątpienia ma zastosowanie, kiedy mówimy o wywiadzie jawnoźródłowym – OSINT. Internet jest obecnie najpowszechniejszym źródłem informacji jawnych, a przy tym łatwo dostępnym szczególnie w świecie zachodnim. Wielu ludzi współcześnie pozyskuje informacje z Internetu, już nie tylko za pomocą komputera, lecz również innych urządzeń mobilnych tj. tablet czy smartphone, który znajduje się już niemalże w każdej kieszeni. Powszechność dostępu do Internetu sprawia, że poza tym, iż chętnie pozyskiwane są informacje z tego źródła, to również społeczeństwo pozostawia o sobie informacje w np. mediach społecznościowych. Same informacje pozostawione przez nas to nie jedyne źródło informacji, gdyż współcześnie w ramach wywiadu jawnoźródłowego w cyberprzestrzeni znaczenie mają metadane, czyli np. gdzie publikujemy informację, na jakim urządzeniu, co znajduje się w naszej historii wyszukiwania etc. To pozwala korporacjom takim jak np. Google do profilowania naszej osoby na potrzeby reklam, ale jest również znaczącym źródłem informacji dla wywiadu, szczególnie kiedy jesteśmy osobami publicznymi.

Na przestrzeni lat wystąpiło kilka przykładów upublicznienia informacji w Internecie, które miały znaczenie dla systemu bezpieczeństwa. Po pierwsze, publikowanie w sieci zdjęć żołnierzy w bazach wojskowych, dzięki czemu możliwe jest oglądanie wyposażenia, usytuowanie obiektów chronionych. Ten typ działania umożliwił atak na bazę Polskiego Kontyngentu Wojskowego w Afganistanie lub w 2007 roku w Republice Iraku atak moździerzowy, czego skutkiem były straty w sprzęcie. Po drugie, ujawnienie wizerunków osób pracujących w instytucjach bezpieczeństwa, posiadających niejednokrotnie ogromną władzę i dostęp do ściśle tajnych informacji i będących podatnymi na werbunek zagranicznego wywiadu. Po trzecie, dziennikarskie doniesienia o podróżach, miejscu pobytu lub zamieszkania najważniejszych osób w państwie, mogące narażać je na różne ataki. Po czwarte, konta w portalach społecznościowych funkcjonariuszy służb i żołnierzy, które regularnie monitorowane przez zagraniczny wywiad mogą dostarczać informacji potrzebnych do profilowania kandydata do werbunku. Po piąte, serwisy gromadzące przyjaciół ze szkół, w tym także o profilach wojskowo-policyjnych i publikowane wspólne zdjęcia wraz z informacjami szczegółowymi mogą narażać funkcjonariuszy pracujących pod przykryciem na dekonspirację[9].

Ilość informacji produkowanych w Internecie znacznie przekracza możliwości ich dokładnej penetracji. Do tego celu wykorzystywane są specjalistyczne wyszukiwarki

[8] R.M. Clark, *Intelligence collection*, Washington 2014, s. 121.

[9] M. Frączek, *Wybrane problemy zastosowania nowoczesnych technologii do gromadzenia danych w zakresie bezpieczeństwa*, [w:] *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa. Historia i współczesność*, M. Górka (red.), Toruń 2016, s. 61–62.

horyzontalne i wertykalne[10] oraz programy automatyzujące wyszukiwanie w jawnych źródłach[11].

OSINT to przede wszystkim informacje publicznie dostępne, ale też te, które nie są w żaden sposób chronione. OSINT to jedynie część informacji, które znajdują się w świecie cyfrowym, a są w kręgu zainteresowania wywiadu.

Tak jak już było wspomniane wcześniej, cyberprzestrzeń to coś więcej niż tylko Internet. To również sieci lokalne, intranety, systemy teleinformatyczne instytucji, systemy obsługujące infrastrukturę, w tym infrastrukturę krytyczną, etc. Te systemy w odróżnieniu do informacji jawnoźródłowych są chronione w mniejszy lub większy sposób. Systemy bezpieczeństwa IT muszą odpierać każdy rodzaj ataku na jakie będą narażone, natomiast atakujący haker musi odnaleźć jeden słaby punkt, który pomoże mu dostać się do systemu. Jak stwierdził były haker Dustin Dykes „System bezpieczeństwa musi wygrywać cały czas. Haker musi wygrać tylko raz”[12].

Na sukces hakerów i cyberszpiegów wpływa wiele czynników. Są to przede wszystkim trzy, które mają największe znaczenie w walce w cyberprzestrzeni. Po pierwsze, sposób myślenia specjalistów bezpieczeństwa IT, po drugie, złożoność systemów bezpieczeństwa lub systemów informatycznych sensu largo oraz po trzecie, najsłabsze ogniwo każdego systemu bezpieczeństwa, czyli ludzki błąd[13].

Sposób myślenia specjalistów bezpieczeństwa IT, administratorów systemów i sieci powoduje, że nie są w stanie postawić się w roli hakera, osoby atakującej system. Specjaliści bezpieczeństwa IT chcą wierzyć, że ich system jest najbezpieczniejszy i nie posiada żadnych wad ani słabości. Programy bezpieczeństwa systemów i sami operatorzy skupiają się przede wszystkim na słabościach całego systemu, a nie zagrożeniach płynących z zewnątrz. Słabości systemu są w znacznej mierze dużo łatwiejsze w ocenie niż potencjalne zagrożenie zewnętrzne. Myślenie wewnętrzne zamiast wyjść poza granice systemu powoduje, że skupiają się nie na tym, co haker lub osoba atakująca próbuje osiągnąć. Osoby odpowiedzialne za bezpieczeństwo systemu nie wykonują oceny zagrożenia prawidłowo z punktu widzenia atakującego i nie poświęcają dostatecznie dużo sił i środków pozostawiając system podatnym na ingerencję zewnętrzną.

Złożoność systemów również ma wpływ na jego słabość w zabezpieczeniach. Duże i skomplikowane sieci komputerowe, oprogramowanie posiadają znacznie więcej niedociągnięć, a co za tym idzie słabości, które są chętnie wykorzystywane przez atakujących hakerów. Co więcej, rozwój technologii i możliwości obu stron konfliktu, każdego dnia wyłania kolejne słabości w częściach systemu, które do tej pory były uważane za bezpieczne. Ciągłe zmiany w sprzęcie informatycznym, aktualizacje oprogramowania, sieci i połączenia bezprzewodowe wystawiają każdego dnia system na nowe zagrożenia. Każda

---

10 Wyszukiwarki horyzontalne tj. Google, Bing, DuckDuckGo wyszukują w powierzchownym Internecie wszystkich stron powiązanych z wyszukiwaną frazą; Wyszukiwarki wertykalne są ograniczone do konkretnej dziedziny tj. medycyna, prawo, inżynieria i wyszukują powiązań z frazą w ramach swojej dziedziny zarówno w Internecie powierzchownym jak i deepweb.

11 Przykładami tego typu programów mogą być np. Lockheed Martin Wisdom lub Maltego.

12 R.M. Clark, dz. cyt., s. 121.

13 Tamże, s. 122.

modyfikacja w systemie tworzy pole do potencjalnej słabości, która może zostać wykorzystana przez hakerów[14].

Błąd ludzki pozostaje nadal domeną wielu zagrożeń, na które narażony jest system bezpieczeństwa czy to konwencjonalny czy cyfrowy, a samo pozyskiwanie informacji w swojej naturze często z niego korzysta. W przypadku cyberprzestrzeni błędy popełniają przede wszystkim operatorzy i osoby odpowiedzialne za bezpieczeństwo systemu. W tych granicach najczęstszymi błędami napotykanymi przez hakerów są złe konfiguracje systemu, połączenia urządzeń z siecią lub niefrasobliwość przy korzystaniu z systemu.

W ramach pozyskiwania informacji z cyberprzestrzeni możemy rozgraniczyć dwa zasadnicze typy: pozyskiwanie informacji z sieci teleinformatycznych lub pośrednie i bezpośrednie wykorzystanie pojedynczych komputerów czy intranetów[15].

Ingerencja w sieci komputerowe i systemy teleinformatyczne opiera się na wielowarstwowych i zróżnicowanych metodach działania. Współczesny rozwój możliwości technologicznych spowodował również rozrost możliwości hakerskich, który z pewnością znajduje zastosowanie w działaniach wywiadu w cyberprzestrzeni. E. Lichocki wyróżnił takie metody ingerencji jak:

- malware, czyli oprogramowanie złośliwe – wirusy, robaki – programy rozprzestrzeniające się w zainfekowanym systemie informatycznym, zmieniając sposób jego funkcjonowania, naruszając możliwości procesora i dysku twardego, uniemożliwiając korzystanie z danych;
- bomby logiczne – programy aktywujące nowe funkcje elementów logicznych komputera, które w efekcie końcowym prowadzą do zniszczenia systemu i oprogramowania;
- konie trojańskie – oprogramowanie, które podłączone do innego programy dostając się do systemu komputerowego umożliwia podejmowanie działań bez wiedzy użytkownika zainfekowanego komputera;
- próbkowanie – uzyskiwanie dostępu do komputera poprzez analizę jego charakterystyki;
- uwierzytelnianie – podszywanie się pod osobę uprawnioną do dostępu;
- ominięcie – omijanie zabezpieczeń systemu;
- czytanie – nieuprawniony dostęp do informacji w systemie;
- kopiowanie – nieuprawnione kopiowanie informacji z systemu;
- kradzież – przejęcie informacji i plików z systemu bez pozostawienia kopii;
- modyfikacja – zmiana zawartości lub charakterystyki informacji i danych zawartych w systemie;
- usunięcie – zniszczenie informacji zawartych w systemie lub całego systemu informatycznego;
- złośliwe podzespoły – umieszczanie w komputerach części, które umożliwiają nieuprawniony dostęp do systemu lub wadliwa konstrukcja systemu;
- tylne drzwi (backdoor) – tworzenie przez twórców oprogramowania wejścia do systemu poza wiedzą użytkownika;
- maskarada – podszywanie się pod użytkownika przez jednego za atakujących system;

[14] Tamże.

[15] Tamże, s. 123.

- przechwycenie transmisji – uzyskanie dostępu do treści przesyłanych pomiędzy komputerami;
- podsłuchiwanie – śledzenie ruchu sieciowego;
- receptory van Ecka – podglądanie przez atakującego replik obrazów przesyłanych z monitora użytkownika;
- DDoS (distributed denial of service, rozproszona odmowa usługi);
- e-mail bombing – przesyłanie do skrzynki ofiary ataku wielkiej ilości danych, co powoduje przepełnienie i nieprawidłowości w działaniu;
- promieniowanie elektromagnetyczne, które swoim działaniem niszczy urządzenia elektroniczne oraz zawarte na nich dane[16];
- Keystroke loggers (Keyloggery) – oprogramowanie lub sprzęt przechwytujące frazy wpisywanie za pomocą klawiatury, dzięki czemu możliwe jest uzyskanie loginów i haseł dostępu do systemu.

Proces pozyskiwania informacji wywiadowczej z cyberprzestrzeni ma wiele zalet, ale jest nie mniej złożony od innych dyscyplin. Cały proces wymaga przede wszystkim personelu, osób obdarzonych wiedzą, umiejętnościami informatycznymi i talentem, które będą się chciały podjąć takich działań na rzecz wywiadu. Proces cyberwywiadu czy cyberszpiegostwa możemy podzielić na pięć zasadniczych etapów – selekcji celu, analizy celu, wykrywania słabości i wrażliwości systemu, eksploracji, czyli właściwego działania oraz wyczyszczenie śladów działalności i pozostawienie „furtki" do przyszłych działań[17].

Selekcja celu ataku jest pierwszą fazą przygotowywania cyberszpiegostwa. Informacje na temat potencjalnych celów są gromadzone z różnych źródeł, publicznych rekordów, społecznych i profesjonalnych sieci internetowych, konferencji branżowych, etc. Wszystkie informacje gromadzone mają na celu jak najlepsze profilowanie jednostki atakowanej, a przy tym mają za zadanie uwypuklenie pierwszych wrażliwych stron, dzięki czemu możliwy jest wybór celu najbardziej podatnego na ingerencję.

Analiza celu i jego mapowanie jest fazą rozpoznania wybranego już obiektu ataku, mającą na celu bezinwazyjne sondowanie go, potwierdzenie obecności urządzeń w systemie i mapowanie połączeń w tym systemie. Analiza ma na celu najlepsze zrozumienie systemu od najmniejszych fragmentów po system jako całość. W uproszczeniu faza ta ma za zadanie stworzenie szczegółowego modelu atakowanego obiektu, bez ryzyka bycia wykrytym przez specjalistów ds. cyberbezpieczeństwa.

Skanowanie obiektu pod kątem potencjalnych wrażliwych punktów to kolejna faza, która nawiązuje kontakt z systemem atakowanym i jego elementami składowymi. Skanowanie słabości może odbywać się zarówno za pomocą i bez Internetu, i wykorzystuje cały wachlarz narzędzi, które zostały wymienione wyżej w artykule. W tym etapie również możliwa jest ludzka ingerencja w system, który nie jest bezpośrednio dostępny z ogólnie dostępnej cyberprzestrzeni.

---

16 T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, za: E. Lichocki, Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego SZ RP, rozprawa doktorska, Wydział Bezpieczeństwa Narodowego Akademii Obrony Narodowej, Warszawa 2009, s. 62–63.

17 R.M. Clark, dz. cyt., s. 126.

Faza określana jako eksploracja systemu to już właściwy moment hackingu i uzyskiwania nieautoryzowanego dostępu do systemu teleinformatycznego. Atakujący uzyskuje dostęp, instaluje potrzebne oprogramowanie, pozyskuje potrzebne informacje i dane.

Ostatnim etapem w omawianym procesie jest zacieranie śladów ingerencji, aby osoby odpowiedzialne za zabezpieczenia nie zorientowały się, że doszło do infiltracji systemu oraz na potrzeby przyszłych eksploracji instalowane są backdoory, czyli „furtki" umożliwiające atakującemu łatwiejsze dostanie się do systemu, bez potrzeby ponownego łamania zabezpieczeń lub instalacja oprogramowania, które w sposób ciągły będzie przesyłało potrzebne informacje z systemu atakowanego do systemu atakującego.

## Cyberszpiegostwo na świecie

Cyberszpiegostwo i wywiad w cyberprzestrzeni to działania wywiadowcze, które są stosowane od niedawna, lecz mają za sobą już dość bogatą historię, biorąc pod uwagę doniesienia prasowe lub wycieki tajnych informacji np. przez Wikileaks.

Sprawą, która wywarła ogromne piętno w masowej świadomości społeczeństwa zachodniego, w kontekście funkcjonowaniu wywiadu w cyberprzestrzeni była sprawa programu PRISM wykorzystywanego przez Agencję Bezpieczeństwa Narodowego Stanów Zjednoczonych. Sprawę tę w 2010 roku ujawnił opinii publicznej Edward Snowden, który później został oskarżony o szpiegostwo i uciekł do Federacji Rosyjskiej. Ujawnione przez Snowdena informacje wskazywały, iż w ramach programu PRISM amerykanie podsłuchiwali i infiltrowali swoich sojuszników (m.in. Niemcy, Wielka Brytania, Japonia i Polska) oraz sieci komputerowe należące do organizacji międzynarodowych tj. ONZ, NATO oraz Unii Europejskiej.

Inwigilacja osób publicznych nie stanowi jednego celu dla służb wywiadowczych. Coraz częściej służby wykorzystują cyberprzestrzeń do gromadzenia informacji o obywatelach, tworząc ich profile. Przykładem są również Stany Zjednoczone, które wykorzystują narzędzie nazwane RIOT, którego zadaniem jest gromadzenie i katalogowanie profili użytkowników Internetu i informacji zamieszczanych przez nich np. w serwisach społecznościowych[18].

Cyberszpiegostwo w sieci jest działalnością częstokroć dobrze zorganizowaną i zaplanowaną, a odkrycie takiej działalności wymaga niewiele mniej czasu niż w przypadku konwencjonalnego szpiegostwa. Jednym z najgłośniejszych incydentów wykradania informacji z cyberprzestrzeni było działalnie chińskiej jednostki wywiadowczej odpowiedzialnej za ataki komputerowe, która ukierunkowana była na amerykańskie instytucje rządowe. Hakerzy zdobyli dostęp do amerykańskich sieci energetycznych oraz ważnych systemów uzbrojenia tj. myśliwce F/A-18 i F-35, śmigłowce Black Hawk, samolot V-22 Osprey, czy system Patriot PAC-3[19].

---

[18] D. Dziwisz, *Cyberbezpieczeństwo – nowy priorytet strategii obrony Stanów Zjednoczonych?*, „Sprawy Międzynarodowe" 2011, nr 3, s. 103–122.

[19] M. Grzelak, *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" 2013/2, s. 112.

Chińska Republika Ludowa zaczęła wyrabiać sobie nawet już markę pod kątem cyberszpiegostwa, szczególnie w zakresie nowoczesnych zaawansowanych technologii. Anegdotą już jest, iż w Chinach został wypuszczony na rynek podrobiony iPhone 7, zanim jeszcze firma Apple dokonała jego oficjalnej premiery i prezentacji. Chińskie służby wywiadowcze i korporacje często usiłują wykorzystać chińskich obywateli i osoby mające rodzinę poza granicami do pozyskiwania informacji. Specjaliści od cyberbezpieczeństwa częstokroć zgłaszają incydenty wymierzone w sieci komputerowe opatrzone adresami IP pochodzących właśnie z Chin. W 2011 roku Firma McAfee ustaliła, iż incydent nazwany Nocnym Smokiem nastąpił z chińskiego adresu IP, a pozyskiwane informacje dotyczyły energetyki. Od listopada 2009 roku pracownicy atakowanych firm byli nękani inżynierią społeczną i próbami phishingu. W 2010 roku niezidentyfikowani sprawcy włamali się do Ministerstwa Finansów Republiki Francuskiej i przekierowali dane dotyczące francuskiej prezydencji w G20 na chińskie strony internetowe, przez co oskarżenia pod adresem Chin stały się uzasadnione[20].

Wywiad w cyberprzestrzeni wykorzystuje osiągnięcia technologii informacyjnych prywatnych firm. Przykładem tego mogą być powtarzające się już od kilku lat oskarżenia pod adresem firmy Kaspersky Labs, która jest podejrzewana o to, że oprogramowanie antywirusowe spod jej marki szpieguje swoich użytkowników (zarówno osoby prywatne, jak i instytucje, przedsiębiorstwa) na rzecz Kremla. Można zauważyć, iż oskarżenia te przybierają w ostatnich dniach na sile. Brytyjskie Centrum ds. Cyberbezpieczeństwa wydało ostatnio ostrzeżenie przed używaniem tego oprogramowania przez instytucje państwowe[21]. To właśnie Federacja Rosyjska jest drugim po Chinach państwem oskarżanym o stosowanie cyberszpiegostwa. Wraz z zastosowaniem wywiadu osobowego i innych dyscyplin wywiadowczych Rosja próbuje wyrównać dysproporcje gospodarcze i technologiczne względem Stanów Zjednoczonych, żyjąc w przekonaniu, iż globalna gospodarka kieruje się właśnie interesami USA kosztem Rosji. Federacja Rosyjska dzięki włamaniom do sieci teleinformatycznych i przechwytywaniu e-maili oszczędza miliardy dolarów na badaniach i rozwoju technologicznym w energetyce, technologiach informacyjnych czy sektorze bezpieczeństwa. Wielka Brytania utrzymuje, iż Rosja stale penetruje cyberprzestrzeń jej systemu finansowego[22].

Rewolucja zastosowania cyberprzestrzeni w działalności wywiadowczej rozwija się w sferze międzypaństwowej, ale nie ominęła również sektora prywatnego, gdzie szpiegostwo przemysłowe przeniosło się również do cyfrowego świata. Cyberprzestrzeń z powodu unikalnych właściwości jakimi się charakteryzuje jest szczególnie narażona na akty cyberszpiegostwa, a co więcej, nie stanowi już monopolu działania dla służb państwowych.

Nie bez znaczenie jest również kradzież informacji przez osoby/grupy niepowiązane z państwem, które włamują się do zabezpieczonych systemów przetwarzających tajne dane, a następnie sprzedają wykradzione informacje czy dokumenty w darkwebie, co również nie powinno ujść uwadze służb wywiadowczych. W tym kontekście należy wspomnieć

20 M. Ciecierski, R. Nogacki, dz. cyt., s. 206–207.

21 G. Corera, *Kaspersky Labs: Warning over Russian anti-virus software*, BBC [w:] http://www.bbc.com/news/uk-42202191 [dostęp: 2.12.2017].

22 M. Ciecierski, R. Nogacki, dz. cyt., s. 207–208.

o działającej od lat grupie Anonymous, czyli grupie hakerów włamujących się i przeprowadzających ataki wobec różnych instytucji, czy przedsiębiorstw. Uznawani są bardziej za wojowników o przekonania, aniżeli realną grupę interesu.

## Podsumowanie

Rozważając problematykę wywiadu w cyberprzestrzeni należy zwrócić uwagę na fakt, iż jesteśmy świadkami stałego „zakorzenienia" się tej dyscypliny w światowej działalności wywiadowczej. Powszechny trend informatyzacji jest już obecnie nie do zatrzymania, dlatego zjawisko cyberszpiegostwa będzie sukcesywnie wzrastać, proporcjonalnie do informacji przetwarzanych w systemach informatycznych. Cyberprzestrzeń na stałe zadomowiła się w społeczeństwie i staje się nieodłączną częścią walki informacyjnej pomiędzy państwami, ale również pomiędzy podmiotami niepaństwowymi.

Cyberszpiegostwo czy cyberwywiad jest bez wątpienia działalnością, która niesie ze sobą ogromne możliwości i zalety. Po pierwsze, relatywnie niskie koszty w porównaniu z innymi dyscyplinami. Po drugie, oszczędność czasu na prowadzeniu skomplikowanej gry wywiadowczej. Czas potrzebny jedynie na znalezienie luki w systemie. Po trzecie, bezpieczeństwo cyberszpiegów, który nie muszą się fizycznie znajdować przy urządzeniu, z którego wykradane są dane, a mogą być po drugiej stronie globu, poza jurysdykcją państwa atakowanego. Po czwarte, wykradane informacje mogą zawierać nie tylko dokumenty oficjalne, ale również korespondencję decydentów politycznych, co z kolei może pomóc w rozpoznaniu zamierzeń polityków, a nie tylko oficjalnych wersji zawartych w dokumentach. Po piąte, cyberszpiegostwo może zapewniać anonimowość sprawców. Zastosowanie technologii anonimizującej może skutecznie uniemożliwić wykrycie prawdziwych atakujących, a tym samym możliwe jest uniknięcie odpowiedzialności i skandalu międzynarodowego. Po szóste, cyberszpiegostwo umożliwia wykradanie jednocześnie wielkich zbiorów informacji, co jest jednocześnie oszczędnością działań, ale również umożliwia ukrycie realnego celu i motywu ataku.

Bez wątpienia cyberprzestrzeń, cyberszpiegostwo, cyberterroryzm i inne działania człowieka w świecie cyfrowym stanowią ogromne wyzwanie dla systemów bezpieczeństwa. Niemniej jednak należy pamiętać, iż działa to w obie strony i oponenci również korzystają z systemów teleinformatycznych do przetwarzania własnych informacji. Na cyberprzestrzeń należy patrzeć nie tylko z punktu widzenia potencjalnych zagrożeń, ale również szans i możliwości, jakie ze sobą niesie wykorzystanie cyberprzestrzeni w działalności wywiadowczej zarówno w sferze państwowej, jak i komercyjnej. Można śmiało powiedzieć, iż cyberprzestrzeń na stałe zagościła w świecie współczesnym obok lądu, morza i powietrza, jako arena walki człowieka z drugim człowiekiem.

**Tytuł w języku angielskim:**
**CYBERSPACE AS A THEATER OF INTELLIGENCE ACTIVITIES**

## Bibliografia

**Publikacje zwarte**

Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Warszawa 2016.

Ciecierski M., Nogacki R., *Bezpieczeństwo współczesnej firmy. Wywiad, szpiegostwo, ochrona tajemnic*, Warszawa 2016.

Clark R.M., *Intelligence Collection*, Washington 2014.

Górka M. (red.) *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa. Historia i współczesność*, Toruń 2016.

Mądrzejowski W., *Przestępczość zorganizowana. System zwalczania*, Warszawa 2017.

Mądrzejowski W., Śnieżko S., Majewski P., *Zwalczanie przestępczości. Wybrane metody i narzędzia*, Warszawa 2017.

Siemiątkowski Z., Zięba A. (red.), *Służby specjalne we współczesnym państwie*, Warszawa 2016.

Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki, organizacji, państwa*, Warszawa 2016.

**Artykuły**

Dziwisz D., *Cyberbezpieczeństwo – nowy priorytet strategii obrony Stanów Zjednoczonych?*, „Sprawy Międzynarodowe" 2011, nr 3.

Grzelak M., *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" 2013/2.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", 9/13, 2013.

**Źródła internetowe**

Corera G., *Kaspersky Labs: Warning over Russian anti-virus software*, BBC [w:] http://www.bbc.com/news/uk-42202191 [dostęp: 2.12.2017].

*Foreign Spies Stealing US Economic Secrets in Cyberspace*, [w:] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf [dostęp: 2.12.2017].