Radosław Bielawski
Bogdan Grenda

Wybrane zagadnienia cyberbezpieczeństwa narodowego

Exante

Recenzenci

prof. zw. dr hab. inż. Ryszard Szpyra
dr inż. Grzegorz Pilarski

Autorzy
ppłk dr inż. Radosław BIELAWSKI
(Akademia Sztuki Wojennej)

płk dr hab. inż. Bogdan GRENDA
(Akademia Sztuki Wojennej)

WYBRANE ZAGADNIENIA CYBERBEZPIECZEŃSTWA NARODOWEGO

exante.com.pl, wydawnictwoexante.pl, Wrocław 2019

Książka sfinansowana ze środków Akademii Sztuki Wojennej

ISBN 978-83-66187-36-8 (PDF)

Exante Wydawnictwo Naukowe
dr Klaudia Pujer
ul. Buforowa 24 lok. 10, 52-131 Wrocław
WWW: exante.com.pl, wydawnictwoexante.pl

Radosław Bielawski
Bogdan Grenda

Wybrane zagadnienia cyberbezpieczeństwa narodowego

Exante

SPIS TREŚCI

WSTĘP

Uwzględniając fakt rozwoju komputerów oraz sieci informacyjnych, które trwają dynamicznie od kilkunastu lat do czasów obecnych, można wskazać na nowe środowisko, w jakim potencjalnie mogą zachodzić konflikty wymierzone w bezpieczeństwo narodowe państwa. Tym środowiskiem jest przestrzeń cybernetyczna.

Niestety w czasie, gdy cyberprzestrzeń staje się cyfrowym odzwierciedleniem fizycznej rzeczywistości, powstają w niej również negatywne formy aktywności[1]. Takim skutkiem korzystania z niej jest wykorzystywanie danych przez przestępców, terrorystów oraz inne nielegalne podmioty. Konsumenci dość często padają ofiarami wirusów i innego szkodliwego oprogramowania, oszustw internetowych czy wyłudzania poufnych danych. Motywacją do działania cyberprzestępców jest zazwyczaj chęć zysku. Druga grupa to tzw. hakerzy, którzy w dążeniu do osiągnięcia celów ideowych dopuszczają się np. kradzieży i niszczenia ważnych danych bądź utrudniają do nich dostęp. Wynikami takiej działalności często jest destabilizacja oraz zagrożenia bezpieczeństwa narodowego państwa.

Kolejną negatywną formą działalności w cyberprzestrzeni jest wojna informacyjna, przez którą przeciwnik dąży do realizacji celów strategicznych godzących w sposób destrukcyjny np. w infrastrukturę krytyczną, w tym technologiczną, państwa (zarządzanie sieciami energetycznymi, transportowymi, bankowymi itp.). Jej istotę należy rozpatrywać w odmienny sposób. Jest ona aktywnością zewnętrzną prowadzoną przez państwo do osiągania celów politycznych. Działa ona na systemy informacyjne państwa oraz ma na celu ochronę systemów własnych przez podobną ingerencją ze strony przeciwnika. Ponadto cechuje się ona przede wszystkim unikaniem bezpośredniej konfrontacji na polu walki, posługując się niekonwencjonalnymi metodami w postaci terroryzmu, walki informatycznej, psychologicznej czy ekonomicznej.

Literatura przedmiotu zawiera wiele modeli walki informacyjnej prowadzonej w cyberprzestrzeni, jakie zostały ukształtowane przez ostatnie lata. Brak jest jednak oceny adekwatności tych modeli do zagrożeń oraz

[1] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe" 2012, 2012 – II, nr 22, s. 126.

ryzyka związanego z zagrożeniami bezpieczeństwa narodowego. Samo bezpieczeństwo informacyjne, jako część bezpieczeństwa narodowego, jest zmienne. Pojawiają się nowe zagrożenia, które w bardzo szybkim tempie oraz przy dużej aktywności w cyberprzestrzeni są w stanie dokonać destabilizacji bezpieczeństwa kluczowych organów administracji państwowej, obiektów wojskowych czy innej ważnej – z punktu widzenia funkcjonowania państwa – jego infrastruktury.

Niniejsze opracowanie jest wynikiem przeprowadzonych badań naukowych, w formie studium teoretycznego. Składa się ze: wstępu, siedmiu rozdziałów głównych, zakończenia, bibliografii załącznikowej, wykazów rysunków i tabel oraz załączników.

W **pierwszym rozdziale** opracowania przedstawiono charakterystykę i podstawowe pojęcia związane z walką informacyjną w cyberprzestrzeni. W ramach tej części odniesiono się do etymologii oraz ewolucji pojęcia – cyberprzestrzeń, scharakteryzowano jej środowisko, przedstawiono znaczenie cyberbezpieczeństwa państwa i jego charakterystykę oraz pojęcia walki i wojny informacyjnej. Tak zestawione treści pozwoliły na stworzenie bazy pojęciowo-znaczeniowej oraz jednoznaczne zrozumienie poruszanych w treści zagadnień oraz terminów. **Rozdział drugi** opracowania poświęcony jest bezpieczeństwu informacyjnemu jako elementowi bezpieczeństwa narodowego. Krótko scharakteryzowano istotę bezpieczeństwa narodowego, ewolucję istoty i pragmatyki bezpieczeństwa państwowego. Nakreślono także informacyjny wymiar bezpieczeństwa narodowego. Rozdział drugi zakończono podsumowaniem i wnioskami. **Rozdział trzeci** pracy traktuje o modelach walki informacyjnej w cyberprzestrzeni. Spośród kilku odnalezionych literaturowych modeli, zdecydowano się zaprezentować i skomentować te, które najbardziej odpowiadają współcześnie prowadzonej walce informacyjnej w cyberprzestrzeni. Wybrano i opisano modele: Wardena, Dugina, Panarina i Libickiego. Całość rozdziału podsumowano i sformułowano wnioski. Kolejny – **czwarty rozdział** opracowania jest próbą oceny zagrożeń bezpieczeństwa narodowego w cyberprzestrzeni. W ramach tej części analizy zdefiniowano obiekty zagrożeń pochodzących z cyberprzestrzeni, które w sposób zdecydowany wpływają na bezpieczeństwo narodowe. Dokonano podziału na zagrożenia systemów wojskowych oraz na infrastrukturę krytyczną państwa. Odnosząc się do nich opisano obiekty zagrożeń oraz metodą studium przypadku (*case study*) dokonano próby badań typowych ataków, które miały miejsce w cyberprzestrzeni i skierowane były na te newralgiczne, z punktu widzenia bezpieczeństwa państwa, obiekty. Kolejnym zagadnieniem wchodzącym w skład tego rozdziału jest ewaluacja obecnego stanu zagrożenia bezpieczeństwa cybernetycznego. Dokonano oceny i wskazano główne kierunki ewolucji tych zagrożeń w bliskiej perspektywie. Końcowe treści skupiono

na ewolucji poziomu ryzyka zagrożeń bezpieczeństwa narodowego w cyberprzestrzeni, proponując metodykę szacowania ryzyka zagrożeń cyberbezpieczeństwa państwa oraz jedną z koncepcji szacowania i minimalizowania ryzyka związanego z zagrożeniami w cyberprzestrzeni narodowej. **Piąty rozdział** książki traktuje o mediach społecznościowych w kontekście cyberbezpieczeństwa narodowego. Uwzględniono w nim charakterystykę i rodzaje mediów społecznościowych. Dokonano analizy wybranych mechanizmów (sposobów) wykorzystania mediów społecznościowych w cyberprzestrzeni. Przedstawiono je w trzech grupach, do których należą: operacje psychologiczne, dezinformacja i propaganda oraz *fake news* i postprawda. W tej części pracy poruszono także aspekty psychologiczne wykorzystania *mass mediów*. Rozdział ten zakończono wnioskami oraz uogólnieniami. **Szósty rozdział** poświęcony jest strategii bezpieczeństwa polityczno-militarnego oraz aspektom prawnym w zapewnieniu cyberbezpieczeństwa. W ramach treści tego rozdziału zawarto analizę strategicznych założeń cyberbezpieczeństwa w kontekście wykorzystania mediów społecznościowych dotyczących cyberbezpieczeństwa Rzeczpospolitej Polskiej (RP), Unii Europejskiej (UE) oraz Organizacji Traktatu Północnoatlantyckiego (NATO), wskazując na podobieństwa, różnice oraz relacje. Wytypowano także instytucje i zespoły odpowiadające za bezpieczeństwo mediów społecznościowych w cyberprzestrzeni zarówno w odniesieniu do elementów narodowych, jak i NATO. Ostatni – **siódmy rozdział** pracy porusza aspekty dotyczące przestępstw dokonywanych przy użyciu mediów społecznościowych. Ważnymi i cennymi treściami są tutaj identyfikacje agresorów i naruszycieli prawa, mających bezpośredni wpływ na kształtowanie cyberbezpieczeństwa narodowego w kontekście bezpośredniego kreowania zagrożeń. Rozdział ten zakończono wnioskami oraz uogólnieniami.

ROZDZIAŁ 1.
Charakterystyka i podstawowe pojęcia związane z cyberbezpieczeństwem

1.1. Etymologia oraz ewolucja pojęcia cyberprzestrzeń

Określenie **cyberprzestrzeń** uważane jest za bardzo nowoczesne, choć jego historia ma już 35 lat. Pierwszy raz posłużył się nim William Gibson, używając tego terminu w powieści „Burning Chrome" opublikowanej w amerykańskim magazynie poświęconym treściom z zakresu *science fiction* – „Omni", w lipcu 1982 roku. Dwa lata później ten sam autor posłużył się określeniem cyberprzestrzeni w przełomowym dziele o nazwie „Neuromancer". W dziele tym cyberprzestrzeń, do której zaprasza autor, określona została jako „Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych (...). Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność (...). Świetlne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje danych"[2]. W oryginalnym brzmieniu opis cyberprzestrzeni w tym dziele miał postać „A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts (...). A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data"[3].

Obydwa z przytoczonych dzieł, dały nie tylko początek pojęcia cyberprzestrzeni, lecz także – co ważne – wskazały podstawowe elementy tego środowiska, do których możemy zaliczyć: „rozległość (zasięg światowy), łączenie wszelkich zasobów w jedną bazę danych, złożoność oraz bezprze-

[2] W. Gibson, *Neuromancer*, (przeł.) P.W. Cholewa, Katowice 2009, s. 59.
[3] W. Gibson, *Neuromancer*, Ace Books, New York 1984.

strzenność rozumianą jako brak możliwości odniesienia cyberprzestrzeni do fizycznych (w tym geograficznych) wymiarów realnego świata”[4].

Należy także zwrócić uwagę, że Gibson w swoich publikacjach wizualizował cyberprzestrzeń, która stała się elementem charakterystycznym dla fantastyki, zwanym **cyberpunkiem**. Był nim nurt, którego przedmiotem było negatywne funkcjonowanie ludzi w zaawansowanym świecie technologii komputerowej[5] i informacyjnej[6]. Można zatem wyodrębnić kilka charakterystycznych dla niego cech. Świat przedstawiany jest w sposób dystopijny i stechnicyzowany, rządzony przez korporacje świata przyszłości. Funkcjonuje w nim zasada *high tech & low life*, oznaczająca dosłownie wysoką technologię i niskie życie. Należy przez to rozumieć zestawienie rozwiniętego technologicznie świata wraz ze światem brudnym, brzydkim i niemoralnym, którego bohaterzy wywodzą się najczęściej z marginesu społecznego[7]. Kolejna cechą cyberpunku jest istnienie związane z technologią kontrkultury, która określa w miarę spójną indologicznie grupę społeczną, wyrażającą sprzeciw wobec zastanej kultury, jak i tej nowotworzonej. W analizowanym nurcie widoczne jest także istnienie sieci przesyłu danych, łączącej świat realny wraz z rzeczywistością, w której odbywa się fabuła. Widoczne jest także duże znaczenie informacji oraz jej przetwarza-

[4] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 9, s. 226.

[5] Na **technologię komputerową** składają się zagadnienia związane ze sprzętem (*hardwar-em*) oraz oprogramowaniem (*softwar-em*). Te pierwsze dotyczy budowy i kierunków rozwoju komputera, budowy i rozwoju urządzeń wejścia i wyjścia współpracujących z komputerem, jak i dostosowania i modyfikacji sprzętu komputerowego do zastosowań w różnych dziedzinach działalności ludzi. Drugie – oprogramowanie – obejmują zagadnienia tworzenia, modyfikowania i zastosowania oprogramowania, w celu umożliwienia różnych zastosowań systemu komputerowego. W swojej istocie jest najbardziej zbliżone do zadań informatyki teoretycznej, rozumianej jako zagadnienia związane z tworzeniem algorytmów.

[6] **Technologia informacyjna** (ang. *Information Technology* – IT) „jest to zespół środków (czyli urządzeń, takich jak komputery, sieci komputerowe, media), narzędzi (w tym oprogramowanie), jak również innych technologii, które służą wszechstronnemu posługiwaniu się informacją. Technologia informacyjna obejmuje więc swoim zasięgiem m.in. informację, komputery, informatykę i komunikację”, G. Friedrichs, A. Schaff (red.), *Mikroelektronika i społeczeństwo. Na dobre czy na złe?* Raport Klubu Rzymskiego, Książka i Wiedza, Warszawa 1987; D.J. Bolter, *Człowiek Turinga,* PIW, Warszawa 1990. Można zatem stwierdzić, że technologia informacyjna rozszerza zakres zainteresowania informacją na inne media niż tylko komputer i oprogramowanie. W stosunku do informatyki jest to istotne rozszerzenie, zwłaszcza w sferze praktycznego zastosowania. Nie chodzi tu tylko o metody zbierania, przechowywania i opracowywania informacji, ale także o możliwości ich prezentacji z wykorzystaniem innych mediów we współpracy z komputerem. Nadaje to technologii informacyjnej ponadprzedmiotowy i interdyscyplinarny charakter integrujący różne dziedziny korzystające z techniki informatycznej i komunikacyjnej.

[7] A. Świech, *Rewolucja dokonana – czym jest cyberpunk?*, „Ha!art” 2002, nr 2/3, s. 30–34.

nia. W nurcie cyberpunku uwypukla się wulgaryzm językowy oraz środowiskowy, a także przestępczy slang.

Oprócz literatury przedmiotu, w której odnajdujemy pierwsze zdefiniowanie pojęcia cyberprzestrzeni, znalazła ona także miejsce w kinematografii. Za przykłady można przytoczyć: trylogię „Matrix"[8] czy „Tron. Dziedzictwo". W ekranizacjach tych cyberprzestrzeń została zobrazowana za pomocą grafiki komputerowej. Pozwoliło to na przypisanie cyberprzestrzeni cech realnej rzeczywistości, którą można nie tylko zobaczyć, ale również dotknąć i kształtować za pośrednictwem odpowiednio przygotowanego interfejsu. Cyberprzestrzeń została tutaj przedstawiona jako zdigitalizowany świat zbudowany na siatce przypominającej kratki w zeszycie, na której poruszają się trójwymiarowe obrazy, z zachowaniem perspektywy zjawisk fizycznych, takich jak grawitacja czy zderzenia poruszających się na niej obiektów.

Na potrzeby pracy ważnym wydaje się dokonanie przeglądu definicji cyberprzestrzeni, które zostały opracowane i przyjęte na podstawie dokumentów rządowych różnych państw, w tym także dokumentów narodowych. Na ich podstawie, możliwe będzie określenie pojęcia bezpieczeństwa cyberprzestrzeni (które dzielimy na bezpieczeństwo wewnętrzne i bezpieczeństwo zewnętrzne w cyberprzestrzeni).

Jedną z najczęściej cytowanych i znanych definicji cyberprzestrzeni możemy odnaleźć w nomenklaturze wojskowej USA. Zgodnie z dokumentem „DOD Dictionary of Military and Associated Terms" cyberprzestrzeń określana jest, jako: „globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery"[9]. W oryginalnym brzmieniu przedstawia się ona następująco: *cyberspace* – „A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[10]. Inny dokument normatywny USA – „Cyberspace Operations" [JP 3-12 (R)], przedstawia cyberprzestrzeń na tle innych niezależnych domen, takich jak: domeny fizyczne – ląd, przestrzeń powietrzna i kosmiczna oraz obszar wód. Zgodnie z tą definicją cyberprzestrzeń to „jedna z pięciu niezależnych domen (środowisk)"[11].

[8] Na która składają się kolejno: *Martix* (1999), *Matrix Reatkywacja* (2003) i *Matrix Rewolucje* (2003).
[9] Tłumaczenie autorskie.
[10] *DOD Dictionary of Military and Associated Terms, As of March 2017*, s. 60.
[11] *Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013*, s. 6.

Cyberprzestrzeń – stała się jak to określono w amerykańskiej strategii – „systemem nerwowym państwa" – „(…) nasza gospodarka i bezpieczeństwo narodowe stały się w pełni zależne od technologii i infrastruktury informatycznej"[12]. Od sprawności i bezpieczeństwa cyberprzestrzeni zależy funkcjonowanie infrastruktury krytycznej[13].

Cyberprzestrzeń rozumiana jest także jako „element globalnego bezpieczeństwa i stanowi ona wyzwanie dla całej społeczności międzynarodowej. Cyberbezpieczeństwo zatem wymaga ciągłego doskonalenia zdolności reagowania na zaistniałe zagrożenia oraz ochrony zasobów państwa w cyberprzestrzeni w ramach współpracy instytucjonalno-prawnej dotyczącej zarówno sfery militarnej jak też cywilnej"[14].

W polskim, aktualnie obowiązującym, prawodawstwie można odnaleźć kolejną definicję określającą cyberprzestrzeń. Zgodnie art. 1, ust. 1b Ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, cyberprzestrzeń rozumiana jest jako: „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (…) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami"[15]. Należy tutaj zauważyć, że definicję sformułowano i przyjęto w taki sposób, aby ułatwić jej wykorzystanie w praktyce, w pracach wdrożeniowych – decyzjach, planach i programach o charakterze militarnym.

Jeden ze współczesnych dokumentów rządowych – „Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej" definiuje cyberprzestrzeń jako: „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami"[16]. Dodatkowo określa on pojęcie **cyberprzestrze-**

---

[12] *The National Strategy to Secure Cyberspace February 2003*, s. 8.

[13] *International Strategy for Cyberspace. Prosperity, Secirity, and Openess in a Networked World, May 2011*, s. 25.

[14] M. Adamczuk, K. Liedel, *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 281.

[15] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2011 r. nr 222 z późn. zm.).

[16] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, s. 7.

ni Rzeczypospolitej Polskiej (CRP)[17]. Zgodnie z nim jest to: „cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji)”[18].

Inna współczesna, słownikowa definicja cyberprzestrzeni wskazuje, że to „przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi siecią internetową”[19].

Oprócz zapisów doktrynalno-prawnych próba wyjaśnienia i zdefiniowania pojęcia cyberprzestrzeni została podjęta także przez wielu uczonych, zajmujących się badaniami naukowymi z tego obszaru wiedzy. Dla przykładu można podać definicję zaproponowaną przez Mirona Lakomego. Według jego podejścia, cyberprzestrzeń stanowi domenę przetwarzania, przechowywania i przesyłania informacji w formie cyfrowej, funkcjonującą w oparciu o transmisję sygnałów cyfrowych oraz promieniowanie elektromagnetyczne. „Jest przestrzenią w swojej istocie niematerialną, ale funkcjonującą dzięki infrastrukturze teleinformatycznej, która te sygnały wytwarza i przesyła (…) użytkownik, oddziałując na interfejs urządzenia informatycznego, osiąga efekt z gruntu niematerialny. Tym samym podejmując działania w świecie materialnym (…) wchodzi w «aterytorialny» świat cyberprzestrzeni”[20].

Uogólniając, na potrzeby niniejszego opracowania można stwierdzić, że cyberprzestrzeń w odróżnieniu do przestrzeni naturalnej – geoprzestrzeni jest przestrzenią wytworzoną przez człowieka i istniejącą tylko i wyłącznie w czasie jego aktywności. Tworzona jest zatem poprzez aktywność ludzką, przez którą jest kształtowana. Z tego powodu można ją uznać za przestrzeń komunikacyjną stworzoną przez system powiązań i relacji sieciowych (np. internetowych), obejmujących swym działaniem systemy komunikacji elektronicznej. Do systemów takich można zaliczyć Internet jako międzynarodową powszechną sieć, która w tym przypadku spełnia rolę łącznika pomiędzy użytkownikami, a tym samym twórcami sieci. Innymi rodzajami połączeń mogą być linie telefoniczne czy fale Hertza.

Podsumowując, można przypisać cechy, którymi charakteryzuje się cyberprzestrzeń. Są nimi niezależność od miejsca odległości, czasu, granic.

---

[17] W analogiczny sposób można zdefiniować **cyberprzestrzeń NATO**, jako – cyberprzestrzeń w obrębie terytorium NATO oraz w miejscach, gdzie funkcjonują przedstawicielstwa NATO.

[18] *Doktryna cyberbezpieczeństwa Rzeczypospolitej*…, *op. cit.*, s. 7.

[19] *Słownik Języka Polskiego PWN*, online – http://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915 [dostęp: 19.04.2017].

[20] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, s. 83.

Poza tym wyróżnia się ona względną anonimowością w odniesieniu do korzystających z niej osób oraz możliwością ustalenia wyposażenia (np. *software*, *hardware, adres IP*). Innymi charakterystycznymi cechami cyberprzestrzeni mogą być:

- „niematerialny charakter,
- brak możliwości określenia granic,
- zdecentralizowanie,
- brak ośrodków kontroli i nadzoru nad jej całością,
- płynny i plastyczny charakter,
- powszechna dostępność,
- przetwarzanie i dokładne obliczanie w czasie rzeczywistym”[21].

1.2. Charakterystyka środowiska cyberprzestrzeni

Cyberprzestrzeń stanowi środowisko[22] elektroniczne, będące częścią pozostałych środowisk: morskiego, lądowego, powietrznego oraz kosmicznego[23]. Relacje pomiędzy poszczególnymi rodzajami środowisk oraz ulokowanie w nich środowiska elektronicznego przedstawia rysunek 1.

Należy przy tym zaznaczyć, że cyberprzestrzeń wymieniona u Wardena jako piąta nie jest nowym, kolejnym po lądowym, wodnym, powietrznym, elektronicznym (wg Howarda), kosmicznym – szóstym środowiskiem działań. Cyberprzestrzeń według współczesnych poglądów jest jedynie elementem, który poszerza i współtworzy środowisko elektroniczne.

[21] M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Cyberkłopoty i Pułapki Sieci” 2010, nr 4(113), s. 1.

[22] Cyberprzestrzeń uważa się za środowisko, ponieważ: po pierwsze zawiera ogół czynników otoczenia, tych ożywionych i nieożywionych, będącymi tworem działania człowieka oraz tych naturalnych, po drugie jest zbiorem wszystkich obiektów oraz relacji między nimi.

[23] S. Czeszejko, *Działania w środowisku elektronicznym a świadomość sytuacyjna pola walki*, „Journal of KONBiN” 2011, nr 18, s. 17.

Rysunek 1. Umiejscowienie środowiska elektronicznego na tle pozostałych środowisk (domen)
Źródło: S. Czeszejko, *Działania w środowisku elektronicznym a świadomość sytuacyjna pola walki*, „Journal of KONBiN" 2011, nr 18, s. 18.

Środowisko elektroniczne można zdefiniować i rozumieć jako „ogół elementów nieożywionych powstałych w wyniku działalności człowieka, występujących w określonym obszarze, pomiędzy którego elementami istnieją wzajemne powiązania, wzajemne oddziaływania i pozostają one we wzajemnej zależności"[24]. Fizycznie środowisko elektroniczne stanowią urządzenia elektroniczne oraz sieci łączące je oraz pozwalające na przekaz danych (informacji) pomiędzy tymi urządzeniami.

1.3. Pojęcie i znaczenie cyberbezpieczeństwa państwa

Cyberbezpieczeństwo to termin wielowymiarowy, na który składa się wiele pojęć, począwszy od bezpieczeństwa informacji i bezpieczeństwa operacyjnego, po bezpieczeństwo systemów komputerowych. Pojęcie te może być również rozumiane w odmiennych kontekstach. W odniesieniu do indywidualnych osób oznacza poczucie bezpieczeństwa oraz ochronę danych osobowych i prywatności. Dla jednostek gospodarczych, cyberbezpieczeństwo to zagwarantowanie dostępności funkcji biznesowych o znaczeniu krytycznym i ochrona poufnych danych, dzięki zarządzaniu bezpieczeństwem operacyjnym i bezpieczeństwem informacji. W odniesieniu do państw, pojęcie to należy rozumieć jako ochronę obywateli, przedsię-

[24] *Ibidem*, s. 18.

biorstw, infrastruktury o znaczeniu krytycznym, jak i państwowych systemów komputerowych przed atakiem lub naruszeniem integralności[25].

Mimo istnienia istotnych różnic definicyjnych, istotę terminu cyberbezpieczeństwo można sprowadzić do zbioru działań i zasobów, które umożliwiają obywatelom, przedsiębiorstwom i państwom osiągnięcie celów informatycznych w sposób bezpieczny oraz niezawodny przy zachowaniu prywatności[26].

W odniesieniu do osób odpowiedzialnych za decyzje polityczne na szczeblu rządowym cele te dotyczą ochrony zdrowia i bezpieczeństwa publicznego, bezpieczeństwa ekonomicznego oraz obrony narodowej. Sfery te są szczególnie ważne z punktu widzenia zarządzania nowoczesnym krajem. Współczesne systemy teleinformatyczne stanowią fundament nowoczesnego społeczeństwa, ponieważ pozwalają rządom na zarządzanie podmiotami – służbami publicznymi, wzrostem gospodarczym i bezpieczeństwem narodowym[27].

Nowoczesne rozwiązania teleinformatyczne sprzyjają osiągnięciu głównych celów władz, do których zaliczyć trzeba: stabilność gospodarczą, bezpieczeństwo, wolność, ład publiczny, bezpieczeństwo publiczne i oświatę. Obszary te mogą przyczynić się do podniesienia standardu i jakości życia obywateli w danym kraju[28].

Trzeba jednak wyraźnie podkreślić, że uzależnienie od systemów teleinformatycznych prowadzi do powstania określonych ryzyk i zagrożeń. Wiele podmiotów pragnąć uzyskać konkretne korzyści, może kierować się np. pobudkami politycznymi i społecznymi oraz koncentrować się jedynie na wykorzystaniu i atakowaniu środowiska cyfrowego coraz intensywniej korzystającego z Internetu. Na tym tle uwidaczniają się wyzwania dla osób decyzyjnych politycznie[29]. Są to między innymi:

- „możliwość zdalnego, szybkiego i anonimowego przeprowadzenia ataku (czas, jaki jest wymagany do przesłania informacji dookoła świata po naciśnięciu klawisza wynosi 150 ms);
- szybki wzrost liczby urządzeń przenośnych, podatnych na zagrożenia, na rzecz tradycyjnych komputerów, których rozwój może zostać spowolniony;

[25] T. Storch, *Cyberbezpieczeństwo – fundament bezpiecznego społeczeństwa w dobie internetu*, TwC Next, Microsoft, 9 marca 2012 r., s. 4. Dokument udostępniony w sieci na licencji Creatove Commons – Uznanie autorstwa. Użycie niekomercyjne. Na tych samych warunkach 3.0 w wersji ogólnej.
[26] *Ibidem*, s. 4.
[27] *Ibidem*, s. 4.
[28] *Ibidem*, s. 4.
[29] *Ibidem*, s. 4.

– wzrost liczby użytkowników Internetu na całym świecie, których zwyczaje mogą prowadzić do powstania nowych luk w zabezpieczeniach”[30].

„W kontekście zmian technologicznych i społecznych cyberbezpieczeństwo w najbliższych latach będzie miało coraz istotniejsze znaczenie dla całej branży teleinformatycznej i utrzymania jej roli, jako siły napędowej w zakresie innowacji, wzrostu gospodarczego, tworzenia miejsc pracy czy rozwoju społecznego. Wraz z rozwojem i intensyfikacją cyberprzestrzeni, jak i rosnącym oddziaływaniem systemów teleinformatycznych na każdy sektor gospodarki, należy także zwiększać poziom cyberbezpieczeństwa w związku z pojawianiem się nowych zagrożeń[31].

Uogólniając, można określić **cyberbezpieczeństwo** jako ochronę przed ewentualnymi **cyberatakami**[32] oraz działania podejmowane na rzecz minimalizacji skutku, jeżeli ataki takie miałyby miejsce.

W kontekście podjętego w książce tematu – mediów społecznościowych – można wyróżnić nowe pojęcie **cyberataku społecznościowego** (ang. *social cyber attack*). Literatura przedmiotu określa je jako „działanie anonimowe lub pod fałszywym pretekstem, mające na celu wysyłanie do mediów społecznościowych spreparowanego przekazu lub też manipulację istniejącej już informacji, celem uzyskania oczekiwanego efektu: paniki, masowych zamieszek czy chaosu”[33].

Cyberbezpieczeństwo można także utożsamić z państwem, na terenie którego odbywają się działania w cyberprzestrzeni. Zatem bezpieczeństwo Rzeczypospolitej Polskiej (RP) w cyberprzestrzeni, inaczej **cyberbezpieczeństwo RP** można zdefiniować jako „proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni”[34].

---

[30] *Ibidem*, s. 4-5.

[31] *Ibidem*, s. 4-5.

[32] **Cyberatak** – „rodzaj działań w przestrzeni wirtualnej (cyberprzestrzeni), których celem jest zablokowanie lub przejęcie stron internetowych, skrzynek pocztowych lub baz danych”, *Słownik Języka Polskiego PWN*, online – https://sjp.pl/cyberatak [dostęp: 29.06.2017]. Inna definicja określa **cyberatak** jako – „celowe zakłócenie prawidłowego funkcjo-nowania cyberprzestrzeni”, *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, s. 5.

[33] T. Grabowski, *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016)*, „Horyzonty Polityki” 2016, nr 7 (20), s. 46.

[34] *Doktryna cyberbezpieczeństwa Rzeczypospolitej…*, *op. cit.*, s. 7., s. 5.

Innym tożsamym terminem związanym z cyberprzestrzenią Rzeczypospolitej Polskiej jest **bezpieczeństwo cyberprzestrzeni RP**. Jest to „część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych”[35].

Sformułowanie krajowej definicji pojęcia „bezpieczeństwo cyberprzestrzeni” stało się przedmiotem działań ukierunkowanych na wypracowanie oraz wdrożenie kompleksowej „Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej”. Dokument ten powstał w oparciu o założenia dla „Rządowego Programu Ochrony Cyberprzestrzeni RP”, w którym wskazano główne kierunki działań podejmowanych wobec szeroko rozumianych cyberzagrożeń, występujących w cyberprzestrzeni oraz tych skierowanych w nią. Treści dokumentu koncentrują się na kwestiach zwalczania cyberprzestępczości, identyfikacji organów właściwych do podwyższania poziomu bezpieczeństwa cyberprzestrzeni, jak również kooperacji między sektorami prywatnym i publicznym na rzecz bezpieczeństwa całej cyberprzestrzeni. Podczas prac legislacyjnych 28 listopada 2012 r. Komitet Rady Ministrów ds. Cyfryzacji zaopiniował dokument pozytywnie. Ostatecznie Rada Ministrów zatwierdziła go 25 czerwca 2013 r.[36].

1.4. Charakterystyka i pojęcie walki oraz wojny informacyjnej

Celem doprecyzowania terminu „walka informacyjna” zasadne jest zdefiniowanie pojęcia samej informacji. W literaturze tematu funkcjonuje wiele ujęć pojęcia „informacja” prezentowanych przez badaczy reprezentujących odmienne obszary nauki. W ujęciu inżynierskim (klasyczna teoria informacji), informacja ściśle wiąże się z teoretyczną koncepcją „systemu komunikacyjnego”, gdzie istnieją następujące elementy: źródło wiadomości, koder, kanał, dekoder, odbiorca wiadomości oraz szum. Teoria informacji jest dziedziną nauki, która przy wykorzystaniu modelu matematycznego charakteryzuje poszczególne elementy „systemu komunikacyjnego”[37].

[35] *Ibidem,* s. 7-8.
[36] Ministerstwo Cyfryzacji, online – https://mac.gov.pl/dzialania/krmc-dopinanie-projektow-przed-koncem-roku [dostęp: 29.06.2017].
[37] R.B. Ash, *Information Theory*, Dover Publications Inc., New York 1990, s. 1-2.

Zarówno w teorii systemów, jak i cybernetyce[38] informacja występuje obok materii oraz energii jako jeden z trzech zasadniczych elementów wymiany pomiędzy układami względnie odosobnionymi a otoczeniem. Wymiana ta ma kształt powiązań informacyjnych skierowanych z otoczenia do wyodrębnionego układu bądź z układu do otoczenia. Zasadnicze zadanie każdego systemu stanowi transformacja (przetwarzanie) zasileń materialnych, energetycznych i informacyjnych zlokalizowanych na wejściach systemu w odpowiednie wyjścia materialne bądź też informacyjne[39]. W cybernetyce informacja występuje w ujęciu realnym (odnoszącym się do samego systemu, struktury i poziomu jego zorganizowania) oraz abstrakcyjnym (dotyczącym przedmiotów lub zdarzeń, wytworów umysłu itp.). Kluczowe jest w tym przypadku powiązanie pomiędzy materią, energią i informacją. Informacja to kluczowy składnik każdego systemu, gdyż wprowadza ład i uporządkowanie[40]. Rozpatrując zagadnienie transformacji (przetwarzania) danych jako jednego z zadań systemu informacyjnego należy wymienić główne formy przetwarzania danych, jakimi są np.: klasyfikacja danych, sortowanie danych, agregacja danych, przeprowadzanie obliczeń z wykorzystaniem danych oraz selekcja danych.

Oczekiwaną cechą informacji jest użyteczność, czyli jej przydatność. Można zatem wyróżnić cztery cechy użytecznej informacji, do których zaliczamy:

- **dokładność** – jeśli informacja ma mieć realną wartość, musi być dokładna. Taka informacja dostarcza wiarygodnego odzwierciedlenia rzeczywistości;
- **aktualność** – aktualna informacja musi być dostępna wtedy, kiedy może być podstawą odpowiednich działań zarządzającego nią. Nie musi to wcale oznaczać, że powinna być dostarczona szybko. Aktualność jest funkcją sytuacji, w jakiej znajduje się zarządzający (użytkownik);
- **kompletność** – informacja kompletna dostarcza odbiorcy wszelkich potrzebnych mu faktów i szczegółów. Obraz sytuacji musi być pełny, jeśli informacja ma być użyteczna. Jeśli informacja jest niepełna, zarządzający nią może sobie wyrobić niedokładny lub zniekształcony obraz rzeczywistości;
- **odpowiedniość** – informacja odpowiednia to informacja użyteczna

[38] **Cybernetyka** to „nauka o procesach sterowania oraz przekazywania i przekształcania informacji w systemach takich jak np. maszyna, organizm żywy, społeczeństwo", *Słownik Języka Polskiego PWN*, online – http://sjp.pwn.pl/sjp/cybernetyka;2553914 [dostęp: 03.05.2017].

[39] S. Mynarski, *Elementy teorii systemów i cybernetyki*, PWE, Warszawa 1979, s. 9-10.

[40] *Ibidem*, s. 140.

dla odbiorcy, w zależności od jego konkretnych potrzeb i warunków[41].

Uznanie informacji za zasób strategiczny państw spowodowało wyłonienie kategorii walki informacyjnej, czyli takiej, w której informację traktuje się zarówno jako broń, jaki i cel ataku. Terminem tym po raz pierwszy posłużono się w latach 90. XX w. W 1994 r. w ramach Uniwersytetu Obrony w Waszyngtonie powołano Szkołę Strategii i Walki Informacyjnej. Powstało wtedy również dzieło Winn Schwartau, który definiował ją jako[42] „działania ukierunkowane na ochronę, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacji albo też zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem”[43].

Niewątpliwie na ewolucję pojęcia walki informacyjnej miała wpływ rewolucja informacyjna dotycząca technologii w zakresie pozyskiwania, przetwarzania i wykorzystania informacji, mająca miejsce pod koniec XX wieku. Wymusiło to dyskusje na temat bezpieczeństwa informacyjnego państwa jako integralnej części bezpieczeństwa narodowego. Kolejną konsekwencją było określenie zagrożeń informacyjnych. Przy takim podejściu należało uwzględnić kilka „uwarunkowań bezpieczeństwa informacyjnego, a przede wszystkim następujące fakty:

- informacja stanowi zasób strategiczny państwa;
- informacja i wynikająca z niej wiedza oraz technologie informatyczne stają się podstawowym czynnikiem wytwórczym;
- szeroko rozumiany sektor informacyjny generuje znaczną część dochodu narodowego;
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego są w znacznej mierze uzależnione od systemów przetwarzania i przesyłania informacji;
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych;
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej;
- technologie informatyczne stały się istotnym elementem funkcjonowania sił zbrojnych;

[41] K. Woźniak, *Informacja*, https://mfiles.pl/pl/index.php/Informacja [dostęp: 28.01.2019].
[42] T. Aleksandrowicz, *Wojna informacyjna. Dlaczego Zachód przegrywa z Rosją?*, online – https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-wojna-informacyjna-dlaczego-zachod-przegrywa-z-rosja
[43] W. Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* 1st, Thunder's Mouth Press, New York 1994.

– media masowe mogą być wykorzystywane jako narzędzia skutecznego zakłócania informacyjnego, np. na drodze dezinformacji”[44].

W jednym z dokumentów doktrynalnych można odnaleźć definicję **walki informacyjnej** (ang. *information warfare* – IW) zaproponowaną przez Amerykański Komitet Połączonych Szefów Sztabów. Określona jest ona jako „działania podjęte w celu osiągnięcia dominacji informacyjnej poprzez wpływ na informacje przeciwnika, jego procesy oparte na informacji, systemy informacyjne oraz sieci komputerowe”. Jako elementy walki informacyjnej można zatem wskazać: destrukcję fizyczną, operacje bezpieczeństwa, operacje psychologiczne, sabotaż i walkę elektroniczną. Natomiast jako narzędzia wykorzystywane w tej walce można wskazać m.in.: dyplomację, propagandę, kampanie psychologiczne, działania na poziomie wpływania na procesy polityczne lub kulturowe, dezinformację, manipulowanie lokalnymi mediami, infiltrację sieci komputerowych i baz danych[45].

W innym dokumencie o charakterze doktrynalnym – instrukcji połączonych sztabów *DOD & Joint Staff – CJCSI 3210.01* walka informacyjna określana jest jako „działania podejmowane dla osiągnięcia przewagi informacyjnej przez wpływanie na informację przeciwnika, jego zależne od informacji procesy, informacyjne systemy i sieci komputerowe przy jednoczesnej obronie własnej informacji, zależnych od informacji procesów, informacyjnych systemów i sieci komputerowych”[46].

Pojęcie walki informacyjnej funkcjonujące w literaturze przedmiotu jest odmiennie określane przez różnych naukowców zajmujących się tą problematyką. Piotr Sienkiewicz definiuje ją jako ogół działań ofensywnych i defensywnych niezbędnych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą walki informacyjnej w ujęciu tego autora jest:

– **zniszczenie** (lub degradacja wartości) zasobów informacyjnych przeciwnika, jak i wykorzystywanych przez niego systemów informacyjnych;
– **zagwarantowanie bezpieczeństwa** własnych zasobów informacyjnych i stosowanych systemów informacyjnych[47].

---

[44] T. Aleksandrowicz, *op. cit*.
[45] *Joint Publication 3-13*, *Joint Doctrine for Command and Control Warfare (C2W)*, *9 October 1998*, s. 13.
[46] *DOD & Joint Staff – CJCSI 3210.01* [w:] *FM 100-6 Information Operations*, Headquarters, Department of the Army, 1996, s. 2-2.
[47] P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?,* red. L.H. Haber, T. 1, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, s. 375.

Inny autor – Leopold Ciborowski – walkę informacyjną postrzega jako „negatywną kooperację wzajemnie realizowaną w sferze zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony podporządkowane jest działanie antagonistyczne strony drugiej”[48].

Część znawców analizowanego zjawiska jest zdania, że nie istnieje jedna, uniwersalna i akceptowana przez wszystkich definicja walki informacyjnej, jednak w większości proponowanych ujęć tego pojęcia występują wspólne treści. Jedną z nich jest postrzegania walki informacyjnej w perspektywie konfliktu, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Tym samym konflikt ten obejmuje fizyczne niszczenie infrastruktury wykorzystywanej przez przeciwnika do działań operacyjnych[49]. „Zatem obecnie słusznie uważa się, że – *cyberwar*, *infowar*, walka informacyjna, cyberterroryzm, *netwar*, informacyjni wojownicy, informacyjna dominacja, obrona w cyberprzestrzeni (ang. *cyberspace defence*) czy informacyjny chaos to neologizmy, dotyczące tego samego, ale bardzo szerokiego pojęcia jakim jest – walka ery informacyjnej (ang. *information age warfare*)”[50].

Należy mieć także świadomość, że walka informacyjna jest różnie rozumiana przez prowadzące ją państwa i organizacje. Wybrane jej interpretacje przedstawia tabela 1.

Rozpatrując pojęcie walki informacyjnej w kontekście zagrożeń dla Rzeczypospolitej Polskiej wartymi uwagi są zapisy, jakie zawarto w dokumentach Federacji Rosyjskiej. Głównym dokumentem jest „Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej”[51], podpisana przez prezydenta Władimira Putina w grudniu 2016 roku. Analiza działań praktycznych dowodzi, że założenia zawarte w tym dokumencie są realizowane. „W zakresie bezpieczeństwa informacyjnego Rosja zdobyła zarówno zdolności ofensywne, jak i defensywne. Media są kontrolowane przez władze a dziennikarstwo opozycyjne znajduje się w stanie szczątkowym. Nastroje społeczne są skutecznie manipulowane. Treści prezentowane przez media zachodnie są albo w Rosji niedostępne, albo dezawuowane”[52].

[48] L. Ciborowski, *Walka informacyjna*, Adam Marszałek, Toruń 1999, s. 187.
[49] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 80.
[50] *Ibidem*, s. 80.
[51] *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej*, 6 grudnia 2016, nr 646.
[52] T. Aleksandrowicz, *Wojna informacyjna*, *op. cit*.

Tabela 1. Interpretacja walki informacyjnej przez wybrane państwa i organizacje

Państwo/ organizacja	Interpretacja pojęcia WI
Polska	Zorganizowana w formie przemocy aktywność zewnętrzna państwa, ukierunkowana na osiągnięcie konkretnych celów politycznych. Jej zamiarem jest niszczenie bądź modyfikowanie systemów informacyjnego komunikowania się przeciwnika lub przepływających przez nie informacji, jak również aktywność, której celem jest ochrona własnych systemów informacyjnego komunikowania i przesyłanych przez nie informacji przed podobnym działaniem przeciwnika. Walkę informacyjną stanowi kooperacja negatywnie wzajemna, przynajmniej dwupodmiotowa, która ma miejsce w sferach: zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdy każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej.
Niemcy	Wielokierunkowe wykorzystywanie informacji i technik łączności, w tym technik przeznaczonych do zakłócania i niszczenia wrogich ośrodków informacji oraz systemów łączności w czasie kryzysu i konfliktu. Zamiarem jest osiągnięcie przewagi strategicznej i taktycznej.
Wielka Brytania	Intencją jest obezwładniania przeciwnika, w tym celu niszczy się różnorodne systemy przeciwnika (komputerowy, finansowy, telekomunikacyjny oraz kontroli ruchu).
USA	Aktywność inicjowana celem uzyskania przewagi przez modelowanie procesów i systemów informacyjnych oraz sieci komputerowych przeciwnika. Typowa pozostaje jednoczesna ochrona własnych zasobów informacyjnych.
Federacja Rosyjska	Całokształt przedsięwzięć, które obejmują: wsparcie, przeciwdziałanie i obronę informacyjną. Prowadzi się je według jednorodnej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem w dziedzinie informacyjnej podczas przygotowania operacji wojskowych oraz prowadzonych działań bojowych.
Organizacja Traktatu Północnoatlantyckiego – NATO (ang. *North Atlantic Treaty Organization*)	Ogół działań informacyjnych prowadzonych w okresie kryzysu i/lub konfliktu zbrojnego. Ich celem jest promowanie sprecyzowanego celu politycznego lub wojskowego w odniesieniu do wskazanego przeciwnika lub przeciwników.

Źródło: za A. Żebrowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000 i podanymi tam źródłami, tj. D.E. Denning, *Walka informacyjna i bezpieczeństwo informacyjne*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002, s. 11; R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002, s. 146; L. Ciborowski, *Walka informacyjna…, op. cit.*, s. 187; P. Gawliczek, J. Pawłowski, *Zagrożenia symetryczne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2003, s. 42.

Zdolności ofensywne natomiast są wynikiem realizacji założeń, zgodnie z którymi Federacja Rosyjska tworzy efektywne kampanie informacyjne wszędzie tam, gdzie dostrzega zagrożenia dla rosyjskich interesów. Służy temu rozwój własnych mediów i wywieranie wpływu na zagraniczną opinię publiczną. Inicjowane są również różnego typu działania, które mają służyć wzmacnianiu ich roli w międzynarodowym środowisku informacyjnym i zapewnianiu im ze strony władz odpowiedniego wsparcia[53].

Z pojęciem walki informacyjnej kolejnym łączącym się pojęciem jest – **cyberwojna**. Niektóre koncepcje, genezy pojęcia cyberwojny upatrują w hierarchiach wojskowych, które stworzyły je celem określenia kolejnego, wirtualnego tym razem pola walki. Cyberprzestrzeń, będąca zjawiskiem modelowanym przez człowieka, jest jednak płynna i trudna do nieambiwalentnego zdefiniowania. Z tego też względu, mając ten fakt na uwadze, można operować pojęciem **cyberkonfliktu** – zjawiskiem odmiennym od cyberwojny, które ma przybliżyć jej zrozumienie[54]. Cyberkonflikt[55] to konflikt, który angażuje rozmaite systemy ludzi, rzeczy, procesów i postrzegania, które wiążą się z sieciami komputerowymi, nie muszą być one w pełni skomputeryzowane. Wobec tego, z konfliktem cybernetycznym można utożsamić każdy konflikt, w którym wygrana bądź przegrana są dla większości jego uczestników zależne od działań prowadzonych w sieciach komputerowych[56].

K. Liedel przedstawia następującą klasyfikację cyberkonfliktów[57]:

- **aktywizm** – to niedestrukcyjna działalność, Internet to narzędzie służące wsparciu prowadzonej kampanii;
- **haktywizm** – kombinacja aktywizmu i działań przestępczych; czerpie on z metod hakerskich wykorzystywanych przeciwko kon-kretnym celom w Internecie. Celem jest zakłócenie ich funkcjo-nowania, nie powodując przy tym poważnych strat; działalność ta ukierunkowana jest nie tylko na zniszczenie zasobów przeciwnika, jej głównym celem jest przede wszystkim zwrócenie uwagi na dany problem;

---

[53] *Ibidem*.

[54] Ch. Demchak, *Cybered Conflict vs. Cyberwar*,
http://www.acus.org/new_atlanticist/cybered-con-flict-vs-cyber-war
[dostęp: 30.06.2017]
za: K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011-I, nr 17, s. 17.

[55] Pojęcie tożsame stosowane w literaturze przedmiotu – **konflikt cybernetyczny**, za: K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011-I, nr 17, s. 17.

[56] *Ibidem*, s. 17.

[57] K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Trio, Warszawa 2010, s. 23-24.

- **cyberterroryzm** – politycznie motywowany atak bądź zapowiedź ataku na komputery, sieci lub systemy informacyjne celem zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na władzy i poszczególnych jednostkach realizacji daleko idących działań o charakterze politycznym i społecznych w szerszym rozumieniu tego słowa; pojęcie to utożsamia się też z wykorzystaniem sieci Internet do komunikowania się, propagandy oraz dezinformacji.

Na tej podstawie **cyberwojnę** można zdefiniować jako „działania prowadzone przez państwa oraz podmioty niepaństwowe, przy użyciu broni cybernetycznych do penetrowania komputerów lub sieci w celu niszczenia, i/lub fałszowania danych, zakłócania lub uszkodzenia systemów. Cyberwojna może dotyczyć stosowania aktów szpiegostwa, przestępstw i wojny gospodarczej. Może również obejmować działania mające na celu wsparcie operacji wojskowych na szczeblu taktycznym i operacyjnym wojny, a także niezależne działania mające na celu uzyskanie efektów strategicznych”[58].

Jak podkreśla W. Smolski, celem wojny internetowej jest „zakłócenie działania, uszkodzenie lub zniszczenie: oprogramowania, komputerów lub sieci informacyjnych państwa bądź organizacji, dokonane przez agresorów niepaństwowych w odpowiedzi na podobny atak przeprowadzony przez innych aktorów niepaństwowych”[59].

Zdaniem tego samego autora wojny internetowe to przeniesienie realnego konfliktu lub napięcia do cyberprzestrzeni. Na tym gruncie dochodzi do wirtualnego starcia sił. Partycypują w nich głównie mniej lub bardziej zorganizowane grupy hakerów, ale także cyberterroryści[60].

Jak wskazuje W. Smolski, wskazana wyżej definicja mieści się w ramach ogólnego pojęcia walki informacyjnej. Jego zdaniem mówiąc jednak o „wojnie internetowej”, mamy na myśli głównie działania, w które zaangażowane są państwa (choć nie wyklucza on, że mogą w niej brać również udział aktorzy niepaństwowi). Podkreśla on, że pojęcie „wojny internetowe” odnosi się jedynie do takich akcji, w których państwa są celami ataków, ale nie są w sposób bezpośredni zaangażowane w walkę w cyberprzestrzeni. Wojnę internetową W. Smolski obrazuje na hipotetycznym przykładzie – „jeżeli hakerzy rosyjscy zaatakują systemy informacyjne USA, na co w odpowiedzi amerykańscy hakerzy uderzą na Rosję, to mamy do czynie-

[58] A. Krepinevich, *Cyber warfare: a “nuclear option”?*, Center for Strategic and Budgetary Assessments 2012, s. 8-9.
[59] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, [w:] *„Rodzinna Europa”. Europejska myśl polityczno-prawna u progu XXI wieku,* H. Malewski, Henryk, P. Fiktus, M. Marsza (red.), E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2015, s. 487-488.
[60] *Ibidem*, s. 487-488.

nia z wojną internetową. Natomiast jeżeli w konflikt w cyberprzestrzeni zaangażowałyby się państwa ze wszystkimi swoimi środkami, to jest to już walka informacyjna"[61].

Ponadto W. Smolski uznaje, że pojęciu „wojny internetowej" bliższy jest termin anglojęzyczny autorstwa J. Arquilli i D. Ronfeldta – *netwar*, rozumiany jako konflikt o niskiej intensywności między państwami i aktorami niepaństwowymi (np. międzynarodowe organizacje terrorystyczne, partyzanci lub handlarze narkotyków)[62]. W wirtualne starcia mogą być zaangażowani również cyberterroryści i – jak podkreśla W. Smolski – takie przypadki już odnotowano (choć jak wskazuje, rola cyberterrorystów w nich nie była dotychczas najważniejsza). Motyw ataków wynikających z konfliktów pomiędzy poszczególnymi grupami stanowi: oprogramowanie, komputery, sieci komputerowe rządu, organizacji użyteczności publicznej, wojska czy firm komercyjnych. Wynika z tego, że aktywność tego rodzaju stanowi istotne zagrożenie dla bezpieczeństwa państwa[63].

Termin cyberterroryzm powstał z połączenia dwóch określeń – cyberprzestrzeni i terroryzmu już w połowie lat 80. XX wieku za sprawą Barry Colina z Institute for Security and Intelligence z Kalifornii[64]. Bardzo szybko zaczęły pojawiać się głosy, iż Stany Zjednoczone za bardzo uzależniają się od komputerów. Już w latach 90. minionego wieku amerykańska Narodowa Akademia Nauk alarmowała, iż w przyszłości terroryści będą w stanie zrobić więcej za pomocą klawiatury niż bomby[65]. W tym samym okresie za sprawą Alvina i Heidi Tofflerów zaczęto używać terminu „elektroniczny Pearl Harbor"[66]. Jest on stosowany niezwykle często przez zarówno polityków, jak i środki masowego przekazu. Zgodnie z antycypowaną wizją, infrastruktura krytyczna Stanów Zjednoczonych zostałaby zaatakowana. Uniemożliwiłoby to normalne funkcjonowanie całego społeczeństwa i spowodowałoby paraliż: metra, systemów telefonicznych, sieci przesyłu energii elektrycznej czy brak możliwości pobrania pieniędzy z banków. Wprawdzie scenariusz ten nigdy się nie urzeczywistnił, ale ostrzeżenia przed nim pojawiają się, zwłaszcza po atakach 11 września 2001 roku. George Bush jeszcze przed atakami z 11 września 2001 roku wskazywał na

---

[61] *Ibidem*, s. 487-488.

[62] J. Arquilla, D. Ronfeldt, *Cyberwar is coming!*, „Comaparative Strategy" 1993, s. 27; za: W. Smolski, *op. cit.*, s. 487-488.

[63] W. Smolski, *op. cit.*, s. 488.

[64] J. Matusitz, *Cyberterrorism: how can American foreign policy by strenghtenedet in the information age?*, „American Foreign Policy Interests" 2005, vol. 27, no. 2, s. 138.

[65] G. Weimann, *Cyberterrorism. How real is the threat?*, United States Institute of Peace, Special Report 119, December 2004, s. 2.

[66] A. Tofller, H. Toffler, *War and anti-war: survival at the dawn of the 21st century*, Boston 1993.

brak odpowiedniego przygotowania Stanów Zjednoczonych na nowe zagrożenia, takie jak: proliferacja broni masowego rażenia, technologia rakietowa oraz wzrost cyberterroryzmu[67]. W 2003 roku Tom Ridge, amerykański sekretarz Departamentu Bezpieczeństwa Krajowego, zwrócił uwagę na światowe zagrożenie, jakim są terroryści podłączeni do sieci[68]. W 2010 roku Richard Clarke, były doradca ds. przeciwdziałania terroryzmowi i bezpieczeństwa w cyberprzestrzeni prezydentów Billa Clintona i George'a Busha oraz Robert Knake kreślili jeszcze bardziej katastroficzną wizję, która zostałaby zapoczątkowana przez awarię jednej z sieci komputerowych Pentagonu i doprowadziłby do awarii dostawców internetowych[69]. W efekcie doszłoby do śmierci dziesiątek tysięcy mieszkańców.

Przy tak nakreślonej etymologii oraz zważając na współczesny wymiar zjawiska, można przyjąć do dalszych rozważań naukowych, że cyberterroryzm jako specyficzna kategoria zagrożeń, obejmuje szereg działań w stosunku do systemów teleinformatycznych, podejmowanych w celu osiągnięcia założonych zamierzeń terrorystycznych[70].

Według amerykańskich uczonych – Irvinga Lachova i Courtney Richardson Internet, ze względu na swoje pięć cech (możliwość komunikacji, oddziaływanie w czasie rzeczywistym, globalny zasięg, brak konieczności stosowania drogiego wyposażenia, możliwość utajnienia przekazywanych danych)[71], wydaje się być doskonałym narzędziem dla działalności grup terrorystycznych. Przede wszystkim pozwala na szybką komunikację w tzw. czasie rzeczywistym. Jest też stosunkowo tanim środkiem komunikacji, co pozwala bez większych nakładów finansowych odwzorowywać funkcje, jakie sprawują instytucje rządowe czy współczesne siły zbrojne. Dodatkowo, dzięki sieci internetowej, nawet małe ugrupowania terrorystyczne mogą mieć światowy zasięg, podobny do zasięgu o wiele większych organizacji. Równie istotne jest to, że przy jego wykorzystaniu można rozpowszechniać różne informacje, nawet te skomplikowane. Jest to możliwe dzięki dużej przepustowości i rozwojowi oprogramowania. Kolejną ważną cechą sieci internetowej jest jej anonimowość, co pozwala grupom terrorystycznym na szerokie zastosowanie i dużą aktywność.

---

[67] G. Weimann, *Cyberterrorism: the sum of all fears?*, „Studies in Conflict and Terrorism" 2005, vol. 28, no. 2, s. 134.

[68] G. Weimann, *Cyberterrorism. How real…*, *op. cit.*, s. 3.

[69] R. Clarke, R. Knake, *Cyber War: the next threat to national security and what to do about it*, Harper-Collins Publishers, New York 2010.

[70] R. Kośla, *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*. Wystąpienie na konferencji w Bemowie, 29 listopada 2002.

[71] I. Lachow, C. Richardson, *Terrorist use of the internet. The real story*, „Joint Force Quartely" 2007, no. 45.

Cyberprzestrzeń jest wykorzystywana również przez terrorystów w celu prowadzenia motywowanej politycznie działalności. Wiele incydentów przypisywanym terrorystom może być formą wandalizmu – działaniem prowadzonym przy cichej akceptacji państwa, co jednak jest trudne do udowodnienia. Klasycznym przykładem są cyberataki z 2007 r. w Estonii na infrastrukturę teleinformatyczną. Sparaliżowały one państwo, blokując dostęp do systemów bankowych oraz sieci komórkowych. O sytuację posądzono głównie Rosję, lecz nie zebrano odpowiednich dowodów, które potwierdziłyby, że władze tego kraju były za nie formalnie odpowiedzialne. Zważywszy na wysokie koszty i potencjalne trudności w organizacji skutecznego cyberataku na dobrze zabezpieczone cele, jest mało prawdopodobne, aby jakaś grupa terrorystyczna była w stanie zainicjować działanie tego typu bez wsparcia władz państwowych[72]. Cyberprzestrzeń wykorzystywana jest również przez terrorystów jako narzędzie komunikacji. Używają jej do: koordynowania podjętych działań, propagandy, dezinformacji, gromadzenia środków finansowych oraz werbowania nowych członków. Ponadto, za jej pośrednictwem ma miejsce udostępnianie materiałów o charakterze instruktażowym[73].

Zebrany powyżej rezerwuar pojęć związanych z cyberbezpieczeństwem oraz walką i wojną informacyjną, często – pomimo definicyjnych różnic w przedstawianiu tej terminologii –powodujących wrażenie ich nieostrości, w tym opracowaniu ma na celu ich rozpowszechnienie.

[72] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni, op. cit.,* s. 127.

[73] M. Adamczuk, *Ewolucja strategii i metod działania islamskich ugrupowań terrorystycznych i ich wpływ na bezpieczeństwo Polski*, „Bezpieczeństwo Narodowe", nr 19, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 211-214.

ROZDZIAŁ 2.
Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego

2.1. Istota bezpieczeństwa narodowego

Bezpieczeństwo ma charakter zarówno przedmiotowy, jak i podmiotowy i określa stan pewności, spokoju i braku zagrożenia. Zgodnie z hierarchią ustanowioną przez amerykańskiego psychologa Abrahama Maslowa stanowi drugą w hierarchii potrzebę ludzką, jest również potrzebą grup społecznych i państw. Dotyczy ono zaspokojenie takich potrzeb, jak: istnienie, przetrwanie, całość, tożsamość (identyczność), niezależność, spokój, posiadanie i pewność rozwoju. Brak zagwarantowania stanu bezpieczeństwa skutkuje niepokojem i poczuciem zagrożenia. Biorąc pod uwagę źródło tego zagrożenia w nauce wyróżnia się bezpieczeństwo wewnętrzne i bezpieczeństwo zewnętrzne[74]. Bezpieczeństwo wewnętrzne oznacza stabilność i harmonijność danego organizmu bądź podmiotu, natomiast bezpieczeństwo zewnętrzne brak zagrożenia ze strony innych podmiotów lub czynników zewnętrznych[75].

Jednym z rodzajów bezpieczeństwa jest **bezpieczeństwo narodowe**, utożsamiane z pojęciem **bezpieczeństwo państwa**. Pojęcie to równoznaczne jest ze zwalczaniem wszystkich potencjalnych niebezpieczeństw. Typologia zagrożeń wyodrębnia czynniki zewnętrzne oraz wewnętrzne. W wyniku dbałości o bezpieczeństwo państwa, przygotowywane są zestawienia, spis kluczowych dla kraju wartości o charakterze wewnętrznym, których konieczność ochrony ma charakter obligatoryjny. W ich skład wlicza się:

- nierozerwalność, spójność terytorialną;
- poziom życia, rozumiany jako system praw i obowiązków społecz-

[74] Analogicznie do pojęcia bezpieczeństwa cyberprzestrzeni, które także dzieli się na bezpieczeństwo – wewnętrzne cyberprzestrzeni i zewnętrzne cyberprzestrzeni.
[75] K. Liedel, *Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego*, online – http://www.liedel.pl/?p=13

nych, jakość egzystencji, poziom ewolucji oraz rozwoju na płaszczyźnie społeczno-gospodarczej, progres możliwości wprowadzania ulepszeń zarówno w aspektach, które uzależnione są od ingerencji człowieka, np. kultura, jak i środowiska naturalnego;
- ciągłość (zdolność przeżycia społeczeństwa oraz kraju rozumianego jako suwerenne terytorium);
- suwerenność polityczna.

Wymienione elementy są tożsame z założeniami kraju w aspekcie bezpieczeństwa oraz wyznaczają kierunek rozwoju w zakresie polityki bezpieczeństwa. Zasoby wydzielane na te potrzeby różnicowane są ze względu na skalę oraz rodzaj zagrożenia. Warto zwrócić uwagę na fakt, że dopasowanie zasobów przeznaczonych na politykę bezpieczeństwa, uzależnione jest zarówno od ilości, jakości zagrożeń, jak również od postrzegania owego ryzyka przez organizm państwowy oraz sumę zasobów i zdolność do ich skutecznego spożytkowania.

Frederick Hartmann opisał determinanty siły oraz niedostatków krajowych, które konstytuują wymiar polityki bezpieczeństwa państwowego. Determinanty te dzielą się na:
- uwarunkowania demograficzne;
- uwarunkowania militarne (ocena zasobów militarnych kraju, stosunek pokładów zbrojeniowych do liczby ludności zdolnej do pełnienia służby);
- uwarunkowania geograficzne (układ, obszar terytorium, czynniki klimatyczne);
- uwarunkowania finansowo-ekonomiczne (perspektywy gospodarczych założeń, pokłady surowców, bilans zysków i strat);
- uwarunkowania społeczne, wynikające z przeszłości historycznej, o podłożu psychologicznym;
- uwarunkowania logistyczno-administracyjne (system polityczny, wartościowanie działań władzy przez społeczeństwo, stosunek ludności do sprawowanych rządów)[76].

W obszarze bezpieczeństwa państwa funkcjonuje podział wynikający z typów zagrożeń oraz środków ich zwalczania. W tej klasyfikacji wyróżnia się: bezpieczeństwo militarne, informacyjne, finansowo-ekonomiczne oraz polityczno-społeczne. Zagrożenie może odnosić się do poszczególnych obszarów, może też być oceniane jako ryzyko całościowe.

W literaturze tematu często można spotkać się z wadliwym rozumieniem bezpieczeństwa narodowego w aspektach teoretycznych, ponieważ niejednokrotnie dokonuje się rozdzielenia poszczególnych jego wymiarów

[76] F.H. Hartmann, *The Relations of Nations*, Macmillan Publishing Co., Inc., London 1978, s. 207.

na osobne, niezależne elementy. Podejście takie jest niezgodne z funkcją i znaczeniem pojęcia bezpieczeństwa narodowego, które stanowi nierozerwalny człon, funkcjonujący w obrębie wymienionych obszarów. Oznacza to, iż kraj w określonej jednostce czasu nie może być zabezpieczony wyłącznie pod względem militarnym, przy założeniu, że zagrożenia dotykają np. obszaru polityczno-społecznego. Idealnym przykładem ilustrującym słuszność powyższego stanowiska będzie przywołanie historii destrukcji Związku Socjalistycznych Republik Radzieckich.

2.2. Informacyjny wymiar bezpieczeństwa narodowego

Bezpieczeństwo informacyjne państwa stanowi integralną część bezpieczeństwa narodowego[77]. **Bezpieczeństwo informacyjne** rozumiane jest jako „stan warunków wewnętrznych i zewnętrznych, który pozwala państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego”[78]. Stan ten jest osiągnięty, gdy spełnione są poniższe przesłanki:

- strategiczne zasoby państwa są wolne od zagrożeń;
- decyzje podejmowane przez władzę bazują na wiarygodnych, istotnych, dokładnych i aktualnych informacjach;
- obieg informacji pomiędzy organami państwa jest niezakłócony;
- nie jest zakłócone funkcjonowanie sieci teleinformatycznych, które składają się na krytyczną infrastrukturę teleinformatyczną państwa;
- państwo zapewnia ochronę informacji niejawnych i danych osobowych obywateli;
- prawa obywateli do prywatności nie są naruszone przez instytucje publiczne;
- obywatele, organizacje pozarządowe i media masowe mają zapewniony dostęp do informacji publicznej[79].

Bezpieczeństwem informacyjnym nazywa się także działania podjęte w celu ochrony danych przed przeciwwskazanym (zamierzonym, jak również niezamierzonym) odtajnieniem, transformacją, destrukcją oraz blokadą przed przekształcaniem ich, jak i wykorzystaniem tych informacji. Wymienione aspekty mają służyć wykluczeniu niebezpieczeństwa informacyj-

[77] T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 15, s. 12.
[78] T. Aleksandrowicz, *Wojna informacyjna…*, *op. cit*.
[79] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011, s. 103.

nego. Analizując ten termin można stwierdzić, iż powyższa definicja ma charakter przestarzałego ujęcia negatywnego. Z upływem czasu informacja zyskała duże znaczenie. Było to spowodowane postępem naukowo-technicznym oraz umysłowym. Zyskanie danych było niejako wymogiem do poprawy funkcjonowania społeczności. Ta płaszczyzna ustanowiła konieczność wystąpienia zjawiska konkurencji. Pobudki do wykreowania korzystniejszych warunków życia, aranżowały popyt na uzyskiwanie danych. Sytuację tę można zobrazować na przykładzie tzw. błędnego koła. Jednostka „A" przy użyciu wszelkich starań próbuje uzyskać dane, które jednostka „B" jak najdokładniej chroni. Dochodzi na tej płaszczyźnie do niezgodności intencji, zamierzeń oraz podjętych działań. Wymienione elementy nie bez powodu nasuwają na myśl skojarzenia z terminem „walka", gdyż po części stanowią one jej desygnaty. Informacja zyskała miano przyczyny tejże rywalizacji, której narzędziami stały się wszystkie metody, umożliwiające uzyskanie, dezorganizowanie oraz ochronę danych. Wspomniana rywalizacja nosi nazwę walki informacyjnej. Biorąc pod uwagę rozrastanie się wartości informacji, pierwotne ujęcie negatywne nie spełniało stawianych oczekiwań. Okazało się merytorycznie zbyt wąskie. Wszystkie obszary bezpieczeństwa państwa warunkowane są istnieniem „wolnej" wymiany, cyrkulacji danych oraz utrzymaniem schematów, mechanizmów opierających się na informacji. Obecnie zyskują one nowe znaczenie w aspektach decyzyjności zarówno w przestrzeni militarnej, jak i cywilnej.

Analizując teraźniejszy wpływ informacji, przypuszcza się, że z biegiem czasu poziomy użytkowania informacji będą zdecydowanie bardziej rozległe. W XXI wieku funkcjonuje praktycznie nieblokowany w żaden sposób wgląd do różnego rodzaju danych, np. ekonomicznych, reklamowych, militarnych. Dostęp ten zmusza kraj do doskonalenia procesów bezpieczeństwa informacyjnego, w celu utrzymania na odpowiednim poziomie ochrony wdrożonych rozwiązań oraz zapewnienia państwu możliwości do aktywnej ewolucji i ekspansji społeczeństwa informacyjnego. Opisane ujęcie określa się ujęciem pozytywnym. Mechanizmy procesów bezpieczeństwa informacyjnego w ujęciu pozytywnym powinny brać pod uwagę, iż informacja tworzy generalny i prospektywiczny zasób obecnego świata oraz buduje fundamentalny determinant produkcyjno-wytwórczy. Trzeba też podkreślić, że niszczenie sprawnego funkcjonowania procesów informacyjnych nie powoduje konieczności pozyskania dużych nakładów finansowych. Konieczność przygotowania efektywnych systemów bezpieczeństwa informacyjnego wzmaga wzrostowa tendencja informatyzacji wojska, wzrost uprawnień mechanizmów łączności oraz wdrażanie nowoczesnych technologii w obszary armii, w tym broni dokładnego rażenia. Obecna walka informacyjna identyfikowana będzie z działaniami zbrojnymi. Powstają przypuszczenia, że walka informacyjna może stać się zastępstwem starć

zbrojnych, a jej zagrożenia będą tożsame z tradycyjnym rozumieniem wojny. Odpowiednio przygotowana pozwoli na zakłócenie nadrzędnych stosunków politycznych na płaszczyźnie światowej, jak i wewnątrzpaństwowej.

Nie sposób pominąć również roli mediów w walce informacyjnej, ponieważ będą one używane bezpośrednio przez wroga jako mechanizmy wytwarzania efektywnego defektu informacyjnego. Rezultat taki mogą osiągnąć kraje o ustroju demokratycznym, posiadające wolne media, z natychmiastowym przepływem danych.

Dostępne sposoby oraz środki walki informacyjnej umożliwiają pozyskiwanie danych na wiele sposobów. Rywalizacja w tym zakresie będzie stale kontynuowana. Obecnie za efektywne mechanizmy walki informacyjnej uznaje się zdalne przesyłanie wirusów do przestrzeni informatycznej. Przy czym warto wspomnieć, że wirusy posiadają zdolność do natychmiastowego powielania się. Nie można pominąć też aspektu tzw. bomb logicznych (wytworzone aplikacje), które uruchamiają się według zaprogramowanych impulsów. Warto zwrócić uwagę również na zatrzymywanie transferu danych oraz rozprzestrzenianie dezinformacji przy wykorzystaniu możliwości masowego przekazu. Obecne mechanizmy walki informacyjnej pozwalają na prowadzenie skutecznej działań, nastawionych na kierowanie schematami decyzyjnymi wroga. Włączenie informacji do państwowego i ukrytego schematu danych konkretnego kraju (w tym informacji nieprawdziwych), w sposób dopasowany do założonych celów, wpłynie na społeczeństwo i wywoła reakcje zgodne z intencją manipulanta.

Biorąc pod uwagę wyżej wymienione fakty, można wysnuć wniosek, iż teraźniejsze metody i techniki walki informacyjnej, dowodzą potrzeby włączenia tej kwestii w proces modernizacji i restrukturyzacji sił zbrojnych, w całokształt działań związanych z rozwojem kraju. Takie postępowanie posiada wyraźną legitymizację. Otóż, trzeba zauważyć, że rywalizacja informacyjna tworzy istotne zagrożenie nie tylko w momencie otwartego konfliktu, ale również poprzez utajnione posunięcia stron zewnętrznych, ukierunkowane na uzyskanie jak największej liczby danych w okresie stabilizacji i pokoju. Procesy te niosą ze sobą ogromne ryzyko zagrożeń.

Do wspomnianego ryzyka zaliczyć można np. możliwość wystąpienia rozruchów, niepokojów społecznych. Nie sposób nie wspomnieć też o niezwykle silnym niebezpieczeństwie, jakie może dotknąć konkretny kraj. Jest nim zagrożenie terrorystyczne. Przypadki aktów terroryzmu mogą być dokonywane przez perfekcyjnie przeszkolone służby specjalne. Tego rodzaju przemoc może stanowić powód do rozpoczęcia jawnej agresji i otwartego konfliktu.

Warto wspomnieć o jeszcze jednym kierunku wykorzystania walki informacyjnej. Mowa o skierowaniu działań, które mają uzyskać negatywne

konsekwencje dla atakowanego kraju. W tym wypadku chodzi o niszczenie wysokiej pozycji i prestiżu danego kraju na tle stosunków międzynarodowych oraz umniejszenie jego wiarygodności w ocenie sojuszników obecnych i potencjalnych. Skutki takich działań wpływają negatywnie na relacje sąsiadujących ze sobą państw. Dodatkowo atrakcyjność tajemnic, informacji ukrywanych przez kraj, z którym graniczy konkretne państwo powoduje ryzyko ataku. Znaczenie wspomnianych informacji niejawnych zwiększa się niejednokrotnie zarówno na poziomie ilościowym, jak i jakościowym – jeśli te informacje niejawne dotyczą dużego kraju lub całych koalicji. Najbardziej narażone na tego rodzaju przemoc są obszary finansowy i społeczno-polityczny. Dlatego też niezwykle ważna jest ochrona informacji niejawnych swojego kraju, ponieważ element ten wpływa na poprawne i niezagrożone funkcjonowanie całego państwa[80].

Podsumowując rozważania dotyczące kwestii bezpieczeństwa informacyjnego w aspekcie informacyjnym oraz mechanizmów walki informacyjnej można założyć, że analogicznie do sytuacji i skutków rewolucji przemysłowej, państwa które uzyskały przewagę w tworzeniu i rozszerzaniu zaplecza; bazy informacyjnej zarówno w gospodarce, jak i pozostałych aktywnościach, będą przodowały w tym zakresie przez długi okres czasu. Uzyskanie tożsamych wyników i poziomu tychże krajów, będzie trudne i spowoduje konieczność pozyskania dużych nakładów finansowych. Szanse na powodzenie będą mimo wszystko znikome.

Przy kreowaniu przestrzeni informacyjnej nie sposób zapomnieć o zapewnieniu oraz dostosowaniu mechanizmów, procesów bezpieczeństwa informacyjnego, w celu umożliwienia jego prawidłowego działania. Nacisk tworzony przez międzynarodową płaszczyznę gospodarczą, na ewolucję i udoskonalanie technologii informacyjnych, niesie ze sobą potrzebę kontroli istoty kraju jako organizmu funkcjonowania narodu i społeczeństwa. Państwo w roli inicjatora rozwoju społecznego zyskuje dodatkowe, ważne znaczenie, ale także przyjmuje na siebie konieczność zadbania o bezpieczeństwo informacyjne.

2.3. Uogólnienia i wnioski

Na podstawie opisanych treści wynikających z analizy literatury przedmiotu oraz działań praktycznych można stwierdzić, że bezpieczeństwo informacyjne, w tym cyberprzestrzeń, jest ważnym elementem bezpieczeństwa narodowego. Zgodnie z typologią, można je podzielić na cztery główne filary – bezpieczeństwo: militarne, informacyjne, finansowo-ekono-

[80] K. Liedel, *Bezpieczeństwo informacyjne…*, *op. cit.*

miczne oraz polityczno-społeczne. Taki funkcjonalny podział można odnieść także do cyberprzestrzeni, w tym także CRP.

Bezpieczeństwo informacyjne zatem jest częścią bezpieczeństwa narodowego, rozumianego w ten sposób, że wpływa znacząco na bezpieczeństwo państwa, spełniając przy tym warunki: utrzymania wysokiego poziomu bezpieczeństwa strategicznych zasobów państwa oraz aktualności informacji jakie dostarczane są do organów władzy państwowej. Przy takim założeniu pozostaje niezakłócony przepływ informacji w państwie oraz, co ważne, funkcjonowanie elementów tworzących krytyczną infrastrukturę państwa jest stabilne. W aspekcie tych czynników należy mieć na uwadze, że zachowanie poziomu bezpieczeństwa dotyczy zarówno działań zamierzonych, jak i niezamierzonych ze strony agresorów korzystających z cyberprzestrzeni.

Dokonując antycypacji wykorzystania informacji i walki z nią można z całym zdecydowaniem konstatować, że obecnie i w niedalekiej przyszłości będzie istniał nieograniczony (lub w bardzo określonym zakresie) wgląd do danych ekonomicznych czy militarnych. To także wpływa na zwiększenie podatności cyberprzestrzeni ma zagrożenia oraz wymusza kreowanie i doskonalenie procesów do doskonalenia procesów bezpieczeństwa informacyjnego, w celu utrzymania na odpowiednim poziomie ochrony wdrożonych rozwiązań oraz zapewnienia państwu możliwości do dalszej ewolucji społeczeństwa informacyjnego.

ROZDZIAŁ 3.
Modele walki informacyjnej w cyberprzestrzeni

3.1. Teoria dekapitacji oraz model Wardena

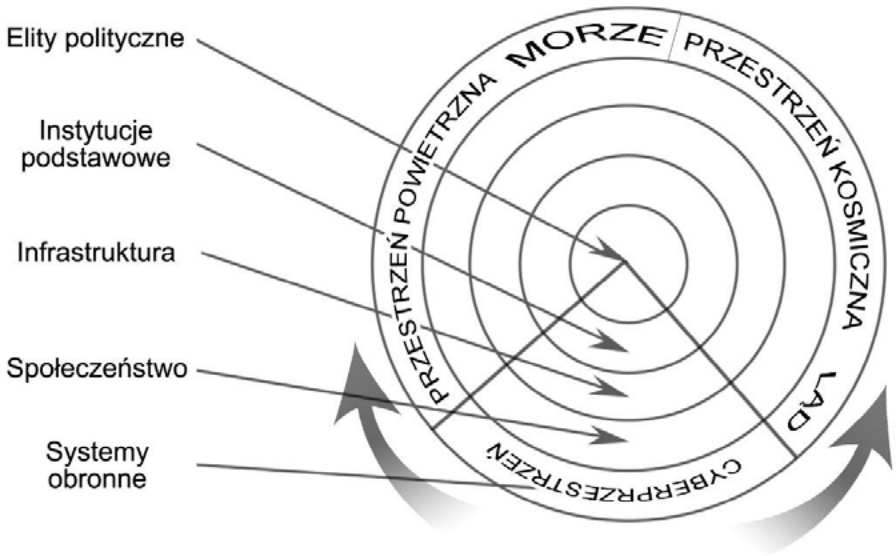
Podstawowym i jednocześnie uniwersalnym narzędziem, pozwalającym na zbadanie przebiegu dowolnego, współczesnego konfliktu jest koncepcja opracowana przez Johna Wardena[81]. Jest ona znana jako model „pięciu wymiarów", „pięciu kręgów" lub „pięciu pierścieni" (rysunek 2) zdefiniowanych przez Wardena na bazie doświadczeń wojny w Zatoce Perskiej[82], a w rodzimym piśmiennictwie naukowym dotyczącym walki informacyjnej kontynuowana przez Piotra Sienkiewicza[83]. Zakłada ona istnienie pięciu wymiarów, poprzez które możliwe jest oddziaływanie na przeciwnika. Są nimi: ląd, morze, przestrzeń powietrzna, przestrzeń kosmiczna i przestrzeń cybernetyczna.

W myśl teorii Wardena przeciwnik jest pojmowany i rozumiany jako system oraz został porównany do funkcjonowania ludzkiego organizmu. Składa się on z powiązanych ze sobą kręgów, pełniących złożone role, które stanowią systemową całość danej organizacji, państwa, gangu przestępczego czy zorganizowanej grupy terrorystycznej. Wroga strona została określona jako:

- **systemy obronne** – definiowane jako komponent aktorów, w skład których wchodzą wszystkie siły i środki wykorzystywane w celu obrony państwa przed przeciwnikiem, np. siły zbrojne oraz inne służby, takie jak policja, straż (np. graniczna);

[81] J. Warden, *The Enemy as System*, Maxwell 1995,
online – http://www.airpower.maxwell.af.mil
/airchronicles/apj/apj95/spr95_files/warden.htm [dostęp: 23.04.2017].
[82] W. Krautz, *Piąty wymiar walki, czyli logiczne konsekwencje modelu Wardena*, online – http://xportal.pl/?p=2110 [dostęp: 28.06.2017].
[83] P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?,* Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, s. 375.

- **społeczeństwo** – definiowane jako ludność, grupy demograficzne, klasy i elity społeczne;
- **infrastruktura** – definiowana jako infrastruktura krytyczna państwa, fizyczne elementy decydujące o jego istnieniu oraz sprawnym funkcjonowaniu w danej działalności, np. drogi, lotniska, fabryki;
- **instytucje podstawowe** – definiowane jako komponent, w którym zachodzą procesy w celu zrealizowania potrzeb organicznych ludności, takie jak: energia elektryczna, gaza, woda, ropa naftowa, zasoby pieniężne, zapasy żywności;
- **elity polityczne** – definiowane jako komponent najwyższego przywództwa, sprawującego kierownictwo lub dowództwo na szczeblu strategicznym, np. w przypadku funkcjonowania państwa może być to rząd[84].



Rysunek 2. Model „pięciu wymiarów" walki według Wardena
Źródło: opracowanie własne na podstawie P. Sienkiewicz, *Wizje i modele wojny…*, *op. cit.*, s. 375.

Teoria zakłada, że systemy obronne uznawane jako pierwszy, zewnętrzny krąg, mogą zostać zniszczone przy użyciu rozmaitych środków militarnych z każdej przestrzeni, oprócz środowiska cybernetycznego. Cyberprzestrzeń ze względu na charakterystyki, które ją wyróżniają, może przenikać przez pozostałe pierścienie, doprowadzając do destrukcyjnego oddziaływania na przeciwnika. Stanowi ona „pole wojny informacyjnej",

[84] W. Scheffs, *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, „Journal of KONBiN" 2011, nr 3(19), s. 127.

pozwalając na swobodny obieg informacji. Całokształt działań, które obejmuje istota konfliktu informacyjnego można podzielić na:

- **ofensywne** – o charakterze obronnym wobec własnych interesów;
- **defensywne** – wymierzone w stronę zaplanowanego ataku i uznane jako konieczne do uzyskania pożądanej przewagi w obszarze informacyjnym nad przeciwnikiem.

Celem tych działań jest osiąganie zamierzonych priorytetów politycznych. W odniesieniu do tak definiowanych działań, które podejmowane są w ramach walki informacyjnej można wyróżnić dwa, zasadnicze założenia, prowadzące do:

- niszczącego oddziaływania i degradacji wartości zasobów informacyjnych strony przeciwnej i używanych przez nią wszelkich systemów informacyjnych;
- zagwarantowania bezpieczeństwa własnym zasobom i systemom informacyjnym, niwelując prawdopodobieństwo przeprowadzenia na nich cyberataków[85].

3.2. Eurazjatycki i atlantycki model Dugina

Aby zrozumieć eurazjatycki model walki informacyjnej, należy w pierwszej kolejności pojąć istotę nurtu ideologicznego, który współcześnie jest promowany przez Aleksandra Dugina – rosyjskiego historyka religii, filozofa, publicystę i specjalistę do spraw międzynarodowych. Swoją teorię opiera na rozważaniach geopolitycznych. Ich genezę stanowi fundamentalne dzieło w tej dziedzinie pt. „Geograficzna oś historii", autorstwa Halforda Mackindera. Jest ono zbiorem rozważań na temat związków zachodzących pomiędzy geografią, historią i polityką. W opracowaniu Mackinder zakłada, że środowisko naturalne ma znajdować się pod absolutną kontrolą człowieka, chociaż ostatecznie ta zależność okazuje się obustronna. Kontynenty stanowią niewielkie wyspy na „wszechświatowym oceanie". Zgodnie z założeniami Mackindera, panowanie na lądzie zapewnia kontrolę i dominację nad obszarem morza. Kluczem do polityki globalnej z europejskiej perspektywy jest obszar eurazjatyckiego Wielkiego Stepu, który autor nazywa *Heartlandem* (serce kontynentu). *Heartland* obejmuje terytorium północnowschodniej części kontynentu eurazjatyckiego; jest to pas lasów i stepów, ciągnący się od Polski i Węgier aż do Mongolii. Panowanie nad „Wyspą Świata" (Europa-Azja-Afryka Północna) wg „Geograficznej osi historii" daje niezrównane możliwości kontroli nad całą planetą z lądu.

[85] P. Sienkiewicz, *Wizje i modele wojny…*, *op. cit.*, s. 375.

W oparciu o powyższe założenia, Dugin dokonał autorskiego podejścia do aspektów geopolitycznych Rosji. Motywem przewodnim jego publikacji jest konieczność rozszerzenia politycznych i militarnych wpływów kraju. Uważa on, podobnie jak Mackinder, iż uzyskanie panowania nad *Heartlandem* może przynieść bardzo duże korzyści geopolityczne. Utożsamia go kolejno z największymi mocarstwami, do których zalicza terytoria Cesarstwa Rosyjskiego, Związku Socjalistycznych Republik Radzieckich oraz obecnej Federacji Rosyjskiej[86]. Na tej podstawie uważa, że Rosja powinna za wszelką cenę dążyć do utrzymania władzy oraz kontroli w tej części globu. Dugin w swojej tezie zauważa istnienie potęgi, zagrażającej panowaniu na lądzie. Za potęgę uznaje cywilizację, która w sposób naturalny została ukształtowana, aby dążyć do rywalizacji oraz bezpośredniej konfrontacji ze wschodnim mocarstwem. Definiuje ją jako *Sea Power*, identyfikowane z potęgą leżącą na zachodniej półkuli ziemskiej, czyli ze Stanami Zjednoczonymi. Aleksander Dugin stwierdza, że obydwie cywilizacje stanowią dwa, wrogie sobie obozy, znajdujące się po przeciwnych częściach świata. Oznacza to, że „władza Morza" (Zachodu) jest symetrycznie przeciwstawna dla „władzy Lądu" (Wschodu). Szeroko rozumiane strategie działania tych państw są rozgraniczone, ze względu na wyznawane przez nie idee. Obszary podporządkowane Eurazji uznają wartości, do których jest zaliczany:

- **kolektywizm** – czyli pogląd akcentujący w kręgach społeczeństwa ważną rolę wspólnot i zbiorowości. Kolektywizm jest przeciwieństwem indywidualizmu narodowego w kontekście poglądowym pojedynczej jednostki. W związku z tym, wartość ta nawołuje do wspierania celów oraz dobra dla grup;
- s**olidarność w relacjach międzyludzkich** – czyli pogląd wywodzący się bezpośrednio z idei kolektywizmu, nawiązujący do zawierania głębokich więzi w określonej zbiorowości. Oznacza także zjednoczenie jednostek wywodzących się z tej samej narodowości;
- **tradycja** – czyli pogląd spajający na podstawie przekazywanych treści kultury określoną grupę społeczną, która uznała dane wartości jako ważne i niezbędne do rozwoju jej kraju oraz jego przyszłości. Kultura w tym przypadku obejmuje: wierzenia, poglądy, sposób myślenia, zachowania, normy społeczne;
- **wartości duchowe**.

Sea Power, jako przeciwwaga dla terenów eurazjatyckich, wyznaje całkiem odmienne idee poglądowe, na bazie których powstała cywilizacja zachodnia. Dugin zdefiniował ją jako obszary atlantyckie, zbudowane w zgodzie z rozpowszechnionymi w nich wzorcami rzymskimi, opartymi na reli-

[86] K. Kaczyńska, *Koncepcja neo–eurazjatyzmu Aleksandra Dugina*, „Nowy Prometeusz" 2013, nr 5, s. 59-69.

gii katolickiej i protestanckiej. Do wartości, jakimi kieruje się strona atlantycka należą:

- **indywidualizm** – przeciwieństwo dla kolektywizmu, rozpowszechnionego oraz wysoce cenionego na terenach eurazjatyckich. Pogląd przyjmujący jednostkę ludzką, jako najwyższe dobro w społeczeństwie; zaś zaspokojenie jej potrzeb, jako kwestie nadrzędne;
- **liberalizm** – ideologia i kierunek polityczny, promujący szeroko pojmowaną wolność jako największą wartość. Jego cechami charakterystycznymi jest indywidualizm, przeciwstawny kolektywizmowi, wiara w równość, tolerancja, autonomia, wolności indywidualne, integralność cielesna oraz pluralizm polityczny;
- **kapitalizm** – system funkcjonowania gospodarki kraju, oparty na prywatnej własności środków produkcji, z których w ostateczności można czerpać zyski materialne. Kapitalizm polega również na nieskrępowanym obrocie dobrami w ramach wolnego rynku;
- **materializm** – to postawa nawiązująca do rozwoju kapitalizmu. Oznacza, że człowiek jest całkowicie skoncentrowany na wartościach materialnych, takich jak: pieniądze, finanse i zyski. Osobą reprezentującą takie stanowisko nie interesują więzi społeczne oraz budowanie solidarności w relacjach międzyludzkich;
- **globalizm** – zespół przekonań w odniesieniu do procesu globalizacji, opierający się na poglądzie zaprowadzenia ogólnoświatowego dobrobytu, emancypacji jednostek, rozprzestrzenianie się wartości (np. praw człowieka) wskutek czego świat ulegnie znaczącym (w dużym stopniu pozytywnym) zmianom;
- **technokracja** – koncepcja ustroju społecznego, w którym władzę oraz stanowiska najwyższego szczebla sprawowaliby eksperci, posiadający specjalistyczną wiedzę w określonej dziedzinie nauki lub gospodarki o wyjątkowym znaczeniu dla właściwego funkcjonowania państwa. Technokraci wierzą, że promowana przez nich koncepcja może wpływać na zmiany w sferach społecznych i kulturowych. W sferze społecznej gwarantuje profesjonalizację na pełnionych stanowiskach dzięki „ekspertom-specom", kierując się motywami jak najlepszego rozwiązania różnych spraw. W sferze kulturowej oferuje w pewnym stopniu możliwości samodoskonalenia się jednostkom. Według ideologii technokratyzmu wiedza naukowa jest dostępna wyłącznie niewielkiej grupie ludzi.

Według założeń sprecyzowanych przez Aleksandra Dugina, Rosja posiada odpowiednie predyspozycje do stania się największym na świecie mocarstwem lądowym, utożsamionym w pierwszych koncepcjach geopolitycznych z *Heartlandem*. Jednak warunkiem niezbędnym do zdobycia takiej

władzy pozostaje pokonanie potęgi zachodniej, *Sea Power*, cywilizacji atlantyckiej identyfikowaną ze Stanami Zjednoczonymi.

Biorąc pod uwagę tezy bazujące na ideologiach filozoficznych oraz uwarunkowaniach geopolitycznych, można wykazać zróżnicowany obieg informacji wykorzystywany w powyższych mocarstwach – Stanach Zjednoczonych oraz Rosji. Amerykańska walka w przestrzeni cybernetycznej posiada charakter sieciocentryczny (ang. *network centric warfare, netcentric warfare*). W najprostszym rozumieniu, pojęcie sieciocentryczności informacyjnego pola walki oznacza platformę, przeznaczoną do szybkiej i najefektywniejszej wymiany informacji, najczęściej na rzecz wojska, przy użyciu zaawansowanych urządzeń elektronicznych. To rozwiązanie ma na celu zapewnienie pożądanej przewagi nad przeciwnikiem poprzez dystrybucję danych, bez względu na lokalizację geograficzną. W ujęciu wykorzystania sieciocentryczności na potrzeby wojsk amerykańskich, zalicza się także:

- utworzenie nowej infrastruktury informacyjnej sił zbrojnych;
- elementy interaktywne, kompatybilne z zasobami infrastruktury;
- bardzo szybkie łącza, umożliwiające skoordynowany przepływ danych.

Na podstawie analizy sił oraz środków stosowanych przez Stany Zjednoczone, Dugin stwierdza, że podejmowane przez nie działania opierają się głównie na zaawansowanych technologiach i wyszkolonych specjalistach w dziedzinie informatyki, posiadających wiedzę w zakresie skutecznej eksploatacji swoich środków. Dzięki temu są w stanie uzyskać przewagę informacyjną, przekazywaną w czasie rzeczywistym, w celu zwiększenia potencjału bojowego poprzez jej dystrybucję do wszystkich potencjalnych odbiorców. Atlantycki model walki sieciowej określono jako sztuczny proces prowadzący do zwiększenia zapotrzebowania przeciwnika na informacje oraz ograniczenia wrogiej stronie dostępu do nich przy jednoczesnym zapewnieniu jak najszerszego dostępu do danych, użytkując mechanizmy sieciowe i instrumenty sprzężenia zwrotnego, dbając przy tym o szczelną ochronę przed oddziaływaniem przeciwnika[87].

W celu zdobycia nad nim przewagi, Dugin sformułował prognozę rozwinięcia i zmodernizowania rosyjskich środków, po raz pierwszy definiując opracowany przez siebie model eurazjatycki. Rosyjską teorię wojen informacyjnych można określić jako przykład interdyscyplinarnej nauki stosowanej. Odnosi się do bardzo szerokiego zakresu działań o charakterze sprowadzającym się do osiągania zamierzonych celów: politycznych, gospodarczych, społecznych, militarnych, wywiadowczych, kontrwywiadowczych, dyplomatycznych, propagandowych, psychologicznych, informa-

[87] A. Dugin, *Gieopolitika postmodierna*, (przeł) P. Sieradzan, „Geopolityka" 2009, nr 1(2).

tycznych, jak również edukacyjnych[88]. Kierując się chęcią dorównania sieciocentrycznej platformie wykorzystywanej przez Stany Zjednoczone, według założeń Dugina, należy powołać kadrę składającą się z wysokich urzędników, intelektualistów, służb specjalnych, politologów, ludzi nauki, działaczy na rzecz kultury oraz patriotycznie zorientowanych dziennikarzy. W ten sposób, możliwy będzie do osiągnięcia efekt łączący w sobie elementy podejścia sieciocentrycznego, rozpowszechnionej na Zachodzie „postmoderny" z rosyjską specyfiką prowadzenia walki informacyjnej[89]. Jest ona określona jako zjawisko skoncentrowane na oddziaływaniu na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w cyberprzestrzeni, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi a stosowane w charakterze **broni informacyjnej**[90]. Aby model eurazjatycki był skuteczny, musi zostać przeprowadzona modernizacja wszystkich rosyjskich instytucji, organizacji, służb oraz łączy sieciowych i komunikacyjnych. Oznacza to, że wektory oddziaływania informacyjnego symetrycznie zestawionych ze sobą modeli byłyby skierowane w przeciwnych kierunkach rażenia sieciowego.

3.3. Model walki informacyjnej Panarina

Kolejnym przykładem schematu prowadzenia walki informacyjnej jest model opracowany przez politologa i profesora Akademii Dyplomatycznej Ministerstwa Spraw Zagranicznych Federacji Rosyjskiej – Igora Panarina. Swoją teorię oparł na konieczności aktywnego przeciwdziałania Rosji wobec Stanów Zjednoczonych w kontekście operacji informacyjnych. Wyróżnia dwa znaczące dla Federacji Rosyjskiej wydarzenia, które określa jako wyraz agresji Zachodu. Są nimi:

- ***pierestojka*** – zakończona rozpadem Związku Socjalistycznych Republik Radzieckich w 1991 r., uznanego za największe, współczesne mocarstwo lądowe na świecie;
- **rywalizacja** – m.in. w aspektach postępu technologii, szczególnie widoczna na początku obecnego tysiąclecia. Według prognoz Panarina zakończy się ona w 2020 r. dominacją *Dobra*, czyli przewagą rosyjskiego modelu eurazjatyckiego nad amerykańskim modelem atlan-

[88] M. Orzechowski, *Koncepcja walki informacyjnej jako element bezpieczeństwa Federacji Rosyjskiej. Wojna w Donbasie jako study case zastosowania elementów walki informacyjnej* [w:] *Polska – Rosja, Polityka bezpieczeństwa Federacji Rosyjskiej*, red. M. Kaszub, M. Minkin, Wydawnictwo UPH, Siedlce 2016, s. 105.

[89] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, OSW, Warszawa 2014, s. 17-18.

[90] M. Orzechowski, *Koncepcja walki informacyjnej…*, *op. cit.,* s. 105.

tyckim[91].

Igor Panarin zakłada, że współczesne ataki informacyjne są inicjatywą wyłącznie Stanów Zjednoczonych w celu sterowania społeczeństwem przy użyciu własnych, bardzo rozwiniętych technologicznie narzędzi agresji informacyjnej. Podobnie jak Aleksandr Dugin, określa je jako procesy sztuczne, opierające się wyłącznie na wysoce zaawansowanych środkach technicznych. W swoich opracowaniach wyróżnia trzy aspekty prowadzenia wojny w cyberprzestrzeni, w zgodzie z założeniami Dugina w kontekście rosyjskiej walki informacyjnej jako rodzaju broni wykorzystującego ludzką świadomość na postrzeganie otaczającej rzeczywistości. Jako pierwszy aspekt Panarin definiuje działania, będące w praktyce faktycznymi operacjami oddziaływania, do których zalicza[92]:

- **sterowanie społeczne** – jest to świadome wywieranie wpływu na zachowanie lub sposób myślenia danej społeczności, którego celem jest osiągnięcie określonych zamierzeń. W kontekście informacyjnym, sterowanie społeczne oznacza oddziaływanie na świadomość ludzką oraz na procesy poznawcze, emocje, motywacje czy kształtowanie trwałych postaw, poprzez selektywne sterowanie dopływem informacji polegającym np. na wpajaniu pozytywnych i negatywnych uprzedzeń, ukierunkowanie zainteresowań, nadawanie informacjom kształtu pożądanego odbioru przez społeczeństwo;
- **manewrowanie społeczne** – jest to intencjonalna forma sterowania jednostkami ludzi dla osiągnięcia zamierzonych korzyści. Manewrowanie społeczne dąży do podporządkowania sobie pewnej zbiorowości obywateli danego państwa przez stronę przeciwnika (np. władze wrogiego kraju) zdefiniowanego jako **infoagresor**. Z pomocą pozyskanych grup, infoagresor może za ich pośrednictwem przejąć kontrolę nad zasobami i strukturami kraju będącego obiektem cyberataku;
- **manipulacja informacją** – działanie polegające na zakamuflowanym oddziaływaniu na zachowania oraz świadomość jednostek i grup społecznych w celu realizacji zaplanowanych zamierzeń. Obejmuje szereg technik, takich jak: moralizatorstwo (np. natrętne pouczenia i upomnienia), prowokacje (np. nakłanianie jednostek do wykonania czynności, której w normalnych warunkach nie dokonałaby), ośmieszanie osób (np. prowokowanie sytuacji, w których podmiot manipulacji jest wyśmiewany), przekazywanie fałszywych lub zniekształconych informacji (np. zmiana formy i treści informacji bądź ich ukrywanie), upowszechnianie stereotypów narodowych bądź rasowych

[91] J. Darczewska, *Anatomia rosyjskiej wojny…*, *op. cit.*, s. 14-15.
[92] *Ibidem*, s. 14.

(np. w postaci skrótowego obrazu grupy ludzi funkcjonujący w świadomości członków innej grupy);
- **dezinformacja** – polega na celowym zafałszowaniu istniejącej informacji i przekazanie jej na forum społeczeństwa, by wprowadzić je w błąd. Dezinformacja ma szczególne znaczenie w aspektach bezpieczeństwa i obronności państwa. Jej przykładem może być wprowadzanie w błąd przeciwnika na temat posiadanej broni atomowej, która w rzeczywistości nie istnieje;
- **fabrykowanie informacji** – proces określony jako wytwarzanie nowej informacji w celu jej zafałszowania a następnie rozpowszechnienia w społeczeństwie;
- **lobbing** – działanie zmierzające do wywierania wpływów przez wyspecjalizowanych rzeczników interesów na organy władzy publicznej oparte na strategii komunikacyjnej. Lobbing uwzględnia uporządkowany cykl, do którego należą: analiza procesów decyzyjnych, polityka określonego organu, własne cele strategiczne, własna analiza SWOT, prowadzenie bieżącego monitoringu wydarzeń;
- **szantaż** – forma działalności przestępczej, bazująca na próbach zmuszenia danej jednostki do wykonania określonego działania, jego zaniechania lub ujawnienia pewnych (częściowo lub w pełni prawdziwych) informacji przy użyciu narzędzi w postaci groźby słownej lub fizycznej przemocy;
- **wymuszanie pożądanej informacji** – forma działalności przestępczej, polegająca na posługiwaniu się groźbami słownymi lub fizyczną przemocą w celu pozyskania informacji o znaczącym i ważnym charakterze.

Następnym czynnikiem wyróżnionym przez Panarina są narzędzia prowadzenia rosyjskiej wojny informacyjnej w cyberprzestrzeni. Po zorientowaniu podjętych działań, stwierdza, że należy posłużyć się odpowiednimi środkami, bezpośrednio oddziałujących na daną zbiorowość ludzi. Wśród tych narzędzi dokonał podziału na tajne i jawne, po czym wyróżnił[93]:
- **propagandę** – jedno z narzędzi oparte na celowym działaniu zmierzającym do ukształtowania poglądów, zachowania i sposobu myślenia określonej grupy ludzi, polegające na manipulacji emocjonalnej oraz intelektualnej. Do rodzajów propagandy zalicza się: propagandę czarną (źródłem informacji jest fałszywy nadawca), propagandę szarą (źródło i pochodzenie informacji dla odbiorcy pozostaje nieznane) i propagandę białą (źródło i pochodzenie informacji jest wiarygodne);

[93] J. Darczewska, *Anatomia rosyjskiej wojny…*, *op. cit.*, s. 14.

- **wywiad** – zdefiniowany jako służba specjalna, powołana do pozyskiwania niejawnych informacji o przeciwniku, zajmująca się ich przetwarzaniem, przechowywaniem, analizą oraz przekazywaniem władzy;
- **komponent analityczny** – w ujęciu prowadzenia wojny informacyjnej jest to działanie opierające się na nieprzerwanej kontroli *mass mediów* przy jednoczesnej analizie bieżącej sytuacji lub zachodzących zmianach w monitorowanym otoczeniu;
- **komponent organizacyjny** – w ujęciu prowadzenia wojny informacyjnej jest to całokształt struktury zarządzającej w procesie toczonych operacji w przestrzeni cybernetycznej, do których można zaliczyć m.in. kanały koordynacyjne i sterownicze lub organy państwowe mające szczególny wpływ na kształt informacji przekazywanych przez media;
- **inne kanały sprzężone** – nawiązujące w znacznej mierze to działań dywersyjnych.

Zwracając uwagę na współczesne realia zachodzących na świecie procesów, Panarin wyodrębnia, w przyjętej przez siebie teorii walki informacyjnej, model łańcucha zarządzania. Musi zostać on całkowicie przystosowany i być adekwatny do narodowego systemu sterowania telekomunikacją. Ponadto ocenia, że skuteczne oddziaływanie za pomocą praktycznych operacji, przy użyciu odpowiednio dobranych narzędzi, powinno zostać wzbogacone o doświadczenia Chin oraz Stanów Zjednoczonych[94]. W tym celu określił sekwencję zarządczą, wykonywaną kolejno w poniższych etapach[95]:

- **planowanie i prognozowanie** – dwa, przebiegające ze sobą równolegle procesy, spełniające odmienne funkcje, jednak stanowiące skuteczny oraz jednolity schemat postępowania. Planowanie operacji informacyjnej oznacza określoną formę postępowania, dotyczy elementów i środków używanych do wdrożenia danego planu. Istotą prognozowania jest zdolność do przewidywania zachodzących zjawisk, na które wpływ oraz ewentualna interwencja są niemożliwe;
- **organizacja i stymulowanie** – organizowanie obejmuje zestaw czynności, opierających się na pozyskaniu niezbędnych zasobów (np. ludzkich, informacyjnych, finansowych), pozwalających na faktyczne wykonanie zamierzonych celów. W ujęciu walki informacyjnej, stymulowanie jest dążeniem do wysłania informacji, stworzeniem do tego odpowiednich warunków i koordynowaniem jej przepływu;

[94] *Ibidem*, s. 16.
[95] J. Darczewska, *Anatomia rosyjskiej wojny…*, *op. cit.*, s. 15.

- **sprzężenie zwrotne** – czyli informacja zwrotna, otrzymywana dzięki oddziaływaniu sygnałów stanu wyjściowego systemu, układu lub procesu na sygnały wejściowe;
- **korygowanie operacji** – polega na poprawie ewentualnych odchyleń w czasie prowadzenia operacji informacyjnej, które mogą być decydujące dla jej obiegu;
- **kontrola wykonania** – koncepcja teoretyczna, która może zostać wdrożona jako działanie praktyczne, na którą składają się: procedury, instrukcje, zasady i mechanizmy. Kontrola wykonania operacji wspomaga proces zarządzania, doprowadzający do pozyskania pożądanej informacji a tym samym osiągnięcia zamierzonych celów.

3.4. Model walki informacyjnej Libickiego

Innym przykładem teorii sprowadzającej się do wieloaspektowej istoty wojny informacyjnej jest współczesny model walki sieciowej opracowany przez Martina Libickiego. Określa on przestrzeń cybernetyczną jako wirtualne medium, znacznie mniej wymierne niż ziemia, woda, przestrzeń powietrzna i kosmiczna, a nawet otoczenie rozchodzenia się widma fal elektromagnetycznych.. Stwierdza, że jednym z podstawowych sposobów zrozumienia funkcjonowania cyberprzestrzeni w roli środowiska wykorzystywanego do prowadzenia ataków sieciowych (cyberataków), jest jego podział na zasadnicze, trzy warstwy (rysunek 3).

Warstwami tymi są:

- **warstwa fizyczna** – zaliczają się do niej wszystkie składowe danego systemu informacyjnego, do których należą: urządzenia elektroniczne (np. komputery), przewody, kanały komunikacyjne i telekomunikacyjne itp. Stanowi ona fundament istnienia dowolnego systemu, nadając mu materialną formę;
- **warstwa syntaktyczna** (znajdująca się ponad warstwą fizyczną) – poziom ten zawiera instrukcje, które projektanci i użytkownicy przekazują komputerowi i protokołom, dzięki którym maszyny współdziałają z innym, rozpoznanym urządzeniem w zakresach: pakietowania, adresowania, trasowania, formatowania dokumentów, manipulowania bazą danych itd. Jest to szczególna sfera w kontekście zagrożeń ze strony sieciowych hakerów, którzy najczęściej w niej działają;
- **warstwa semantyczna** (stanowiąca ostatni element w hierarchii i znajdująca się nad pozostałymi warstwami) – zawiera informacje, które są przechowywane w stworzonych do tego urządzeniach, czyli

pamięci komputerów. Niektóre informacje, takie jak tabele wyszukiwania adresu lub kody kontroli drukarki, są przeznaczone do manipulacji systemem; są one w formie semantycznej (dotyczącej samej informacji), ale w składni syntaktycznej (dotyczącej procesu). Inne informacje, takie jak instrukcje cięcia lub informacje o kontroli procesu dotyczą komputerów sterowanych automatycznie[96].

Rysunek 3. Podział funkcjonowania cyberprzestrzeni na warstwy według modelu Libickiego
Źródło: opracowanie własne.

Bazując na przyjętych przez siebie założeniach w odniesieniu do warstwowej budowy cyberprzestrzeni, Libicki wyróżnił siedem form prowadzenia w niej walki informacyjnej[97]. Pojęcie wojny sieciowej definiuje jako zaistniały konflikt, który uaktywnia procesy, do których zalicza: szczególną ochronę, manipulację, degradację i niedostarczenie informacji. Uwzględniając zachodzące zjawiska jako praktyczne operacje, zdefiniował poniższe schematy, dokonując typologii oddziaływania sieciowego na:

– **walkę systemów dowodzenia i kierowania** [ang. *Command and Control Warfare* (C2W[98])] – jako konflikt uniemożliwiający sprawną realizację procesów decyzyjnych na najwyższych szczeblach zarówno

[96] M.C. Libicki, *Cyberdeterrence and cyberwar*, RAND Corporation 2009, s. 12.
[97] M.C. Libicki, *What is Information Warfare?*, National Defense University, Center for Advanced Concepts and Technology, Washington D.C. 1995, s. 1.
[98] Akronim od anglojęzycznych słów – ang. *Command and Control* (oznaczanych często jako – C2) – dowodzenie i kierowanie.

dowodzenia, jak i kierownictwa oraz przenikanie informacji do wykonawców powierzonych funkcji;

- **walkę wywiadowczą** (ang. *Intelligence Based Warfare* – IBW) – jako konflikt polegający na dwóch, jednocześnie przebiegających działaniach: ochronie i monitoringu swoich własnych systemów informacyjnych oraz podjęcia wszelkich wysiłków i zaangażowania środków, zmierzających do pozbawienia strony przeciwnika istotnych danych lub zasobów wiedzy, które potencjalnie mogłyby doprowadzić go do dominacji na polu walki;
- **walkę elektroniczną** (ang. *Electronic Warfare* – EW) – jako konflikt stosujący własne środki emisji elektromagnetycznej w celu zakłócenia przepływu informacji lub całkowitego uniemożliwienia działań wrogiej stronie bądź wykorzystywanym przez niego wszelkim środkom technicznym. Spośród form walki radioelektronicznej można wyróżnić: aktywną i pasywną walkę radioelektroniczną oraz wsparcie elektroniczne;
- **wojnę psychologiczną** (ang. *Psychological Operations* – PSYOPS) – jako konflikt zawierający system zabiegów, najczęściej o charakterze propagandowym, wymierzony w społeczeństwo w celu wywarcia na nie wpływu oraz zaprowadzenia zmiany poglądów na określony temat przy użyciu zasobów zmanipulowanej informacji;
- **wojna „hakerska"** lub **wojny hakerów**[99] (ang. *hackerwar software based attacks on information systems*) – jako konflikt dążący do zaatakowania systemów łączności oraz komputerów przeciwnika przez osoby będące w posiadaniu licznych i praktycznych umiejętności z zakresu informatyki, które są w stanie naruszyć bezpieczeństwo informacyjne oraz pozyskać przechowywane zasoby;
- **ekonomiczną walkę informacyjną** (ang. *Information Economic Warfare* – IEW) – jako konflikt opierający się w głównej mierze na blokowaniu dopływu informacji, fałszowaniu i manipulowaniu jej treścią

[99] **Haker** – „osoba o bardzo dużych praktycznych umiejętnościach informatycznych, odznaczająca się znajomością wielu języków programowania, a także świetną znajomością systemów operacyjnych oraz bardzo dobrą orientacją w Internecie. Hakerzy, którzy mają bardzo dobrą wiedzę, mogą wpłynąć nawet na lepszy poziom bezpieczeństwa banków i instytucji państwowych, ale mogą im także zaszkodzić. W języku potocznym słowo **haker** stało się synonimem komputerowego włamywacza i przestępcy komputerowego, który korzystając ze zdalnych środków dostępu, dokonuje włamań do systemów informatycznych dla zabawy bądź w innym celu. Należy jednak pamiętać, że sam *hacking* nie jest czymś złym. Jest to szukanie nowych rozwiązań, wzbogacanie umiejętności, po to, by być najlepszym w danej dziedzinie informatyki. Hakera można nazwać dopiero przestępcą, gdy wykorzystuje wiedzę w celu popełnienia przestępstwa",
Encyklopedia Gazety Prawnej, online – http://www.gazetaprawna.pl/encyklopedia/prawo/hasla/332774,haker.html [dostęp: 02.07.2017].

w celu osiągnięcia zaplanowanych zamierzeń wymierzonych w funkcje gospodarcze państwa, które w znacznym stopniu mogą doprowadzić do destabilizacji jego bezpieczeństwa narodowego;
- **wojnę cybernetyczną** (ang. *cyberwar*) – jako konflikt sprowadzający się do wykorzystania komputerów, łączy sieciowych i każdych innych środków zdolnych do przechowywania lub rozsyłania informacji celem przeprowadzenia cyberataku na systemy przeciwnika po zaplanowaniu wielowariantowych scenariuszy, często o charakterze futurystycznym[100].

3.5. Uogólnienia i wnioski

Przedstawiona istota wybranych modeli walki informacyjnej w przestrzeni cybernetycznej wskazuje przede wszystkim na wieloaspektowość oraz wielowariantowość prowadzonych w niej działań. Stanowią one teoretyczne założenia wykorzystania cyberprzestrzeni do osiągania zamierzonych celów, najczęściej za pomocą aktów cybernetycznych. Zatem nie może być ona rozumiana jako jednolity, wirtualny obszar, pozwalający na określony zespół wykonywanych w niej czynności. Należy podkreślić, że opracowane i opisane wyżej modele nie są ze sobą w żaden sposób powiązane lub posiadają wyłącznie kilka wspólnych cech. Wskazuje to na zróżnicowane spojrzenie na środowisko cybernetyczne i wojny informacyjne, dające duże możliwości wpływania na zachodzące w niej procesy. Jednym z czynników zorientowanych na złożoność cyberprzestrzeni jest jej podział na warstwy, zgodnie z modelem walki sieciowej według Libickiego. Koncepcja ta zwraca szczególną uwagę na fakt, że żadna z wymienionych warstw nie może istnieć bez urządzeń elektronicznych. Teoria dekapitacji według Wardena zakłada, iż największe oddziaływanie na przeciwnika jest możliwe przy trafnie określonym środku ciężkości (ang. *Centre of Gravity* – CoG) przy użyciu charakterystyk cyberprzestrzeni, przenikających wszystkie, zdefiniowane kręgi. Rosyjskie modele wojny informacyjnej uwzględniają podział technologiczny na Wschód (Rosja) i Zachód (Stany Zjednoczone) oraz wartości narodowe i kulturowe, które mają kluczowe znaczenie dla dalszego rozwoju praktycznych działań prowadzonych w przestrzeni cybernetycznej. Dodatkowo wyróżniają one nie tylko zacho-

[100] J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Difin, Warszawa 2014, s. 211; R. Bielawski, A. Radomska, *Selected models of information warfare in cyberspace*, „Security and Defence Quarterly" 2017, nr 1(14), s. 35-50.

dzące w niej procesy wymierzone w społeczeństwo, ale także narzędzia, czyli wszelkie środki bezpośrednio oddziałujące na daną zbiorowość ludzi po zorientowaniu zespołu działań. Aby proces ten przebiegał zgodnie z określonymi standardami, dokonano ustalenia łańcucha zarządzania, skupionego wyłącznie na procesach informacyjnych.

ROZDZIAŁ 4.
Ewaluacja zagrożeń bezpieczeństwa narodowego w cyberprzestrzeni

4.1. Obiekty zagrożeń z cyberprzestrzeni wpływające na bezpieczeństwo narodowe

Analizując literaturę przedmiotu można dokonać podziału obszarów zagrożeń ataków cybernetycznych, których przedmiotem są organy państwa. Jedna z literaturowych propozycji dzieli je na trzy podstawowe systemy: wojskowe, przedsiębiorstw oraz wchodzące w skład tzw. infrastruktury krytycznej państwa[101]. W dalszej analizie celowo pominięto systemy kluczowych przedsiębiorstw państwa. Badania wstępne dowiodły, że element ten wpływa na bezpieczeństwo cyberprzestrzeni w najmniejszym stopniu.

4.1.1. Zagrożenia cybernetyczne systemów wojskowych[102]

Bezpieczeństwo cyberprzestrzeni na świecie, jak również w poszczególnych krajach, utrzymywane jest przez brak ujawnienia niejawnych informacji, za które odpowiadają służby zajmujące się bezpieczeństwem teleinformatycznym państwa. Zazwyczaj ich działalność skupiona jest w strukturach militarnych, które nie ujawniają swoich możliwości, mając na uwadze ewentualne zagrożenia związane z utratą cennych informacji, w przypadku rozpoznania ich systemów przez przeciwnika. Przedmiotem ataków na systemy wojskowe państwa mogą być: informacje o położeniu satelitów, rozmieszczeniu wojsk i broni, prowadzących badania nad nowymi rozdziałami broni, systemów łączności itp. Najwięcej włamań tego typu zanotowano podczas trwania zimnej wojny, a głównie odpowiadają za to agenci innych wywiadów.

---

[101] M. Jędrzejewski, *Analiza systemowa zjawiska infoterroryzmu*, AON, Warszawa 2002, s. 22.

[102] Fragmenty niniejszego rozdziału pierwotnie opublikowano w: B. Grenda, *Sieciocentryczne zarządzanie siłami powietrznymi,* „Journal of KONBiN" 2011, nr 3(19), s. 299-314.

Współcześnie uznaje się działania militarne w cyberprzestrzeni za środowisko prowadzenia walki. Poszczególne kraje rozwijają swoje zdolności obronne w cyberprzestrzeni. Tworzą zatem odpowiednie struktury w siłach zbrojnych, jak również prowadzą badania nad nowymi rodzajami cyberbroni, budując w ten sposób własne zasoby odstraszania potencjalnych przeciwników. Państwa tworzą także strategie dotyczące obrony, jak również oficjalnie mówią o atakach odwetowych w cyberprzestrzeni. W tym kontekście należy wspomnieć o amerykańskim projekcie o nazwie „Olympic Games", którego celem było powstrzymanie irańskiego programu nuklearnego m.in. za pomocą specjalnie opracowanego do tego celu robaka – Stuxnet. Kwestie cyberobrony zostały także ujęte w dwóch ostatnich deklaracjach przyjętych na szczytach NATO w 2010 i 2012 r. Trudno jednak stwierdzić, czy atak na jednego z członków Sojuszu Północnoatlantyckiego rzeczywiście uruchomi wszystkie mechanizmy związane z art. 5 traktatu waszyngtońskiego[103] i jaka będzie skala ewentualnych działań w tym zakresie[104].

Przed przystąpieniem Polski do NATO (przed rokiem 1999) obronność była integrowana z pojęciem „obrony narodowej". Celem działań było niwelowanie zagrożeń o charakterze militarnym oraz zjawisk pokrewnych. Współcześnie wypracowana definicja określa, iż obronność jest dziedziną bezpieczeństwa narodowego, która obejmuje zintegrowane przeciwstawianie się zagrożeniom polityczno-militarnym przy wykorzystaniu wszystkich wojskowych, jak również cywilnych zasobów państwa, zorganizowanych w systemie obronnym.

Na podstawie „Strategii Obronności Rzeczpospolitej Polskiej" można sformułować priorytety w zakresie obronności, do których należą:

- zapewnienie niepodległości i suwerenności PR, jej integralności i nienaruszalności granic;
- obrona jak również ochrona każdego obywatela RP;
- tworzenie warunków do podwyższania zdolności obronnych kraju, jak również zapewnienie gotowości do realizacji obrony w układzie narodowym i sojuszniczym;
- tworzenie warunków do zapewniania ciągłości realizacji zadań przez organy administracji publicznej oraz inne podmioty właściwe w obszarze bezpieczeństwa narodowego, w tym odpowiedzialne za funkcjonowanie gospodarki i innych obszarów istotnych dla życia i bez-

[103] Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. z 2000 r. Nr 87, poz. 970).

[104] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu* [w:] *Bezpieczeństwo narodowe* II – 2012*,* nr 22, BBN, Warszawa 2012, s. 128–129.

pieczeństwa obywateli;
- rozwijanie partnerskiej współpracy wojskowej z innymi państwami, np. z sąsiadami;
- realizacja zadań wynikających z członkostwa Polski w NATO oraz w Unii Europejskiej;
- zaangażowanie w międzynarodowe operacje reagowania kryzysowego, prowadzone w pierwszej kolejności przez NATO, UE oraz Organizację Narodów Zjednoczonych (ONZ)[105].

Nieprzewidywalny charakter współczesnego bezpieczeństwa zmusza siły zbrojne, jak również jednostki odpowiedzialne za funkcjonowanie Systemu Obronnego Państwa do tego, aby był on przygotowany na prawdopodobne zagrożenia, a także posiadał wystarczający zasób środków do reagowania na nie. Dodatkowo osoby odpowiedzialne za ten system powinny być odpowiednio przeszkolone i gotowe do działania w poszczególnych stanach gotowości państwa[106]. Gotowość obronna państwa jest to stan stabilności elementów systemu obronnego państwa do utrzymania bezpieczeństwa narodowego, skutecznego działania w sytuacjach nadzwyczajnych, w tym także możliwość przeciwstawiania się wszelkim zagrożeniom kryzysowym oraz wojennym[107], a także tym pochodzącym z cyberprzestrzeni.

Gotowość obronną państwa możemy podzielić na:
- stałą gotowość obronną kraju – jest to stan utrzymywany w czasie pokoju, gdy stosunki międzynarodowe układają się poprawnie, natomiast możliwe konflikty rozstrzygane są na drodze dyplomatycznej. Główne zadanie w ramach obronności to: utrzymanie sprawności oraz doskonalenie Systemu Obronnego Państwa;
- gotowość obronną w czasie kryzysu – jest to stan podniesienia gotowości obronnej w czasie pojawienia się symptomów bezpośredniego zagrożenia kryzysowego oraz wojennego. Główne zadania w ramach obronności to: osiąganie przez całe siły zbrojne wyższych stanów gotowości bojowej, realizacja określonych zamierzeń związanych z militaryzacją oraz obroną cywilną;
- gotowość obronną w czasie wojny – jest to stan, który osiąga się w razie stwierdzenia bezpośrednich przygotowań do agresji lub w wyniku jej dokonania. Główne zadania w ramach obronności to: rozwinięcie sił zbrojnych Rzeczpospolitej Polskiej, przegrupowanie

[105] *Strategia Obronności Rzeczpospolitej Polskiej*, Warszawa 2009, s. 8-10.
[106] J. Wojnarowski, *Gotowość systemu bezpieczeństwa narodowego*, Wydawnictwo, Warszawa 2010, s. 21.
[107] I. Dziubek, *Antyterrorystyczne przygotowanie żołnierzy wojsk lądowych. Wybrane problemy*, AON, Warszawa 2010, s. 33.

ich do rejonów operacyjnego przeznaczenia, zademonstrowanie politycznej woli państwa do przeciwstawienia się agresji zbrojnej[108].

Celem kierowania obronnością państwa jest przede wszystkim zagwarantowanie w okresie pokoju, kryzysu oraz wojny odpowiednich warunków do szybkiego i kompetentnego podejmowania decyzji, jak również dostosowania działań przez organy władzy, administrację publiczną i organy dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej[109] (SZ RP).

System obronny RP można podzielić na trzy podsystemy: kierowania, militarny (stanowią go SZ RP) oraz niemilitarny. Podsystem militarny złożony jest z Sił Zbrojnych RP i jest podstawowym systemem obronnym państwa przeznaczonym do skutecznej realizacji polityki bezpieczeństwa.

W związku z powyższym należy podkreślić, że system obrony państwa oraz cyberbezpieczeństwo to ogniwa wyżej wskazanej typologii. Należy także mieć na uwadze, że stan taki może eskalować zgodnie ze stopniami gotowości bojowej oraz kryzysowej, co wydaje się być logiczne.

Cyberbezpieczeństwo w kontekście militarnym zależy niewątpliwie od stopnia zaawansowania technologicznego. W tym aspekcie zaawansowanie takie można utożsamić z **sieciocentrycznością**, a ściślej **walką sieciocentryczną** (ang. *Network Centric Warfare*). Etymologia tego pojęcia wywodzi się z literatury anglojęzycznej i dotyczy organizacji procesu gromadzenia, przetwarzania, selekcji oraz dystrybucji informacji, który zapewnia dostępność potrzebnych danych we właściwym miejscu i czasie. Co ważne w procesie tym pomijany jest czynnik lokalizacji geograficznej[110].

Ideą sieciocentryczności jest zwiększenie potencjału nie przez rozbudowę ilościową środków i stanu liczbowego sił, a przez efektywne wykorzystanie i dystrybucję przez dowódców aktualnej i wiarygodnej informacji. Według J. Garstki – jednego z twórców tej koncepcji, podstawą jest założenie zwiększenia efektywności działań, poprzez połączenia z globalną strukturą sieciową wszystkich jej składników, tj. środków decyzyjnych, sensorów oraz efektorów. Ma to zapewnić, pomimo odległości, uzyskanie zsynchronizowanej czasowo oraz przestrzennie świadomości sytuacji wszystkich uczestników sieci. Innymi słowy, tę samą informację powinien mieć każdy element w danym systemie[111].

Według analityków Pentagonu są dwa sposoby udrożnienia przyszłych systemów. Po pierwsze – zbieranie danych z różnych źródeł w centralnym

---

[108] I. Dziubek, *Edukacja obronna w Polsce*, Zysk i S-ka, Poznań 2013, s. 124-127.

[109] *Strategia Obronności Rzeczpospolitej…*, *op. cit*., s. 11-13.

[110] A.K. Cebrowski, J.J. Garstka, *Network Centric Warfare, Its Origin and Future* [w:] *Proceedings of the Naval Institute* 124:1, January 1998, s. 28-35.

[111] J.J. Garstka, *Theory and practise of Network Centric Warfare*, Materiały z konferencji „Conference Documentation from Network Centric Warfare Conference", London, 10-11th September 2001.

magazynie informacji, z którego korzystać mogliby różni odbiorcy, zgodnie ze swoimi potrzebami i uprawnieniami. Po drugie – masowe udrożnienie systemu opartego o IP, w którym każdy odbiorca ma przydzielony własny adres IP i trafia do niego informacja indywidualna[112].

Walka sieciocentryczna jest definiowana jako opierająca się na przewadze informacyjnej koncepcja prowadzenia operacji, według której wzrost siły bojowej jest generowany poprzez połączenie w sieć informacyjną sensorów, decydentów oraz systemów walki w celu osiągnięcia wspólnej świadomości, zwiększania szybkości dowodzenia, jak również tempa operacji, skuteczności uzbrojenia, odporności na uderzenia przeciwnika oraz stopnia synchronizacji działań. Działania sieciocentryczne mają znaczną przewagę informacyjną nad siłę bojową poprzez wydajne połączenie na polu (czyli w przestrzeni walki) różnych jednostek organizacyjnych dysponujących wiedzą. Sieciocentrycznym polem walki jest przestrzeń, która obejmuje powietrze i przestrzeń kosmiczną, ląd, wodę, a także siły, jak również środki własne i przeciwnika, pogodę, teren i spektrum elektromagnetyczne w obszarze działań oraz w obszarze zainteresowań[113]. Przestrzeń walki sieciocentrycznej jest bardzo złożona ze względu na swoją wielowymiarowość, jak również dużą liczbę zróżnicowanych elementów ją tworzących. Nie ogranicza się ona do przestrzeni trójwymiarowej, rozciąga się również na spektrum elektromagnetyczne, jak też tzw. przestrzeń informacyjną[114]. Przestrzeń, w której toczy się walka sieciocentryczna, dzieli się np. na domeny, warstwy i sieci.

Wśród domen wyróżniamy[115]:

- **domenę fizyczną** – są to działania tradycyjne. W jej zakres wchodzą uderzenia, obrona oraz manewr we wszystkich wymiarach (lądowym, morskim, powietrznym i kosmicznym). Znajdują się w niej stanowiska dowodzenia, systemy uzbrojenia i sieci, które je łączą;
- **domena informacyjna** – obejmuje ona tworzenie, przetwarzanie oraz współużytkowanie informacji. W tej domenie następuje wymiana informacji między siłami biorącymi udział w walce, komunikowanie się odpowiednich ośrodków dowodzenia i sztabów, jak również przekazywanie intencji dowódców. Domena informacyjna powinna być szczególnie chroniona i broniona, ponieważ jej wpływ na wzrost zdolności bojowych jest bardzo duży, szczególnie w walce o zdobycie

[112] A.K. Cebrowski, *Network Centric Warfare*, *An Emerging Military Response to the Information Age.* Command and Control Research and Technology Symposium, Naval War Collage, Newport, RI, June 2003.
[113] *Concept for Future Joint Operations*, Joint Chiefs of Staff, 1997, s. 83.
[114] B. Grenda, *Sieciocentryczne zarządzanie siłami powietrznymi,* „Journal of KONBiN" 2011, nr 3(19), s. 301-302.
[115] *Ibidem*.

przewagi informacyjnej;

- **domena poznawcza** – istnieje ona jedynie w umysłach uczestników walki sieciocentrycznej. Elementami tworzącymi tę domenę są: przywództwo, morale, spójność jednostki, jakość wyszkolenia, świadomość sytuacji czy opinia publiczna. W tej domenie zawarte są też: zamiary działania, doktryny, taktyka postępowania oraz procedury działania.

Omawiana przestrzeń walki sieciocentrycznej składa się również z warstw, które dzielimy na[116]:

- **warstwę dowodzenia** – jest tą częścią składową przestrzeni walki sieciocentrycznej, w której dobrze wyszkolony personel dokonuje oceny sytuacji, analizuje poszczególne zadania, planuje działania oraz bezpośrednio zarządza walką;
- **warstwę walki** – to samoorganizująca się sieć elementów ugrupowania bojowego bazująca na wiarygodnej wiedzy o sytuacji bojowej;
- **warstwę informacyjną** – która polega na korelacji danych z sensorów a informacja dostarczana jest do systemów walki na wszystkich szczeblach;
- **warstwę sensorów** – która składa się z licznych różnorodnych urządzeń rozpoznawczych, np. bezzałogowych systemów powietrznych, naziemnych stacji radiolokacyjnych lub czujników ruchu. Ich zadaniem jest zbieranie informacji o sytuacji na lądzie, morzu czy w powietrzu, jak i w przestrzeni elektromagnetycznej[117].

Ostatnim elementem podziału walki sieciocentrycznej są sieci, które dzielimy na[118]:

- **sieć informacyjną** – która umożliwia wymianę, przetwarzanie, przechowywanie oraz ochronę informacji. W jej skład wchodzą: kanały łączności, węzły informatyczne, systemy operacyjne i zarządzanie informacjami. Możliwości techniczne tej sieci pozwalają na wygenerowanie przez sieć czujników świadomości sytuacyjnej, co jest podstawą uzyskania przewagi informacyjnej. Świadomość sytuacyjna jest spełniona, jeśli mamy dostateczną wiedzy na temat sił własnych i przeciwnika[119];
- **sieć czujników** – zapewnia ona walczącym siłom uzyskanie świadomości sytuacji w przestrzeni walki. Sieć ta jest postrzegana jako ze-

---

[116] *Ibidem*.

[117] E. Michalewski, *Analiza systemów sieciocentrycznych*, Polskie Stowarzyszenie Zarządzania Wiedzą, „Seria: Studia i Materiały" 2010, nr 32, s. 147–149.

[118] B. Grenda, *Sieciocentryczne zarządzanie siłami…*, *op. cit.*

[119] D. Mąka, P. Sienkiewicz, *Sieciocentryczna infrastruktura procesów decyzyjnych*, „Zeszyty Naukowe AON" 2009, nr 2.

staw czujników peryferyjnych znajdujących się np. na platformach rozpoznawczych oraz oprogramowania czujników. Czujniki oraz jego oprogramowanie są nałożone na sieć informacyjną, czyli są podłączone do niej w taki sposób, aby zapewnić przepływ informacji;

- **sieć dowodzenia** – jest to sieć zapewniająca dowodzenie platformami bojowymi w przestrzeni walki. Sieć ta umożliwia wykorzystanie świadomości przestrzeni walki przez zapewnienie działającym siłom możliwości wykonania manewru, precyzyjnego uderzenia, pełnowymiarowej ochrony, jak również ześrodkowania zasobów logistycznych w wymaganym miejscu i czasie. W skład sieci dowodzenia wchodzą platformy bojowe i oprogramowanie platform bojowych, które działają z wykorzystaniem sieci informacyjnej. Platformy bojowe są rozmieszczone w przestrzeniach: kosmicznej, powietrznej, informacyjnej (cyberprzestrzeni); na lądzie, morzu.

Aby system dowodzenia i kierowania właściwie spełniał swoje funkcje, powinien być użyteczny dla korzystających z niego systemów bojowych, pozwalać na tworzenie wielu obwodów funkcyjnych oraz umożliwiać rozdzielanie informacji między różne obszary w zależności od wykonywanych zadań, jak również ich przeznaczenia. System musi być także dynamiczny – zdolny do reagowania na szybko zmieniającą się sytuację taktyczną. W celu obsługi rozproszonych jednostek mobilnych, mogących także funkcjonować w różnych zmiennych obszarach i warunkach działania, istnieje konieczność rozbudowy systemu łączności, który będzie skupiał w sobie funkcje telekomunikacyjne, nawigacyjne jak też identyfikacyjne. Mogą to być np. systemy transmisji danych LINK. Systemy te składają się z sieci terminali. Tworzą cyfrowy, wielofunkcyjny system dystrybucji informacji – MIDS (ang. *Multifunctional Information Distribution System*). Zapewnia on utajony, odporny na zakłócenia transfer informacji w czasie rzeczywistym pomiędzy mobilnymi jednostkami różnych rodzajów wojsk, co jest zgodne z koncepcją walki sieciocentrycznej. Należy podkreślić, iż głównym celem istnienia tego systemu nie jest zastąpienie klasycznej sieci łączności mobilnej, lecz jej uzupełnienie, szczególnie w zakresie współpracy różnych rodzajów wojsk i obsługi wysoce mobilnych jednostek na wszystkich możliwych szczeblach dowodzenia. Szczególnie operacje powietrzne obejmują wiele funkcji dowodzenia oraz kierowania np. opracowanie i zobrazowanie danej sytuacji, system wskazywania celów, planowanie zadań, przygotowanie i rozpowszechnianie rozkazów oraz meldunków, które w znacznym stopniu uzależnione są od systemów transmisji danych. Podstawowymi mechanizmami wykorzystywanymi do przesyłania informacji o śledzeniu celów są taktyczne łącza danych zwane taktycznymi systemami transmisji

danych. W NATO określane są one z ang. *Tactical Data Link1*, zaś w USA – *Tictical Digital Information Link* – TAIL[120].

Oto przykłady stosowanych łącz informacyjnych[121], w zastosowaniach militarnych:

- **Link 1** – cyfrowe, dwukompleksowe łącze zaprojektowane pod koniec lat 50. XX w. przez instytucje NATO do celów wymiany informacji typu punkt – punkt przez jednostki obrony powietrznej. Łącze to miało na celu zobrazowania sytuacji powietrznej między centrami kierowania i meldowania a połączonymi z centami operacji powietrznych z prędkością 1200/2400 b/s. Państwa NATO wykorzystują Link 1 głównie w systemach obrony powietrznej.
- **Link 4A (TADIL C)** – jest używany do naprowadzania samolotów myśliwskich. Jest to łącze sieciowe, działające na zasadzie podziału czasu w paśmie UHF z prędkością 5000 b/s. Istnieją dwa łącza tego typu: Link 4A oraz Link 4C. Pierwsze z nich odgrywa ważną rolę w systemie teleinformatycznym Sojuszu – dostarcza siłom połączonym informację taktyczną w formacie cyfrowym w kierunku ziemia-powietrzne, powietrze-ziemia oraz powietrze-powietrze. Link 4 zaprojektowano w celu zapewnienia komunikacji fonicznej używanej do naprowadzania lotnictwa taktycznego łącznością cyfrową. Link 4A jest to łączę pewne, lecz wiadomości nie są szyfrowane ani odporne na wszelkie zakłócenia. Link 4C służy do zapewnienia komunikacji między samolotami myśliwskimi.
- **Link 11/11B (TADIL A/B)** – jest to półdupleksowe łącze sieciowe, które działa przez cykliczne odpytywanie przez stacje kontroli (NCS). Link 11 wykorzystuje sieciowe techniki komunikacyjne oraz standardowy format wiadomości w celu wymiany informacji w formacie cyfrowym między systemami powietrznymi, naziemnymi i morskimi na wysokiej oraz bardzo wysokiej częstotliwości. Łącze to używane jest również przez liczne systemy służące do rozpoznania, jak również do wywiadu elektronicznego. Link 11 to łącze bezpieczne, lecz podatne na zakłócenia elektromagnetyczne. Pozwala na wymianę informacji o trasach powietrznych, nawodnych oraz podwodnych, danych z systemu wczesnego ostrzegania, jak również danych dowodzenia między elementami systemu dowodzenia, ale nie pozwala na sterowanie statkami powietrznymi.
- **Link 16 (TADAL J)** – jest to wielofunkcyjne, bezpieczne i odporne na zakłócenia łącze danych przeznaczone do wymiany wiadomości o ustalonym formacie oraz fonicznych z użyciem połączonego tak-

[120] *Understanding LINK-16*, Northrop Grumman, San Diego 2010, s. 1-3.
[121] B. Grenda, *Sieciocentryczne zarządzanie siłami …*, *op. cit.*

tycznego systemu dystrybucji informacji lub równoważnych terminali. Link 16 nie różni się od podstawowej koncepcji cyfrowej wymiany informacji taktycznej, prowadzonej z użyciem Link 4 czy Link 11. Link 16 oferuje techniczne oraz operacyjne usprawnienia w stosunku do obecnie wykorzystywanych standardów jak również usprawnia ich niedoskonałości np. odporność na zakłócenia, wzrost bezpieczeństwa transmisji i prędkości przesyłania danych, identyfikowanie źródła danych, wzrost ilości/rozdrobnienia wymienianych informacji, ograniczenie rozmiaru terminala danych. Link 16 może być instalowany w kabinach samolotów bojowych, zapewnia bowiem prowadzenie bezpiecznej łączności fonicznej, względne nawigowanie, jak również identyfikowanie informacji o położeniu wszystkich jednostek uczestniczących w operacji. Za pomocą łącza przekazywane są informacje o zagrożeniach załogom samolotów będących poza zasięgiem wykrywania ich radarów pokładowych lub ostrzegawczych.

- **Link 22** – jest utajonym, odpornym na zakłócenia wielokanałowym cyfrowym informacyjnym łączem transmisji danych w relacjach radiowych, takich jak: KF czy UKF. Zgodnie z założeniami, Link 22 powinien zapewniać połączenie powietrznych, morskich, podwodnych oraz lądowych zautomatyzowanych systemów taktycznych w sposób umożliwiający skompilowanie wspólnego obrazu sytuacji, zarządzanie statusem i użyciem systemów uzbrojenia, jak również dowodzenia i kierowania.

W systemach informacyjnych, w których jedną z funkcji jest zaspokojenie potrzeb informacyjnych użytkowników, należy uwzględnić możliwość pojawienia się w nich wiadomości zawierających informacje zbędne lub tzw. **luki informacyjnej** (brak pożądanej informacji). Efektywny system informacyjny powinien zawierać: efektywne metody oraz narzędzia identyfikacji oraz redukcji luk informacyjnych. Powinny one umożliwiać kontrolę i minimalizację rozbieżności między wiedzą użytkownika (dowódcy), jego potrzebami informacyjnymi, a dostarczaną mu informacją. Luki informacyjne, czyli brak pełnej informacji w procesie podejmowania decyzji powodują, iż informację niepełną przyjmuję się jako wystarczającą lub uzupełnia się luki informacyjne, informacjami nierelewantnymi, które decydent uznaje tylko za relewantne (np. informacje niesprawdzone, subiektywne szacunki dokonywane na niepewnych podstawach lub nieprawdziwe). Jest to jedna z przyczyn popełniania błędów w podejmowaniu decyzji. Niezbędne staje się wykorzystanie odpowiednich narzędzi, umożliwiających wykrycie oraz usunięcie tych nieprawidłowości.

Do narzędzi, które wyszukują luki informacyjne należy pakiet DIANA (wspomaganej komputerowo DIAgnostycznej ANAlizy i Projektowania Sys-

temów Zarządzania)[122], którego metodykę opracowano w wyniku wieloletnich badań[123]. Pozwala ona przeprowadzić wszechstronną analizę diagnostyczną systemu zarządzania, dokonać zmian usprawniających, jak również zaprojektować nową strukturę organizacyjną wraz ze sprawdzeniem efektywności wprowadzanych zmian na modelu symulacyjnym[124]. Jeden z nowoczesnych pakietów – DIANA-11 wykorzystuje model systemu zarządzania w postaci polihierarchicznej wielopoziomowej przestrzennej sieci powiązań informacyjnych składający się z: poziomu celów i zasobów, poziomu komórek organizacyjnych, poziomu pracowników oraz poziomu czynności elementarnych.

W skład bloków funkcjonalnych DIANA-11 wchodzi[125]:

- blok wprowadzania danych – umożliwia wprowadzenie danych z konkretnego obiektu;
- blok wspomaganej komputerowo analizy diagnostycznej – dokonuje się kompleksowej analizy diagnostycznej badanego obiektu, której wyniki są wykorzystywane do opracowania kolejnych wersji uprawnień – ponownie modelowanych oraz diagnozowanych, aż do uzyskania zadowalającego projektu. Blok analizy diagnostycznej pakietu DIANA-11 zawiera 62 algorytmy wykrywające różne nieprawidłowości na poszczególnych poziomach modelu, np. ślepe uliczki informacyjne; nierównomierne obciążenie komórek; źródła błędów i opóźnień, rozbieżność hierarchii stanowisk, nieodpowiedni przydział ludzi, brak powiązań z celami, dublowanie czynności, brak synchronizacji w czasie, dysfunkcjonalność, ukryte sytuacje konfliktowe, nieodpowiednie predyspozycje, niewłaściwy podział komórek, nieadekwatne zasoby itd.;
- blok wspomaganego komputerowego projektowania struktur organizacyjnych – DIANA-11 wykorzystuje zalążki, czyli najbardziej istotne dla projektowanych komórek organizacyjnych stanowiska. Miarą jakości projektowanych komórek jest tzw. siła powiązań, która świadczy o zawartości wykonywanych wewnątrz komórek czynności, zaś jakość całego projektu określa tzw. miara rozproszenia – charakteryzująca powiązania między komórkami. W trakcie projektu dąży się do uzyskania maksymalnej siły powiązań oraz minimalnej miary rozpro-

---

[122] E. Michalewski, *Podstawy metody analizy diagnostycznej i projektowania systemów zarządzania (metoda DIANA)*, IBS PAN, Seria: Badania Systemowe, t. 34, Warszawa 2004, s. 148-151.

[123] E. Michalewski, *Wspomagane komputerowo diagnoza i projektowanie systemów informacyjnych zarządzania,* Wyższa Szkoła Informatyki Stosowanej i Zarządzania, Seria: Monografie, Warszawa 2008, s. 127.

[124] E. Michalewski, *Podstawy metody analizy…*, *op. cit.*

[125] E. Michalewski, *Analiza systemów sieciocentrycznych…*, *op. cit.*, s. 149-151.

szenia. Konsekwentna realizacja prowadzi do uzyskania kompletnego projektu organizacyjnego badanego systemu zarządzania. DIANA-11 umożliwia sprawdzenie wielu wariantów projektu organizacyjnego, najpierw na modelu, aby wybrać i wdrożyć najlepszy wariant;
- blok wspomaganego komputerowo projektowania Systemu Informowania Kierownictwa (SIK) – wyodrębnia tzw. dendryty startowych zadań. Są to zadania, wybrane przez grono menadżerów badanego obiektu, spośród wszystkich zadań realizowanych w tym obiekcie, jako te, których wyniki stanowią najważniejszą informację niezbędną przy podejmowaniu decyzji.

Pakiet DIANA-11 zawiera obiekt testowy, umożliwiający wszechstronną naukę w zakresie opanowania metodyki wspomaganej komputerowo analizy oraz projektowania złożonych struktur zarządzania. Spośród partnerów wersji użytkowej pakietu DIANA można wymienić np.: Centralę Narodowego Banku Polskiego, Ministerstwo Obrony Narodowej, Komendę Główną Policji, Służbę Celną RP i wiele innych. Wadą tego pakietu, z punktu widzenia wykorzystania w systemach sieciocentrycznych, jest jego dedykowalność dla jednego tylko obiektu[126].

Dokonując analizy zagrożeń cybernetycznych systemów wojskowych można przytoczyć przykłady cyberataków, których celem były siły zbrojne. Jednym z takich incydentów, przeprowadzonych na dużą skalę był cyberatak z 2016 roku na szwedzkie siły zbrojne. Atak wymusił wyłączenie systemu informatycznego wykorzystywanego do ćwiczeń wojskowych. Szef służby prasowej szwedzkich sił zbrojnych Philip Simon potwierdził, że doszło do ataku na system Caxcis i został on zamknięty zgodnie z raportem Reuters w dniu 25 stycznia 2017. Sieć Caxcis używana do ćwiczeń wojskowych praktycznie nie działała przez kilka godzin, bowiem doszło do infiltracji i eksfiltracji informacji niejawnych oraz przekształcenia stanowisk roboczych w „komputery-zombie", które miały posłużyć do dalszych ataków. W grudniu 2016 roku szef wojskowego MUST Gunnar Karlson po raz pierwszy wskazał właśnie na Rosję jako źródło cyberataków i operacji informacyjnych. Dodał również, iż takie działania mają na celu zdestabilizowanie państwa.

Zamknięcie systemu zbiegło się w czasie z przygotowaniami armii do planowanych ćwiczeń pk. AURORA-17, które planowane były na wrzesień 2017 roku. Są to największe ćwiczenia wojskowe tego typu, w których udział biorą wszystkie rodzaje szwedzkich wojsk oraz przedstawiciele innych państw – żołnierze Danii, Finlandii, Estonii, Francji, Norwegii, Niemiec, a także Amerykanie (ogółem 19 tys. żołnierzy). Z opublikowanego w marcu 2017 r. raportu szwedzkich służb specjalnych SAPO wynika, że

[126] E. Michalewski, *Analiza systemów sieciocentrycznych…*, *op. cit.*, s. 150-151.

Rosja prowadzi przeciwko Szwecji wojnę psychologiczną, której celem są decydenci oraz opinia publiczna.

Innym przykładem związanym z Siłami Zbrojnymi jest incydent, który miał miejsce w styczniu 2017 roku, podczas uroczystego powitania amerykańskich żołnierzy, którzy przybyli w celu wzmocnienia wschodniej granicy NATO. W uroczystości w Żaganiu udział wzięli przedstawiciele najwyższych władz państwowych – m.in. premier Beata Szydło oraz minister Antoni Macierewicz. Podczas powitania żołnierzy, hakerzy dokonali włamania na oficjalną stronę miasta Żagań. Ich celem było wezwane do protestu przeciwko obecności amerykańskich wojsk na terenie Polski, za pomocą treści „Nie dla wojsk USA w Polsce", oraz określając sojuszników jako „nowi Krzyżacy" czy „amerykańscy okupanci". Fałszywe treści zostały usunięte oraz podjęto próby działań skierowane na poszukiwaniu sprawców tego wykroczenia.

4.1.2. Zagrożenia cybernetyczne infrastruktury krytycznej państwa

Systemy, obiekty budowlane, usługi oraz instalacje wchodzące w skład tzw. infrastruktury krytycznej państwa (IKP/IK), to inaczej systemy: bankowo-finansowe, energetyczne, telekomunikacyjne; dostarczające wodę, realizujące transport, służby do działań w sytuacjach wyjątkowych. Z uwagi na swoją działalność przechowują one informacje ważne dla ochrony państwa czy bezpieczeństwa jego obywateli. Ich sprawne działanie gwarantuje minimum niezbędne do funkcjonowania gospodarki kraju i decyduje o jego istnieniu. Wyróżniamy osiem elementów tej infrastruktury[127]:

- **telekomunikacyjna** (ang. *telecommunication*) – obejmuje wszelkie środki umożliwiające nadawanie, odbiór lub transmisję (czasami również zobrazowanie) informacji za pomocą przewodów, fal elektromagnetycznych lub sieci optycznej np. systemy łączności lotniczej (m.in. sieć AFTN, system ACARS), satelity geostacjonarne lub sieci komputerowe m.in. komercyjne, wojskowe lub akademickie itp.;
- **system energetyczny** (ang. *Electrical Power System)* **–** całokształt współpracujących ze sobą podczas produkcji urządzeń technicznych bądź pozyskiwania, przetwarzania, przesyłania, dystrybucji oraz użytkowania energii, jak również transport i magazynowanie surowców niezbędnych do jej produkcji;
- **produkcja, magazynowanie i transport gazu ziemnego oraz ropy**

[127] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, s. 33.

naftowej (ang. *Oil and Gas Delivery and Storage*) **–** obejmuje całokształt procesów, do których w szczególności zalicza się wydobycie ropy naftowej i gazu ziemnego, ich bezpieczne magazynowanie, przetwarzanie i transport tych surowców organicznych za pomocą rurociągów, transportem morskim, kolejowym lub kołowym;

- **system bankowy i finansowy** (ang. *Banking and Finance*) – to całokształt instytucji oraz normy, określające ich wzajemne powiązania oraz zachodzące relacje z otoczeniem. Stanowią system przepływu bilionów dolarów, poczynając od indywidualnych depozytów po transfer dużych sum pieniędzy z jednego krańca świata na drugi;
- **transport** (ang. *transportation*) – zdefiniowany jako zdolność do przemieszczania ludzi lub ładunków w danej i określonej przestrzeni z wykorzystaniem odpowiednich i przystosowanych do podmiotów transportu środków za pomocą np. transportu lotniczego, morskiego, rzecznego, kolejowego, drogowego osób i towarów, włączając w to cały system wsparcia oraz zabezpieczenia logistycznego;
- **system zaopatrzenia w wodę** (ang. *Water Supply System*) – stanowi układ współdziałających elementów, których priorytetowym zadaniem jest zaopatrzenie w wodę odbiorców o zasięgu np. terytorialnym. Składa się na niego: ujęcie wody, wodociągi, zbiorki wody, system filtrowania oraz oczyszczania wody, dostarczania jej dla rolnictwa, przemysłu, staży pożarnych, jak również indywidualnych odbiorców;
- **służby ratownicze** (ang. *Emergency Service*) – w USA system alarmowy 911 – komunikacja z policją, służbą zdrowia oraz strażą pożarną – obejmuje szeroko pojmowany zespół działań dążący do zapewnienia bezpieczeństwa życia i zdrowia osób oraz ich mienia na rzecz ochrony ludności. Działalność służb ratowniczych zmierza do stworzenia i utrzymania sprzyjających warunków środowiskowych do przeżycia. Oprócz państwowych służb ratowniczych (m. in. policja, służba zdrowia, straż pożarna) funkcjonują służby o charakterze społecznym, takie jak: Tatrzańskie Ochotnicze Pogotowie Ratunkowe, Wodne Ochotnicze Pogotowie Ratunkowe, Górskie Ochotnicze Pogotowie Ratunkowe oraz stowarzyszenia komercyjne;
- **ciągłość funkcjonowania władzy i służb publicznych** (ang. *Continuity of Government Services*) – to zespół wszystkich elementów, które zapewniają funkcjonowanie lokalnych, regionalnych oraz centralnych władz, jak również systemu publicznego: bezpieczeństwo, służba zdrowia czy obrona. W Polsce gwarantem utrzymania ciągłości władzy państwowej jest pełnienie funkcji Prezydenta RP, postrzeganego przez społeczeństwo jako – jednostka obdarzona największym mandatem zaufania, stojąca na straży nienaruszalności terytorium

oraz granic państwa.

Istotę oraz nieco inną klasyfikację infrastruktury krytycznej w Polsce określa ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.[128]. Skupia się ona w szczególności na podziale, pozwalającym na podjęcie wszelkich sił i środków, w przypadku kiedy praca któregokolwiek z systemów zostanie zakłócona. Ma to na celu przywrócenie wcześniejszego stanu sprawności. W zgodzie z nią, w skład elementów decydujących o istnieniu państwa wchodzą poniższe instalacje, instytucje i systemy (art. 3 u.z.k.):

- zaopatrzenia w energię i paliwa;
- łączności i sieci teleinformatycznych;
- finansowe;
- zaopatrzenia w żywność i wodę;
- ochrony zdrowia;
- transportowe i komunikacyjne;
- ratownicze;
- zapewniające ciągłość działania administracji publicznej;
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

W wyniku nieprzewidzianych zdarzeń spowodowanych czynnikami, takimi jak: siły natury (w tym klęski żywiołowe: powodzie, huragany, wyładowania atmosferyczne) lub będących konsekwencją działalności człowieka, infrastruktura krytyczna może ulec zniszczeniu, uszkodzeniu a jej działanie może zostać zakłócone bądź chwilowo przerwane. Z tego powodu może być zagrożone życie i mienie obywateli danego kraju. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państwa. Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetowych wyzwań, z którymi musi zmierzyć się państwo. Istota zadań związanych z infrastrukturą krytyczną sprowadza się nie tylko do zapewnienia jej odpowiedniego stopnia ochrony przed zagrożeniami o różnym charakterze, lecz również do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, stosunkowo łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki. Ochrona infrastruktury krytycznej została zdefiniowana jako wszelkie działania dążące do zapewnienia funkcjonalności, ciągłości pracy i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków,

[128] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm.), dalej: u.z.k.

w tym szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków lub innych zdarzeń zakłócających jej prawidłowe funkcjonowanie[129].

W celu szybkiego odzyskania właściwego funkcjonowania infrastruktury krytycznej w Polsce został opracowany „Narodowy Program Ochrony Infrastruktury Krytycznej" (NPOIK). Podstawą prawną, która posłużyła do jego powstania są zapisy art. 5b, ust. 1 u.z.k. NPOIK obejmuje elementy umieszczone w jednolitym wykazie obiektów, instalacji, urządzeń i usług, które wchodzą w skład infrastruktury krytycznej z podziałem na zdefiniowane w u.z.k. systemy. Uwzględniając fakt, że Rzeczpospolita Polska jest członkiem organizacji, takich jak: Unia Europejska, Organizacja Traktatu Północnoatlantyckiego, Organizacja Bezpieczeństwa i Współpracy w Europie oraz innych organizacji międzynarodowych, NPOIK akceptuje również międzynarodowe porozumienia, których RP jest stroną. Nadrzędnym celem NPOIK jest utworzenie odpowiednich warunków do poprawienia poziomu bezpieczeństwa infrastruktury krytycznej w kraju. Osiągnięcie tego zamierzenia wymaga spełnienia pewnych warunków w postaci szeregu celów pośrednich, do których można zaliczyć[130]:

- zdobycie określonego poziomu świadomości, wiedzy i kompetencji wszystkich uczestników NPOIK w zakresie znaczenia jego kluczowych elementów dla sprawnego funkcjonowania państwa oraz sposobów i metod ich ochrony;
- wprowadzenie metodyki, opartej na zasadach postępowania, które polegają na skutecznej analizie lub ocenie ryzyka, uwzględniając pełny wachlarz możliwych zagrożeń (w tym metodyki z podziałem określonego postępowania w przypadku wystąpienia zagrożeń o bardzo małym prawdopodobieństwie i tych o katastrofalnych skutkach);
- wdrożenie skoordynowanego i bazującego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony infrastruktury krytycznej;
- budowanie partnerstwa oraz kształtowanie dobrych relacji pomiędzy uczestnikami procesu ochrony infrastruktury krytycznej, wpływających w korzystny sposób na współpracę;
- wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych wyłącznie między poszczególnymi uczestnikami procesu ochrony infrastruktury krytycznej.

Oprócz podstawowych elementów koniecznych do funkcjonowania państwa wskazanych w NPOIK, wyróżnia się europejską infrastrukturę krytyczną. Została ona zdefiniowana jako infrastruktura zlokalizowana na

[129] *Infrastruktura krytyczna*, Rządowe Centrum Bezpieczeństwa,
online – http://rcb.gov.pl/infrastruktura-krytyczna/ [dostęp: 11.07.2017].
[130] *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, Warszawa 2013, s. 8.

terytorium państw członkowskich Unii Europejskiej, której zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa kraje. Europejska infrastruktura krytyczna wyznaczana jest w dwóch sektorach – sektorze energetycznym i sektorze transportu[131].

Biorąc pod uwagę infrastrukturę krytyczną państwa, jako zespół elementów stanowiących potencjalne obiekty oddziaływania cyberprzestępczości, można przytoczyć kilka przykładów takich ataków mających miejsce w Polsce. Pierwszym z nich jest cyberatak przeprowadzony w czerwcu 2015 r. na Polskie Linie Lotnicze LOT (PLL LOT) zlokalizowane na terenie Portu Lotniczego Okęcie w Warszawie. Zaatakowane zostały systemy łączności, które uniemożliwiły przesyłanie planów lotów ze statków powietrznych do stacji naziemnych. W efekcie, nie wykonano standardowych, koniecznych procedur przed przystąpieniem do realizacji lotu każdego samolotu komunikacyjnego. Ruch lotniczy wstrzymano na sześć godzin. W tym czasie odwołano łącznie jedenaście lotów, a kilka z nich było opóźnionych, co skutkowało narażeniem na poniesienie kosztów przewoźników lotniczych. Dodatkowo terminowego rejsu nie odbyło ok. 1,4 tys. pasażerów. Problem z systemami przesyłania informacji udało się opanować po dwudziestu jeden godzinach[132]. Szef linii lotniczej wyjaśnił, że atak polegał wyłącznie na zatrzymaniu obiegu informacji na serwerach i uniemożliwiał generowanie nowych danych, jednak nie miał nic wspólnego z systemem rezerwacyjnym czy układaniem list pasażerów. Zatem dane osobowe klientów LOT–u nie były zagrożone ani nie zostały skradzione. Sytuacja ta przyniosła katastrofalne skutki dla zasobów finansowych PLL LOT. Istnieje podejrzenie, że cyberatak mógł zaliczać się do rodzaju DDoS, i mógł zostać przeprowadzony z wielu miejsc jednocześnie za pomocą „komputerów-zombie", *botów* czy trojanów.

Kolejnym przykładem aktu cyberprzestępczości, godzącego w bezpieczeństwo elementów infrastruktury krytycznej państwa, jest cyberatak przeprowadzony w lutym 2017 r. na sieć polskich banków. Udało się go wykryć oraz opanować dopiero po kilku dniach od zauważenia nieprawidłowości. Obiektami ataków były: jeden duży, jeden średni i dwa małe banki, które odkryły w swojej sieci zaawansowane złośliwe oprogramowanie, nieznane wcześniej używanym przez nie programom antywirusowym. Zainfekowane zostały zarówno komputery pracowników, jak i serwery bankowe. Jako źródło tego typu zagrożenia wskazano witrynę internetową Komisji Nadzoru Finansowego. Przypuszcza się, że to właśnie na stronie

[131] *Ibidem*, s. 45-46.

[132] *Atak hakerów na PLL LOT*, online – http://www.polskieradio.pl/69/273/Artykul/1465337,Atak-hakerow-na-PLL-LOT-celem-ataku-system-naziemny-lotniska-bez-wplywu-na-system-rezerwacji [dostęp: 14.07.2017].

Komisji Nadzoru Finansowego (KNF) pierwotnie umieszczono elementy niezidentyfikowanego, złośliwego oprogramowania. Ze względów bezpieczeństwa wyłączono ją od razu po jego wykryciu, aby żaden z użytkowników nie padł ofiarą negatywnego oddziaływania ataku. Mechanizm działania aktu bezprawnej ingerencji mógł polegać na tym, że pracownik banku, wchodząc na zainfekowaną wcześniej stronę KNF, mógł nieświadomie zainfekować także system swojej instytucji. To wydarzenie doprowadziło do zachwiania wizerunku Komisji Nadzoru Finansowego z uwagi na to, że stanowi ona główny organ odpowiedzialny za promowanie, wyznaczanie i egzekwowanie zasad bezpieczeństwa informacyjnego w tym sektorze. W efekcie sama stała się na skutek własnych zaniedbań i niedopatrzeń, pośrednim narzędziem ataku na banki[133]. Wraz z przejęciem kontroli nad serwerami bankowymi warto zwrócić uwagę na klientów instytucji, w szczególności tych, którzy korzystają z kont internetowych. Analizując ten przykład cyberataku mogło dojść do kradzieży danych osobowych oraz środków przechowywanych na koncie. Z tego powodu bardzo ważne jest uświadamianie społeczeństwa na temat wdrażania wszelkich środków na komputerach prywatnych, które mogłyby wpłynąć na podniesienie poziomu cyberbezpieczeństwa. Może należeć do nich np. bieżąca aktualizacja i konieczność zainstalowania programów antywirusowych. KNF zapewnił, że pracownicy banków nie są podłączeni do baz danych ani systemów transakcyjnych, więc prawdopodobnie wykradzione dane nie stanowiły większego niebezpieczeństwa.

Oprócz przypadków ataków informacyjnych w Polsce, które zakłóciły funkcjonowanie infrastruktury krytycznej, można wyróżnić także kilka międzynarodowych wydarzeń. Należy do nich incydent zaistniały w grudniu 2015 r. w zachodniej części Ukrainy. Nastąpiła wówczas nieprzewidziana przerwa w dostawie energii elektrycznej. Jako źródło problemu określono nieprawidłowości i usterki występujące w pięćdziesięciu siedmiu podstacjach zasilania, które mogły być skutkiem zakłócenia pracy w systemie monitorowania spowodowane przez jedną z elektrowni. W styczniu 2016 r. ukraiński oddział organizacji CERT–UA (ang. *Computer Emergency Response Team of Ukraine*) wystosował oficjalne oświadczenie, z którego wynikało, że awaria była efektem ataku hakerskiego na systemy ICS (ang. *Industrial Control Systems* – przemysłowe systemy sterujące) tych elektrowni. Przemysłowe systemy sterujące odpowiadają m.in. za transport ropy i gazu za pomocą rurociągów i gazociągów, dystrybucję wody, przesyłanie energii elektrycznej czy sterowanie światłami drogowymi. Na

[133] M. Rudke, *Cyberatak: Będzie więcej ataków na banki i ich klientów*, online – http://www.rp.pl/Banki/302059917-Cyberatak-Bedzie-wiecej-atakow-na-banki-i-ich-klientow.html [dostęp: 14.07.2017].

tej podstawie można stwierdzić, że ICS są podstawą dla funkcjonowania współczesnego, nowoczesnego społeczeństwa. Stanowią one potencjalnie nietrudny obiekt do przejęcia nad nim kontroli poprzez zaangażowanie do działań przestępczych środków informacyjnych, ze względu na brak odpowiedniego zabezpieczenia. W zdecydowanej większości przypadków ataków na systemy informatyczne skutki są ograniczone zaledwie do strat finansowych. Ataki na systemy ICS natomiast mogą również zniszczyć urządzenia o znaczeniu krytycznym oraz zagrozić bezpieczeństwu państwa a nawet w skrajnych warunkach życiu ludzi. Analizując cyberatak – który miał miejsce na Ukrainie – dowiedziono, że został on przeprowadzony w trzech, złożonych etapach. Pierwszy z nich polegał na zainfekowaniu przemysłowych systemów sterujących metodą tzw. *spear-phishingu*, przy użyciu dokumentów Microsoft Office, dołączonych jako załącznik do wiadomości email. Pliki pakietu Office zawierały złośliwe makropolecenia. Drugi etap ataku polegał na przejęciu systemu ICS i uniemożliwienia jego odzyskania poprzez usunięcie plików systemowych z systemów sterujących elektrowni. Ostatni etap obejmował działania w oparciu o ataki typu DDoS, ukierunkowane na centra obsługi klienta różnych elektrowni, przeprowadzone w formie zmasowanych fikcyjnych połączeń telefonicznych, które opóźniły moment wykrycia problemu przez firmę. Stwierdzono, że w tych atakach użyto znanego od 2007 r. szkodliwego oprogramowania z rodziny BlackEnergy. W 2014 r. wykryto również inne jego odmiany, które zgromadziły informacje dotyczące infrastruktury SCADA[134] (ang. *Supervisory Control And Data Acquisition*) – infrastruktury odpowiedzialnej za nadzór nad przebiegiem procesów technologicznych bądź produkcyjnych.

Innym przykładem przestępczej działalności w przestrzeni cybernetycznej jest atak informacyjny, który miał miejsce w maju 2017 r. Posiadał on charakter zmasowany a jego oddziaływanie, według oświadczenia firmy Kaspersky Lab oraz Avast Software, objęło aż siedemdziesiąt cztery państwa i niespełna sześćdziesiąt tysięcy urządzeń. Z ostatecznego raportu wynikało, iż podczas ataku doszło do zainfekowania siedemdziesięciu pięciu tysięcy komputerów w niemal stu państwach na całym świecie. Ustalono, że ten bezprawny akt został przeprowadzony przez cyberprzestępcę, który wykradł oprogramowanie typu *ransomware* – WanaCrypt0r 2.0. Zostało one opracowane i stworzone przez amerykańską NSA (ang. *National Security Agency* – Agencja Bezpieczeństwa Narodowego), której *ransomware* najprawdopodobniej miał posłużyć do wykonywania zadań z zakresu wywiadu elektronicznego. Cykl cyberataku miał następujący przebieg: po otwarciu przez dowolnego użytkownika zainfekowanych wirusem plików

[134] *Krytyczna infrastruktura zagrożona cyberatakami*, online – http://di.com.pl/krytyczna-infrastruktura-zagrozona-cyberatakami-54699 [dostęp: 15.07.2017].

na komputerze, na jego ekranie pojawiał się komunikat w języku angielskim – *Oops, your important files are encrypted*, co można przetłumaczyć – *Ups, Twoje ważne pliki są zaszyfrowane*). W zamian za odblokowanie zaszyfrowanych i zarażonych danych, przestępca domagał się żądania w postaci wypłacenia okupu o sumie wynoszącej trzysta dolarów w bitmonetach[135]. Najprawdopodobniej złośliwy program wykorzystał lukę w systemie operacyjnym Windows, która mogła być usunięta przez bieżące aktualizacje oprogramowania po zidentyfikowaniu problemu. W wyniku tego ataku informacyjnego zostały poszkodowane m.in. poniższe kraje wraz ze swoimi instytucjami[136]:

- Rosja – komputery należące do Ministerstwa Spraw Wewnętrznych i największego operatora obsługującego sieci komórkowych w kraju – firmy *Megafon*;
- Hiszpania – sieć komórkowa *Telefónica* oraz przedsiębiorstwa Ministerstwo Energetyki;
- Wielka Brytania – narodowy system zdrowia (ang. *National Health Service* – NHS). Z tego powodu zablokowano lub utrudniono dostęp do danych pacjentów, przez co odwołano setki zaplanowanych operacji i zabiegów. Celem ataku była również fabryka Nissan Motor Manufacturing UK Ltd, produkująca samochody Renault.

Oddziaływanie tego cyberataku dotknęło także: Ukrainę, Tajwan, Indie, Portugalię, Chiny, Włochy i Stany Zjednoczone.

4.2. Aktualny stan oraz zagrożenia bezpieczeństwa cybernetycznego

W ostatnich latach obserwuje się wyraźny wzrost liczby (częstości) ataków cybernetycznych łączących różne metody i narzędzia. Infekcja oprogramowaniem złośliwym urzeczywistnia się przede wszystkim w wyniku nieprzestrzegania podstawowych zasad bezpieczeństwa. Nadrzędnymi jej przyczynami są brak bieżących aktualizacji systemu operacyjnego oraz oprogramowania użytkowego, a także niestosowanie oprogramowania antywirusowego lub brak regularnych jego aktualizacji. Zaniedbania w tych obszarach powodują, że zwiększa się podatność komputera na cyberatak. Co więcej, przeglądanie zainfekowanej witryny lub nawet przypadkowe uruchomienie załącznika niezaufanej wiadomości z poczty elek-

[135] **Bitmoneta** – rodzaj waluty elektronicznej – tożsame z *bitcoin*.
[136] R. Muczyński, *Największy cyberatak w historii?*, online – http://www.nowastrategia.org.pl/najwiekszy-cyberatak-w-historii/ [dostęp: 15.07.2017].

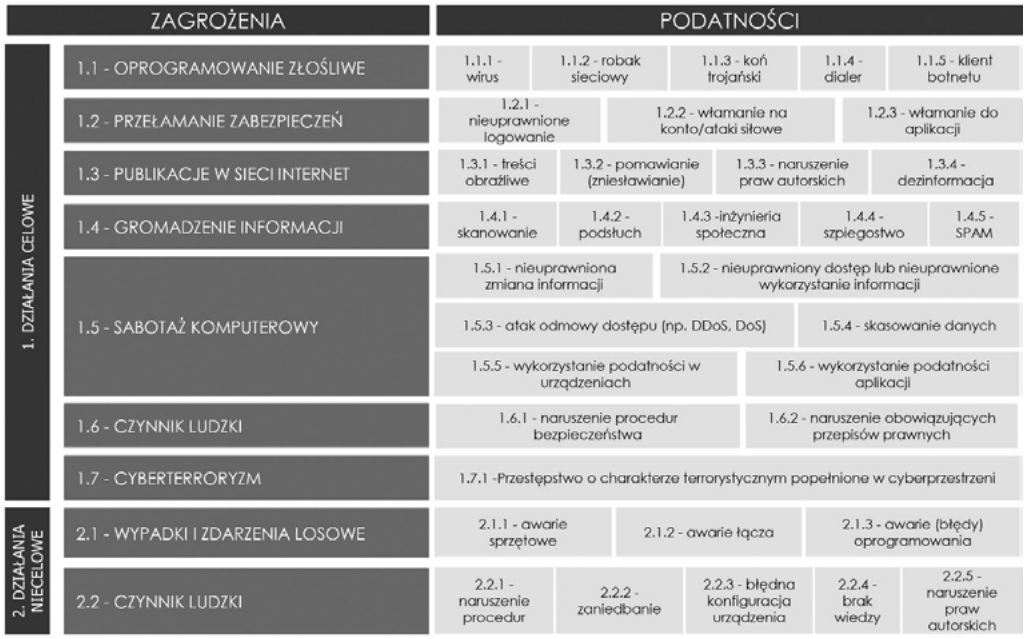
tronicznej może być przyczyną infekcji komputera oprogramowaniem złośliwym. Wyżej wskazane sytuacje dotyczą nie tylko pobierania i uruchamiania plików z sieci Internet, ale też kopiowania danych z niepewnych (a więc potencjalnie niebezpiecznych) nośników. W dalszym ciągu czynnikami, które przyczyniają się do skali skuteczności ataków pozostają: zaniedbania bezpieczeństwa systemów, brak właściwych procedur w instytucjach oraz dedykowanych zespołów czy pracowników odpowiedzialnych za reagowanie na incydenty. Problemem w dalszym ciągu pozostaje również tendencja do szukania oszczędności kosztem bezpieczeństwa teleinformatycznego[137].

W „Raporcie o stanie cyberbezpieczeństwa RP w 2015 r." wskazuje się, że w sytuacji zainfekowania systemu komputerowego staje się on niebezpieczny i może stać się narzędziem:

- „kradzieży wrażliwych danych – uzyskiwania danych z zainfekowanych komputerów;
- przeprowadzania dalszych ataków na inne systemy teleinformatyczne, co w przypadku gdy ataki te zostaną przeprowadzone z zarażonych systemów należących do instytucji państwowych może narazić zarówno poufność, integralność, jak i dostępność przetwarzanych w tych systemach informacji oraz wpłynąć negatywnie na obraz poziomu bezpieczeństwa państwa;
- wykonywania działań mających na celu bezprawne uzyskiwanie korzyści majątkowych;
- rozsyłania niechcianej korespondencji;
- pozyskiwania danych osobowych;
- ukrywania faktycznego adresu IP poprzez wykorzystanie zainfekowanego komputera do niezgodnej z prawem aktywności w sieci Internet;
- propagacji infekcji na inne komputery"[138].

Wśród niebezpieczeństw mających wpływ na bezpieczeństwo narodowe w cyberprzestrzeni mają wpływ nie tylko zagrożenia, ale także podatności systemów komputerowych. Najczęściej występujące aktualnie zagrożenia i podatności w cyberprzestrzeni z podziałem na działania celowe oraz niezamierzone przedstawia rysunek 4.

[137] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*, CERT.GOV.PL, Warszawa 2016, s. 14.
[138] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku…*, *op. cit.*, 14.



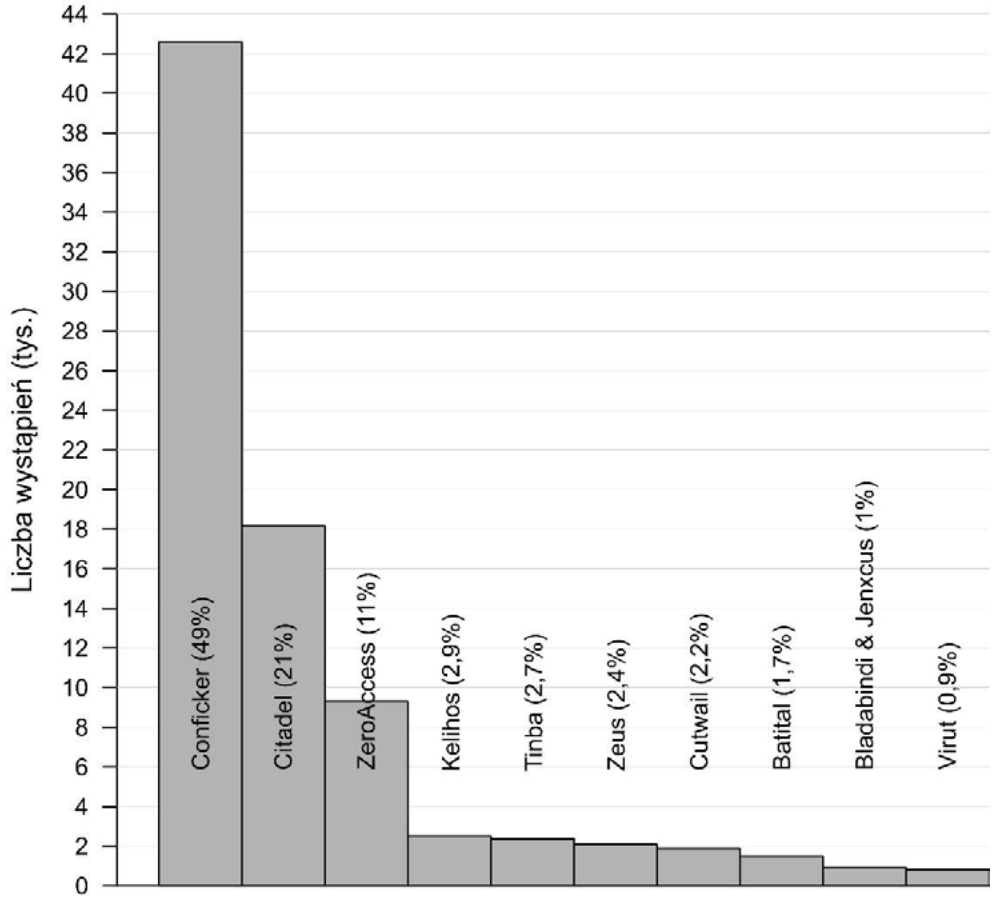
Rysunek 4. Zagrożenia oraz podatności systemów komputerowych mające wpływ na bezpieczeństwo w cyberprzestrzeni

Źródło: opracowanie własne na podstawie *Katalog zagrożeń*, CERT.GOV.PL, 2017, s. 1.

Jednym z celów ataków, wpływających na bezpieczeństwo informacyjne państwa, są próby połączeń stacji roboczych należących do infrastruktury teleinformatycznej instytucji administracji państwowej z siecią **botnet**[139].

[139] **Botnet** (inaczej **bot**) to grupa zhakowanych komputerów, które są kontrolowane w sposób zdalny. Autorem botnetu może być jedna lub kilka osób. Celem ich działania jest infekcja komputerów szkodliwym programem. Poszczególne komputery wchodzące w skład botnetu często nazywane są „botami" lub „komputerami-zombie". Aby dołączyć komputery do botnetu, atakujący używają zazwyczaj jednej z dwóch metod: tzw. ataku *drive-by download* lub wiadomości e-mail. Aby przeprowadzić infekcję z użyciem sposobu *drive-by download*, atakujący musi znaleźć popularną stronę internetową zawierającą możliwą do wykorzystania „lukę" systemową. Następnie na stronie musi zostać umieszczony własny kod wykorzystujący daną „lukę" w przeglądarce internetowej, np. Google Chrome czy Internet Explorer. Zazwyczaj kod ma za zadanie przekierować użytkownika przeglądarki na stronę kontrolowaną przez atakującego, z której zostanie pobrany i zainstalowany kod bota. Metoda infekcji z użyciem poczty e-mail jest znacznie prostsza. Atakujący wysyła dużą partię spamu, a w wiadomościach tych znajduje się określony plik, np. dokument programu Word lub inny plik ze szkodliwym kodem lub odnośnikiem do strony, na której znajduje się szkodliwy kod. W obu przypadkach, gdy przygotowany kod znajdzie się już na komputerze ofiary, staje się on częścią botnetu. Botnety najczęściej są używane w atakach DDoS (atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów). Wykorzystują one moc obliczeniową i przepustowość wielu komputerów, aby wysyłać do określonej strony ogromną ilość ruchu w celu zablokowania jej. Mimo że istnieje wiele odmian ataków DDoS, ich cel pozostaje taki sam.

W okresie dwóch lat (lata 2013-2015), w wyniku prowadzonych badań zanotowano 13235 faktycznych incydentów[140], polegających na próbach tego typu szkodliwych połączeń. Najczęściej występujące botnety w polskiej administracji państwowej, wraz z ich procentowym udziałem zobrazowano na rysunku 5.



Rysunek 5. Najczęściej występujące botnety w administracji państwowej w latach 2013-2015

Źródło: opracowanie własne na podstawie *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 16.

Jest nim zablokowanie działania strony. Często tego typu ataki skierowane są na sektor bankowości internetowej. Z kolei cyberprzestępcy używają ich przeciwko stronom internetowym banków. Botnety są także używane do wielu innych działań: dzięki nim spamerzy wysyłają z zainfekowanych komputerów wiele fałszywych wiadomości e-mail, a cyberprzestępcy używają ich w transakcjach wykorzystujących karty kredytowe, https://plblog.kaspersky.com/botnet/6302/ [dostęp: 03.07.2017].

[140] *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 15.

Najbardziej aktywnym botem był **Conficker** – 49% występujących ataków w Polsce. Conficker znany także jako Downup, Downadup lub Kido to jeden z groźniejszych znanych dotychczas zagrożeń komputerowych. Pojawił się on w 2008 roku, a jego apogeum odnotowano w 2009 roku. W lutym tego samego roku wykazano, że wirus mógł zainfekować ok. 12 milionów komputerów na całym świecie[141]. Należy także zwrócić uwagę, że działanie wirusa było bardzo dynamiczne. W marcu 2009 roku stwierdzono, że najbardziej „zainfekowanymi państwami" są: Wietnam 13%, Brazylia 12%, Filipiny 11%, Indonezja 10%, Algieria 7, USA i Indie – 5% oraz Włochy i Rosja poniżej – 5%[142]. W kwietniu 2009 roku sytuacja dotycząca infekcji, pod względem ich kategoryzacji na liczbę wykrytych infekcji przypadającą na poszczególne państwa świata uległa dużym zmianom. Najbardziej ataki odczuły takie kraje, jak: Chiny 16,8%, Rosja 10,8%, Brazylia 10% oraz Korea, Wietnam, Indie i Ukraina – poniżej 5%[143]. Dane procentowe w zależności od ilości zainfekowanych systemów przypadających na poszczególne kraje, w czasie najwyższej liczby infekcji botem Conficker zestawiono w załączniku (załącznik 1), w postaci wykresów słupkowych.

Conficker, który zaatakował masowo użytkowników komputerów na przełomie marzec-kwiecień 2009 roku ogólnie, pomimo dużej liczby ataków, nie wyrządził znaczących szkód. Jednakże jedna z jego odmian, nazywana odmianą – E i uważana za najgroźniejszą była źródłem ataków na infrastrukturę krytyczną państw. Do takich incydentów możemy zaliczyć ataki na elementy infrastruktury wojskowej – na lotnictwo francuskiej marynarki wojennej, gdzie został sparaliżowany system dystrybucji planów lotów. Skutkowało to powrotem do tradycyjnych form komunikacji: telefonicznej, faksowej i pocztowej. Najprawdopodobniej botnet został zainicjowany poprzez złącze USB w jednej ze stacji komputerowych wchodzących w sieć francuskiej marynarki wojennej – Intramar[144]. Innymi celami ataków Conficker-a były okręty i łodzie podwodne brytyjskiej marynarki wojennej – Royal Navy (75% floty[145]), biura niemieckiej Bundeswehry, a także

[141] J. Nazario, *Two Weeks of Conficker Data and 12 Million Nodes*, 2009, online – https://www.arbornetworks.com/blog/asert/two-weeks-of-conflicker-data/ [dostęp: 05.07.2017].
[142] A. Rhodes, *Do you have Conficker? Find out in your OpenDNS account*, 2009, online – https://umbrela.cisco.com/blog/blog/2009/04/02/do-you-have-conficker-find-out-in-your-opendns-account/ [dostęp: 05.07.2017].
[143] *IBM ISS Managed Security Services,* March 31, 2009.
[144] K. Willsher, *French fighter planes grounded by computer virus*, 2009, online – http://www.telegr aph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html [dostęp: 05.07.2017].
[145] *Ibidem*.

systemy szpitali w angielskim Sheffield. Poza tym celem ataków były systemy rady miejskiej Manchesteru oraz system niższej izby angielskiego parlamentu. Działanie bota polegało na wyłączeniu automatycznych aktualizacji i blokowaniu stron internetowych. Dodatkowo unieszkodliwiał on programy antywirusowe oraz inne bariery obronne (m.in. kasując punkty przywracania systemu). Po zagnieżdżeniu się w systemie, robak łączył się z ukrytymi serwerami i przesyłał na nie wrażliwe dane znalezione na komputerze. Kolejnym przypadkiem był incydent z początku 2010 roku. Conficker spowodował chaos w policyjnej sieci komputerowej Manchesteru i zmuszając funkcjonariuszy do sprawdzania informacji w zewnętrznych komputerach.

Jednym z najbardziej aktywnych botnetów w 2013 roku w Polsce był Citadel – aż 16040 połączeń (21%), którego apogeum aktywności zanotowano w kwietniu 2013 roku[146]. „Citadel jest nazwą złośliwego oprogramowania, które powstało na bazie opublikowanego kodu źródłowego bota Zeus[147]. W 2011 roku kod źródłowy Zeusa wyciekł i został opublikowany. Od tego czasu, na jego bazie powstało wiele różnych odmian, z których jedną jest Citadel. Przestępcy, którzy tworzą Citadela, odsprzedają oprogramowanie (tzw. *crimeware pack*) zawierające program budujący *malware*[148] oraz panel kontrolny botnetu. Następnie klienci sami dbają o zainfekowanie systemów komputerowych oraz zbieranie i wykorzystywanie danych”[149]. Działanie Citadel ukierunkowane jest głównie na sektor bankowy. Botnet działa w ten sposób, że po zalogowaniu się przez klienta do serwisu transakcyjnego banku otrzymuje on informację, że na jego rachunek wpłynęły środki pochodzące z przestępstwa. Bank jednocześnie prosi o zwrot

---

[146] *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 15.

[147] **Zeus** (inaczej **ZeuS**) został zaprojektowany z myślą o tworzeniu botnetów oraz wykradania z komputerów mieszkańców USA oraz Wielkiej Brytanii danych osobowych – głównie informacji niezbędnych do zalogowania się do e-kont. Po uzyskaniu takich danych operator botnetu może się podszyć pod użytkownika. W ten sposób wykradając środki finansowe z jego konta. Zgodnie z tą logiką działały pierwsze wersje tego oprogramowania. Jest ono nadal rozwijane i wyposażane w nowe funkcje. Najnowsza wersja oznaczona jest symbolem v.1.3.4.x. Zaimplementowano w niej funkcje, znane z niektórych legalnych programów – tzn. możliwość podłączenia się do wybranego komputera i przejęcia nad nim pełnej kontroli,
https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted
[dostęp: 03.07.2017].

[148] ***Malware*** – pochodzi od słów *malicious*, co oznacza złośliwy oraz *software* oznaczające – oprogramowanie. Jest to **złośliwe oprogramowanie** (w literaturze informatycznej jako synonim często spotyka się – **szkodliwe oprogramowanie**, w skład którego wchodzą programy, aplikacje czy skrypty, mające szkodliwe, przestępcze, groźne lub destrukcyjne działanie w stosunku do użytkownika komputera), *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, PISM, Warszawa 2009, s. 101.

[149] *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 17.

skradzionych środków, a nawet grozi konsekwencjami karnymi na wypadek braku współpracy i w celu ułatwienia transferu wypełnia za klienta dane do przelewu (wysokość kwoty oraz rachunek odbiorcy). Komunikat ten dzięki takiej socjotechnice wymusza na kliencie zatwierdzenie oszukańczego przelewu za pomocą używanego przez klienta sposobu autoryzacji.

Kolejnym botnetem, którego dużą aktywność zanotowano w ostatnich latach w Polsce jest ZeroAccess (11% aktywności w latach 2013-2015). **Rootkit**[150] ZeroAccess jest niebezpiecznym złośliwym oprogramowaniem. Infekcja systemu komputerowego następuje często poprzez instalację podrobionego programu Adobe Reader lub aktualizację skryptu Java. W rozprzestrzenianiu się botnetu często pomaga brak regularnej ochrony antywirusowej. Tworzące się dziury systemowe ułatwiają przedostanie się złośliwego oprogramowania do systemu komputerowego. Po tym jak ZeroAccess dostanie się do systemu tworzy trudne do wykrycia struktury, które dodatkowo pomagają cyberoszustom pobierać na komputer rożne złośliwe i infekujące programy. Dodatkowo infekcja jest trudno wykrywalna, co powoduje, że jest ona jedną z najbardziej niebezpiecznych zagrożeń internetowych. W dodatku ma ona tendencję do agresywnego użycia zasobów systemowych i przejmowania kontroli nad przeglądarką, co skutkuje irytującymi przekierowaniami np. Google na inne strony, które rozpowszechniają złośliwe oprogramowanie i tym podobne zagrożenia. ZeroAccess jest także używany do infekowania użytkowników podrobionymi programami antyszpiegowskimi, które są specjalnie zaprojektowane do wyłudzania pieniędzy od nieświadomych użytkowników komputerów, poprzez wykradanie danych osobistych, takich jak: hasła, loginy i informację o kartach kredytowych.

W pierwszym kwartale 2016 roku odnotowano największy udział ZeroAccess wśród wszystkich zagrożeń w cyberprzestrzeni[151]. Wykorzystując moc obliczeniową zainfekowanego systemu, posłużył on do generowania kryptowaluty Bitcoin oraz wymuszał zainicjowanie kliknięcia w reklamy typu *pay per click*[152].

---

[150] ***Rootkit*** – to program zaprojektowany w celu zapewnienia hakerom uprawnień administracyjnych do systemu komputowego bez wiedzy jego użytkownika, T.M. Arnold, *A Comparative Analysis of Rootkit Detection Techniques*, University of Houston, Clear Lake 2011, s. 5.

[151] *Cyberbezpieczeństwo. Wyzwania i zagrożenia w 2017 roku*, 2017,
online – http://aspolska.pl/cybe
rbezpieczenstwo-wyzwania-i-zagrozenia-w-2017-roku/ [dostęp: 06.07.2017].

[152] ***Pay per click*** (używany akronim – PPC) – „jest modelem biznesowym rozliczeń za reklamę w Internecie. Reklamodawca płaci nie za samo wyświetlenie reklamy, lecz za realne kliknięcia użytkowników w link lub baner reklamowy. Opłata jest wnoszona przez reklamodawcę za każde przekierowanie z reklamy na jego stronę internetową. Model PPC jest

Trzy najczęściej występujące botnety, w celu porównania ich charakterystycznych cech, zebrano w tabeli 2.

Kolejnym godnym uwagi zagrożeniem jest Tinba. W latach 2013-2015 jego aktywność w polskiej administracji państwowej oszacowana została na 2,7% (liczba wystąpień 2 361)[153]. W 2015 roku średni poziom dziennej liczby zainfekowanych komputerów wyniósł 4,3 tys. Jego głównym celem był sektor bankowy. Działanie Tinba oparte jest na metodzie na tzw. poczekalnię. Podczas logowania się do banku, wprowadzony login i hasło klienta, dzięki dodanemu skryptowi, przesyłane jest na serwer hakerów. Na komputerze klienta przez okres około minuty lub dłużej wyświetlany jest komunikat stwierdzający przesyłanie danych oraz ich aktualizację. W tym czasie odbywa się logowanie przez hakerów do bankowości internetowej klienta, sprawdzanie jego środków finansowych, przygotowanie oszukańczej transakcji, a następnie pobranie informacji z banku o konieczności podania numeru wygenerowanego przez Token w celu autoryzacji i przeprowadzenia transakcji. Po tych czynnościach na komputerze nieświadomego użytkownika skrypt wyświetla komunikat o problemach z uwierzytelnieniem i generuje prośbę o wprowadzenie dodatkowego numeru wygenerowanego przez Token w celu prawidłowego przeprowadzenia procesu uwierzytelnienia tożsamości klienta. Nieświadomy użytkownik wprowadzając numer z Tokena autoryzuje oszukańczą transakcję myśląc, iż dokonuje dodatkowego uwierzytelnienia swojej tożsamości. W celu opóźnienia identyfikacji kradzieży po wykonaniu przelewu, na zainfekowanym komputerze wyświetlany jest przez trojan komunikat przez hakerów o pracach modernizacyjnych i przymusowej przerwie w pracy bankowości internetowej. Wyżej opisany mechanizm może być stosowany również w przypadku autoryzacji transakcji internetowej za pomocą kodów SMS. Ponadto dzięki takim *malware*-om, przestępcy mogą utworzyć nowy przelew zdefiniowany i posiadając już hasło i login do systemu transakcyjnego klienta, mogą samodzielnie dokonywać transakcji oszukańczych z użyciem utworzonego przez siebie przelewu zdefiniowanego, ponieważ takie przelewy nie wymagają dodatkowej autoryzacji.

---

wykorzystywany do rozliczeń w wyszukiwarkach internetowych i sieciach kontekstowych. Z powodzeniem sprawdza się również w przypadku stron internetowych, na których ich właściciele udostępniają miejsce na reklamę",
https://marketingwsieci.pl/slownik-e-marketingu/ppc-pay-per-click/
[dostęp: 30.01.2019].

[153] *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 16.

Tabela 2. Charakterystyka najczęściej występujących zagrożeń typu botnet w Polsce w latach 2013-2015

Nazwa botnetu / Charakterystyka	Conficker	Citadel	ZeroAccess
Infekcja	– podatność w MS MS08–067 – dyski wymienne typu USB – sieci lokalne	– inne złośliwe oprogramowanie – wiadomości *e-mail* – strony *phisingowe* – pulpit zdalny – dyski wymienne i współdzielone	– inne złośliwe oprogramowanie – *cracki* oraz generatory kluczy
Połączenia	– adresy URL oraz P2P w celach aktualizacyjnych – zatrzymanie usług bezpieczeństwa – blokada stron związanych z bezpieczeństwem	– pobieranie złośliwego oprogramowania zawierającego *ransomware* – wyłączenie systemów bezpieczeństwa – połączenia URL – pobieranie konfiguracji	– pobieranie i uruchamianie innych plików – wyłączenie systemów bezpieczeństwa – wysyłanie informacji o komputerze – przenoszenie na inne pliki
Kradzież i gromadzenie	– rozsyłanie wiadomości spam – kradzież wrażliwych danych i haseł – ataki DDoS[154]	– kradzieże finansowe – kradzieże danych osobowych – gromadzenie danych wrażliwych i haseł dostępu – dane FTP – poczta elektroniczna – rozsyłanie wiadomości spam – ataki DDoS	– przechwytywanie ruchu sieciowego (w tym przeglądarki internetowej) – kliknięcia w reklamy przynoszące korzyści finansowe (PPC) – wykorzystanie mocy obliczeniowej do wytwarzania bitcoin-ów – ataki DDoS

[154] **Ataki DDoS** (ang. *Distributed Denial of Service* – rozproszona odmowa dostępu) „to jedna z metod wykorzystywanych do blokowania internetowych serwisów lub blokowania łączy internetowych. Wyróżnia się 2 podstawowe rodzaje ataków DDoS: **atak wolumetryczny** (polegający na masowej wysyłce niechcianych danych na wskazany adres IP, w wyniku czego ilość napływających danych jest tak duża, że łącze/a internetowe nie są w stanie przyjąć tych wszystkich danych) oraz **atak aplikacyjny** (inaczej typu *slow*, polegający na wyczerpaniu zasobów informatycznych aplikacji internetowej, np. mocy obliczeniowej lub pamięci)", *Co to jest atak DDoS i jak się przed nim chronić?*, Dataspace 2017, s. 3, https://dataspace.pl/assets/ddos_broszura_web.pdf [dostęp: 31.01.2019].

Nazwa botnetu / Charakterystyka	Conficker	Citadel	ZeroAccess
Sposoby ochrony i obrony	– aktualizacja systemu operacyjnego – używanie silnych haseł – używanie oprogramowania antywirusowego – instalacja narzędzia MSRT	– aktualizacja systemu operacyjnego – używanie oprogramowania antywirusowego – używanie bezpiecznych przeglądarek internetowych – systemy antyspamowe	– aktualizacja systemu operacyjnego – używanie oprogramowania antywirusowego – używanie legalnego oprogramowania

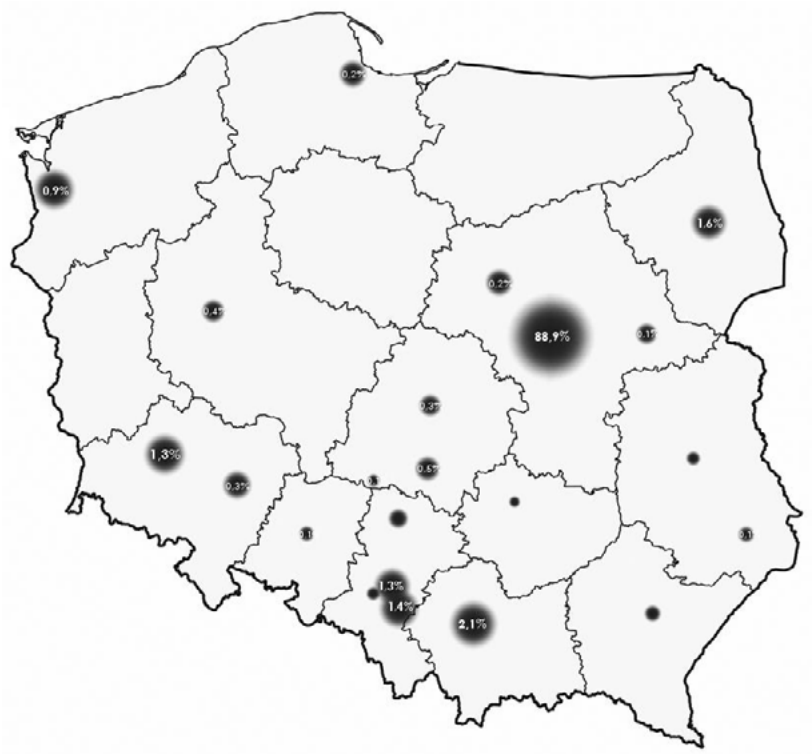
Źródło: za *Raport o stanie bezpieczeństwa…, op. cit.*, s. 18.

Innym, poruszanym już w pracy, zagrożeniem typu botnet jest Zeus oraz jego jedna z odmian nazwana GameOver Zeus[155]. W tej wersji trojana skupiono się na eliminacji najsłabszego ogniwa – scentralizowanego systemu dystrybucji informacji. Poprzednie wersje Zeus-a oparte było o jeden (lub kilka) zdefiniowanych adresów, pod którymi dostępne było centrum zarządzania. Pozwalało to łatwo namierzyć takie adresy i poprzez ich blokowanie zahamować rozprzestrzenianie się oraz szkodliwe działanie botnetu. Badany wariant trojana wykorzystuje dwa nowe kanały komunikacyjne do pobierania nowych rozkazów. Działanie tej wersji trojana skupione jest na pozyskiwaniu informacji osobistych użytkowników, takich jak hasła czy dane finansowe. Gdy ofiara pracująca z systemem Windows kliknie zainfekowany załącznik, z komputera pobierane są żądane dane, a zarażona maszyna zaczyna wysyłać wiadomości spamowe mające na celu przyciągniecie kolejnych ofiar i szybie rozprzestrzenienie ataku w Internecie. Aktywność botneta GOZ skupiona była głównie w USA (25% infekcji, około 1 mln zainfekowanych systemów) oraz Europie[156] (załącznik 2).

W Polsce aktywność Zeus-a w ostatnich latach zdecydowanie zmalała (w latach 2013-2015 ok. 2,4% ataków). Jeśli chodzi o lokalizację ataków w Polsce, to głównie zlokalizowane one były w województwie mazowieckim (89,2%) – rysunek. 6. Z uwagi na bezpieczeństwo narodowe, należy zauważyć, że lokalizacja ta znajduje się w obszarze administracji rządowej oraz obsługuje przedsiębiorstwa kluczowe dla zapewnienia bezpieczeń-

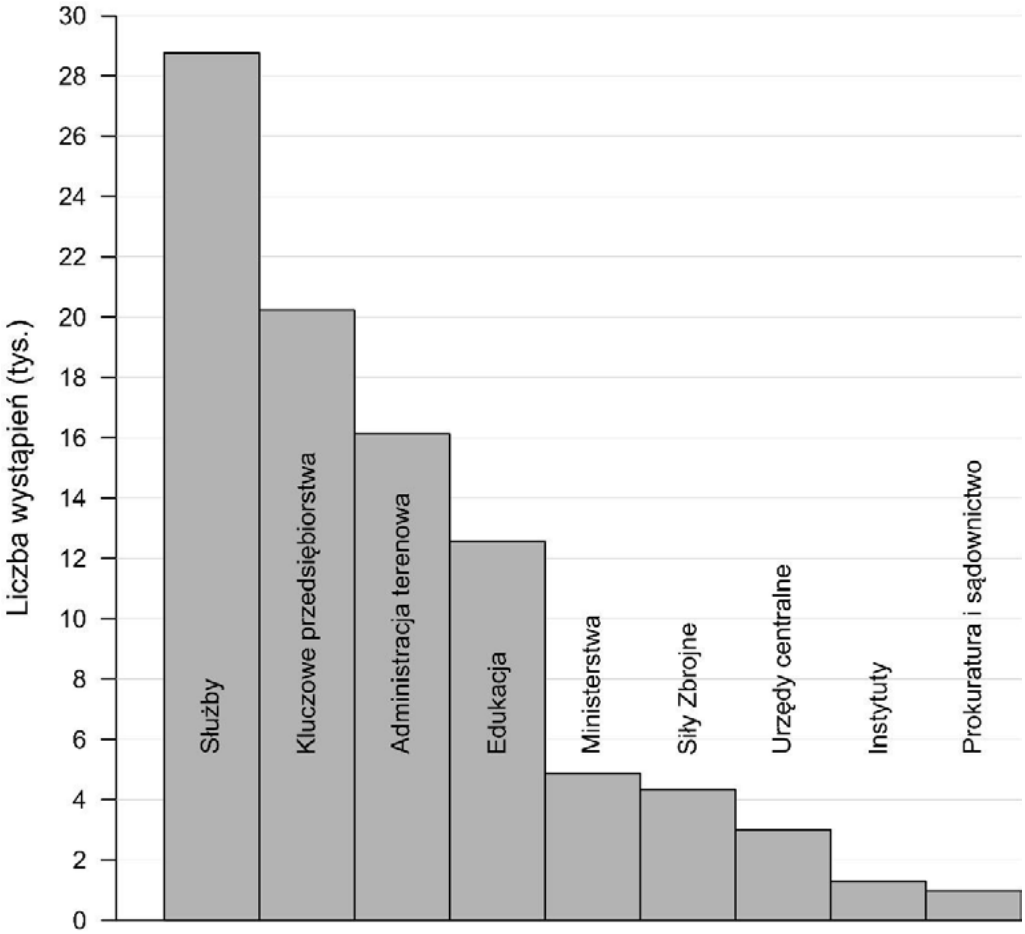
[155] W literaturze często nazywany jest akronimem pełnej jego nazwy – **GOZ**.
[156] *ZeuS – P2P+DGA variant – mapping out and understanding the threat*, 2012, online – https://www.cert.pl/news/single/zeus-wariant-p2pdga-analiza-nowego-zagrozenia/ [dostęp: 05.07.2017].

stwa i integralności państwa. Skupione są tam także instytucje z obszaru administracji rządowej. Poza województwem mazowieckim, najwięcej złośliwych połączeń odnotowano w obszarach, w których rozlokowane są strategiczne przedsiębiorstwa – duże miasta, takie jak: Białystok, Szczecin, Kraków czy Trójmiasto.



Rysunek 6. Aktywność zainfekowanych botnetem Zeus hostów w administracji państwowej w latach 2013-2015
Źródło: *Raport o stanie bezpieczeństwa*…, *op. cit.*, s. 23.

Wyżej określone, współczesne zagrożenia pochodzące z cyberprzestrzeni i mające wpływ na administrację państwową, a tym samym wpływające na bezpieczeństwo narodowe w cyberprzestrzeni, możemy podzielić na sektory społeczno-gospodarcze (rysunek 7), na które one oddziaływują.



Rysunek 7. Najczęściej występujące botnety w administracji państwowej w latach 2013-2015

Źródło: opracowanie własne na podstawie *Raport o stanie bezpieczeństwa…, op. cit.*, s. 19.

Analiza danych ujętych na rysunku7 wskazuje, że na pierwszym miejscu (w latach 2013-2015) pod względem ataków, plasują się służby (30,72%, 28755 ataków), czyli jednostki powoływane przez państwo lub jego organy do spełniania części jego podstawowych zadań, takich jak bezpieczeństwo wewnętrzne. Kolejną grupą są kluczowe przedsiębiorstwa (21,62%, 20 235 ataków) i administracja terenowa, wraz z urzędami wojewódzkimi (7,22%, 16 118 ataków)[157]. Na szóstym miejscu, pod względem liczby ataków znalazły się Siły Zbrojne Rzeczypospolitej Polskiej (SZ RP). Powyższa analiza, z podziałem na sektory społeczno-gospodarcze państwa pozwala konstatować, że ataki typu botnet są skierowane i mają decydujący wpływ na poziom bezpieczeństwa narodowego w cyberprzestrzeni.

[157] *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 19.

Podsumowując, można stwierdzić, że wyraźny spadek zagrożeń typu botnet nastąpił w 2015 roku. Powodem takiego stanu rzeczy były działania skierowane przeciwko temu zagrożeniu, w tym przeciwko systemom kierującym grupami zarażonych komputerów tzw. *Command & Control* – C&C. Ponadto intensywnie rozpowszechniano wiadomości dotyczące ochrony systemów przez botnetami, uświadamiając użytkowników o zagrożeniu. Do praktyk takich należało: instalowanie i zautomatyzowanie uaktualniania programów zabezpieczających, zwiększenie poziomu zabezpieczeń w ustawieniach przeglądarki internetowej, ograniczenie użytkowników do przeglądania Internetu czy uaktualnienie i instalacja poprawek systemowych[158].

W ostatnich latach obserwowany jest wzrost zagrożeń typu inżynieria społeczna z kategorii *phishing*. Przykładowo w roku 2013 zanotowano 34 takie zagrożenia, rok później – 119, a w 2015 roku 257 takich zagrożeń[159]. Atakowanymi podmiotami były zazwyczaj administracja i infrastruktura krytyczna (głównie kluczowe przedsiębiorstwa państwa). Najczęstszymi incydentami, których celem była administracja, były podmioty wykorzystujące wizerunek: grupy helpdesk, firmy DHL oraz Poczty Polskiej, a także dużych banków, takich jak: PKO, ING, Alior, mBank, Pekao. Wiadomości zawierały linki do witryn wyłudzających dane osobowe (w tym dane wrażliwe) oraz dane autoryzacyjne do serwisów bankowości elektronicznej. Złośliwe oprogramowanie przesyłane było w formie archiwum, a także w formie dokumentu programu Microsoft Office, z rozszerzeniem pliku typu .doc z dołączonym makrem w formie tzw. *dropper*. Stanowi je złośliwe oprogramowanie, które po uruchomieniu może się replikować i infekować inne pliki oraz programy. Może ono także zajmować miejsce na dysku twardym oraz pamięć, spowalniając w ten sposób pracę komputera lub zupełnie ją zatrzymując. Może też uszkadzać lub usuwać dane, czyścić dane na dysku twardym komputera, kraść informacje osobiste, przejmować kontrolę nad ekranem i wysyłać do użytkowników z listy kontaktów spam, aby rozpowszechniać się na inne komputery.

Wśród incydentów, w których celem uczyniono infrastrukturę krytyczną, najczęściej wykorzystywano wizerunek firmy DHL, Poczty Polskiej oraz grupy asystent. Wiadomości w większości przypadków były wzbogacone o złośliwe oprogramowanie w formacie wykonywalnym, ukryte w archiwach (w niektórych przypadkach zabezpieczonych hasłem przekazywanym w treści wiadomości), a także w formacie dokumentu tekstowego MS

[158] *Boty i sieci typu „bot" — rosnące zagrożenie*, online – https://pl.norton.com/botnet [dostęp: 07.07.2017].
[159] *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 41.

Office lub odnośników w formacie HTTP do zasobów hostujących[160] oprogramowanie złośliwe. Część z ataków zawierała odnośniki do witryn wyłudzających dane. Zakres tematyczny przesyłanych wiadomości w większości wykorzystywał schemat niezapłaconej faktury bądź odbioru paczki. Jak podkreśla się w raporcie, grupa incydentów ukierunkowanych na infrastrukturę krytyczną była, bardziej niż w przypadku ataków na administrację, spersonalizowana w rozumieniu liczby odbiorców, konkretnych osób obranych za cel oraz wykorzystania wizerunku. Zakłada się, że takie działanie wynikało z chęci pozyskania przez atakującego danych firmy celem odsprzedaży ich na drodze szantażu lub czarnym rynku[161].

Można stwierdzić, że cyberprzestrzeń niesie ze sobą różnego rodzaju zagrożenia. Do najbardziej typowych i powszechnych współcześnie zaliczyć można niebezpieczeństwo:

- utraty danych;
- zainfekowanie komputera szkodliwym oprogramowaniem, np. robaki, wirusy itp.;
- blokowanie dostępu do usług;
- *spam* (niepotrzebne lub niechciane wiadomości elektroniczne);
- śledzenia aktywności użytkowników i ingerowanie w ich prywatność;
- wyłudzanie danych osobowych oraz kradzież tożsamości;
- zniesławienie/znieważenie na forum internetowym;
- naruszania praw własności intelektualnej, np. prawa autorskie;
- oszustw związanych z zawieraniem transakcji drogą elektroniczną.

4.3. Perspektywa i ewaluacja zagrożeń państwa w cyberprzestrzeni

Analizując przyszłość zagrożeń pochodzących z cyberprzestrzeni można posłużyć się szacunkami przygotowanymi przez Instytut Kościuszki. Według jego perspektywy przewiduje się 5 podstawowych zagrożeń, wśród których wyróżniamy: Internet rzeczy, zwiększenie się aktywności cyberterrorystów oraz rozwój tzw. Darknetu, wzrost napięcia międzynarodowego związanego z cyberatakami, jak i intensyfikacja prac legislacyjnych w obszarze cyberbezpieczeństwa[162].

[160] **Hosting** – jest to udostępnianie przez dostawcę usług internetowych zasobów umieszczonych na serwerach.
[161] *Raport o stanie bezpieczeństwa…*, *op. cit.*, s. 43.
[162] *Pięć wyzwań cyberbezpieczeństwa w 2017 roku*,
online – http://www.cyberdefence24.pl/520039,piec-wyzwan-cyberbezpieczenstwa-w-2017-roku [dostęp: 09.07.2017].

Pierwszym z nich jest **Internet rzeczy**. W ostatnich latach dynamiczny wzrost liczby ataków był wykonywany nie tylko za pomocą systemu komputerowego, ale również za pośrednictwem tzw. Internetu rzeczy (ang. *Internet of Things* – IoT), dzięki któremu urządzenia mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem instalacji elektrycznej lub sieci komputerowej. Przykładowo w 2016 roku do największego w historii ataku DDoS wykorzystano głównie zainfekowane wcześniej kamery internetowe oraz rejestratory obrazu. Szacuje się, że ten rok i przyszłe lata przyniosą wzrost ataków z wykorzystaniem IoT. Powodem takiego stanu rzeczy jest wyposażanie coraz to większej liczby urządzeń w aplikacje oraz możliwość łączenia się w sieć, co ważne często bez przeprowadzenia testów bezpieczeństwa. W efekcie takie urządzenia stają się podatne na ataki, zwłaszcza przy braku zaleceń zmiany domyślnych haseł, które zazwyczaj nie stanowią tajemnicy.

Drugim określonym niebezpieczeństwem może stać się – zwiększenie się aktywności cyberterrorystów oraz rozwój tzw. Darknetu. Stanowi go zbiór różnych anonimowych stron internetowych, sklepów, for dyskusyjnych i innych serwisów dostępnych w Internecie. W przeciwieństwie do zwykłych stron internetowych, nie są one dostępne przez adres www i nie można ich znaleźć w zwykłych wyszukiwarkach jak Google (dedykowaną przeglądarką jest np. Grams). Działanie sieci polega na przekazaniu ich adresów przez osoby je tworzące. Darknet ułatwia popełnianie wielu wykroczeń i przestępstw tak o charakterze cyfrowym, jak i klasycznym (np. handlu narkotykami). Szacuje się, że walka z tym zjawiskiem będzie główną płaszczyzną współpracy między podmiotami odpowiedzialnymi za zapewnienie cyberbezpieczeństwa państwa. Rozwój Darknetu może również przełożyć się na wzrost zagrożenia związanego z wykorzystaniem cyberataków przez grupy terrorystyczne. W opinii Komandora Wiesława Goździewicza, radcy prawnego w NATO Joint Force Training Centre w Bydgoszczy, jest wyłącznie kwestią czasu, kiedy zobaczymy pierwszy udany atak hakerski spowodowany przez cyberterrorystów. Nie jest wykluczone, że narzędzia potrzebne do jego przeprowadzenia pozyskane zostaną właśnie w Darknecie[163].

„Trzecim zdefiniowanym zagrożeniem jest wzrost napięcia międzynarodowego związanego z cyberatakami. Apogeum tak prowadzonej walki informacyjnej zostało unaocznione w 2016 r. zarówno w konsekwencji cyberataków, jakie miały miejsce podczas kampanii prezydenckiej w USA, jak i podczas konfliktu na Ukrainie”[164].

[163] https://cybersecforum.eu/pl/nas-czeka-obszarze-cyberbezpieczenstwa-2017-r-publikujemy-prognozy-ekspertow/ [dostęp: 31.01.2019].
[164] *Ibidem*.

„Kolejną niepewnością jest wzmożenie i intensyfikacja prac legislacyjnych w obszarze cyberbezpieczeństwa. Okazuje się bowiem, że rosnąca ilość cyberzagrożeń w połączeniu z niewystarczającymi zasobami prawnorynkowymi umożliwiającymi zapewnienie wysokiego poziomu cyberbezpieczeństwa (…) [wymuszają silny nacisk – przyp. aut.] (…) na tworzenie nowych regulacji w tym obszarze. Oprócz starań ze strony instytucji publicznych, również sektor prywatny będzie musiał jeszcze lepiej zadbać o swoje cyberbezpieczeństwo, szczególnie, że coraz bardziej narażony jest on na zagrożenia wynikające z cyberprzestrzeni”[165]. Szczególnie ważne są tutaj elementy wchodzące w skład systemu przedsiębiorstw, jako zagrożenia z cyberprzestrzeni, których przedmiotem są organy państwa. Z tego powodu, z punktu widzenia bezpieczeństwa państwa, sektor małych i średnich przedsiębiorstw dostrzega potrzebę podjęcia inicjatyw dotyczących ochrony przed zagrożeniami, pochodzącymi z cyberprzestrzeni (51% uznaje cyberbezpieczeństwo za istotny czynnik wpływający na rozwój firmy). Dowodzi to, że następuje systematyczny wzrost świadomości polskich przedsiębiorstw na temat konsekwencji potencjalnych ataków. Wśród zagrożeń, które w opinii małych i średnich firm mogą spowodować największe straty finansowe, znalazły się DDoS oraz malware, które zostały określone jako najtrudniejsze do wykrycia. Według szacunków nadal będą one utrzymywać się na wysokim poziomie. Poza kwestami bezpieczeństwa osobowego oraz bezpieczeństwa narodowego należy uznać, że cyberataki wiążą się z ogromnymi stratami dla firm zarówno materialnymi, jak też wizerunkowymi. Zanotowane w Polsce w 2015 r. incydenty naruszenia informacji w 33% przełożyły się na straty finansowe, w 31% na ujawnienie lub modyfikację danych, a w 16% na utratę reputacji. Jak wynika z danych zebranych w raporcie z 2016 roku, 4% polskich firm w wyniku cyberataków straciło ponad 1 mln zł, a 5% odnotowało przestój w działalności dłuższy niż 5 dni[166].

Ostatnim z tej grupy zagrożeń w niedalekiej perspektywie wydaje się być – brak oraz zwiększająca się potrzeba pozyskania wykwalifikowanych cyberspecjalistów. Osoby te są niezbędne, jako dydaktycy –„kompetentni profesorowie, najlepiej z doświadczeniem z sektora prywatnego. Łączą oni bowiem wiedzę teoretyczną z praktyką. Skuteczny system kształcenia cyberspecjalistów wymaga multidyscyplinarnego podejścia, dlatego nie może ograniczać się tylko i wyłącznie do ekspertów technicznych”[167].

---

[165] https://cybersecforum.eu/pl/nas-czeka-obszarze-cyberbezpieczenstwa-2017-r-publikujemy-prognozy-ekspertow/ [dostęp: 31.01.2019].

[166] *Liczba cyberataków na firmy w Polsce rośnie znacznie szybciej niż na świecie*, 2016, online – https://www.pwc.pl/pl/media/2016/2016-01-12-liczba-cyberatakow-na-firmy-w-polsce-rosnie.html [dostęp: 10.07.2016].

[167] https://cybersecforum.eu/pl/nas-czeka-obszarze-cyberbezpieczenstwa-2017-r-

Dokonując analizy stanu zagrożeń oraz reasumując wyżej zawarte treści, można przyjąć kryterium zagrożenia państwa i przedstawić je w trzech płaszczyznach: technicznej, prawnej oraz edukacyjnej. Zagrożenia techniczne to podstawowy obszar, na którym istnieją możliwości zapobiegania im, jak również możliwości wykrywania incydentów, a także reagowania na nie. W tym obszarze istnieje możliwość zastosowania fizycznych (sprzętowych) oraz logicznych (programowych) zabezpieczeń. W tym zakresie mieszczą się również różnego rodzaju organizacyjne mechanizmy mające na celu ochronę systemów teleinformatycznych i przetwarzanych tam danych. Drugi istotny obszar, który wykorzystywany jest dla zapobiegania, jak i zwalczania zjawisk niepożądanych w tym zakresie jest prawo. Poprzez określenie czynów zabronionych, a także nałożenie pewnych obowiązków związanych z oferowaniem i wykorzystywaniem technologii informacyjnych, jak również komunikacyjnych, prawodawca stara się oddziaływać na osoby, które posługują się tego typu urządzeniami. Kolejne trudności związane są z dynamicznym rozwojem technologii – prawodawca zazwyczaj reaguje na postęp technologiczny, próbując nadążyć za zmianami, zazwyczaj pozostając w tyle. Stworzenie odpowiednich ram prawnych, jak również wdrożenie rozwiązań technicznych nie gwarantuje skutecznej ochrony. Współcześni użytkownicy, korzystający z usług opartych na technologiach informacyjnych i komunikacyjnych, są często nieświadomi zagrożeń. Zdarza się także, że mają świadomość zagrożenia, a mimo to je lekceważą. W wielu przypadkach potwierdza się reguła, że człowiek to najsłabsze ogniwo w systemie zabezpieczeń. Nawet najskuteczniejsze zabezpieczenia techniczne na nic się nie zdadzą, jeśli nie będą iść w parze z ostrożnością oraz rozwagą użytkowników. Trzeci obszar, równie ważny, dotyczy działań edukacyjnych, które opierają się na wiedzy na temat zagrożeń i świadomości użytkowników, co do możliwości zminimalizowania ryzyka związanego z korzystaniem z nowych technologii[168], w ten sposób ograniczając zagrożenia wpływające na bezpieczeństwo narodowe.

4.4. Ewaluacja poziomu ryzyka zagrożeń bezpieczeństwa narodowego w cyberprzestrzeni

Literatura przedmiotu oraz ustanowione akty prawne (normy) pozwalają na zarządzanie ryzykiem[169] w bezpieczeństwie informacyjnym w za-

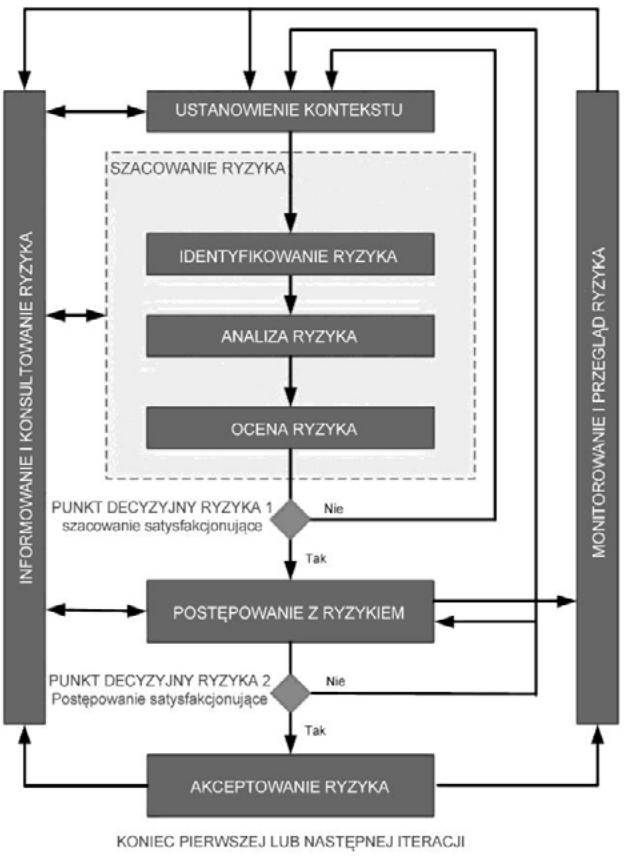
publikujemy-prognozy-ekspertow/

[168] A. Podraza, P. Potakowski, K. Wiak, *Cyberterroryzm zagrożeniem XXI wieku*, Difin, Warszawa 2013, s. 142-144.

[169] **Ryzyko** – „to prawdopodobieństwo, że podmiot poniesie straty w następstwie podjęcia

kresie zagrożeń pochodzących z cyberprzestrzeni. Poprzez zarządzanie ryzykiem należy rozumieć działania polegające na jego szacowaniu, postępowaniu z ryzykiem, jego akceptowaniu (w zakresie określonego poziomu ryzyka), monitorowaniu ryzyka oraz o informowaniu o występującym ryzyku.

Zarządzanie ryzykiem w bezpieczeństwie informacji zazwyczaj odbywa się zgodnie z modelem przedstawionym na rysunku 8.



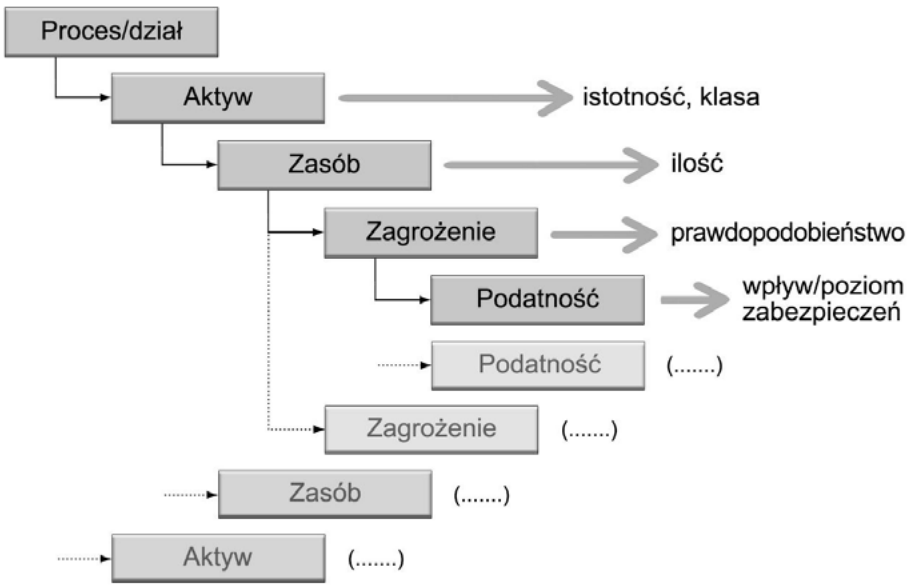
Rysunek 8. Schemat blokowy procesu zarządzania ryzykiem w bezpieczeństwie informacji

Źródło: PN-ISO/IEC 27005:2010 Zarządzanie ryzykiem w bezpieczeństwie informacji; PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN, Warszawa 2013.

---

danej decyzji. Także takie działanie czy przedsięwzięcie, w którym nie wszystkie zmienne są oszacowane lub nie dadzą się oszacować na bazie rachunku prawdopodobieństwa. Ryzyko różni się od niepewności tym, że dotyczy zjawisk powtarzalnych, które można w pewnej mierze skalkulować",
Encyklopedia Zarządzania, online – https://mfiles.pl/pl/index.php/Ryzyko [dostęp: 11.07.2017].

Kluczowym procesem zarządzania ryzykiem jest jego szacowanie. Innymi słowy jest to komplementarny, całościowy proces analizy i oceny ryzyka, na który zgodnie ze schematem przedstawionym na rysunku 8, składają się kolejno: identyfikowanie, analiza i ocena ryzyka. Kluczowymi elementami w tym procesie są **aktywa** – czyli to, co ma decydującą wartość dla organizacji (czy państwa). Określa się wartość aktywów, szacuje się prawdopodobieństwo wystąpienia zagrożeń, podatności aktywów na zagrożenia oraz wpływ zagrożenia na bezpieczeństwo aktywów oraz stosowane zabezpieczenia. Z praktycznego punktu widzenia ważnym jest zasób, czyli miejsce, gdzie przetwarzane są dane. Zatem przetwarzane dane są aktywami, a miejsce ich przetwarzania zasobem. Z tak zaprojektowanych etapów analizy możemy pozyskać informację, że o ile każdy z aktywów ma swoją wartość, to wartość zasobu, na którym znajdują się te aktywa jest dużo wyższa. Wynika to z faktu, że jest sumą wartości aktywów znajdujących się na nim. Jak wskazuje W. Gełzakowski, nie jest konieczne zabezpieczenie każdego z systemów oddzielnie[170]. Wzajemne zależności pomiędzy poszczególnymi elementami obrazuje rysunek 9.



Rysunek 9. Struktura analizy ryzyka w bezpieczeństwie informacji
Źródło: W. Gełzakowski, ISO 27005 Analiza ryzyka, https://www.centrum-doskonalenia.pl/wdrozenie-i-certyfikacja-iso/normy-iso/iso-27005-analiza-ryzyka/ [dostęp: 31.01.2019].

[170] W. Gełzakowski, *ISO 27005 Analiza ryzyka*, https://www.centrum-doskonalenia.pl/wdrozenie-i-certyfikacja-iso/normy-iso/iso-27005-analiza-ryzyka/ [dostęp: 31.01.2019].

Krok 1 – Identyfikacja aktywów

Jak określono wcześniej kluczowym elementem procesu szacowania ryzyka są aktywa. Stąd niezbędne jest przeprowadzenie inwentaryzacji aktywów państwa i określenie ich wartości dla bezpieczeństwa państwa. Podczas określania wartości aktywu należy wziąć pod rozwagę, jaki wpływ na funkcjonowanie państwa będzie miała jego utrata lub inne niestabilności oraz problemy. Im większy zakres oddziaływania, tym większa wartość aktywu. Wartość najlepiej oceniać biorąc pod uwagę znaczenie dla państwa i wyrażać w dowolnie przyjętej skali – względną ocenę istotności aktywu w stosunku do pozostałych aktywów. Stosując skalę np. czterostopniową, ważne jest określenie znaczenia poszczególnych wystąpień[171] (tabela 3).

Tabela 3. Istotność aktywów w szacowaniu ryzyka bezpieczeństwa informacyjnego

Poziom istotności	Opis
Bardzo duży	utrata lub naruszenie bezpieczeństwa aktywu powoduje przerwanie procesów ważnych z punktu widzenia bezpieczeństwa narodowego
Znaczący	utrata lub naruszenie bezpieczeństwa aktywu może mieć wpływ na realizację procesów ważnych z punktu widzenia bezpieczeństwa narodowego
Średni	utrata lub naruszenie bezpieczeństwa aktywu powoduje utrudnienia w normalnym funkcjonowaniu procesów ważnych z punktu widzenia bezpieczeństwa narodowego
Pomijalny	utrata lub naruszenie bezpieczeństwa aktywu nie ma wpływu na funkcjonowanie procesów ważnych z punktu widzenia bezpieczeństwa narodowego

Źródło: opracowanie własne na podstawie W. Gełzakowski, *op. cit.*

Liczebność zasobów/ilość miejsc przetwarzania informacji może mieć wpływ na bezpieczeństwo aktywów. W sytuacji ochrony aktywu przed utratą poufności, w im większej ilości zasobów/miejsc przetwarzania ten aktyw się znajduje, tym wyższe jest ryzyko zagrożenia informacji. W odniesieniu do aktywów, które powinny być dostępne, zwiększenie ilości miejsc, gdzie one się znajdują skutkuje zwiększeniem ich dostępności. Omawiana metodyka wymaga doprecyzowania liczby zasobów/miejsc przetwarzania, na których analizowany aktyw się znajduje oraz określenia wpływu tej liczby na podatność aktywu[172].

[171] W. Gełzakowski, *op. cit*.
[172] *Ibidem*.

Krok 2 – Identyfikacja zagrożeń

Chcąc zabezpieczyć aktywa czy zasoby, należy dokonać identyfikacji zagrożeń[173] w odniesieniu do konkretnego wcześniej określonego aktywu. Ważne jest to, aby wskazane zagrożenia odzwierciedlały rzeczywistość. W obszarze kompletności szacowania ryzyka, powinna być brana pod rozwagę jak największa liczba zagrożeń (także tych mało realnych) – ale należy pamiętać, że ważnym komponentem procesu analizy ryzyka jest możliwość uzyskania aktualnych i miarodajnych wyników. Zbyt wielowymiarowa analiza – o mniej istotne elementy – może skutkować tym, że w momencie jej zakończenia już będzie nieaktualna[174].

Krok 3 – Określenie prawdopodobieństwa

Z uwagi na fakt, że zagrożenia występują z różną częstotliwością, w analizie ryzyka można posłużyć się pojęciem prawdopodobieństwa wystąpienia zagrożenia. Ponadto, jak wskazuje W. Gełzakowski, zazwyczaj można wykorzystać trzystopniową skalą, określając ryzyko jako – wysokie, średnie i pomijalne (tabela 4).

Tabela 4. Skala prawdopodobieństwa wystąpienia ryzyka bezpieczeństwa informacyjnego

Poziom ryzyka	Opis
wysokie	występuje często (np. raz w miesiącu) lub regularnie z ustaloną częstotliwością
średnie	wystąpiło w ostatnim roku lub zdarza się nieregularnie
pomijalne	nie wystąpiło ani razu w ciągu roku

Źródło: W. Gełzakowski, *op. cit.*

Celem szacowania prawdopodobieństwa wystąpienia incydentu jest ustalenie częstości, z jaką mogą pojawiać się określone zagrożenia. Pod uwagę powinny być brane następujące okoliczności:

- doświadczenie szacującego oraz statystyki dotyczące podobnych zdarzeń;
- w przypadku zagrożeń antropogennych atrakcyjność zasobu lub efektu skutku dla wywołującego incydent;
- dla zagrożeń o charakterze przypadkowym położenie geograficzne, warunki pogodowe itp., które mogą oddziaływać na powstawanie błędnych działań użytkowników zasobów informacyjnych lub syste-

[173] Identyfikacji zagrożeń dokonano powyżej.

[174] *The Security Risk Management Guide*, Microsoft Corporation, 2006; W. Gełzakowski, *op. cit.*

mów teleinformatycznych;
- rodzaje podatności;
- istniejące zabezpieczenia.

Krok 4 – Określenie podatności

Jeśli ustalone zostały określone – aktywa (co chronimy), istotność (dlaczego chronimy) oraz zagrożenia (przed czym chronimy), należy dodatkowo ustalić słabe strony aktywów – tzn. cechy i właściwości aktywu. Podatność określa się właśnie w tym celu – określania słabych stron tego, co należy chronić, zapewniając wysoki poziom bezpieczeństwa narodowego.

Krok 5 –Określenie wpływu zagrożenia a poziom zabezpieczeń

Końcowymi elementami analizy ryzyka są kwestie wiążące się z oceną wpływu zagrożenia na: poufność, integralność i dostępność (tabela 5) oraz określenie poziomu implementowanych zabezpieczeń[175] (tabela 6).

Tabela 5. Ocena wpływu zagrożenia wystąpienia ryzyka bezpieczeństwa informacyjnego

Poziom istotności	Opis
krytyczny	wystąpienie zagrożenia powoduje dużego zagrożenia bezpieczeństwa narodowego
średni	wystąpienie zagrożenia może mieć duży wpływ na zagrożenie bezpieczeństwa narodowego
pomijalny	wystąpienie zagrożenia nie powoduje wystąpienia dużego zagrożenia bezpieczeństwa narodowego
nie dotyczy	wystąpienie zagrożenia nie ma wpływu na aktyw

Źródło: W. Gełzakowski, *op. cit.*

Tabela 6. Poziom wdrożonych zabezpieczeń bezpieczeństwa informacyjnego

Poziom zabezpieczeń	Opis
wysoki	występujące zabezpieczenie chroni skutecznie przed znanymi zagrożeniami
średni	występują częściowe zabezpieczenia, które chronią tylko wybrane obszary państwa lub nie są w pełni skuteczne
niski	praktycznie brak jest jakichkolwiek zabezpieczeń lub są one nieskuteczne
nie dotyczy	wystąpienie zagrożenia nie ma wpływu na aktyw

Źródło: W. Gełzakowski, *op. cit.*

[175] W. Gełzakowski, *op. cit*.

Krok 6 – Określenie ryzyka szczątkowego

Ryzyko aktywu określa, „na ile obawiamy się realnej utraty bezpieczeństwa [narodowego – przyp. aut.] tego aktywu na tle pozostałych aktywów w sytuacji, kiedy nie stosujemy jeszcze żadnych zabezpieczeń. Lista aktywów, posortowana wg ich ryzyka, stanowi podstawę do określenia, jakie zabezpieczenia powinny być zastosowane w celu ochrony najbardziej ryzykownych aktywów. W celu uzyskania porównywalnych ze sobą ryzyka aktywów, należy ustalić sposób ich obliczania. Żeby móc obliczyć ich wartość należy podstawić do poniższego wzoru wartości liczbowe przypisane do poszczególnych pozycji. Wielkości nie są istotne, ważna jest ich powtarzalność”[176].

Ryzyko aktywu jest obliczane według odpowiedniej zależności matematycznej. Po wyborze i wdrożeniu zabezpieczeń należy ponownie przeprowadzić szacowanie ryzyka, ale już z uwzględnieniem poziomów zabezpieczeń, jakie zostały zapewnione dzięki wdrożonym zabezpieczeniom – są one nazywane **ryzykiem szczątkowym**. Sposób obliczenia ryzyka aktywu oraz ryzyka szczątkowego w formie zależności matematycznych przedstawiono w załączniku[177] (załącznik 3).

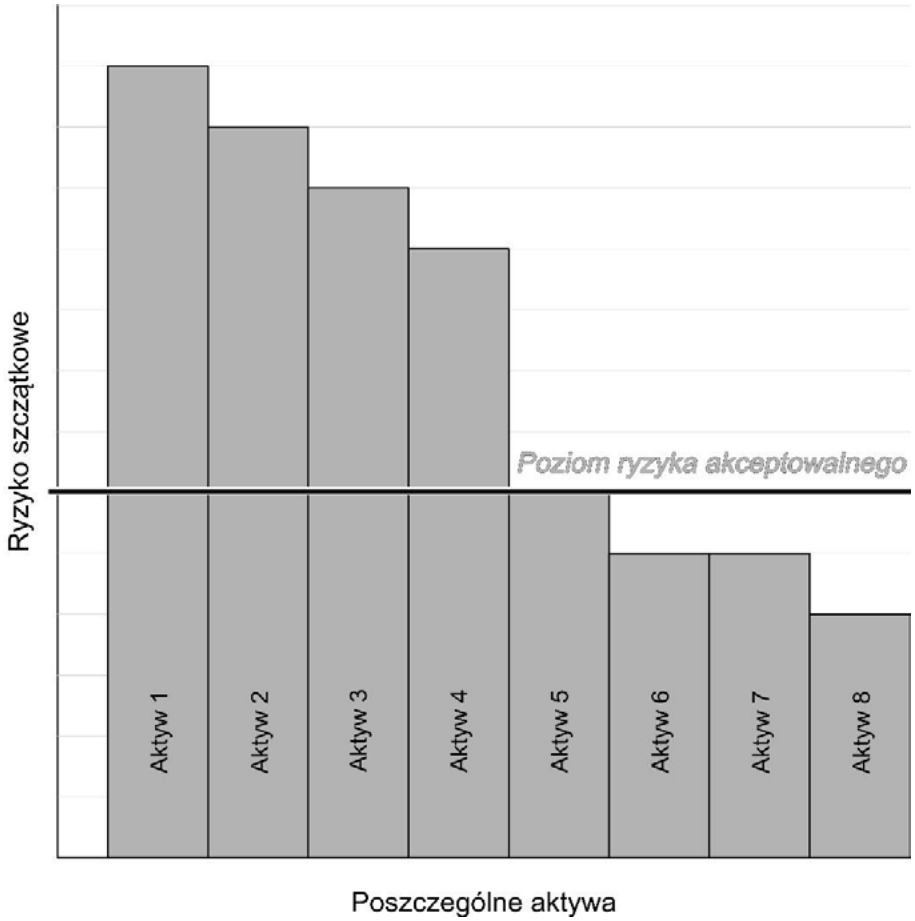
W efekcie uzyskujemy ryzyka szczątkowe aktywów, dla których organa państwa określają i akceptują poziom tzw. ryzyka akceptowalnego jako ustaloną wartość ryzyka, poniżej którego ryzyka aktywów zostają uznane za akceptowalne (rysunek 10), a w odniesieniu do państwa taki poziom, jaki nie zagraża bezpieczeństwu narodowemu w cyberprzestrzeni. Jest to ostatni etap szacowania ryzyka[178].

Należy zwrócić uwagę, że zestawienie aktywów wg ryzyka wyznacza listę aktywów najbardziej ryzykownych dla państwa. Na podstawie tej listy powinno się dobierać odpowiednie zabezpieczenia (uwzględniając istniejące), natomiast na podstawie ryzyka szczątkowego przygotować plan postępowania z ryzykiem[179].

Szacowanie ryzyka z uwzględnieniem identyfikacji zasobów, podsystemów, funkcji i zależności od innych systemów ważnych z punktu widzenia funkcjonowania cyberprzestrzeni Rzeczypospolitej Polskiej (CRP) jest konieczne z uwagi na zapisy zawarte w „Polityce Ochrony Cyberprzestrzeni RP”. Celem takiej działalności jest określenie oraz implementacja docelowych wytycznych do realizacji szacowań ryzyka, jak i szablonów sprawoz-

[176] *Ibidem*.
[177] *Ibidem*.
[178] *Ibidem*.
[179] *Ibidem*.

dań uwzględniających dane odnoszące się do rodzajów ryzyka, zagrożeń oraz słabych punktów stwierdzonych w każdym z sektorów gospodarki RP.



Rysunek 10. Graficzny wynik szacowania ryzyka z uwzględnieniem poziomu ryzyka akceptowalnego
Źródło: opracowanie własne na podstawie W. Gełzakowski, *op. cit.*

Celem strategicznym, który wynika z wyżej wskazanego dokumentu, jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa[180]. Szacowanie ryzyka wiążącego się z funkcjonowaniem cyberprzestrzeni jest szczególnym elementem procesu bezpieczeństwa cyberprzestrzeni, determinującym i uzasadniającym działania podejmowane w celu jego obniżenia do akceptowalnego poziomu. Z tego też względu każda jednostka administracyjna powinna przekazać do 31 stycznia każde-

[180] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, s. 6.

go roku do ministra właściwego ds. informatyzacji sprawozdanie podsumowujące wyniki szacowania ryzyka. Powinno ono zawierać ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów zdiagnozowanych w każdym z sektorów, w których poszczególna instytucja działa, i za które odpowiada. Jego dopełnienie powinny stanowić informacje o sposobach postępowania z ryzykiem. Minister właściwy ds. informatyzacji, we współpracy z zaangażowanymi instytucjami określa jednolitą metodykę przeprowadzania analiz ryzyka. Ponadto Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL) przedstawia ministrowi właściwemu ds. informatyzacji, w celu unifikacji, katalogi zawierające specyfikę zagrożeń oraz podatności, które mogą mieć wpływ na bezpieczeństwo cyberprzestrzeni RP[181].

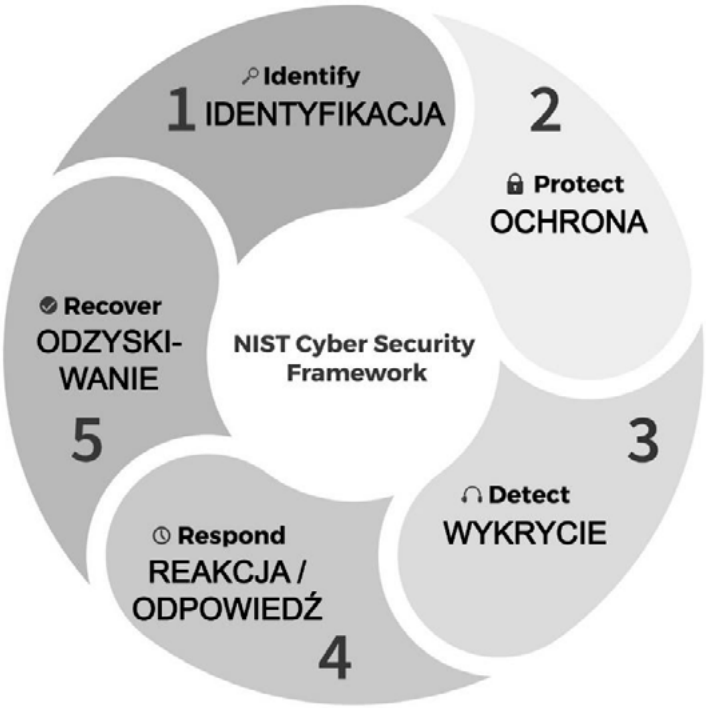
Dokonując oceny ryzyka zagrożeń bezpieczeństwa w CRP, z uwagi na coraz to większą popularność w środowisku biznesowym oraz pozytywne rekomendacje, warto poruszyć zagadnienie amerykańskiej koncepcji – *NIST*[182] *Cybersecurity Framework*. Pomimo że jest ona kierowana do dostawców infrastruktury krytycznej w Stanach Zjednoczonych, przedstawia skuteczny model bezpieczeństwa oparty na ryzyku dla spółek różnych branż na całym świecie, w tym także tych, których działalność skupiona jest na bezpieczeństwie narodowym.

Koncepcja *NIST Cybersecurity Framework* składa się z 5 etapów, następujących po sobie, w cyklicznym procesie – zgodnie ze schematem zobrazowanym na rysunku 11.

Wśród pierwszych kroków proponowanych przez program NIST jest identyfikacja (ang. *Identify*) – określenie i sklasyfikowanie najbardziej wartościowych aktywów informacyjnych oraz ustalenie, gdzie zlokalizowane są najbardziej wartościowe dane w systemie i kto ma do nich dostęp. Takie podejście pozwala na ustalenie poszczególnych szczebli ochrony aktywów, w taki sposób, że klasyfikuje je na te, które wymagają dużej konsekwencji oraz stanowczości w zbieraniu, przekazywaniu i przechowywaniu danych (zwane **aktywami wrażliwymi**) w kontekście bezpieczeństwa informacyjnego oraz te, które takich czynności nie wymagają. Poza tymi czynnościami etap ten obejmuje ocenę ryzyka, zarządzanie aktywami i procesy zarządzania. Kolejnym podstawowym etapem jest ochrona (ang. *Protect*). Obejmuje on wdrożenie odpowiednich zabezpieczeń w celu zapewnienia świadczenia usług informatycznych i ochrony zasobów informacyjnych. W tym celu należy wykorzystać takie środki, jak: kontrola dostępu, bezpieczeństwo danych i świadomość użytkowników.

[181] *Ibidem*, s. 11.

[182] Nazwa pochodzi od akronimu – *National Institute of Standards and Technology* (Narodowy Instytut Standaryzacji i Technologii USA).



Rysunek 11. Schemat blokowy procesu zarządzania ryzykiem w bezpieczeństwie informacji
Źródło: opracowanie własne na podstawie *University of Arizona Cybersecurity Framework*, ver. 004, 8/29/2016, s. 2.

Następnym elementem schematu *NIST Cybersecurity Framework* jest wykrycie (ang. *Detect*). Obejmuje przedsięwzięcia związane z opracowaniem i wdrożeniem odpowiednich systemów w celu szybkiego zidentyfikowania zdarzeń w cyber-przestrzeni RP. Polega on na ciągłym monitorowaniu i wykrywanie zagrożeń i podatności. Kolejny – czwarty etap to reakcja/odpowiedź (ang. *Respond*). W ramach tego kroku opracowuje się działania, które należy podjąć po zidentyfikowaniu zdarzenia w cyberprzestrzeni. Zawiera takie elementy, jak: planowanie reakcji, planowanie komunikacji, analiza zdarzeń, łagodzenie konsekwencji ataków itp. Ostatnim elementem koncepcji jest odzyskiwanie (ang. *Recover*). Etap ten skupia się na opracowaniu i przeprowadzeniu odpowiednich działań mających na celu przywrócenie wszelkich usług, które zostały zakłócone z powodu negatywnego zdarzenia w cyberprzestrzeni państwa. Należy skupić się na odporności środowiska cyberprzestrzeni, tak aby chronić ją przed atakami w przyszłości.

4.5. Uogólnienia i wnioski

W rozdziale zaprezentowano wieloaspektowe i wielowymiarowe podejście do ewaluacji zagrożeń bezpieczeństwa narodowego w cyberprzestrzeni. Podejmując to zagadnienie uznano, że w pierwszej kolejności należy zdefiniować obiekty państwowe, które stając się celami ataków cybernetycznych, mogłyby wywołać znaczące niestabilności bezpieczeństwa narodowego. Do systemów tych należą: ważne obiekty wojskowe, systemy przedsiębiorstw oraz inne wchodzące w skład infrastruktury krytycznej państwa. Przytoczone przykłady sytuacji z kraju i ze świata mające miejsce w ostatnim czasie dowiodły, że określone obiekty państwowe są podatne na zagrożenia, a atak na nie może wywołać reperkusje w postaci niestabilności bezpieczeństwa narodowego. Należy przy tym podkreślić, że przytoczono przykłady cyberataków z ostatnich lat. Miało to na celu przedstawienie współczesnych zagrożeń cyberbezpieczeństwa wskazanych w odniesieniu do systemów oddziaływujących na bezpieczeństwo państwa – systemy: wojskowy oraz wchodzące w skład infrastruktury krytycznej.

W odniesieniu do systemów wojskowych wskazano na sieciocentryczność, jako podatność możliwych ataków. Dokonując oceny ich zagrożeń wskazano na domenę informacyjną, w kontekście warstw: dowodzenia, informacyjna i sensorów, a w odniesieniu do sieci – informacyjna i dowodzenia. Obszary te, z uwagi na przetwarzanie informacji, wymagają szczególnej ochrony, a możliwe cyberataki mogą znacząco wpłynąć oraz zdestabilizować system militarny państwa. Kolejnym celem mogą być systemy transmisji danych, których przykładem jest LINK. Wyszczególniono typy tego rodzaju systemów, wskazując na stopień zaawansowania technologicznego. W odpowiedzi na luki informacyjne zaproponowano system DIANA.

Należy uznać, że w odniesieniu do infrastruktury krytycznej najczęstszymi elementami rażenia wchodzącymi w jej skład są transport lotniczy oraz system energetyczny kraju. Ten fakt może zarazem wskazywać, że cyberataki w przyszłości będą znacznie częściej wymierzone przeciwko właśnie tym obiektom – elementom IK. Zagrażają one rozwojowi ekonomicznemu kraju oraz mogą mieć również charakter polityczny. W środowisku międzynarodowym cyberprzestępcy posługują się dostępnym im lub wykradanym oprogramowaniem szpiegowskim, np. w celach wymuszenia okupu od przypadkowych użytkowników Internetu.

Na podstawie aktualnego stanu, informacji wynikających z krajowych raportów zagrożeń bezpieczeństwa cybernetycznego, określono zagrożenia oraz podatności na nie systemów komputerowych mające wpływ na bezpieczeństwo w cyberprzestrzeni, do których należą botnety oraz ich pochodne.

Krótkoterminowa perspektywa analiza pozwoliła antycypować 5 podstawowych zagrożeń w cyberprzestrzeni, do których należą: Internet rzeczy, zwiększenie się aktywności cyberterrorystów oraz rozwój Darknetu, wzrost napięcia międzynarodowego związanego z cyberatakami oraz intensyfikacja prac legislacyjnych w obszarze cyberbezpieczeństwa.

Dokonując ewaluacji poziomu ryzyka zagrożeń bezpieczeństwa narodowego w cyberprzestrzeni, na potrzeby określania poziomu ryzyka w cyberprzestrzeni, zaproponowany został model i proces zarządzania ryzykiem w bezpieczeństwie informacji. W rozdziale odniesiono się do krajowej polityki obrony cyberprzestrzeni, w której określono wymogi z punktu widzenia właściwego funkcjonowania CRP. Głównym zamierzeniem, jak się okazało, jest wdrożenie docelowych wytycznych do realizacji szacowań ryzyka oraz szablonów sprawozdań zawierających dane dotyczące rodzajów ryzyka, zagrożeń oraz słabych punktów. W tym celu zaproponowano także biznesową koncepcję *NIST Cybersecurity Framework*. Wydaje się, że jej założenia mogą dobrze korespondować z wymogami polityki bezpieczeństwa cyberprzestrzeni RP.

ROZDZIAŁ 5.
Media społecznościowe a zagrożenia bezpieczeństwa narodowego

5.1. Charakterystyka i rodzaje mediów społecznościowych[183]

Media społecznościowe, nazywane często ich anglojęzyczną nazwą – ang. *social media* to „wszelkie działania, praktyki oraz zachowania pośród społeczności ludzi, którzy łączą się online, aby dzielić się informacjami jak również wiedzą czy opiniami. Dialog online umożliwia im liczne aplikacje oraz miejsca wymiany oraz przekazywania informacji w formie słów, video jak również dźwięku"[184]. Jak zauważa E. Krok, pojęcie *social media* dotyczy społecznych środków przekazu, które bazują na łatwo dostępnych technologiach informatycznych. Jednostkom, społecznością jak również całym społecznościom, licznym organizacjom media społecznościowe dostarczają innowacyjnych narzędzi do szybkiej, skutecznej i taniej komunikacji[185].

Jedną z pierwszych definicji *social media* zaproponował H. Rheingold, przedstawiając je jako „skupisko społeczne, wyłonione w Internecie w sytuacji, gdy jednostki, wykorzystując sieć, prowadzą wystarczająco długie publiczne konwersacje, z dużym zaangażowaniem emocjonalnym, aby wytworzyć osobiste relacje z innymi jednostkami w cyberprzestrzeni"[186].

[183] Fragmenty niniejszego rozdziału pierwotnie opublikowano w: R. Bielawski, A. Ziółkowska, *Media społecznościowe, a kształtowanie bezpieczeństwa państwa* [w:] *Człowiek a technologia cyfrowa – przegląd aktualnych doniesień*, red. Paulina Szymczyk, Kamil Maciąg, Wydawnictwo Naukowe TYGIEL, Lublin 2018, 86-99.

[184] K. Fabjaniak-Czerniak, *Internetowe media społecznościowe jako narzędzie public relations* [w:] *Zarządzanie w sytuacjach kryzysowych niepewności,* red. K. Kubiak, Warszawa 2012, s. 173.

[185] E. Krok, *Media społecznościowe elementem systemu zarządzania wiedzą w firmie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2011, nr 656, s. 49; D. Kaznowski, *Podział i klasyfikacja social media, Networked Digital Ag*e,
online – http://networkeddigital.com/2010/05/10/podzial-i-klasyfikacja-social-media/ [dostęp: 28.08.2017].

[186] H. Rheingold, *The virtual community. Homesteading on the electric fronter*, Addison-

W ujęciu D. Kaznowskiego media społecznościowe to „społeczne środki przekazu podlegające kontroli, które mogą być wykorzystywane na dowolną skalę, zawierające zarówno treści przekazu, jak i możliwe punkty widzenia odnoszące się do informacji”[187].

M. Grębosz, D. Siuda, G. Szymański za D. Kazanowskim wskazują na następujące atrybuty mediów społecznościowych:

- możliwość wykorzystania na dowolną skalę;
- swobodny dostęp dla wszystkich zainteresowanych;
- nieskończona możliwość modyfikacji;
- wolny dostęp do tworzenia oraz odbioru treści;
- realizacji dzięki idei społecznego współuczestnictwa;
- bezpośredni wpływ grupy na końcową wartość informacji;
- brak odgórnej koordynacji między twórcami;
- dostępność treści;
- rozprzestrzenienie treści;
- relatywnie krótki czas publikacji tworzonych treści;
- niewymuszony sposób powstawania treści[188].

Obserwując wzrost liczbowy kont portali internetowych E. Krok stwierdza, że media społecznościowe wyznaczają nowy kierunek rozwoju Internetu. Relatywnie łatwy dostęp i nieskomplikowana obsługa narzędzi „wytwórczych” sprawia, że tworzenie i odbiór treści są nieograniczone. Media społecznościowe zacierają granicę między nadawcą a odbiorcą, zaś kierunek przekazu informacji jest dwustronny. Wielką zaletą *social media* jest szybkość –treści są przesyłane bardzo sprawnie, bez opóźnień[189].

M. Grębosz, D. Siuda, G. Szymański podają, że komunikacja w Internecie jest możliwa dzięki współistnieniu czterech podstawowych elementów:

- nadawcy, który posiada dostęp do maszyny kodującej czyli urządzenia, z którego nadawana i przesyłana jest informacja (np. komputer, tablet, telefon);
- odbiorcy, który posiada dostęp do maszyny dekodującej, czyli urządzenia, które odbiera informacje, np. komputer;
- komunikatu w formie kodu, wysyłanego do odbiorcy przez nadawcę w postaci tekstu, obrazu, nagrania video czy dźwięku;
- kanału, który wykorzystywany jest do przesyłana informacji, będącej

---

Wesley, Reading MA, 1993, s. 6.

[187] D. Kaznowski, *Social media – społeczny wymiar Internetu* [w:] *E-marketing. Współczesne trendy. Pakiet startowy*, red. J. Królewski, P. Sala, PWN, Warszawa 2016, s. 89.

[188] *Ibidem*, s. 89-90; M. Grębosz, D. Siuda, G. Szymański, *Social Media Marketing*, Wydawnictwo Politechniki Łódzkiej, Łódź 2016, s. 12-13.

[189] E. Krok, *op. cit.*, s. 49.

jednocześnie nośnikiem kodu[190].

Dla komunikacji w sieci znamienna jest jej dwukierunkowość. Polega ona na tym, iż nadawca i odbiorca mogą w tym samym czasie pełnić obie role. Do ewentualnych zakłóceń, występujących w przypadku komunikacji internetowej można zaliczyć:

- „brak połączenia lub jego zerwanie;
- zapory;
- brak możliwości otworzenia przesyłanego pliku;
- brak oprogramowania;
- ograniczenia sprzętowe"[191].

Jeden z teoretyków – W. Gustowski definiuje Internet jako „multimedialny oraz globalny kanał komunikacyjny między ludźmi i organizacjami, który umożliwia dwustronne komunikowanie się"[192]. Ten sam autor jest zdania, iż jest to także rodzaj nowego społeczeństwa, które funkcjonuje w cyberprzestrzeni, zwanej przestrzenią wirtualną. Internet jako globalne medium komunikacyjne ułatwia komunikację między ludźmi, jak również sprzyja nawiązywaniu i utrwalaniu kontaktów[193]. Jednym z efektów upowszechniania się Internetu stało się powstanie mediów społecznościowych opartych na więzach łączących ich użytkowników[194].

Dialogowość *social media* to ich główny atrybut. W ramach komunikacji typu ***intercast***[195] ma miejsce natychmiastowe sprężenie zwrotne, jak również wysoki stopień interakcji między nadawcą a odbiorcą. Wspólnymi cechami mediów społecznościowych są również: multimedialność, polifoniczność, jednoczesne oddziaływanie na kilka różnych zmysłów. Wynika to z faktu, że publikowane tam komunikaty wykorzystują tak tekst, jak i obraz czy video. Sposobność tworzenia zaangażowania odbiorców, pobudzenia interakcji czy dyskusji to jedne z głównych kierunków wykorzystania *social media*. Dotarcie do zainteresowanej grupy docelowej jest stosunkowo proste, podobnie jak samo formułowanie komunikatów, które później przekazywane są dalej przez użytkowników, przy wykorzystaniu np. mar-

[190] M. Grębosz, D. Siuda, G. Szymański, op. cit., s. 9; M. Roszmann, K. Wilczewska, *Internet jako nowoczesne medium komunikacji w społeczeństwie*,
online – http://kneb.wpit.am.gdynia.pl/?p=513 [dostęp: 28.08.2017].

[191] M. Roszmann, K. Wilczewska, *Internet jako nowoczesne medium komunikacji w społeczeństwie*, online – http://kneb.wpit.am.gdynia.pl/?p=513 [dostęp: 28.08.2017]; l.M. Grębosz, D. Siuda, G. Szymański, *op. cit*., s. 9-10.

[192] W. Gustowski*, Komunikacja w mediach społecznościowych*, Novae Res – Wydawnictwo Innowacyjne, Gdynia 2012, s. 33; M. Grębosz, D. Siuda, G. Szymański, *op. cit*., s. 11.

[193] W. Gustowski*, Komunikacja w mediach społecznościowych*, Novae Res – Wydawnictwo Innowacyjne, Gdynia 2012, s. 33; M. Grębosz, D. Siuda, G. Szymański, *op. cit*., s. 205.

[194] R. Hanna, A. Rohm, V.L. Crittenden, *We're All connectwd: The Power of the socal media ekosystem*, „Business Horizons" 2011, vol. 54, no. 3, s. 265-273.

[195] W sensie – współkomunikowanie się.

ketingu szeptanego. Dialog jako nadrzędna cecha mediów społecznościowych niesie liczne szanse, ale i zagrożenia. Odpowiedź odbiorcy może być niekorzystna. Może on również poprowadzić dyskusję w niekorzystnym dla drugiej strony kierunku.[196].

M. Grębosz, D. Siuda, G. Szymański do cech odróżniających *social media* od tradycyjnych mediów, zaliczają:

- „zasięg – mają one możliwość dotarcia do licznej grupy odbiorców;
- dostęp – są powszechnie dostępne licznym odbiorcom bezpłatnie lub za niewielką opłatą;
- użytkowanie – tworzenie treści za pośrednictwem mediów społecznościowych nie wymaga specjalnych umiejętności, wystarczy zdolność korzystania z nowych technologii;
- natychmiastowość – stanowią przestrzeń natychmiastowej reakcji;
- trwałość – przekazy mogą ulec zmianom niemal w tym samym momencie, w którym zostały opublikowane – zarówno przez funkcję edycji, jak i dodawania komentarzy do tekstu"[197].

Na podstawie literaturowych propozycji można dokonać klasyfikacji mediów społecznościowych. Poniżej, w formie graficznej, przedstawiona została typologia ze względu na ich funkcję – rysunek 12.

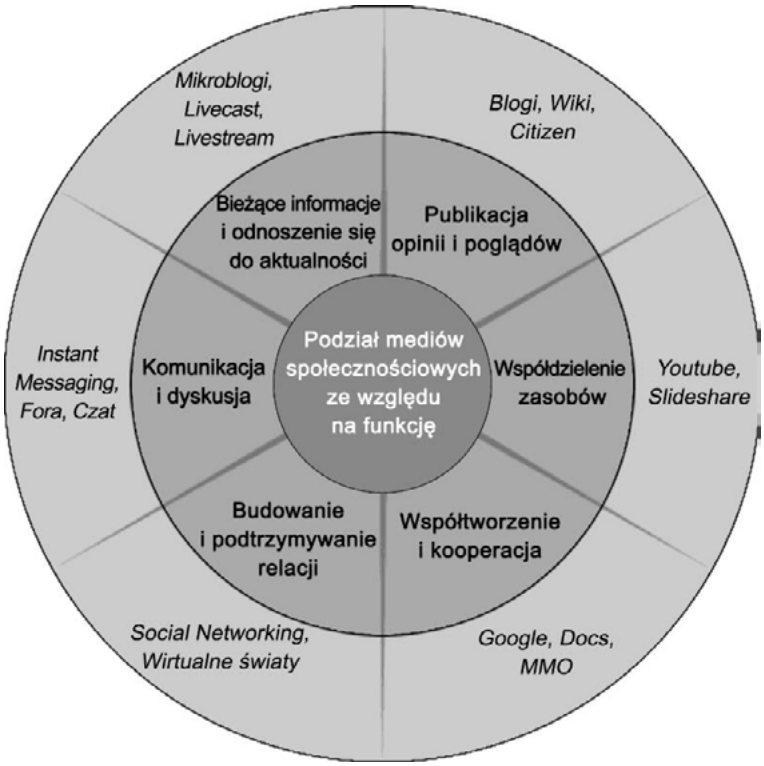
W przypadku klasyfikacji ze względu na funkcję, media społecznościowe D. Kazanowski dzieli na:

- **służące publikacji opinii i poglądów** – to można rzec „fundamentalna" kategoria mediów społecznościowych. Zasadniczym zadaniem serwisów (aplikacji/usług) kwalifikowanych do tej kategorii jest umożliwienie wszystkim zainteresowanym otwartego i nieskrępowanego wyrażania opinii, jak również swych poglądów. Przykładowe rozwiązania z tej kategorii to: blogi, mechanizmy wiki czy serwisy dziennikarstwa obywatelskiego. Kategoria ta chyba najwyraźniej odzwierciedla postulat wolności dostępu do tworzenia i odbioru treści. Blogi, wiki i serwisy dziennikarstwa społecznego to jedne z najstarszych rozwiązań mediów społecznościowych;
- **służące współdzieleniu zasobów** – to kategoria, dla której filarem jest idea Web 2.0. Zaliczają się do niej różnego typu zasoby, które użytkownicy współdzielą w sieci (filmy wideo, zdjęcia, obrazy, prezentacje, aplikacje itp.). Przechowuje i udostępnia się je z poziomu

[196] P. Szews, Medialny fanpage – szanse i zagrożenia, „Media i Społeczeństwo" 2015, nr 5, s. 12 za: K. Fabjaniak-Czerniak, *Internetowe media społecznościowe…*, s. 182–183.

[197] M. Grębosz, D. Siuda, G. Szymański, *op. cit.*, s. 15 za: M. Gladwell, C. Shirky, *From Innovation to Revolution. Do Social Media Make Protests Possible?*,
online – https://www.foreignaffairs.com/articles/2011-01-19/innovation-revolution [dostęp: 28.08.2017].

serwerów sieciowych. Inaczej niż w przypadku modelu wiki, rozwiązania bazujące na tej kategorii nie są nastawione na tworzenie bazy wiedzy, ale budowanie bazy zasobów przetwarzanych i przechowywanych w chmurze. Przykłady funkcjonowania to: YouTube, Flick oraz Slideshare;



Rysunek 12. Klasyfikacja mediów społecznościowych ze względu na funkcję
Źródło: http://networkeddigital.com/2010/05/10/podzial-i-klasyfikacja-social-media/ [dostęp: 28.08.2017].

- **nastawione na współtworzenie lub kooperację** – to relatywnie rzadko prezentowana kategoria mediów społecznościowych. Jej atrybut to mała „atrakcyjność medialna". Ich cechą charakterystyczną jest z góry założony cel, w postaci uzyskania wyniku kooperacji uczestników. W odniesieniu do blogów czy wiki użytkownicy z góry nie zakładają, że będą uczestniczyć w tworzeniu treści (czy też suma ich kooperacji da wynik), z kolei w przypadku rozwiązań, takich jak Google Docs czy gier MMO (ang. *Massive Multiplayer Online Games*) tak właśnie jest.
- **nastawione na budowanie i podtrzymywanie relacji** – to najszerzej obecnie zaadoptowana (z racji tego, że jest również najbardziej przystępną) kategoria *social media*. Dotyczy głównie serwisów typu

social networking[198]. Ich główna rola sprowadza się do budowania i podtrzymywania relacji pomiędzy ludźmi.;

- **nastawione na komunikację i dyskusję** – jest to grupa mediów społecznościowych, w której oś społecznej interakcji stanowią dyskusja i debata. Tego typu rozwiązania są jednym z najstarszych w sieci. W kategorii tej uwzględnić należy: fora oraz komunikatory internetowe (ang. *instant messaging*) oraz czat. Współcześnie tego typu rozwiązania są coraz częściej integrowane z innymi typami serwisów *social media* – głównie *social networking.* Nierzadko są wykorzystywane równolegle (np. czat podczas transmisji na żywo);
- **nastawione na bieżące informowanie i odnoszenie się do aktualności** – celem jest głównie relacjonowanie i odnoszenie się do bieżących wydarzeń. Rozwiązania tworzone w ramach tej kategorii skupiają się na tym, co dzieje się w czasie rzeczywistym. Do tej kategorii zaliczają się: mikroblogi, ale również serwisy alertowe (powiadomienia obywatelskie) czy mniej znane w Polsce serwisy typu ***livestream*** (które są pewnego rodzaju agregatorami najnowszych wydarzeń) czy ***livecast***.

5.2. Wybrane mechanizmy (sposoby) wykorzystania mediów społecznościowych w cyberprzestrzeni narodowej

5.2.1. Operacje psychologiczne z wykorzystaniem mediów społecznościowych

Jednym ze sposobów wykorzystania mediów społecznościowych w kształtowaniu cyberprzestrzeni państwa są **operacje psychologiczne** (ang. *psychological operations* – **PsyOps**). Należą one do działań defensywnych operacji informacyjnych, które są prowadzone w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika.

Pierwszym w polskim piśmiennictwie – oficjalnym dokumentem, który definiował tego rodzaju operacje, był „Regulamin działań Wojsk Lądowych" z 2002 r. W publikacji tej określono, że „działania psychologiczne to planowe oddziaływanie psychologiczne w czasie pokoju, kryzysu i wojny, skierowane do wrogich, przyjaznych lub neutralnych odbiorców, wpływa-

[198] Pojęcie wyjaśnione w dalszej części pracy.

jące na ich postawy i zachowania z zamiarem osiągnięcia pożądanych, z punktu widzenia prowadzącego je, celów politycznych i wojskowych”[199].

Współczesna literatura definiuje operacje psychologiczne w oparciu o inne podejście. W projekcie „Doktryny Bezpieczeństwa Informacyjnego RP” są one określone jako „operacje mające na celu wpływanie na emocje, motywacje, obiektywne rozumowanie, a ostatecznie zachowanie rządów państw obcych, organizacji, grup i osób będących celami tych operacji, tak aby osiągnąć efekt w postaci wzmocnienia lub nakłonienia do zachowań korzystnych dla realizacji własnych interesów. Mogą być wykorzystywane zarówno w czasie pokoju (klęsk żywiołowych, stanów kryzysowych i alarmowych), jak i podczas wojny[200].

Poza terminem operacji psychologicznych często mamy do czynienia z jego tożsamym terminem – **wojna psychologiczna**. Ujęcie słownikowe mówi, że to „jedna z dziedzin psychologii wojskowej, zajmująca się różnymi formami dywersji, prowokacji, wywiadu, szpiegostwa i propagandy, mająca na celu demoralizację przeciwnika, osłabienie jego woli walki i wiary we własną sprawę, szerzenie paniki, fałszowanie informacji itp. Celem działań jest zarówno armia przeciwnika, jak i całe społeczeństwo”[201]. Można ją także zdefiniować jako „system sposobów i metod planowego oddziaływania na poglądy, moralność, postawy narodu przeciwnika w celu spowodowania określonych zmian psychologicznych i ideologicznych, a przez to doprowadzenie do zmiany układu sił politycznych i osłabienia ideologicznego podstaw władzy w danym państwie”[202].

Pojęcie wojna psychologiczna oznacza zorganizowane, długofalowe i agresywne oddziaływanie środkami politycznymi, propagandowymi, dyplomatycznymi, kulturalnymi i emocjonalnymi na świadomość, psychikę oraz morale ludności cywilnej i sił zbrojnych. Celem działania wojny psychologicznej jest osłabianie odporności moralno-politycznej społeczeństwa, wprowadzanie chaosu i dezinformacji oraz obniżenie przez społeczeństwo zaufania do polityki i władzy państwowej.

Przy podejściu *stricte* wojskowym – zgodnym z NATO – oraz, co ważne, korespondującym z dokumentami doktrynalnymi RP, PsyOps można zdefiniować jako „operacje planowane, prowadzone w celu przekazania wybranych informacje i wskaźników dla zagranicznych odbiorców tak aby wpływać na ich emocje, motywacje, obiektywne rozumowanie, a ostatecznie

[199] *Regulamin działań Wojsk Lądowych*, DWLąd, Warszawa 2002.
[200] *Doktryna Bezpieczeństwa Informacyjnego RP – projekt*, BBN, Warszawa 2015, s. 4.
[201] *Encyclopedia PWN*, online
https://encyklopedia.pwn.pl/encyklopedia/wojna%20psychologiczna.
html [dostęp: 11.08.2017].
[202] *Encyclopedia PWN*, online – https://encyklopedia.pwn.pl/haslo/wojna-psychologiczna;3997505.html [dostęp: 11.08.2017].

zachowanie rządów państw obcych, organizacji, grup i osób"[203]. W odniesieniu do operacji krajowych, bazując na powyższych definicjach można stwierdzić, że domeną PsyOps dla RP jest wzmocnienie zachowania korzystnych celów strategicznych państwa, czyli zapewnienie korzystnych i bezpiecznych warunków dla realizacji interesów narodowych poprzez eliminację zewnętrznych i wewnętrznych zagrożeń bezpieczeństwa narodowego.

W ujęciu NATO można wyróżnić dwa rodzaje operacji psychologicznych:

- **operacje psychologiczne zaczepne** – mające na celu osłabienie chęci walki przeciwnika i jego ludności. Polegają one na tym, że po odnalezieniu słabego punktu w polityce przeciwnika rozpoczyna się skoncentrowany pod względem czasu, miejsca i sposobu atak na wybrany obiekt oddziaływania. Odbywa się to poprzez radio, telewizję, prasę (reportaże, artykuły), kampanię plakatową i ulotkową oraz – co dziś szczególnie ważne – Internet. Skuteczna operacja psychologiczna osłabia morale przeciwnika i wprowadza w jego szeregach wątpliwości, co do słuszności realizowanej polityki, zdolności własnych wojsk, wartości zawartych sojuszy itp.;
- **operacje psychologiczne obronne** – mają na celu wzmocnienia morale własnej ludności, a także pozyskanie wsparcia sił neutralnych i niezaangażowanych. Realizowane są one przez osłabienie prestiżu przeciwnika, podważenie jego autorytetu, uprzedzanie i dyskredytowanie jego przekazu informacyjnego[204].

Omawiając temat operacji PsyOps możemy posłużyć się także inną ich klasyfikacją, zawierającą poziom prowadzonych przez strony operacji psychologicznych. Zgodnie z nim dzielimy je na trzy poziomy:

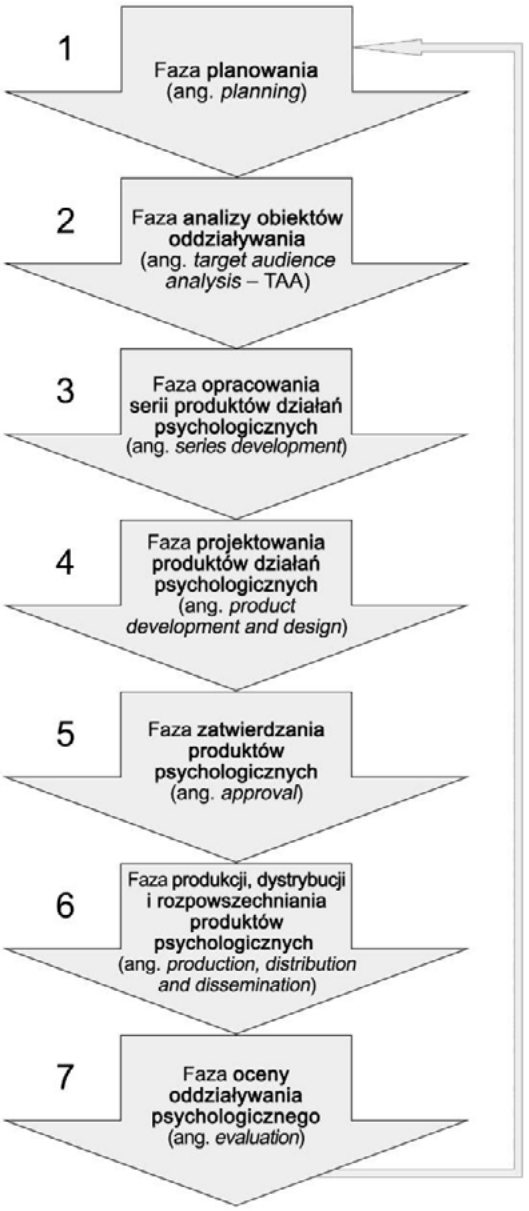
- **strategiczne operacje psychologiczne** – obejmują one działania psychologiczne realizowane przez agencje rządowe RP;
- **operacyjne operacje psychologiczne** – prowadzone są one w ramach operacji (również w stanie pokoju) na określonym obszarze. Mają one na celu wsparcie skuteczności Sojuszniczego Dowództwa Sił Połączonych (ang. *Joint Forces Command* – JFC);
- **taktyczne operacje psychologiczne** – prowadzi się je na obszarze odpowiedzialności dowódcy taktycznego, w celu wsparcia misji.

Właściwe przeprowadzenie operacji psychologicznych zdeterminowane jest odpowiednimi procedurami. Jedną z takich propozycji, stosowanych w NATO, jest wielowymiarowy proces określany mianem połączonego – ang. *Joint PSYOP Process*. Jest on zgodny z wyżej wymienioną klasyfikacją pozio-

[203] *DOD Dictionary of Military…*, *op. cit.*
[204] T. Grabowski, *Metody walki informacyjnej…*, *op. cit.*, s. 35.

mów prowadzenia PsyOps, czyli prowadzi się go na wszystkich szczeblach: operacyjnym (np. poprzez Departament Obrony USA) i taktycznym.

Określeniem – *Joint PSYOP Process* (ang. *Joint Psychological Operations Process*) nazywa się proces, w skład którego wchodzi 7 niezwykle istotnych, następujących po sobie faz (rysunek 13):



Rysunek 13. Fazy procesu połączonego – Joint PSYOP Process
Źródło: opracowanie własne na podstawie *Joint Publication 3-13.2…, op. cit.*, s. 14.

- planowania (ang. *planning*);
- analizy obiektów oddziaływania (ang. *target audience analysis* – TAA);
- opracowania serii produktów działań psychologicznych (ang. *series development*);
- projektowania produktów działań psychologicznych (ang. *product development and design*);
- zatwierdzania produktów psychologicznych (ang. *approval*);
- produkcji, dystrybucji i rozpowszechniania produktów psychologicznych (ang. *production, distribution and dissemination*);

oceny oddziaływania psychologicznego (ang. *evaluation*)[205].

W pierwszym etapie (faza planowania) w stanie pokoju, jak również w chwili poprzedzającej działania militarne prymarne będzie zatwierdzenie i akceptacja programów psychologicznych. W celu zobrazowania i ułatwienia zrozumienia realizacji procesu, można odnieść go do struktur USA. Najważniejszym reprezentantem administracji rządowej Stanów Zjednoczonych, który włączony jest do owej procedury będzie podsekretarz obrony ds. politycznych (ang. *Under Secretary of Defense for Policy* – USD/P). Następnym podmiotem biorącym udział w prezentowanym procesie jest zastępca sekretarza obrony ds. operacji specjalnych i konfliktów o niewielkim natężeniu (ang. *Assistant Secretary of Defense for Special Operations and Low Intensity Conflicts* – ASD SO/LIC). Głównym, militarnym organem zaangażowanym w akceptację produktów i programów psychologicznych jest Sztab Połączony (ang. *Joint Staff*). Następni w hierarchii będą właściwi geograficznie dowódcy sił amerykańskich (ang. *Geographic Combatant Commander*), a także dowódcy Połączonych Zespołów Zadaniowych (ang. *Commander of Joint Task Force* – COMJTF).

Omawiana faza zawiera przepływ danych, bazujący na przesyłaniu planu operacji psychologicznych począwszy od pierwszego szczebla do podsekretarza obrony USA ds. politycznych. Ukończony projekt operacji psychologicznych posiada podstawowe informacje, takie jak: plan działań psychologicznych, sugestie celów psychologicznych, zagadnienia przekazu (jak również zagadnienia, których powinno się w owym przekazie unikać), przypuszczalne obiekty oddziaływania, przedstawicieli armii odpowiedzialnych za akceptację produktów psychologicznych; techniki dopasowywania źródła przekazu, kanałów dystrybucji i rozpowszechniania, źródeł sponsorowania, jak również oceny efektywności wywieranego wpływu. Na tym etapie zachodzi konieczność konsultacji z Biurem Sekretarza Obrony (ang. *Office of the Secretary of Defense* – OSD), innymi organami oraz ze Sztabem Połączonym.

[205] *Joint Publication 3-13.2, Psychological Operations,* 07 January 2010, s. 14.

Biorąc pod uwagę płaszczyznę taktyczną, początkowa faza procesu projektowania działań psychologicznych przygotowywanych przez amerykańskie siły zbrojne łączy precyzowanie celów działań psychologicznych (ang. *Psychological Operations Objectives* – POs), wspierających celów działań psychologicznych (ang. *Supporting Psychological Operations Objectives* – SPOs), potencjalnych obiektów oddziaływania (ang. *Potential Target Audiences* – PTAs) i początkowe kryteria oceny psychologicznej. Etap ten jest zazwyczaj połączony z militarnym procesem podejmowania decyzji, wykorzystywanym w armii USA. Zawiera on określenie celów działań psychologicznych, wspomagających dyspozycje dowódcy ogólnowojskowego. Owe zamiary i cele zwykle są definiowane, precyzowane przez wyższe etapy struktury działań psychologicznych, jak również wyznaczają granice przygotowywania planu owych działań.

Kolejna – druga faza – czyli analiza podmiotów oddziaływania oparta jest na sprawdzeniu oraz ocenie przypuszczalnych obiektów oddziaływania. Najlepszym obiektem wywieranego wypływu będą unitarne zespoły, posiadające identyczne warunki środowiskowe i tożsame pobudki, tj. pragnienia oraz potrzeby.

Dowódca wspierający przy pomocy odpowiednich sił i środków jest odpowiedzialny za uzyskiwanie informacji, koniecznych do rozpoczęcia i dokonania analizy przypuszczalnych obiektów oddziaływania. Warunki informacyjne, opisujące szacunki dokonanej analizy są zazwyczaj wymienione w początkowej fazie planowania, w obszarze organizacji rozpoznania. Informacje te zbierane są z wielu źródeł, do których dostęp jest wolny lub ograniczony. W ramach wykonywania zadań fazy drugiej zarówno w zbiorowości, jak i wśród indywidualnych odbiorców przeprowadza się analizę sposobów i możliwości wywierania na nie wpływu. Umożliwia to wytyczenie konkretnych metod wpływu na podmioty oddziaływania przy założeniu, iż uzyskana reakcja będzie najkorzystniejsza pod względem interesów wojsk USA. Rezultaty dokonanej analizy wytyczają punkt początkowy dla przeprowadzenia kolejnych faz procesu, a co za tym idzie – uzyskania celów uwzględnionych w przyjętych programach działań psychologicznych. Wspomnianą analizę dokonuje się w ciągu całego procesu, biorąc pod uwagę: aktualizację informacji uzyskanych podczas wykonywania operacji, modyfikacje mające miejsce w otoczeniu ich realizacji, jak również wyłanianie się zmian w środowisku egzystowania rozpoznanych do tej pory obiektów oddziaływania. W obszarze analizy podmiotów oddziaływania, wyłączając wymienione determinanty wrażliwości i warunki, precyzowane są również tzw. linie perswazyjne. Linie perswazyjne to nic innego, jak odpowiednia argumentacja, używana w celu osiągnięcia wymaganego zachowania, jak i stosunku obiektów oddziaływania. Dodatkowo warto zwrócić uwagę na symbole i podatność. Symbolem nazywa się op-

tyczne, wizualne, dźwiękowe przedmioty charakteryzujące się kulturowym oraz kontekstowym znaczeniem dla podmiotu oddziaływania. Podatnością określa się szansę „otwartości" podmiotu oddziaływania na prowadzoną agitację.

W trzecim etapie odbywa się przygotowywanie serii produktów działań psychologicznych. Dane zebrane w procesie analizy podmiotów oddziaływania używane są w celu precyzowania produktów, projektowania akcji oraz serii produktów psychologicznych. Kadra działań psychologicznych przygotowuje serie produktów, projektuje posunięcia, wybiera najkorzystniejsze media, jak również nakreśla plan wykonania manewrów z obszaru działań psychologicznych. Poszczególne serie produktów dotyczą odpowiedniego zamiaru działań psychologicznych, a także konkretnego obiektu oddziaływania. Odrębne serie produktów są kolejno sprawdzane zgodnie z kryterium użyteczności, czasu wykonania, przypuszczalnego wypływu oraz liczby produktów, precyzyjności, dokładności wykorzystywanej linii perswazyjnej oraz powszechności i osiągalności zasobów potrzebnych do ich wykorzystania. Etap ten to wieloelementowy, kreatywny wysiłek kilku osób, których celem będzie uzyskanie efektu synergii odmiennych produktów oraz działań psychologicznych, wykonywanych zgodnie z zamierzeniem uzyskania konkretnej zmiany postępowania wybranego obiektu oddziaływania. Przypuszczalny efekt ostateczny jest metodą uzyskania wspierającego zamiaru działań psychologicznych. Uzyskane do tej pory doświadczenia umożliwiają wyszczególnienie wniosku, że stosunkowo rzadko wykorzystany odrębnie produkt psychologiczny faktycznie oddziałuje na postępowanie podmiotu oddziaływania. Rezultaty kontynuowanych badań wykazują, iż najlepszą metodą reorganizacji zachowania obiektu oddziaływania będzie wewnętrznie harmonijna oraz zsynchronizowana seria produktów oraz posunięć psychologicznych, wykonywanych przy bazowaniu na dostosowane środki przekazu. W celu dokładnego przygotowania serii produktów psychologicznych trzeba włączyć procedurę, w skład której wchodzi 5 poszczególnych etapów: zaprojektowanie arkusza, szkicu projektu serii produktów; przygotowanie planu dystrybucji serii produktów; zaprojektowanie wykresu/tabeli wykonania serii produktów; przygotowanie schematu transmisji i wykonanie dokładnej kontroli owej serii. Faza przygotowania arkusza projektu serii implikuje konieczność zaprojektowania serii produktów posunięć o charakterze psychologicznym. Największą skuteczność owego kroku zyskuje się w momencie wykorzystania metody pracy zespołowej, która umożliwia uzyskanie odmiennych metod rozwikłania konkretnej kwestii w obszarze tzw. planu kompleksowego (ang. *comprehensive plan*). Głównym problemem tej fazy będzie analiza zaprojektowanego szkicu pod względem uzyskania odpo-

wiedzi na pytanie: W jaki sposób namówić podmiot oddziaływania do zmiany teraźniejszych postaw na pożądane?

Arkusz umożliwia dopasowanie konkretnych produktów, wywołujących u adresata pożądane zachowania. W następnym etapie dokonuje się projektowania arkusza dystrybucji serii produktów. W skład tych działań wchodzi wybór: czasoprzestrzeni propagowania odpowiednych produktów owej serii i kolejności serii. Istotne jest także wytypowanie ilości, częstotliwości i czasu koniecznego do rozpropagowania konkretnej serii. Trzecią fazą będzie wykonanie wykresu wytworzenia serii produktów. Wykres ten ma charakter graficznego przedstawienia pomysłu, którego celem będzie uzyskanie koordynacji oraz korelacji wszystkich produktów, usunięcie przypuszczalnych sporów, zaprezentowanie dowódcom i sztabom wspierającym metody włączenia konkretnej serii i dostosowanie terminów połączonych z wykonaniem produktów.

Czwarta faza – projektowanie wykresu transmisji serii umożliwia odpowiednią koordynację transmisji przy wykorzystaniu mediów. Jest to bardzo ważne ze względu minimalizowania szumów swojego przekazu przez techniki walki elektronicznej. Zazwyczaj dostrajania dokonuje oficer działań informacyjnych, jak również oficer walki elektronicznej. Końcowym etapem będzie sprawdzenie, kontrola serii produktów psychologicznych zgodnie z dobranymi wymogami. Zawierają one: czas wprowadzania konkretnej serii, typy produktów oraz ich połączenia, kombinacje, sekwencje stosowanych produktów, dobór argumentów, zakładane spory, mogące zaistnieć podczas wdrażania wielu serii, jak również powszechność potrzebnych zasobów.

Kolejnym etapem omawianego procesu jest projekcja produktów posunięć/operacji psychologicznych. Faza ta dzielona jest na dwa etapy: przygotowanie planu, koncepcji produktu i jego projektu. W czasie kiedy konstruowanie planu produktu odnosi się do przestrzeni koncepcyjnej, to etap projektowania prezentuje przede wszystkim ramy techniczne włączenia gotowej koncepcji prototypu albo jego wersji pierwotnej. Omawiany etap rozpoczyna się w chwili ukończenia pracy nad wcześniejszym etapem – przygotowania serii produktów psychologicznych. Projekty przygotowane w trzeciej fazie, w formie: arkuszy, szkiców koncepcji, arkuszy dystrybucji serii, jak również wykresu realizacji serii produktów w połączeniu z rezultatami pracy realizowanej w poprzedniej fazie, określają podstawę do zaprojektowania modelu, pierwowzoru produktu psychologicznego.

Wyróżnia się trzy prymarne kategorie produktów psychologicznych, tj. wizualno-obrazowe, dźwiękowe oraz audiowizualne. Ich zadaniem jest wywieranie wpływu na konkretnych adresatów. Warto wspomnieć, że stałe oraz ruchome fragmenty potencjału amerykańskich operacji psychologicznych, wojsko oraz środki przeznaczone do działania w strukturach

państw sojuszniczych oraz ich armii, jak również subiekt komercyjny stanowią dokładne przygotowanie oraz techniczne wyposażanie, aparat konieczny do zaprojektowania i przygotowania pozostałych typów produktów psychologicznych. Harmonogramy posunięć psychologicznych posiadają listę mediów, wybranych do produkcji tworzyw, produktów psychologicznych, jak również ich dystrybucji w ramach wykonania dyspozycji dowódcy. Istotną dyspozycją tego etapu będzie oszacowanie zrozumienia oraz szczebla akceptacji wystosowanych przez produkty psychologiczne przesłanek, argumentów do podmiotów wpływu. Początkowe próby produktów umożliwiają wytyczenie założeń, na postawie których przeprowadzone zostaną testy wtórne całości serii, zaraz po jej dystrybucji. Wynikiem kroków prowadzonych podczas tego etapu jest zaprojektowanie arkusza produktu psychologicznego (ang. *Product Action Worksheet* – PAW), nazywanego również dyspozycją przygotowania wspomnianego produktu. Arkusz jest nie tylko podstawą do sporządzenia produktu, ale także wyznacza podstawę do zaprojektowania narzędzi testowo-badawczych, używanych w czasie prowadzenia prób i testów pierwotnych oraz wtórnych.

Faza komercyjna oraz faza materializacji prowadzone są na podstawie danych zebranych w arkuszu analizy podmiotów wpływu oraz szkicu planów, koncepcji serii kompatybilnej z arkuszem rozpowszechniania i dystrybucji całości serii. Rezultatem przygotowania produktu jest zarys, schemat produktu przedstawiony w informacjach zebranych w dyspozycji przygotowania produktu psychologicznego. Warto wspomnieć, iż pojedynczy produkt przygotowany jest na podstawie jednego arkusza sporządzenia produktu psychologicznego. Arkusz ten posiada konkretne dane, tj. cel poczynań, operacji psychologicznych; numer akcji, serię, dodatkowy – tzw. wspierający cel zabiegów psychologicznych; pozostałe, dystrybuowane produkty, podmioty wpływu, argumenty wykorzystywane na użytek zadań psychologicznych, deskrypcję środków przekazu, datę włączenia pierwowzoru określonego produktu, projekt akcji; jak również wskazówki w oparciu, o które wykonane zostaną testy produktu.

Celem etapu piątego będzie natomiast akceptacja serii przygotowanych produktów psychologicznych. Dokładnie zrealizowany i skuteczny proces aprobowania serii produktów, jak również szybkie kierowanie przygotowaniem owej serii łącznie z ich legalizacją ma prymarne znaczenie dla uzyskania odpowiedniej podpory psychologicznej dla rozpoczynanych oraz kontynuowanych operacji. Podczas etapu piątego całe serie poddawane są formalnej kontroli, przeprowadzanej przez kadrę działań psychologicznych. Pierwszym szczeblem wytyczonym do zaakceptowania serii produktów będzie dowódca jednostki zadań psychologicznych, która zajmuje się przygotowaniem całej serii produktów. Podczas omawianego schematu akceptacji serii, szacowana jest możliwość: konkretnej serii produktów do

uzyskania planowanego wyniku, reakcji, kompatybilność informacji zamieszczonych we wszystkich produktach, ich korelacja, jak również środki przekazu wytyczone do rozpowszechniania. Po uzyskaniu aprobaty owej serii przez dowódcę, produkty te są formalnie zgłaszane do zaakceptowania w ramach przygotowanego schematu akceptacji serii, w celu osiągnięcia końcowej aprobaty, zgody odpowiedniego zwierzchnika. Następnie seria zostaje zgłoszona do realizacji i dystrybucji. Akceptacja produktów prowadzona jest na najniższym poziomie dowodzenia, co jest tożsame z rozkazem sekretarza obrony USA. Prerogatywy dotyczące końcowej akceptacji serii mogą być odsyłane do poziomu dowódcy jednostki manewrowej, aby uzyskać akceptację terminową i rozpocząć wdrażanie całej serii produktów. W momencie zaakceptowania, wyrażenia zgody na serię pierwowzorów produktów psychologicznych zostaje ona zgłoszona do dowódcy grupy zadaniowej posunięć/operacji psychologicznych (ang. *Psychological Operations Task Force* – POTF) lub dowódcy Elementu Wsparcia Psychologicznego (ang. *Psychological Operations Support Element* – PSE) na poziomie operacyjnym lub do dowódcy kompanii taktycznych działań psychologicznych (ang. *Tactical Psychological Operations Company* – TPC) na poziomie taktycznym w celu przeanalizowania serii. Po zaakceptowaniu całości serii przez dowódcę kompanii taktycznych działań psychologicznych, końcowe organy wytyczone do skontrolowania konkretnej serii przed ostatecznym organem zatwierdzającym to koordynator działań informacyjnych dywizji i dowódca dywizji. Wspomagana jednostka może dokonać zmian określonej drogi przepływu koncepcji produktów, a karda posunięć psychologicznych może posiadać dodatkowe wyjścia, przygotowane do wdrożenia w celu kontynuowania wsparcia psychologicznego. W sytuacji, kiedy seria nie uzyska akceptacji zostaje ona wysłana z powrotem do organu projektującego produkt w celu poprawy i ulepszenia całości serii. Po akceptacji seria wysyłana jest do następnych poziomów dowodzenia, a końcowo wystawiona zostaje do akceptacji dowódcy dywizji albo połączonego zespołu zadaniowego. Ostatnia wymieniona jednostka ma możliwość odrzucenia koncepcji serii i wysłania jej po raz kolejny do organu działań psychologicznych, zajmujących się przygotowaniem projektu serii. Może ona również zaakceptować serie po poprawkach, ale także dokonać akceptacji serii produktów, mimo wątpliwości zaprezentowanych przez jednostki podwładne. Zazwyczaj, kiedy modyfikacje są nieznaczne, dowódca akceptuje serię, dodając wytyczne koniecznych zmian. Tylko w przypadku, kiedy seria produktów jest w dużym stopniu niezgodna z planami przedstawionymi w arkuszach, zachodzi możliwość całkowitego jej odrzucenia, cofnięcia serii produktów psychologicznych.

Etap szósty to produkcja i dystrybucja zaprojektowanych produktów. Według amerykańskich wytycznych, po zamknięciu procedury akceptacji

i zatwierdzenia serii, uruchamia się następny etap procesu kontynuowanych zadań psychologicznych. W skład tej fazy wchodzi: eksplikowanie treści, próby pierwotne, produkcja, kolportaż, rozpowszechnianie, jak również testy wtórne wszystkich przygotowanych produktów. Schemat prób wykonywany jest podczas fazy szóstej i kontrolowany w ciągu następnego etapu. Ważną częścią omawianej fazy będzie tłumaczenie, eksplikowanie serii produktów, odbywające się po ich akceptacji, dokonanej przez wspieraną jednostkę. Najkorzystniejszym dla USA wyjściem jest wydelegowanie do tego zadania osób wykształconych, znających wiele języków obcych oraz mających dostęp do informacji utajnionych. Dzięki temu tłumaczenie jest przygotowane w sposób prawidłowy. Wybór takich osób odbywa się przy wykorzystaniu klasyfikacji na kategorie użyteczności konkretnych umiejętności. Wyróżnia się trzy kategorie:

- **kategoria nr I** – charakteryzuje się łatwością w używaniu języka obcego (rodzima biegłość), a także zaawansowanym stopniem użycia języka angielskiego (lokalny tłumacz, personel wyłączony z przestrzeni operacji; nie są konieczne wymogi kontroli z obszaru danych osobowych. Niewielki poziom zaufania z punktu widzenia tłumaczenia skomplikowanych tekstów);
- **kategoria nr II** – mieszkańcy posiadający obywatelstwo amerykańskie, wybrani i skontrolowani przez służby wojskowe Stanów Zjednoczonych, mający możliwość dostępu do informacji utajnionych;
- **kategoria nr III** – osoby z obywatelstwem USA, po przejściu kontroli przez służby wojskowe Stanów Zjednoczonych, z dostępem do informacji utajnionych, posiadających charakter dokumentów ściśle tajnych (osoby te posiadają umiejętność rozumienia sensu wszystkich dyskusji w miejscowym dialekcie, wykonywania połączeń telefonicznych, rozumienia treści komunikatów radiowych i telewizyjnych w owym dialekcie oraz sensu ustnych doniesień).

Zgodnie ze stanowiskiem amerykańskim, następną, ważną fazą wdrażania etapu szóstego będzie kontrola jakości. Kontrolę przeprowadza się bez względu na rodzaj środków produkcji produktów psychologicznych. Sprawdzenia dokonuje osoba, pracownik zespołu produkcji materiałów psychologicznych przy pomocy tłumacza. Przy produktach wizualnych obszar produkcyjny sprawdza od początku, czy założenia produkcji są zgodne z zaakceptowanym pierwowzorem. Dodatkowo, tłumacz ma za zadanie sprawdzić eksplikację, oceniając, czy translatowana treść jest zgodna z oryginałem.

Materiały dźwiękowe przechodzą kontrole pod względem jakości sygnału. Kontrola polega na sprawdzeniu, czy dany produkt jest zrozumiały w obcym języku i na jakim poziomie zachodzi zgodność z oryginałem. Z kolei produkty audiowizualne sprawdzane są pod względem kompaty-

bilności ze skryptem, jakości nagrania oraz odpowiedniego formatu zapisu, pozwalającego na ich odtworzenie. Ważną funkcją grupy sprawdzającej jest uzyskanie pewności, że owy produkt nie posiada kulturowych rozbieżności i błędów. Koniec procesu kontroli oznacza początek produkcji masowej produktów psychologicznych. Używając stałych oraz ruchomych, mobilnych środków produkcji, postulując o uzyskanie dodatkowych środków przydzielanych przez urząd administracji Stanów Zjednoczonych, profile amerykańskich zadań psychologicznych wykonują schemat produkcji serii produktów psychologicznych. Po zakończeniu owego procesu, fabrykat przesyłany jest do obiektów dystrybucji. Całość jest kompatybilna z zaakceptowanymi poprzednio ramami czasowymi. Rozesłanie wytworów dokonywane jest przy wykorzystaniu drogi lądowej, powietrznej oraz przy użyciu systemów teleinformatycznych. Rozpowszechnianie prowadzone jest przy użyciu środków transportu armii amerykańskiej oraz państw sojuszniczych, organizacji i firm krajowych, jednostek komercyjnych oraz pozostałych placówek rządowych. Środki dystrybucji wybiera się, dokonując analizy wpływu oraz przestrzeni, zasięgu działań. Do sposobów rozpowszechniania produktów psychologicznych zalicza się m.in.: łącza internetowe, emisje radiowe, kolportaż ulotek drogą powietrzną, emisje telewizyjne. Każdorazowo wykorzystywane do wykonania przekazu psychologicznego źródło jest używane zgodnie z wcześniej przygotowanym planem, ustalonym z władzami docelowej społeczności. Istotną częścią takiej dystrybucji jest odpowiednie zrozumienie docelowego społeczeństwa: jego norm, zwyczajów, kultury regionalnej. Mechanizm ten umożliwia uzyskanie zaufania regionalnego adresata. Najlepszą, przynoszącą największe efekty metodą wsparcia, wykonania zadania dowódcy ogólnowojskowego jest duża częstotliwość komunikacji bezpośredniej z regionalnymi władzami, przywódcami oraz przedstawicielami mieszkańców.

Nie sposób pominąć końcowego, siódmego etapu procesu. Jest nim oszacowanie wpływu działań psychologicznych. Najważniejszym punktem tego etapu jest oszacowanie poziomu uzyskanych, zrealizowanych celów posunięć psychologicznych, jak również całkowitego oddziaływania serii produktów na postępowanie podmiotów wpływu. Trzeba wspomnieć, że każda seria stanowi jeden z kilku mechanizmów, metod wywierania wpływu na postępowanie podmiotu oddziaływania. Z tego wynika, iż recenzowanie oddziaływania zadań psychologicznych na postępowanie podmiotu wpływu ma charakter złożony, gdzie konieczne jest porównanie obiektywnych metod oceny z subiektywnym zdaniem osoby oceniającej. Rezultat wpływu psychologicznego bazuje na dwóch torach postępowania: dokonaniu prób początkowej i wtórnej oraz uzyskaniu efektywności posunięć psychologicznych w wybranym odcinku czasowym.

Impact indicators to tzw. wskaźniki wpływu, na podstawie których prowadzona jest końcowa część zadania, czyli szacowanie stopnia użyteczności wspierających celów działań oraz celów głównych (wskaźnikiem użyteczności jest realizacja podstawowych zamierzeń działań psychologicznych). Wspomniane wskaźniki wybiera się podczas projektowania działań, wdrażanych na etapie pierwszym, podlegającym usystematyzowaniu na etapie drugim. Trzeba jednak zauważyć, że konkretne gromadzenie informacji, jak również ich analiza wykonywane są w ostatnim etapie przedstawionego procesu. Warto w tym miejscu zwrócić uwagę na precyzyjne określania metod szacowania efektywności posunięć psychologicznych. W szereg najczęściej używanych ocen wlicza się: ocenę skuteczności (ang. *Measure of Effectiveness* – MOE) polegającą na odnajdywaniu bezpośredniej relacji między dystrybuowanym przekazem, a konkretnym postępowaniem obiektu oddziaływania, ocenę osiągnięcia celu (ang. *Measure of Objective* – MOO) polegającą na symulacji odpowiedzi na pytanie, czy podmiot oddziaływania postępuje zgodnie z wytyczonymi celami operacji (określonymi przez dowódcę) w ramach stosowanych wobec niego posunięć psychologicznych oraz oszacowanie wyników (ang. *Measure of Merit* – MOM), czyli reakcji podmiotu oddziaływania na operację psychologiczną, ocenę działalności (ang. *Measure of Performance* – MOP) prezentującą poziom zgodności wdrażanych przedsięwzięć z poprzednio przygotowanym planem.

Ważne, przy szacowaniu wpływu posunięć psychologicznych, będzie wytypowanie kryteriów owej oceny. Typowanie kryteriów ma początek na etapie planowania. Kryteria te wybiera się w celu wykazania modyfikacji zauważalnych w postępowaniu podmiotu wpływu, po wdrożeniu zadań operacji psychologicznych. Założenia zyskują zazwyczaj charakter pytań, a omawiane poprzednio wskaźniki oddziaływania są pewnego rodzaju odpowiedzią na zadane pytania. Ważne jest zwrócenie uwagi na wpływ sytuacji mających charakter spontaniczny (ang. *spontaneous events*) oraz zdarzeń, które nie są rezultatem posunięć psychologicznych. Najważniejszym punktem końcowego etapu zadań psychologicznych, zgodnie z ustaleniami amerykańskich regulaminów, będzie analiza nurtów widocznych w postępowaniu podmiotów oddziaływania podczas całej operacji, przed nią i po niej. Stanowi to zadanie rygorystyczne, całkowicie uwarunkowane dobrym, całościowym planowaniem, konkretną, doprecyzowaną analizą oraz zharmonizowaniem pracy wszystkich włączonych elementów.

Trzeba wspomnieć, iż amerykańskie operacje psychologiczne nastawione są na ciągły rozwój i modyfikacje potencjału na każdej, możliwej płaszczyźnie ich wdrożenia. Wszelkie wymogi, założenia projekcji i realizacji zarówno wpływu psychologicznego, jak i aspektu informacyjnego bazują na dokładnym opracowaniu celów operacji stawianych organom wyde-

legowanym do ich wdrożenia. Dlatego też, w sposób bardzo dokładny określa się płaszczyznę zainteresowań posunięć psychologicznych w aspektach militarnych oraz politycznych. Omawiane struktury poddawane są stałej kontroli w celu dokładnego zagospodarowania zasobów oraz zniwelowania możliwości powielenia wkładanego wysiłku. Zgodnie z tą ideą operacje psychologiczne są wyspecjalizowane, dostosowane w aspektach użytkowych oraz z punktu widzenia położenia geograficznego.

Ze względu na szeroki zasięg operacji prowadzonych przez siły USA, koniecznym było wprowadzenie ilościowego rozłożenia potencjału, zasobów operacji psychologicznych. Jedynym wyjściem, rozwiązaniem owego utrudnienia jest zatem powołanie wyszkolonych grup, rezerw personalnych na przestrzeni krótkich odcinków czasowych. Wspomniane rezerwy osobowe oddelegowane zostaną do działań wspierających siły wykonujące operacje psychologiczne. Konieczność natychmiastowej reakcji na intensywne zmiany sytuacji psychologicznej w konkretnym położeniu geograficznym implikowała potrzebę wdrożenia dodatkowego wyposażenia oraz ekwipunku, sprzętu militarnego na użytek posunięć psychologicznych sił zbrojnych USA. Przykłady dodatkowo włączonych sprzętów stanowić mogą: samolot działań psychologicznych EC-130E, mobilne systemy mediów operacji specjalnych, rozgłośnie elektroakustyczne, bomby ulotkowe. Imponująca ilość dostępnych zasobów wskazywała konieczność zaprojektowania całego schematu rozpowszechniania w dwóch płaszczyznach: tradycyjnej – rzeczywisty, faktyczny transport oraz nowoczesnej – poprzez systemy teleinformatyczne.

Operacje psychologiczne sił zbrojnych USA mają możliwość kompletowania informacji używanych przede wszystkim do wieloaspektowej analizy i szacowania efektywności wywieranego wpływu. Kluczowe znaczenie posiada jednak dostosowana aparatura proceduralna. W USA wytyczono skrupulatną i szczegółową procedurę zorganizowania oraz wdrożenia działań psychologicznych. Opisana powyżej procedura wyróżnia siedem etapów. Umożliwia to precyzyjne wdrożenie kolejnych kroków, nawet w sytuacji małego doświadczenia personelu lub niedokładnej wiedzy z tego obszaru.

Uogólniając, można stwierdzić, że cele i zadania operacji psychologicznych można zawrzeć w trzech punktach:

- zniechęcenie przeciwnika do podejmowania działań oraz osłabienie jego agresywnych zamiarów lub potencjalnie przeciwnych obiektów oddziaływania;
- zwiększenie zaangażowania, zainteresowania i wsparcia ze strony potencjalnych sojuszników bądź przyjaznych podmiotów;
- pozyskanie poparcia i współpracy ze strony środowisk niezaangażo-

wanych lub niezdecydowanych[206].

W trakcie konfliktów zbrojnych działania psychologiczne prowadzone są zwykle przez wyspecjalizowane organa propagandowo-agitacyjne. Takie właśnie działania są prowadzone poprzez powszechny dostęp do technologii komunikacyjnych oraz Internetu. Dodatkowo cechą charakterystyczną jest wykorzystywanie sprzeczności, wynikających z różnic religijnych, etnicznych czy społecznych. W celu złamania stanu moralnego a w efekcie pozbawienie go chęci walki, stosuje się takie techniki, jak: chaos, panikę, sabotaż i dywersję, a także inspiruje się ruchy zbrojne. Częstymi praktykami są także obietnice polepszenia warunków życia, swobód i przestrzegania praw człowieka[207].

Przykładem operacji psychologicznej z wykorzystaniem mediów społecznościowych jest prowadzona od 2014 roku wojna informacyjna przez Rosję na Ukrainie. W celu przybliżenia tego typu działań, należy wskazać kilka faktów, które mają wpływ na kształtowanie się **społeczeństwa informacyjnego**[208] na Ukrainie w ciągu ostatnich 15 lat. Od 2001 roku oligarchowie sprawowali kontrolę nad największymi stacjami telewizyjnymi i radiowymi na Ukrainie. Media były cenzurowane, rynek prasy na Ukrainie nigdy nie był rozwinięty, co było przyczynkiem do masowego korzystania z Internetu. Dodatkowo pojawienie się w 2008 roku Facebooka (FB) zwróciło uwagę nielicznej, ale bardzo aktywnej części społeczeństwa, która stworzyła sieć (ang. *trusted network*), korzystającą z tzw. **mądrości tłumu** (ang. *wisdom of the crowd*) – sieć zaufanych osób, które wycofały się z mediów tradycyjnych i zorganizowały odrębne grupy, które nie tylko wymieniały się wiadomościami, ale stworzyły także wizję tego, jak musi się zmienić państwo.

Zainicjowany Euromajdan – fala protestów i demonstracji przeciwko prezydentowi, która przekształciła się w ogólnonarodową rewolucję – bazował w dużej mierze na FB. Za jego pomocą organizowano obronę podczas ataków, koordynowano dostawę leków i jedzenia dla osób, które całodobowo mieszkały na Majdanie. Co ważne, było to także narzędzie, dzięki któremu w czasie demonstracji antyrządowych, prowadzona była działalność informacyjna. Dzięki Facebook'owi możliwe było prowadzenie dzia-

---

[206] Z. Modrzejewski, *Operacje informacyjne*, Akademia Obrony Narodowej, Warszawa 2014.

[207] A. Żebrowski, W*alka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016.

[208] **Społeczeństwo informacyjne** – termin ten po raz pierwszy został wprowadzony w 1963 roku przez Japończyka – T. Umesao i spopularyzowany przez K. Koyama w 1968 roku. Jest ono określane jako społeczeństwo, w którym towarem nadrzędnym jest informacja traktowana jako szczególne dobro niematerialne, często ważniejsze od dóbr materialnych, służących do zaspokojenia bytu ludzkiego.

łalności skupionej na: promowaniu osób wyjątkowo medialnych, manipulacjach, kłamstwach, plotkach itd. Takie działania doprowadziły do **tabloidyzacji polityki**[209] oraz spowodowały popularyzację mediów społecznościowych, których przykładem jest Facebook.

Należy zauważyć, że media społecznościowe podczas agresji Rosji wobec Ukrainy często były wykorzystywane dla rozpowszechnienia paniki, nienawiści, tworzenia atmosfery nieufności i podejrzeń. Takie praktyki bardzo silnie oddziaływały na media tradycyjne, a więc na całe społeczeństwo. Za przykład można podać wydarzenia z 14 lipca 2014 roku – półtora miesiąca przed faktycznym rozpoczęciem rosyjskiej ofensywy na Donbas. Wiele szanowanych mediów informowało o wypadku z rosyjską haubicą samobieżną, która jechała na Ukrainę. Podstawą tej informacji był wpis jednego z **blogerów**[210] na FB – którego publikacja zawierała niepotwierdzone i jak się okazało nieprawdziwe treści. Ukraińskie przykłady wykorzystania *social media* nie są unikatowe. Dzisiaj sieci społecznościowe są skutecznym narzędziem nie tylko wpływania na ludzi, lecz także kształtowania i wpływania na polityki na całym świecie. Wartym uwagi jest fakt, że po kryzysie gospodarczym w 2008 roku tradycyjne media zaczęły tracić zyski. Doprowadziło to do redukcji liczby dziennikarzy, w zamian za korzystanie i publikowanie treści za pomocą mediów społecznościowych. Faktem pozostaje także to, że Rosja zatrudniła około 600 trolli internetowych, których działania skupione są na rozpowszechnianiu wpisów rosyjskiej telewizji informacyjnej – Russia Today oraz z innych rosyjskich źródeł informacyjnych, zwiększając ich rankingi, co z kolei wpływa na media tradycyjne. Takie praktyki spotkały się z reakcją niektórych państw. Dla przykładu można podać armię brytyjską, która stworzyła jednostkę wojskową – Brygadę 77, liczącą 1,5-2 tys. żołnierzy. Jej zadaniem jest walka informacyjna (oraz psychologiczna) głowienie na FB oraz przekazywanie pozytywnych treści o polityce i rządzie Brytanii[211].

---

[209] **Tabloidyzacja –** upodobnienie się stylem do tabloidów, popularnych gazet zajmujących się plotkami i nieistotnymi sensacjami. Przyczynami tego zjawiska jest pojawienie się w mediach trzech tendencji: obniżenie standardów dziennikarskich, zmniejszenie ilości informacji twardych (ekonomicznych czy politycznych) oraz eksponowanie informacji miękkich, takich jak: sensacja, skandal czy rozrywka, H. Kurtz, *Media Circus – The Trouble with America's Newspapers*, New York 1993, s. 143-147.

[210] **Bloger** (inaczej: blogger, blogowicz) – to osoba publikująca swój blog (publikowany publicznie – np. w sieci Internet – blog, zwykle z możliwością komentowania jego poszczególnych wpisów), *Słownik Języka Polskiego PWN*, online – https://sjp.pl/bloger [dostęp: 19.08.2017].

[211] M. Dobranowska-Wittels, *Decydująca rola źródeł informacji dla sytuacji politycznej na przykładzie Ukrainy*, online – http://www.kirkland.edu.pl/ru/2012-12-19-12-21-29/83-biblioteka/315-piddub [dostęp: 19.08.2017].

5.2.2. Dezinformacja i propaganda[212]

W współczesnym polskim piśmiennictwie definicję dezinformacji (propagandy) możemy odnaleźć między innymi w cytowanym wcześniej projekcie „Doktryny bezpieczeństwa informacyjnego". Określa ona że dezinformacja (propaganda) „to rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich), w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego, lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń"[213]. Należy zauważyć, że projekt doktryny nie rozróżnia terminów – dezinformacja i propaganda, traktując je tożsamo. Na potrzeby tej pracy pojęcia te zostaną odróżnione.

Analizując etymologię terminu dezinformacja, należy zwrócić uwagę na to, że składa się ono z przedrostka –„dez" oraz słowa właściwego. Przedrostek ten oznacza wyraz złożony wskazujący na zaprzeczenie, pozbawienie lub odwrotność tego, co nazywa drugi człon złożenia[214] – informacja.

Dezinformacja, to według jednej z zachodnich definicji „sfabrykowane świadectwa, taktyka oczerniania oraz sfabrykowane dokumenty wykorzystane do zdyskredytowania przeciwnika"[215]. Według innego źródła jest to „tworzenie i rozpowszechnianie wprowadzających w błąd lub fałszywych informacji w celu wyrządzenia szkody wizerunkowi kraju wybranego za cel"[216].

W polskim piśmiennictwie pojęcie dezinformacji pojawiło się już w 1929 roku. Instrukcja Oddziału II Sztabu Głównego Wojska Polskiego wyjaśnia, że dezinformacja polega na „podaniu wywiadowi przeciwnika wiadomości ukrywających własne zamierzenia oraz na zmuszaniu go do traktowania informacji podanej przez wywiad własny, jako prawdziwej, względnie zmuszaniu wywiadu obcego do analizy inspirowanych wiadomości przez czas dłuższy"[217]. Jeden ze współczesnych słowników języka polskiego definiuje dezinformację jako „wprowadzenie kogoś w błąd poprzez podanie mylących bądź fałszywych informacji"[218].

---

[212] Fragmenty niniejszego rozdziału pierwotnie opublikowano w: R. Bielawski, A. Ziółkowska, *Media społecznościowe…, op. cit.*

[213] *Doktryna Bezpieczeństwa Informacyjnego…*, *op. cit*., s. 4.

[214] *Słownik Języka Polskiego PWN*, online – http://sjp.pwn.pl/slowniki/dez%20.html [dostęp: 19.08.2017].

[215] R. Deacon, *Spyclopaedia*, Futura, Londyn 1989, s. 400.

[216] R.M. Bennett, *Espionage: An Encyclopedia of Spies and Secrets*, Virgin Books, Londyn 2002, s. 69.

[217] A. Pepłoński, *Wojna o tajemnice*, Wydawnictwo Literackie, Kraków 2011, s. 335.

[218] *Słownik Języka Polskiego PWN*, online – https://sjp.pwn.pl/szukaj/dezinformacja.html [dostęp: 25.08.2017].

Literatura rosyjska z kolei określa dezinformację jako „rozpowszechnianie za pośrednictwem prasy i radia wiadomości fałszywych, celem wprowadzenia w błąd opinii publicznej. Dezinformacji dopuszcza się, przykładowo, anglo-amerykański blok imperialistyczny, który przedstawia jako agresywną, niezmiennie pokojową politykę Związku Sowieckiego i innych krajów demokracji ludowej”[219].

Istnieją także różne klasyfikacje dezinformacji. Ze względu na sfery oddziaływania wyróżniamy cztery jej rodzaje:

- **dezinformacja polityczna** – prowadzona w wewnętrznej i zewnętrznej sferze państwa, przez centralne ograny kierownictwa państwa. W aspekcie wewnętrznym celem dezinformacji politycznej jest społeczeństwo własnego państwa i ma ono za zadanie kształtowanie pożądanych opinii, zachowań i postaw współobywateli. Dezinformacja w polityce zagranicznej ma na celu stworzenie pozytywnego wizerunku własnego państwa w obszarze polityki międzynarodowej. W przypadku, kiedy prowadzona polityka powoduje krytykę i sprzeciw społeczności międzynarodowej, zadaniem dezinformacji jest ukrycie swoich rzeczywistych celów i intencji, a także dążenie do uzyskania akceptacji i poparcia dla własnych działań;
- **dezinformacja ekonomiczna** – jej celem jest wprowadzenie przeciwnika w błąd, co do stanu prawdziwych osiągnięć ekonomiczno-gospodarczych, stanowiących rezerwuar obronny państwa;
- **dezinformacja naukowo-techniczna** – ma na celu ukrycie przed potencjalnym przeciwnikiem rzeczywistego stanu osiągnięć i odkryć naukowych, zgromadzonego doświadczenia, zmian teorii sztuki wojskowej, nowych modeli wyposażenia wojskowego, a także sposobów wykorzystania nowości i innowacji technologicznych, a także perspektyw i możliwości ich wdrożenia;
- **dezinformacja wojskowa** – jej celem jest przeciwnik, wojska własne oraz otoczenie. Oddziaływanie na przeciwnika tyczy się zazwyczaj przekazywania przez jego systemy rozpoznania błędnych informacji. Celem dezinformacji skierowanej do własnych sił zbrojnych jest spowodowanie takich ich działań, aby umocniły one przekonanie przeciwnika o prawdziwości wniosków wyciągniętych z rozpoznania. Dezinformacja wojskowa obejmuje zatem przekazywanie błędnych informacji – plotek, pogłosek, dokumentów, a także demonstrowanie działań wojskowych, w których celem jest zmylenie przeciwnika w kwestii prawdziwych zamierzeń, planów i przedsięwzięć o znaczeniu wojskowym. W wypadku dezinformacji wojskowej, wyróżnia się także działania ofensywne i defensywne. Pierwsze z nich mogą po-

[219] A. Golicyn, *New Lies For Old, Londyn*, The Bodley Head, 1984, s. 4-5.

zwolić na uzyskanie efektu zaskoczenia oraz utrzymanie inicjatywy, drugie zaś mają za zadnie poprawić bezpieczeństwo działań i stworzenie warunków do ich realizacji[220].

W odniesieniu do mediów społecznościowych można stwierdzić, że dezinformacja prowadzona jest na dwóch poziomach – taktycznym i strategicznym (w ujęciu wojskowym dodatkowo na poziomie operacyjnym). Zatem dezinformacja:

- **taktyczna** – charakteryzuje się stosunkowo krótkim czasem (zazwyczaj w skali miesięcy) oddziaływania i ma na celu wprowadzenie w błąd w jednej lub kilku łączących się ze sobą kwestiach. Analitycy amerykańscy dzielą dezinformację taktyczną na trzy rodzaje: polityczną, wojskową i ekonomiczną[221]. Obejmuje ona doraźne działania, których przykładami mogą być: opublikowanie sfabrykowanej notatki wewnętrznej polityka wyznaczonego do skompromitowania, podsunięcie nieprawdziwych danych technicznych uzbrojenia, zawyżonych lub zaniżonych danych statystycznych celem wywołania wrażenia, że stan gospodarki państwa jest w lepszej (albo gorszej) kondycji od rzeczywistej. Przekazywane są także pogłoski i plotki mające na celu odwrócenie uwagi społeczeństwa lub jego zastraszenie i zdemoralizowanie[222];
- **strategiczna** – polega na systematycznym przekazywanie fałszywych sygnałów politycznych, informacji i fabrykacji, celem wytworzenia wypaczonego obrazu powodującego wadliwą analizę sytuacji. Ten rodzaj dezinformacji prowadzony jest przez centralne organy kierownicze państwa. Jej celem jest wprowadzenie w błąd przeciwnika, co do podstawowych kwestii jego polityki; wywołanie zamętu w ocenie fundamentalnych zamiarów i ambicji drugiej strony. Prowadzi się ją przy pomocy kanałów politycznych, dyplomatycznych, ekonomicznych, naukowo-technicznych, wojskowych, specjalnych (cywilny i wojskowy wywiad i kontrwywiad), poprzez służby policyjne, służby do walki z narkotykami, służby do walki z terroryzmem, jednostki walki elektronicznej, jednostki rozpoznania wojskowego. W działaniach wykorzystuje się mniejszości narodowe, religijne i etniczne, or-

[220] T. Grabowski, *Metody walki informacyjnej…*, *op. cit.*, s. 42, za: A. Modrzejewski, *Operacje informacyjne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2014 oraz A. Żebrowski, *Walka informacyjna w asemetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016.

[221] J. Lenczowski, *Soviet Disinformation: An Overview, Background*, no. 465, The Heritage Foundation, Waszyngton DC 1985, s. 6.

[222] T. Grabowski, *Metody walki informacyjnej…*, *op. cit.*, s. 42, za: A. Żebrowski, Walka informacyjna, op. cit.; R. Brzeski, *Wojna informacyjna – wojna nowej generacji*, Wydawnictwo Antyk Marcin Dybowski, Komorów 2014.

ganizacje nacjonalistyczne, a nawet terrorystyczne i przestępcze o charakterze międzynarodowym.

Szczególnym rodzajem dezinformacji jest **dezinformacja wojskowa**, której celem jest uzyskanie efektu zaskoczenia, co warunkuje osiągnięcie powodzenia prowadzonych działań (operacji). Definiuje się ją jako „zamierzone przekazywanie przygotowanych (fałszywych) informacji, pogłosek, specjalnie opracowanych dokumentów oraz demonstrowanie działań wojsk, których celem jest wprowadzenie w błąd przeciwnika w odniesieniu do prawdziwych zamierzeń, planów i przedsięwzięć o znaczeniu militarnym”[223].

Literatura przedmiotu przewiduje kilka zasad, których przestrzeganie daje pewne prawdopodobieństwo odniesienia sukcesu w odniesieniu do dezinformacji. Należą do nich poniższe zasady:

- **celowości** – dezinformacja musi mieć jasno określony cel, który określa oczekiwany rezultat;
- **przygotowania** – to gwarancja dostępu do sił i środków koniecznych do realizacji oraz wsparcia dezinformacji, w tym z planem ich wykorzystania po zaistnieniu określonych skutków pośrednich;
- **kompleksowości** – określa stosowanie różnych form, metod oraz sposobów, podczas wykorzystania dostępnych sił i środków, a także kanałów przekazu dezinformacji;
- **scentralizowanego kierowania** – polega ona na ścisłym rozgraniczeniu zadań, koordynacji i współpracy między poszczególnymi zespołami, ograniczeniu inicjatywy osób wykonujących zadania na niższych szczeblach;
- **wiarygodności** – przewiduje prowadzenie procesu dezinformowania w taki sposób, by dezinformacja posiadała cechy informacji prawdziwej; oznacza to, że nie może być ona nieadekwatna w stosunku do sytuacji czy też nielogiczna;
- **dublowania** – uwzględnia ona sytuację, w której fałszywe informacje pochodzą z możliwie największej liczby źródeł, co daje w rezultacie efekt wzajemnego uwiarygodnienia;
- **elastyczności** – w sytuacji, gdy zostaje wywołany niepożądany efekt, albo w przypadku tylko częściowego sukcesu, trzeba przerwać proces dezinformowania bez wskazywania początkowego celu, a także należy określić nowe zadania oraz – w miarę możliwości – zamienić wykonawców tych zadań;
- **terminowości** – polega ona na wydzieleniu przeciwnikowi wystarczającej ilości czasu na: otrzymanie informacji, zrozumienie i prze-

[223] M. Wrzosek, *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON” 2012, nr 2(87), s. 23.

tworzenie jej, a także na reakcję, ale z drugiej strony zbyt mało na gruntowną analizę otrzymanej informacji i wykrycie błędnych informacji;
- **ciągłości** – przewiduje, że przesłanie nieprawdziwych informacji powinno przebiegać regularnie, a intensywność dezinformacji nie może wzrastać tuż przed rozpoczęciem aktywnych działań;
- **spójności** – jest zgodnością celu procesu dezinformacji z celem polityki zagranicznej państwa prowadzącego dezinformację i działalnością sił zbrojnych, a także musi zawierać logiczny związek pomiędzy formułowanymi przekazami;
- **nieszablonowości** – przewiduje unikanie wcześniej używanych technik i/lub zmianę sposobu ich wykorzystywania;
- **skrytości** – jest utrzymaniem własnych przedsięwzięć w tajemnicy przed agresorem, otoczeniem zewnętrznym, a także przed własnymi siłami, a nawet osobami, które wykonują konkretne szczegółowe zadania[224].

Przechodząc do pojęcia propagandy, można przytoczyć jej współczesne rozumienie, które między innymi przedstawia „Encyklopedia PWN". Odnajdujemy w niej definicję propagandy jako „celowe oddziaływanie na zbiorowości i jednostki zmierzające do pozyskania zwolenników i sojuszników, wpojenia pożądanych przekonań i wywołania określonych dążeń i zachowań"[225].

Propaganda jest także różnie rozumiana i przedstawiana przez analityków zajmujących się tego rodzaju mechanizmami wykorzystania mediów społecznościowych. W formie stabelaryzowanej przedstawiono je w tabeli 8.

Wyróżniamy jej kilka klasyfikacji. Jedna z nich, różnicująca ze względu na rodzaje źródeł, wyróżnia propagandę:
- **białą** – gdy nadawca jest znany;
- **szarą** – gdy źródło przekazu może, lecz nie musi być poprawnie określone a podawane przez nie dane nie są precyzyjne;
- **czarną** – gdy źródło przekazu ukrywa prawdziwego nadawcę a dane są sfabrykowane i zawierają fałszywe informacje[226].

---

[224] T. Grabowski, *Metody walki informacyjnej…*, *op. cit.*, s. 43-44 za: A. Modrzejewski, *Operacje informacyjne*, *op. cit*. oraz A. Żebrowski, *Walka informacyjna, op. cit.*

[225] *Encyclopedia PWN*, online – https://encyklopedia.pwn.pl/haslo/propaganda;3962718.html [dostęp: 11.08.2017].

[226] T. Grabowski, *op. cit*., s. 38; *Войны и их классификация*, online – http://voina-i-mir.ru/article/109 [dostęp: 25.08.2017].

Tabela 7. Definicje propagandy proponowane przez współczesnych naukowców

Autor	Definicja
A. Pratkins, E. Aronson	„Zręczne posługiwanie się obrazami, sloganami i symbolami, odwołujące się do naszych uprzedzeń i emocji; jest komunikowaniem pewnego punktu widzenia, mającym na celu skłonienie odbiorcy do dobrowolnego przyjęcia tego punktu widzenia za swój".
B. Dobek-Ostrowska	„Technika wpływania na zachowania obywateli, kierowania opinią publiczną i manipulowania. Opiera się na najnowszych osiągnięciach naukowych i wynikach badań empirycznych w zakresie psychologii społecznej, socjologii, politologii, teorii komunikowania i innych naukach społecznych".
H. Kula	„Celowe upowszechnianie wiadomości, opinii, poglądów, teorii, wyjaśniających otaczającą rzeczywistość i zjawiska życia społecznego".
R. Brzeski	„Proces intencjonalnego rozpowszechniania poglądów i przekonań, specyficzny proces komunikowania się, w którym nadawca stara się manipulować odbiorcami drogą rozbudzania emocji oraz zwodniczą lub pokrętną argumentacją".
L. Fraser	„Sztuka skłaniania innych do działań odmiennych od zachowań, które poczyniliby bez propagandy".
Ł. Szurmiński	„Umotywowana politycznie, celowa i systematyczna próba kształtowania percepcji i ludzkich postaw, realizowana głównie za pomocą środków masowej komunikacji w celu zapewnienia sobie poparcia opinii publicznej dla podejmowanych działań".

Źródło: tabela za T. Grabowski, *op. cit.*, s. 37 i podanymi tam źródłami, tj. T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, 2(24), s. 53-54; R. Brzeski, *op. cit.,* s. 193–194; Ł. Szurmiński, *Pojęcie propagandy*, 2016, online – http://www.id.uw.edu.pl/~lukasz.szurm/Anatomia%20propagandy/2.%20Poj%C4%99ie%20propagandy.pdf [dostęp: 25.08.2017].

Ze względu na kierunki oddziaływania wyróżnia się propagandę zewnętrzną oraz wewnętrzną. Ze względu na zależność w czasie wymienia się propagandę poprzedzającą, towarzyszącą oraz następczą.

W literaturze przedmiotu istnieje pojęcie – **Propaganda 2.0.** Jest ona związana z rozwojem tzw. Sieci 2.0. W analogicznym znaczeniu do niej, ten rodzaj propagandy odróżnia się możliwością generowania treści przez użytkowników danych mediów społecznościowych. Zanikają ograniczenia wynikające z położenia geograficznego i czasowe, a decentralizacja i anonimowość osób zamieszczających materiały propagandowe w sieci utrudnia zlokalizowanie i zneutralizowanie źródeł propagandy. Takie wykorzy-

stanie *mass mediów* daje unikalne możliwości manipulacji tekstem, dźwiękiem oraz obrazem. Dobrym tego przykładem jest serwis YouTube. Z powodzeniem wypiera on z życia, szczególnie wśród młodzieży, czyli tzw. *digital natives*[227], telewizję, radio oraz inne środki masowego przekazu, omijając przy tym ich największą wadę czyli – ograniczenia czasowo-przestrzenne[228]. Oznacza to, że serwis można obejrzeć w każdej chwili i w każdym miejscu. Dodatkową zaletą jest możliwość zamieszczenia komentarzy oraz wyboru opcji – lubię (czyli podoba mi się) lub nie lubię (nie podaba mi się).

Współczesne wykorzystywanie propagandy za pomocą mediów społecznościowych charakteryzuje się umiejętnym posługiwaniem się słowami, ale również działaniem multimedialnym, gdzie dużą rolę odgrywają: fotografie, rysunki, obrazy, nagrania wideo, a także pieśni, defilady, manifestacje, wiece i inne środki. Propaganda skierowana jest do odbiorcy masowego i wykorzystuje wiedzę naukową o tym, jak poprzez kreowane emocje wpływać na ludzkie zachowania. Oprócz funkcji informującej zawiera inną – wydaje się znacznie ważniejszą funkcję – tzw. komunikowanie perswazyjne[229].

Zatem chcąc odróżnić dezinformację od propagandy należy wykazać parę różniących je kwestii. Jak wcześniej stwierdzono, dezinformacja odnosi się do pewnego rodzaju informacji, jednakże jest jej przeciwieństwem, informacją fałszywą, kłamliwą lub rzekomą, która wprowadza w błąd odbiorcę. Zasadniczym założeniem interpretacyjnym pojęcia „dezinformacja" jest jej celowość – tzn. nieprawdziwa informacja jest przekazywana po to, aby osiągnąć określony efekt, dać odbiorcy wiedzę pozorną, bezużyteczną lub wręcz szkodliwą, która następnie posłuży do podejmowania przez niego błędnych decyzji, korzystnych z punktu widzenia dezinformatora. Niewykluczone jest także osiągnięcie efektu niezamierzonego, wynikającego z błędnego zrozumienia treści informacyjnej przez odbiorcę lub jej zniekształcenia np. przez media społecznościowe[230]. Natomiast propaganda

---

[227] ***Digital natives*** (cyfrowe pokolenie) – tworzy grupę ludzi urodzonych po 1995 roku, których charakteryzuje nagminne użytkowanie sieci Internet (średnio ok. 4 h dziennie), w tym także sieci mobilnej, np. za pomocą telefonu komórkowego. Inne nazwy tej grupy użytkowników sieci to: pokolenie @, dzieci neostrady, pokolenie SMS, pokolenie N (od ang. *net* – sieć), cyfrowe pokolenie, generacja Y, pokolenie www: wszystko, A. Skudrzyk, *Homo videns – nowe media a język młodego pokolenia*, Uniwersytet Śląski, Katowice 2017, s. 156-157.

[228] M. Lakomy, *Demokracja 2.0., Interakcja polityczna w nowych mediach*, Wydawnictwo WAM, Kraków 2013.

[229] Wyjaśnione szerzej w dalszej części pracy dotyczącej aspektów psychologicznych wykorzystania mediów społecznościowych.

[230] M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnych*, Warszawa 2005, s. 8.

jest powszechnie kojarzona z praktyką okłamywania całych społeczeństw przez władze państwowe, szczególnie funkcjonujące w państwach totalitarnych. Jako taka skierowana była do potencjalnego przeciwnika lub opinii międzynarodowej, ale przede wszystkim do własnego społeczeństwa[231]. Dodatkowo należy podkreślić, że ani dezinformacja, ani propaganda nie są celem, a środkiem do osiągnięcia określonego, z reguły długofalowego, celu politycznego lub wojskowego.

5.2.3. Fake news i post-prawda

Kolejną grupą działań w walce informacyjnej, przy wykorzystaniu mediów społecznościowych, mających wpływ na bezpieczeństwo narodowe są *fake news*. Tym anglojęzycznym terminem określamy taki rodzaj informacji, których przekaz ma za zadanie wywoływać szokujące, nacechowane emocjonalnie przekazy. Można zdefiniować *fake news* jako informację nieprawdziwą, przekazywaną i proliferowaną przez *mass media*. Jej celem jest przekaz nieprawdziwej informacji a przez to wprowadzenie odbiorcy w błąd. W ten sposób wywoływane są określone emocje i nastawienie do danej kwestii.

Zadaniem *fake news* jest szokowanie i budzenie kontrowersji oraz silne emocje u odbiorcy. Kwesta przekazu faktów jest tutaj drugorzędna. *Fake news* jest zatem „podsycany" emocjami a nie faktami, dlatego często bazuje na przekonaniach religijnych, wartościach, poglądach, stereotypach, uprzedzeniach etc. Aby *fake news* był skuteczny jako narzędzie masowej perswazji, musi odnosić się do koncepcji już istniejących w świadomości jakiejś grupy społecznej[232].

Fake news pociąga ze sobą istotne szkody społeczne. Dezinformacja lub selektywny wybór faktów, a także nadawanie im nowego kontekstu służy najczęściej do manipulowania dużymi grupami społecznymi. W rezultacie stwarza to duże zagrożenie skierowane przeciwko systemowi demokratycznemu.

Głównym celem działania *fake news* jest kształtowanie opinii publicznej. W tym przypadku określenie „publiczna" odnosi się do grupy ludzi, którzy w określonej dziedzinie mają wspólny interes. Opinią możemy tutaj nazwać: *wrażenie, własną postawę wobec jakiegoś tematu*. Opinia publiczna stała się partnerem organizacji, zyskując również podmiotowość. Z pojęciem – opinia publiczna również wiąże się nierozerwalnie psychologiczna **zasada społecznego dowodu słuszności**. Polega ona na tym, że opinia

[231] T. Kacała, *Dezinformacja i propaganda w kontekście…*, *op. cit.*, s. 51.
[232] *Raport: „Fake news z perspektywy polskich dziennikarzy" – wyniki badań*, Public Dialog, 2017, s. 6.

kształtowana jest przez ludzi poprzez obserwacje zachowań innych członków grupy społecznej, do której przynależą. W szczególności dotyczy to osób nieposiadających wystarczającej wiedzy, odczuwających niepokój czy niepewność i niepotrafiących ocenić danej sytuacji.

Wyróżnia się trzy podstawowe typy *fake news*:

- **całkowita nieprawda** – z premedytacją podaje się nieprawdziwe, sprzeczne, sfabrykowane fakty lub informacje;
- **prawda jest sporna** – odbiorca wprowadzony jest w błąd, poprzez nadanie odpowiedniego kontekstu faktom lub przedstawianie ich w sposób selektywny;
- **manipulacja cytatem** – umiejętne umieszczanie wypowiedzi danej osoby w kontekście; wycinanie zdań, co zmienia w ten sposób sens wypowiedzi. Dzięki temu podkreślana jest konkretna teza[233].

W związku z coraz większym rozpowszechnianiem się *fake news* zarówno rządy niektórych krajów, jak i międzynarodowe firmy, korporacje i organizacje widzą uzasadnioną potrzebę w opracowaniu struktur, których celem będzie wprowadzenie i ujednolicenie rozwiązań zapobiegających rozpowszechnianiu tego typu szkodliwych wiadomości. Facebook, który ze względu na swój zasięg oraz popularność jest jednym z głównych (w mediach społecznościowych) źródłem proliferacji *fake news* zapowiedział, iż wprowadzi nowe narzędzia do monitorowania, a następnie usuwania takich treści. Dotychczas usunięciu uległy dziesiątki tysięcy fałszywych kont, które były używane przy różnych kampaniach, m.in. dotyczących Brexitu[234]. Jedna z największych firm w USA – Google – zapowiedziała w roku 2017 wprowadzenie dużych zmian w „silniku" programu i algorytmach. Mają one powodować przesuwanie na dalsze pozycje w wynikach wyszukiwania tych stron, na których pojawiają się lub rozprzestrzeniane są wiadomości *fake news*. Ponadto, korporacja stworzyła zespół 10 tys. pracowników oddelegowanych do sprawdzania tego typu stron, w celu dokładniejszej ich weryfikacji.

Oprócz kampanii, które zapowiedziały duże informatyczne koncerny, istnieje również kilka zasad, stosując się do których można uchronić siebie przed działaniem *fake news*. Są one dostępne w wielu serwisach popularyzujących informacje na ten temat[235].

Z pojęciem *fake news* łączy się termin – **post-prawda** (ang. *post-truth*). Oznacza on rzeczywistość kultury politycznej, w której fakty są mniej waż-

---

[233] *Raport: „Fake news…, op. cit.,* s. 7.

[234] Potoczna nazwa procesu opuszczania przez Wielką Brytanię struktur Unii Europejskiej, zapoczątkowanego po referendum w czerwcu 2016 roku.

[235] Por. A. Łuczyńska, *Jak radzić sobie z fake news?*, Fundacja Szkoła z Klasą, 2017, s. 1-2 (licencja CC-BY-SA 3.0), Por.
https://migracje.ceo.org.pl/sites/migracje.ceo.org.pl/files/10_wskazowek_fake_news.pdf

ne w kształtowaniu opinii publicznej niż odwoływanie się do emocji i osobistych przekonań. Post-prawda to inaczej uciekanie od prawdy, przekazywanie niepełnej prawdy oraz nieprawdy.

Po raz pierwszy pojęcie post-prawdy zainicjowane zostało w 1992 roku przez Steve Tesich. Użył on tego pojęcia w odniesieniu do wydarzeń wojskowo-politycznych w USA. Stwierdził, że afera Irangate[236] oraz wojna w Zatoce Perskiej zostały potraktowane o wiele łagodniej niż afera Watergate, dotycząca skandalu politycznego, w efekcie którego prezydent USA Richard Nixon ustąpił ze stanowiska. W tym przypadku nie chodziło o zatajenie prawdy, lecz o powszechne zachowania osłabiające znaczenie prawdy – o zbiorową niechęć do skonfrontowania się z realnością.

Można zauważyć, że współcześnie, pomimo szerokiego dostępu do wiadomości propagowanych przez ***mass media***, ulegamy post-prawdzie. Wydaje się, że dzieje się tak z dwóch przyczyn. Po pierwsze – współczesne publikowane wiadomości/przekazy czy informacje oraz ich treści są często anonimowego autorstwa i nie podlegają one żadnej formie weryfikacji. Poza tym poszukuje się informacji nie tyle obiektywnej i prawdziwej, lecz atrakcyjnej, szokującej czy śmiesznej, zatem takiej, która nacechowana jest emocjonalnie. Po drugie – wykształciło się tzw. **upartyjnienie prawdy**, co należy rozumieć w ten sposób, że często jest ona niewygodna i istnieje ogólne przyzwolenie społeczne na przekazywanie informacji mijających się z nią. Poza tym wywołuje ona u odbiorcy mniej emocji.

Stopień upartyjnienia prawdy można oszacować za pomocą trzech kryteriów: zaangażowania władzy we własność mediów i ich zarządzanie, linii programowej organizacji medialnej i partyjnej afiliacji czytelników. M. Marzec wyróżnia pięć poziomów upartyjnienia mediów, tj.:

- **bardzo wysoki poziom upartyjnienia** – media należą do władz lub liderów partii politycznych. Przedstawiciele władzy mają wpływ na zarządzanie, produkcję, zawartość i finansowanie *mass mediów*. Budżet jest szczególnie silnym środkiem oddziaływania na użytkowników;
- **wysoki poziom upartyjnienia** – władza nie ma oficjalnych więzów z mediami społecznościowymi. Posiadają one jednak duży wpływ na właścicieli mediów i dziennikarzy poprzez ich emocjonalne zaangażowanie i lojalność. Powszechnie wiadomo także, że dane medium popiera określoną formację polityczną. Takie poparcie wynika z reguły z konotacji historycznych;
- **średni poziom upartyjnienia** – występuje on w sytuacji, gdy kon-

[236] **Afera Irangate** – skandal polityczny, który miał miejsce w Stanach Zjednoczonych w latach 1986-1987. Powodem było ujawnienie przez media informacji na temat nielegalnej, tajnej sprzedaży broni do Iranu.

kretny środek masowego przekazu popiera daną grupę polityczną w sposób warunkowy. Linia redakcyjna danego medium jest przychylna władzy konkretnej formacji, ale nie popiera jej bezwarunkowo, pozwalając na krytykę jej poczynań. Możliwe jest także odwrócenie kierunku sympatii. Medium stara się zachować pewien stopień obiektywności, wyrażając pochlebne opinie o opozycji, jeśli ta na to zasługuje;

- **niski poziom upartyjnienia** – poparcie medium jest udzielane w nieprzewidywalnych formach – *ad hoc*. Poparcie medium jest więc wynikiem konkretnych działań przedstawicieli władzy i nie jest dane raz na zawsze;
- **najniższy poziom upartyjnienia** – to taki, w którym media są neutralne w stosunku do partii politycznych. Nie udzielają poparcia żadnej opcji politycznej. Taki stan rzeczy jest konsekwencją odpowiednich zapisów w statucie lub decyzji gremiów właścicielskich albo zarządu. Jednak nie oznacza to, że media pozostają zupełnie poza sferą polityki, wręcz przeciwnie, realizują obowiązek informacyjny[237].

Podsumowując, należy stwierdzić, że zagadnienia *fake news* oraz post-prawdy są jednymi z najważniejszych zagadnień dotyczących zmian, jakie zachodzą we współczesnych mediach, komunikacji międzyludzkiej, a także w sposobach wpływania na opinię publiczną. W światowych oraz rodzimych mediach oraz ośrodkach akademickich trwa współcześnie debata na temat post-prawdy oraz zagrożeń, jakie stanowią one dla systemu demokratycznego[238].

5.3. Aspekty psychologiczne wykorzystania mediów społecznościowych[239]

Manipulacja jest to intencjonalne, zaplanowane działania mające na celu przekonanie kogoś do konkretnego postępowania, akceptacji określonych kwestii. Działania te polegają na wdrażaniu odpowiednich taktyk, w taki sposób, aby osoba poddawana manipulacji nie była tego świadoma. Manipulacja oddziałuje na procesy myślowe osoby manipulowanej oraz jej uczucia i emocje. Proces manipulacji nie bierze pod uwagę pragnień i interesów osoby manipulowanej, a jedynie interesy manipulanta. Manipulant

[237] M. Marzec, *Media w procesie komunikowania politycznego – władza, wpływ a może symbioza?*, „Palimpsest" 2010, nr 1, s. 21-22.
[238] *Raport: „Fake news z perspektywy…*, *op. cit.*, s. 6.
[239] Fragmenty niniejszego rozdziału pierwotnie opublikowano w: R. Bielawski, A. Ziółkowska, *Media społecznościowe…, op. cit.*

dba wyłącznie o swoje zyski, niejednokrotnie wykorzystując inne osoby. Proces manipulacyjny ma być prowadzony w taki sposób, aby manipulowany zyskał przekonanie, iż jego postępowanie jest zupełnie dobrowolne.

Źródła wyróżniają trzy typy manipulacji:

- automatyzm psychologiczny – polegający na tym, iż ludzkie reakcje na konkretne bodźce są bezrefleksyjne;
- manipulowanie swoim wizerunkiem;
- manipulowanie środowiskiem/otoczeniem – bazujące na prezentowaniu otoczenia w taki sposób, aby osoba poddana manipulacji odpowiadała na określone zapotrzebowanie.

W literaturze wskazywanych jest kilkanaście typów manipulacji, używających w tym celu:

- relatywizmu;
- inferencji nieposiadającej sensu;
- argumentacji personalnej;
- preparowania skutków;
- kreacji rzeczywistości na podstawie fałszywych przesłanek;
- zbiorowego potwierdzenia/dowodów słuszności;
- wpływu na emocje;
- schematów i stereotypów;
- zniekształcania, zmiany sensu wypowiedzi;
- powoływania się na jednostki uznane za autorytet.

Jedną z technik manipulacyjnych jest **dysonans poznawczy**. Metoda ta polega na fakcie racjonalizowania postępowania niezgodnego ze stałymi poglądami konkretnej osoby poprzez szukanie usprawiedliwienia, wytłumaczenia przybranej postawy.

Do prymarnej terminologii w obszarze zagadnień manipulacji zalicza się pojęcie perswazji i manipulacji. Adresat perswazji jest poinformowany o zamiarach manipulanta, przy manipulacji intencja jest całkowicie ukryta.

Warto zauważyć, iż zazwyczaj rolę mediów określa się mianem destruktywnej, co oznacza, że media w tym rozumieniu manipulują stosując przekaz perswazyjny najczęściej o charakterze wartościującym. Media pełnią przede wszystkim rolę opiniotwórczą, przedstawiając różne fakty w konkretnym ujęciu/perspektywie wpływają na ocenę zbiorowości oraz nakłaniają społeczeństwo do konkretnych zachowań. Wyróżnia się kilka podstawowych technik, które wykorzystywane są przez media w celu manipulowania publiką:

- brak możliwości sprawdzenia kłamstwa;
- wykorzystywanie autorytetów dla uwiarygodnienia kłamstwa;
- przekładanie prawdy nad fikcją;
- prezentowanie kilku wiadomości jednocześnie, aby adresat wycią-

gnął nieprawdziwe wnioski;
- przeinaczenie lub wyolbrzymianie wiadomości w celu wzbudzenia paniki, wybuchu emocji;
- interpretowanie prawdziwych faktów;
- dodawanie informacji tendencyjnej, niezwiązanej z tematem;
- przekazywanie kłamstwa zamiast informacji prawdziwej;
- przedstawienie faktu prawdziwego w kontekście zmieniającym jego wydźwięk;
- przekazanie wiadomości w taki sposób, aby adresat samodzielnie doszedł do pożądanych wniosków.

Wiadomości tendencyjne, nieobiektywne nabierają wiarygodnego charakteru poprzez wykorzystanie osoby/autorytetu, której zadaniem będzie przedstawienie komunikatu. Działanie takie dodatkowo ukrywa prawdziwe zamiary nadawcy. Najdoskonalsza sytuacja dla nadawcy jest wtedy, gdy odbiorca nie ma możliwości sprawdzenia informacji.

Media wpływają na świadomość publiki poprzez **intoksykację**, czyli tzw. zatrucie. Intoksykacja polega na powolnym, regularnym wdrażaniu kłamstw, wiadomości niepełnych między informacje prawdziwe. W tym celu wykorzystuje się także odpowiedni język komunikatów. Postępowanie takie ma zmodyfikować obraz rzeczywistości odbiorcy.

Jednym z istotnych wyznaczników destruktywnej roli mediów jest negatywne nacechowanie, opiniowanie oraz wyłączenie z tzw. życia zbiorowości, z życia politycznego: osób zasłużonych dla kraju – patriotów, osób sprzeciwiających się aborcji i eutanazji, osób krytykujących islamofobię, rzekome autorytety, nie modernistów, nie żydofilów, jednostek popierających lustrację i homofobię.

W Internecie manipulacji dokonuje się przede wszystkim przy użyciu:
- rozpowszechniania mechanizmu stereotypów;
- włączania tzw. szumu informacyjnego;
- tworzenia tzw. informacyjnego chaosu;
- przekazywania sprzecznych wiadomości, kłamstw i kreowania tzw. półprawdy.

W celu nie reagowania na działania manipulacyjne należy mieć świadomość, iż manipulacja jest prowadzona przez media cały czas. Warto także kontrolować, analizować swoje emocje i reakcje na odbierane bodźce. Osobę, która nie podlega biernie technikom manipulacyjnym mediów nazywamy świadomym konsumentem mediów. Przyjęciu owej postawy sprzyja:
- stronienie od emocjonalnego postrzegania świata;
- wyszukiwanie konkretnych, przydatnych wiadomości dotyczących relacji politycznych;

- poszukiwanie różnych źródeł wiadomości w celu ich porównywania;
- wystrzeganie się uznawania jednostek medialnych za ekspertów;
- świadomość, iż to media poprzez ustalony *public relations* (PR) kreują wizerunek (wzbudzają szacunek albo niechęć);
- świadomość, że w mediach także pracują osoby zdolne do kłamstwa;
- świadomość, iż decyzyjność dotyczącą czasu transmisji, formy przekazu danych posiada redakcja.

W celu przeprowadzenia dokładnej kontroli przekazanych informacji warto dowiedzieć się czy:

- osoba uznawana za eksperta faktycznie posiada odpowiednie informacje, dające podstawę do obiektywnego wyrażania sądów i opinii;
- ilość i jakość wiedzy „eksperta" jest potwierdzona w sposób formalny (wykształcenie, doświadczenie);
- osoba eksperta jest bezstronna;
- wydana opinia jest tożsama z regułami naukowymi.
- dokonano porównania opinii eksperta z innymi jednostkami uważanymi za specjalistów w danej kwestii.

Neuromarketing to jedna z metod manipulowania otoczeniem. Informacje z zakresu neurologii pomagają nakłaniać jednostki, np. do robienia zakupów, w taki sposób, by odbiorca był pewien, iż decyzyjność należała całkowicie do niego. W tej technice najczęściej stosuje się odwołanie do symboli, zamiast konkretnego, prostego przekazu.

W skutecznej manipulacji bardzo przydatne okazują się sofizmaty (tak postępowali sofiści, scjentolodzy oraz osoby wykorzystujące neurolingwistyczne programowanie). Należą do nich: wieloznaczności, brak spójności składniowej, mnogość znaczeń, opinie pozbawione sensu, ekwiwokacje, dyskurs prowadzący do zinterpretowania nieprawdziwych wniosków, zapętlenie wypowiedzi, paradoksy.

Media społecznościowe oraz ich wykorzystanie charakteryzuje się tym, iż odbiorcami przekazywanych przez nie treści jest duża liczba osób. W kontekście tej tematyki, w aspekcie psychologicznym można podjąć rozważania dotyczące tzw. **psychologii tłumu**. Tłum daje jednostkom złudne poczucie siły oraz zatraca indywidualność jednostki. Propaguje idee i zachowania często odmienne od indywidualnego postępowania jednostki. W tłumie człowiek podatny jest na sugestie, traci samokontrolę. W zbiorowości zanika także zdolność poprawnego postępowania. Najczęściej zbiorowisko, tłum określa się mianem: impulsywnego, nieposiadającego krytycyzmu, nerwowego, intuicyjnego, nielogicznego, instynktownego, łatwowiernego, nieetycznego, podatnego na rozkazy. Zbiorowość nie jest w stanie zatrzymać, kontrolować swoich zachowań, odruchów oraz myślenia schematycznego. Tłum nie jest odporny na powtarzalne informacje.

W tłumie osoby wyrażają pewnego rodzaju zgodę na prezentowane poglądy, opinie oraz emocje.

Inną stosowaną w mediach społecznościowych techniką jest tzw. **komunikowanie perswazyjne**. Jego podstawą jest perswazja[240], jako technika wpływania, oczarowywania, nakłaniania, tłumaczenia, przy czym obiektem perswazji może być jednostka, idee, wartości czy przedmioty oraz zjawiska. Komunikowanie perswazyjne tym się różni od informacyjnego, że przedmiotem wymiany nie jest obiektywna, rzetelna informacja a celem ustalenie prawdy. Zasadniczą wartością jest takie oddziaływanie na odbiorcę, by nakłonić go do akceptacji postaw zgodnych z intencją nadawcy, bez stosowania nacisków. Można powiedzieć, że jest kompleksowym, interaktywnym procesem, gdzie nadawca i odbiorca są połączeni werbalnymi i niewerbalnymi relacjami. Dodatkowo nadawca stara się wpływać na odbiorcę, by ukształtować lub zmodyfikować postawy. Interaktywność jest konsekwencją postawy odbiorcy, który jest skłonny podporządkować się nakłaniającemu, w zamian za realizację postaw. Obaj uczestnicy wchodzą w specyficzny układ zależności.

5.4. Uogólnienia i wnioski

W odniesieniu do mediów społecznościowych, w kontekście kształtowania cyberbezpieczeństwa narodowego, należy podkreślić ich cechy: możliwość szerokiego wykorzystania, łatwy dostęp (niezwiązany z nakładem finansowym), możliwość umieszczania treści w czasie rzeczywistym, w sposób dwukierunkowy – od i do nadawcy. Dodatkowo wykazano ich cechy w stosunku do tradycyjnych mediów, takie jak: zasięg, dostęp, użytkowanie, natychmiastowość oraz trwałość. Jednym z wyróżników *social media* jest ich dialogowość, polegającą na możliwości współkomunikowania się – sprzężenia zwrotnego pomiędzy nadawcą, a odbiorcą. Jest ona dodatkowo wspomagana multimedialnością, odziaływującą na większość zmysłów ludzkich.

W odniesieniu do mediów społecznościowych, w kontekście kształtowania cyberbezpieczeństwa narodowego, należy podkreślić ich cechy: możliwość szerokiego wykorzystania, łatwy dostęp (niezwiązany z nakładem finansowym), możliwość umieszczania treści w czasie rzeczywistym, w sposób dwukierunkowy – od i do nadawcy. Dodatkowo wykazano ich cechy w stosunku do tradycyjnych mediów, takie jak: zasięg, dostęp, użytkowanie, natychmiastowość oraz trwałość. Jednym z wyróżników *social*

[240] W tym rozumieniu – przekonywanie do racji/zachowań/poglądów, zazwyczaj za pomocą argumentacji.

media jest ich dialogowość, polegającą na możliwości współkomunikowania się – sprzężenia zwrotnego pomiędzy nadawcą, a odbiorcą. Jest ona dodatkowo wspomagana multimedialnością, odziaływującą na większość zmysłów ludzkich.

Wśród mechanizmów (sposobów) wykorzystania mediów społecznościowych w cyberprzestrzeni narodowej wyróżniono trzy ich grupy: operacje psychologiczne, dezinformację i propagandę oraz *fake news* i postprawdę. W ramach operacji psychologicznych, prowadzonych w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika, odróżniono je od wojny psychologicznej w cyberprzestrzeni, wykazując jej długofalowe i agresywne oddziaływanie środkami politycznymi, propagandowymi, dyplomatycznymi, kulturalnymi i emocjonalnymi. Skierowane są one na świadomość, psychikę oraz morale ludności cywilnej i sił zbrojnych. W aspekcie militarnym wskazano na siedmioetapowy, skomplikowany i długoterminowy, proces – *Joint PSYOP Process*, którego celem jest właściwe przeprowadzenie operacji psychologicznych w NATO. Współcześnie, za przykład wojny informacyjnej można podać spór rosyjsko-ukraiński. W odniesieniu do dezinformacji, w celu jej efektywnego użycia, zostały wyróżnione zasady, takie jak: celowość, zasada przygotowania, kompleksowość, scentralizowane kierowanie, wiarygodność, zasada dublowania, elastyczność, terminowość, ciągłość, spójność, nieszablonowość oraz skrytość. Ważna, z punktu widzenia mediów społecznościowych, jest Propaganda 2.0. Pojęcie to jest ściśle związane z działalnością polegającą na generowaniu (w czasie rzeczywistym) treści przez użytkowników serwisów. Daje to duże możliwości szybkiego rozprzestrzeniania przekazów, w tym także o treściach propagandowych. W odniesieniu do dezinformacji i propagandy należy stwierdzić, że pomimo literaturowego utożsamiania tych terminów, wykazano różnice w ich znaczeniu. Dezinformacja odnosi się do przekazywanie nieprawdziwej wiadomości, a celem takiego działania jest wprowadzenie odbiorcy w błąd, przy założeniu że odbiorca, na tej podstawie, podejmie decyzje z korzyścią dla dezinformującego. Propaganda natomiast dotyczy szerszego grona odbiorców – okłamywania całych społeczeństw przez władze państwowe. Poza tymi dwoma mechanizmami wykorzystania mediów społecznościowych w cyberprzestrzeni, współcześnie na uwagę zasługuje *fake news* oraz post-prawda. Treści typu *fake news* poza nieprawdziwym przekazem, który *de facto* stanowi drugorzędną rolę, powoduje wzbudzanie silnych emocji, przez zazwyczaj nacechowane emocjonalnie kontrowersyjne przekazy. Jest to, jak się okazuje, trafny sposób na kształtowanie opinii publicznej. Wśród *fake news* wyróżniono ich trzy rodzaje – całkowita nieprawda, prawda sporna oraz manipulacja cytatem, które są powszechnie stosowane w *mass mediach*. Współcześnie łączącym się z *fake news* mechanizmem jest post-prawda, rozumiana jako kultura

polityczna, w której w kształtowaniu opinii mniej ważne są fakty, które dominowane są przez odwoływanie się do osobistych emocji i przekonań.

Poruszając aspekty psychologiczne wykorzystania mediów społecznościowych należy wskazać na manipulację, jako jedną z form oddziaływania na użytkowników mediów społecznościowych wraz z ich trzema typami: automatyzmem psychologicznym, manipulowaniem wizerunkiem lub środowiskiem. Wyróżniono tutaj także indoktrynację, jako sposób wpływu *mass mediów* na świadomość opinii publicznej. Polega ona na powolnym, regularnym wdrażaniu kłamstw, wiadomości niepełnych między informacje prawdziwe, w celu wpajania zamierzonych ideologii i doktryn. W walce informacyjnej prowadzonej za pomocą mediów społecznościowych wyróżnia się także metodę – neuromarketing. Polega on na takim zmanipulowaniu odbiorcy, aby odczuwał on swoją dużą decyzyjność. Takie działania realizowane są za pomocą odwoływania się do symboli, zamiast prostego przekazu treści. W działaniu za pomocą mediów społecznościowych korzysta się często z psychologii tłumu. W ten sposób wykorzystuje się słabości ludzkie, polegające w tym przypadku na złudnym poczucie przez jednostkę siły a w efekcie utratę samokontroli.

ROZDZIAŁ 6.
Strategia bezpieczeństwa polityczno-militarnego oraz aspekty prawne w zapewnieniu cyberbezpieczeństwa w kontekście wykorzystania mediów społecznościowych

6.1. Strategiczne założenia cyberbezpieczeństwa w kontekście wykorzystania mediów społecznościowych

6.1.1. Strategiczne założenia cyberbezpieczeństwa Rzeczypospolitej Polskiej w kontekście wykorzystania mediów społecznościowych

Jednym z najważniejszych dokumentów dotyczących szeroko rozumianych pojęć związanych z bezpieczeństwem i obronnością państwa jest „Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej”[241] (SBN RP). Została ona oficjalnie zatwierdzona 5 listopada 2014 r. przez Prezydenta Polski Bronisława Komorowskiego na wniosek Prezesa Rady Ministrów. Ważnym asumptem określającym charakter tego dokumentu jest jego jawność. SBR RP wyznacza główne kierunki zmian zachodzących w kryteriach bezpieczeństwa narodowego. Jednocześnie obejmuje istotne zalecenia wprowadzonych zmian z punktu widzenia funkcjonowania sił zbrojnych, ale także w odniesieniu do innych elementów współdecydujących o zdolności obronnej kraju. Opracowanie SBN RP było jednym z etapów prac podjętych w celu dokładnego zdefiniowania interesów narodowych oraz opisania głównych celów Rzeczypospolitej Polskiej w dziedzinie bezpieczeństwa narodowego przy równoległym wyznaczeniu kierunków rozwojowych, dążących do osiągnięcia założonych zamierzeń. Następnym, zaplanowanym krokiem w perspektywie przyszłościowych działań w ra-

[241] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2014.

mach budowania potencjału obronnego w momencie zatwierdzenia SBN RP, było wydawanie kolejnych dokumentów oraz podejmowanie decyzji dotyczących transformacji zasobów sił zbrojnych, systemu obronnego i bezpieczeństwa. Efektem tych prac miała być tajna Dyrektywa Obronna.

„Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej" w sposób całościowy i bardzo otwarty, wymagający niekiedy uściślenia, precyzuje główne zagadnienia w kontekście bezpieczeństwa narodowego. Wskazuje również na optymalne sposoby wykorzystania na potrzeby bezpieczeństwa wszystkich zasobów pozostających w dyspozycji państwa w sferze obronnej, ochronnej, społecznej i gospodarczej. Za realizację jej postanowień odpowiadają ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, organy samorządu terytorialnego oraz inne podmioty, w zobowiązaniach których pozostają kwestie nawiązujące do zakresu bezpieczeństwa państwa na różnych szczeblach; poczynając od władzy centralnej i kończąc na regionalnej. Zatwierdzony przez Prezydenta RP dokument zastępuje i uzupełnia wydany w 2007 r. wcześniejszy format Strategii Bezpieczeństwa Narodowego, powstały na bazie art. 4a, pkt. 1, ppkt 1 ustawy o powszechnym obowiązku obrony RP[242].

SBN RP jest podzielona na cztery zasadnicze części w postaci rozdziałów opisujących odrębną problematykę. W pierwszym z nich zostało określone położenie Polski jako podmiotu bezpieczeństwa. Państwo posiada suwerenność, jest samodzielne o ustroju demokratycznym oraz zdolne do zdefiniowania własnych interesów narodowych i celów strategicznych. Potrzeby te wynikają z konieczności zagwarantowania odpowiedniego poziomu bezpieczeństwa w odniesieniu do zdolności zapewnienia stabilnego rozwoju kraju oraz poprawy warunków życia jego obywateli. Wymienione kryteria wynikają z doświadczeń historycznych, istniejących obecnie warunków polityczno-ustrojowych oraz znaczącego potencjału, jakim dysponuje Rzeczpospolita Polska. W tej części została ukazana pozycja państwa w Europie i na świecie. Nawiązuje ona przede wszystkim do współpracy z sojusznikami, takimi jak Unia Europejska oraz Organizacja Traktatu Północnoatlantyckiego, będących dla Polski gwarantem umocnienia poziomu bezpieczeństwa narodowego w dwóch aspektach. Unia Europejska zapewnia formę wsparcia opartą na rozwoju o charakterze społeczno-gospodarczym, zaś Organizacja Traktatu Północnoatlantyckiego stanowi najważniejszą formę polityczno-wojskowej kooperacji. W kontekście zagwarantowania bezpieczeństwa międzynarodowego i utrzymania pokoju, SBN RP wymienia Polskę jako członka innych organizacji, do których należą Organiza-

[242] Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 1967 r. nr 44, poz. 220).

cji Narodów Zjednoczonych (ONZ) oraz Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE). Oprócz aktywnego uczestnictwa w powyższych strukturach organizacyjnych, Polska jest zobligowana do prowadzenia działań dążących do utworzenia odpowiednich warunków, do określenia interesów narodowych oraz celów strategicznych na rzecz bezpieczeństwa państwa i jego obywateli. Na tej podstawie w dokumencie opisano następujące interesy narodowe w dziedzinie bezpieczeństwa:

- dysponowanie narodowym potencjałem bezpieczeństwa zapewniającym gotowość i zdolność do przeciwdziałania zagrożeniom, w tym odstraszania, a także obrony i ochrony przed nimi oraz likwidowania ich następstw;
- silna pozycja międzynarodowa Polski, poprzez członkostwo w wiarygodnych systemach bezpieczeństwa międzynarodowego;
- indywidualna i zbiorowa ochrona obywateli przed zagrożeniami ich życia i zdrowia oraz przed naruszeniem, utratą lub degradacją ważnych dla nich materialnych i niematerialnych dóbr;
- zapewnienie swobody korzystania przez obywateli z praw i wolności, bez działania na szkodę dla bezpieczeństwa innych osób i bezpieczeństwa państwa oraz zapewnienie tożsamości narodowej i dziedzictwa kulturowego;
- zapewnienie stałego i zrównoważonego rozwoju potencjału społecznego i gospodarczego państwa, ze szczególnym uwzględnieniem ochrony środowiska naturalnego oraz warunków życia i zdrowia ludności jako podstawy ich egzystencji[243].

Biorąc pod uwagę ten określony układ interesów narodowych zostały opracowane odpowiadające im cele strategiczne. Należą do nich pojęcia obejmujące zakres: rozwoju współpracy międzynarodowej, potencjału bezpieczeństwa oraz obronnego, zagwarantowania chronionego funkcjonowania przestrzeni cybernetycznej i aspekty społeczno-gospodarcze. Do celów strategicznych zalicza się m.in.:

- utrzymywanie i demonstrowanie gotowości zintegrowanego systemu bezpieczeństwa narodowego do wykorzystywania szans, podejmowania wyzwań, zmniejszania ryzyka a także przeciwdziałania zagrożeniom;
- rozwój adekwatnego do potrzeb potencjału obronnego i ochronnego, a także możliwości państwa oraz zwiększenie jego interoperacyjności w ramach NATO i Unii Europejskiej;
- rozwijanie bliskiej współpracy ze wszystkimi państwami sąsiednimi oraz budowanie partnerskich relacji z innymi państwami, w tym słu-

[243] *Strategia Bezpieczeństwa Narodowego…*, *op. cit.*, s. 10-11.

żących przeciwdziałaniu i rozwiązywaniu kryzysów i konfliktów w skali międzynarodowej;
- doskonalenie i rozwój krajowego systemu zarządzania kryzysowego w kierunku zapewnienia jego wewnętrznej spójności i integralności oraz umożliwienia dobrej współpracy w ramach systemów zarządzania kryzysowego organizacji międzynarodowych, w których Polska sprawuje członkostwo;
- ochrona granic Polski, które stanowią zewnętrzną granicę UE;
- przeciwdziałanie przestępczości zorganizowanej, w tym także gospodarczej;
- zapewnienie bezpiecznego funkcjonowania cyberprzestrzeni RP;
- zapewnienie bezpieczeństwa energetycznego i klimatycznego, a także ochrony środowiska, różnorodności biologicznej i zasobów naturalnych (w szczególności zasobów wodnych), a także kształtowanie zagospodarowania przestrzennego kraju w sposób zwiększający odporność na różne zagrożenia – militarne, naturalne i technologiczne;
- pogłębianie świadomości społecznej w sferze bezpieczeństwa oraz zwiększanie kompetencji obywateli pozwalających na właściwe reagowanie w sytuacjach kryzysowych[244].

Zarówno wymienione interesy narodowe a także cele strategiczne przekładają się na faktyczne działania oraz zadania, stosowane w warunkach umożliwiających ich skuteczne wykonanie. Narzędziem niezbędnym do realizacji interesów narodowych oraz celów strategicznych jest strategiczny potencjał bezpieczeństwa narodowego. Jego systematyczne umacnianie oznacza nie tylko dbałość instytucji i rządu Rzeczpospolitej Polskiej o pojęcia związane z obronnością, jak i bezpieczeństwem państwa, ale także wskazuje na dostosowanie się do wymogów UE oraz NATO. Strategiczny potencjał bezpieczeństwa narodowego obejmuje system bezpieczeństwa narodowego, w ramach niego podsystemy: kierowania i wykonawcze, potencjały – obronny, ochronny, społeczny, gospodarczy, energetykę oraz system transportowy.

W drugiej części strategii dokonano podziału środowiska bezpieczeństwa Polski na globalne, krajowe oraz regionalne. W wymiarze globalnym, oprócz aspektów związanych z zagadnieniami odnoszącymi się do współpracy z ONZ czy groźby w postaci użycia broni masowego rażenia, uwzględniono rolę wojen informacyjnych w cyberprzestrzeni. SBN RP określa je jako – *cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty*. W wymiarze światowym oznacza konfrontację pomiędzy podmiotami niepaństwowymi, dążącymi do uzyskania zamierzonych celów poprzez najczęściej nielegalne działania w przestrzeni cybernetycznej, do

[244] *Ibidem*, s. 11-12.

których można zaliczyć m.in. wymuszenia, wirtualne szpiegostwo, hackerstwo, przesyłanie złośliwego oprogramowania lub różne formy terroryzmu. Natomiast *cyberwojna* jest to konflikt nastały w cyberprzestrzeni pomiędzy stronami przynależnymi do konkretnych krajów. Omawiany dokument – strategia – zakłada dynamiczny rozwój cyberprzestępczości w przyszłości. Powód do eskalacji zdarzeń w tym kontekście stanowią współczesne trendy nawiązujące do prowadzenia działań w Internecie z uwagi na nieograniczony zasięg w sieci i możliwość zachowania anonimowości. Z tego względu, coraz większa popularność cyberkonfliktów oraz cyberwojen może w istotny sposób godzić w bezpieczeństwo narodowe Rzeczpospolitej Polskiej, jak i użytkowników Internetu. Wobec rosnącego uzależnieniu od technologii teleinformatycznych, szeroko pojmowane spory w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw[245]. W ramy wspomnianych sporów w cyberprzestrzeni, w obliczu postępującego na świecie globalizmu, może być w przyszłości wpisana zorganizowana, informacyjna działalność przestępcza gangów lub cyberterrorystów, która w efekcie może doprowadzić do niestabilności Polski. Analizując krajowy wymiar bezpieczeństwa informacyjnego, SBN RP zakłada, że sprawne i niezagrożone działanie systemu teleinformatycznego w Polsce stanowi warunek konieczny do nieprzerwanego, niezakłóconego funkcjonowania kraju. To stwierdzenie powinno przekładać się w głównej mierze na stworzeniu warunków, dla wypracowania takich atrybutów *social media*, jak:

- dostępność – oznacza to, że media internetowe powinny działać w sposób publiczny i być dogodne dla każdego użytkownika w sieci;
- integralność – w przypadku mediów społecznościowych integralność można rozpatrzeć w kontekście przechowywanych w nich danych. Określa ona pewną spójność, dającą gwarancję bezpieczeństwa, opierająca się na np. mandacie zaufania *usera*[246], który polega na tym, żeby jego dane nie zostały zmienione, usunięte lub dodane w nieautoryzowany przez niego sposób.

W związku z problemem integralności danych w mediach społecznościowych, wyzwanie stanowi wykreowanie poufności danych przetwarzanych w systemach informacyjnych administracji publicznej (lub ważnych instytucji państwowych) oraz wszystkich użytkowników Internetu. Rozwiązaniem tej kwestii może okazać się wprowadzenie ujednoliconych zabezpieczeń teleinformatycznych wraz z polityką ochrony mediów społecznościowych.

[245] *Ibidem*, s. 18-19.
[246] Rozumiane jako – użytkownika.

Biorąc pod uwagę regionalne aspekty bezpieczeństwa cyberprzestrzeni, a także zapewnienie w niej mediów społecznościowych, SBN RP przewiduje przedsięwzięcie wszelkich sił i środków skoncentrowanych na działaniu państwa w określonym regionie w celu ochrony oraz obrony swojej przestrzeni cybernetycznej. Skupia się przede wszystkim na polityce organizacji i struktur współpracy międzynarodowej, w pracach których uczestniczy Rzeczpospolita Polska. Ważnym gwarantem jest również współpraca dwustronna z wybranymi państwami, w szczególności z państwami NATO i UE.

Część trzecia wyodrębniona w dokumencie skupia się wokół koncepcji działań na szczeblu strategicznym oraz strategii operacyjnej. Zauważono, że określone interesy narodowe i cele strategiczne Polski w powiązaniu z diagnozą środowiska bezpieczeństwa narodowego definiują priorytety polityki bezpieczeństwa i obronnej. Zwracają one uwagę na potrzebę zrównoważonego umiędzynarodowienia i samodzielności w zakresie bezpieczeństwa Polski, w tym zwiększenia strategicznej odporności kraju na różnego rodzaju zagrożenia[247]. Wśród nich, znajdują się zagrożenia wynikające z użytkowania cyberprzestrzeni. SBN RP precyzuje trzy główne priorytety polityki bezpieczeństwa, w których podkreśla znaczenie współpracy z organizacjami międzynarodowymi na rzecz obronności i ochrony Rzeczpospolitej Polskiej. Spośród szeregu wymienionych działań o charakterze obronnym, ochronnym, społecznym i gospodarczym (dwóch ostatnich związanych ze sferą bezpieczeństwa), zapewnienie bezpieczeństwa polskiej cyberprzestrzeni umiejscowiono w aspektach ochronnych. W tym kontekście oznacza to, że państwo powinno realizować w dziedzinie cyberbezpieczeństwa zagadnienia związane zarówno z rozwojem zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Z tego powodu szczególną wagę zyskują poniższe czynności, przekładające się na faktyczne działania, do których należy:

- współpraca i koordynacja z podmiotami sektora prywatnego w celu opracowania działań ochronnych (przede wszystkim w aspekcie finansowym, energetycznym, transportowym, telekomunikacyjnym i opieki zdrowotnej);
- prowadzenie działań o charakterze prewencyjnym i profilaktycznym mających na celu ochronę cyberprzestrzeni;
- wypracowanie i stosowanie właściwych procedur komunikacji społecznej;
- rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni – zadania prewencyjne a także ściganie sprawców;
- prowadzenie walki informacyjnej w cyberprzestrzeni;

[247] *Ibidem*, s. 27.

- współpraca sojusznicza na poziomie działalności operacyjnej, służąca do aktywnego zwalczania cyberprzestępstw (w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych w cyberprzestrzeni)[248].

„Strategia Bezpieczeństwa Narodowego RP" porusza również w tej części aspekty bezpieczeństwa informacyjnego. Opisano w niej ważną istotę ochrony informacji niejawnych jako jeden z najważniejszych obszarów, od którego zależy sprawne funkcjonowanie systemów bezpieczeństwa państwa. W tym celu zdefiniowano strategiczne zadania, które obejmują w szczególności:

- zapewnienie bezpieczeństwa informacyjnego państwa poprzez zapobieganie nieautoryzowanego dostępu do informacji niejawnych i ich ujawnieniu;
- zapewnianie bezpieczeństwa informacji niejawnych, w aspekcie personalnym, technicznym i fizycznym;
- akredytację systemów teleinformatycznych służących do przetwarzania informacji niejawnych;
- zapewnienie realizacji krajowej władzy bezpieczeństwa, służącej do umożliwienia międzynarodowej wymiany informacji niejawnych.

W podrozdziale poświęconym działaniom społecznym w sferze bezpieczeństwa, zawarto kwestię funkcjonowania mediów na rzecz bezpieczeństwa narodowego. Strategicznym zadaniem w tym aspekcie jest zawężenie współdziałania administracji i służb z mediami. Celem takiego działania jest budowanie i pogłębianie świadomości społecznej w zakresie odpowiedniego reagowania na pojawiające się zagrożenia. Ponadto, w założeniu SBN RP, położono nacisk na prowadzenie działalności o charakterze edukacyjnym, mającej na celu szerzenie wiedzy na temat odpowiedniego identyfikowania zagrożeń i skutecznego reagowania w takich sytuacjach[249].

Czwarta część SBN RP określa problematykę z zakresu koncepcji przygotowań działań strategicznych oraz strategię preparacyjną. Okazuje się, że różnorodność wyzwań i nieprzewidywalność zagrożeń sprawia, że system bezpieczeństwa narodowego może być zdolny do wszechstronnej reakcji na pojawiające się problemy: od lokalnych i ograniczonych w skutkach do obejmujących całe państwo. W ramach działań przygotowawczych, w celu odpowiedniego reagowania na ataki pochodzące z cyberprzestrzeni, wyodrębniono następujące podsystemy: kierowania bezpieczeństwem narodowym, obronny, ochronne, społeczne oraz gospodarcze.

Aspekty związane z funkcjonowaniem cyberprzestrzeni RP ujęto w podsystemie ochronnym. Odnosi się on do powołania instytucji właści-

[248] *Ibidem*, s. 35.
[249] *Ibidem*, s. 39.

wych do spraw cyberbezpieczeństwa. Do najważniejszych zadań przygotowawczych w tym zakresie należy podjęcie wysiłków skoncentrowanych na wdrożeniu i skoordynowanym rozwijaniu systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym. Konieczne jest trafne sprecyzowanie zasad prowadzenia aktywnego przeciwdziałania oraz budowa narodowego systemu obrony cybernetycznej, w tym rozwijanie Krajowego Systemu Reagowania na Incydenty Komputerowe w cyberprzestrzeni RP. Ważną kwestią jest również to, aby działania zmierzające do uzyskania tego stanu pozostały spójne z systemami państw sojuszniczych. Ważne okazuje się opracowanie narodowego ośrodka koordynacji, wspierającego organizację współpracy pomiędzy poszczególnymi podmiotami realizującymi zadania w zakresie cyberbezpieczeństwa i wymianę informacji oraz promowanie dobrych praktyk w obszarze bezpieczeństwa cybernetycznego. W założeniu SBN RP niezbędne jest nabycie pełnych kompetencji do rozpoznawania, zapobiegania i zwalczania cyberzagrożeń oraz zdolności do wytwarzania polskich rozwiązań technologicznych przeznaczonych do zapewnienia odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni. Początkiem procesu zwiększania odporności systemu teleinformatycznego Rzeczypospolitej Polskiej powinno być stworzenie obszarów bezpieczeństwa wyselekcjonowanych systemów teleinformatycznych, istotnych dla bezpieczeństwa państwa oraz odpowiednio zabezpieczonych dróg komunikacji między nimi. W dalszej kolejności, planowane jest zbudowanie jednolitej platformy teleinformatycznej, umożliwiającej bezpieczne przetwarzanie i wymianę danych pomiędzy jednostkami administracji publicznej. Istotne okazuje się także zwiększanie świadomości użytkowników o zagrożeniach w cyberprzestrzeni poprzez zwiększenie intensywności działań edukacyjnych na wszystkich poziomach nauczania, odbywanych w formie szkoleń i kampanii społecznych. Wskazane jest uruchomienie specjalnych kierunków studiów związanych z bezpieczeństwem funkcjonowania w cyberprzestrzeni oraz rozwijanie programów badawczych w tym obszarze[250].

Media w systemie bezpieczeństwa narodowego ujęte zostały w ramach działalności realizowanych przez podsystem społeczny. Określono wytyczne opracowane w celu dalszego rozwijania i pogłębiania współpracy przedstawicieli instytucji państwowych, a także mediów zaangażowanych w ochronę bezpieczeństwa narodowego. „Strategia Bezpieczeństwa Narodowego RP" zakłada, że w przyszłości niezbędna będzie zwiększenie przygotowania służb prasowych instytucji państwowych i dziennikarzy zajmujących się problematyką bezpieczeństwa narodowego. Wskazuje się także na zwiększenie ukierunkowania działania mediów publicznych na tę tema-

[250] *Ibidem*, s. 49.

tykę, z uwagi na rosnące znaczenie działalności prowadzonej w przestrzeni cybernetycznej[251].

Warto zauważyć, że Rzeczpospolita Polska również podejmuje wszelkie wysiłki zmierzające do podniesienia poziomu bezpieczeństwa swojej przestrzeni cybernetycznej. Do jednych z takich działań należy konferencja, w której wzięli udział cywilni oraz wojskowi specjaliści w dziedzinie zapewnienia cyberbezpieczeństwa. Odbyła się ona w 2016 roku, z podziałem na dwie edycje. Pierwsza z nich miała miejsce 8 kwietnia w Warszawie, natomiast druga 27-28 września tego samego roku w Krakowie. Z uwagi na poruszaną podczas niej tematykę została powołana pod nazwą Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL 2016. Problematykę tej konferencji skoncentrowano wokół kwestii budowania narodowych zdolności służących wzmacnianiu krajowego systemu cyberbezpieczeństwa, które pozwalałyby na prowadzenie skutecznych i suwerennych działań w cyberprzestrzeni. Organizacja CYBERSEC PL powstała zgodnie z zasadami zaproponowanymi przez Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC EU. Założeniem obydwu podmiotów było stworzenie praktycznych rekomendacji dla zapewnienia bezpieczeństwa w cyberprzestrzeni w wymiarze unijnym (CYBERSEC EU) i narodowym (CYBERSEC PL). Bazą do tworzenia rekomendacji każdorazowo uczyniono sesje i panele dyskusyjne o charakterze warsztatów w ramach czterech ścieżek tematycznych tj. „Państwo", „Wojsko", „Przyszłość", „Biznes"[252].

Biorąc pod uwagę pierwszą ścieżkę tematyczną – „Państwo", celem opracowanych dla niej rekomendacji w kontekście cyberbezpieczeństwa było przede wszystkim poszukiwanie skutecznych rozwiązań, mających na celu ochronę infrastruktury krytycznej Polski. Nawiązuje to bezpośrednio do konieczności wzmacniania roli państwa w aspekcie sprawowania kontroli nad wszelkimi działaniami prowadzonymi w cyberprzestrzeni. W tym panelu uczestnicy konferencji skupili się także na współpracy publiczno-prywatnej. Opracowane rekomendacje przedstawiają w głównej mierze stanowiska przyjęte przez większość prelegentów, udzielających się podczas CYBERSEC PL 2016. Na tej podstawie przyjęto, że:

- z punktu widzenia zapewniania bezpieczeństwa infrastruktury krytycznej niezbędne będzie wypracowanie procedur w celu właściwej współpracy między wszystkimi najważniejszymi interesariuszami. Oczekuje się, że procedury te powinny być sprawdzane i praktykowane w ramach organizowanych ćwiczeń. Zakłada się dodatkowo, że ich opracowanie stanie się skutecznym narzędziem walki z proble-

[251] *Ibidem*, s. 53.
[252] *CYBERSEC PL 2016. Rekomendacje*, Polskie Forum Cyberbezpieczeństwa, Warszawa 2016, s. 1.

mem fragmentaryzacji działań;
- cyberbezpieczeństwo powinno być traktowane jako jeden z elementów systemu, którego celem jest opracowanie strategii zapewniania bezpieczeństwa infrastruktury krytycznej;
- oprócz działań planistycznych, oczekuje się wdrożenia realnych działań ukierunkowanych na zapewnianie bezpieczeństwa;
- operatorzy i właściciele elementów infrastruktury krytycznej powinni aktywnie włączać się w procesy pracy nad dobrymi praktykami oraz starać się je stosować;
- operatorzy powinni wdrażać istniejące wewnętrzne standardy, a implementacja powinna być nadzorowana przez regulatorów sektorowych;
- w odniesieniu do nieprzestrzegania standardów powinno się wdrożyć system sankcyjny;
- cyberbezpieczeństwo infrastruktury krytycznej powinno być zapewniane w całym łańcuchu dostaw – odpowiednie podmioty powinny dokonywać certyfikacji funkcjonujących produktów, w odniesieniu do możliwości istnienia *backdoor*-ów;
- ministrowie odpowiedzialni za systemy infrastruktury krytycznej powinni aktywniej angażować się w działania dotyczące podnoszenia jej bezpieczeństwa;
- należyte działania w zakresie cyberbezpieczeństwa infrastruktury krytycznej wymagają odpowiedniego finansowania;
- w Polsce konieczny jest rozwój prac badawczo-rozwojowych (B+R), szczególnie nakierowanych na bezpieczeństwo automatyki przemysłowej[253].

W ramach omówienia ścieżki tematycznej – „Wojsko" – uczestnicy zainteresowali się kwestią zwiększenia roli polskiej armii w zapewnianiu cyberbezpieczeństwa. Jest ona szczególnie ważna z uwagi na szczyt NATO, który odbył się w dniach 8-9 lipca 2016 roku w Warszawie. Posiedzenie szefów państw oraz rządów po raz pierwszy miało miejsce na terenie Rzeczpospolitej Polskiej, co było dowodem chęci przedstawicieli rządu Polski na kontynuowanie współpracy z Organizacją Traktatu Północnoatlantyckiego. Zrodziło to konieczność podjęcia dalszych kroków w zakresie kształtowania polityki cyberbezpieczeństwa państwa, aby były kompatybilne z systemami oraz standardami Sojuszu Północnoatlantyckiego. Biorąc pod wagę wszystkie te okoliczności, ustanowiono kilka z poniższych rekomendacji dla Rzeczpospolitej Polskiej w celu modernizacji Sił Zbrojnych na rzecz polepszenia sposobu walki z cyberzagrożeniami:

[253] *Ibidem*, s. 6-7.

- skuteczne działanie państwa w cyberprzestrzeni wymusza ustalenie jego misji, wizji i strategii. Na tej podstawie oczekuje się ustalenia ról i kompetencji poszczególnych podmiotów;
- w ramach strategii narodowej powinno się dążyć do opracowania i określenia jednoznacznych zadań, jakie w cyberprzestrzeni powinny prowadzić Siły Zbrojne RP;
- działania nakierowane na zwiększanie bezpieczeństwa cyberprzestrzeni, realizowane przez podmioty cywilne i wojskowe nie powinny być traktowane oddzielnie (z uwagi na to, że są to działania komplementarne, powinny być ustanowione zasady współpracy, pozwalające osiągać efekt synergii);
- obszarami współpracy mogą być m.in. wykrywanie zagrożeń i wymiana informacji w tym zakresie, a także opracowanie zasad przeciwdziałania zagrożeniom;
- wysoka zdolność sił zbrojnych wynika z pięciu elementów: efektywnej struktury organizacyjnej (w tym właściwego systemu dowodzenia), systemu łączności i informatyki wspierającego efektywną strukturę organizacyjną, procedur, ludzi oraz wyposażenia. Sektor prywatny może realnie wesprzeć Siły Zbrojne RP w zakresie budowy tych elementów;
- by sektor prywatny mógł wspierać rozwój cyberzdolności Sił Zbrojnych RP, konieczne jest stworzenie właściwych ram prawnych. Sugeruje się na przykład, aby akt prawny – Rozporządzenie Rady Ministrów z dnia 4 października 2010 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym (Dz.U. 2010 nr 198 poz. 1314 z późn. zm.) uzupełnić o sektor IT i cyberbezpieczeństwa;
- z punktu widzenia zwiększenia zdolności Sił Zbrojnych RP do prowadzenia działań w cyberprzestrzeni, kluczowe jest korzystanie z doświadczeń sojuszników;
- walka z zagrożeniami hybrydowymi jest szczególnym obszarem, gdzie współpraca między systemem cywilnym i wojskowym jest niezbędna;
- wsparcie ze strony organizacji pozarządowych powinno być realizowane i rozwijane – inicjatywy, takie jak: CYBERSEC PL, Polska Obywatelska Cyberobrona;
- sugeruje się opracowanie rodzimego odpowiednika DARPA[254] – ośrodka R&D z sektora prywatnego, który na zlecenie sił zbrojnych tworzyłby cyberrozwiązania. W związku z tym, polski odpowiednik

[254] DARPA (ang. *Defense Advanced Research Projects Agency*) – Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności.

DARPA mógłby być zlokalizowany np. przy Polskiej Grupie Zbrojeniowej (PGZ)[255].

Kolejną omawianą ścieżką tematyczną była „Przyszłość". Jako jedyna została podzielona na trzy zasadnicze części. Wnikliwa próba przeanalizowania wyzwań i problemów, nawiązywania współpracy oraz utworzenia tzw. cyberedukacji miały na celu podnoszenie świadomości w zakresie rosnącej luki zatrudnienia w dziedzinie IT i cyberbezpieczeństwa, jak również wyznaczenie priorytetów systemu edukacji w tym obszarze. W kontekście wyzwań i problemów, zauważono niektóre z poniższych kwestii dyskusyjnych:

- państwo powinno być zdolne do oszacowania, jakie zdolności w zakresie cyberochrony i cyberobrony chce osiągnąć paralelnie. Do tego powinno móc określić zapotrzebowanie na specjalistów i ich kompetencje;
- poszukuje się specjalistów o profilu technicznym, ale także cyberprawników, cybermenedżerów czy cyberdyplomatów, a także „integratorów rozwiązań" – posiadających „cyfrową wyobraźnię" i umiejętność rozpoznania i zrozumienia globalnych trendów cyfrowych. Dodatkowo mających zdolności do projektowania całościowych rozwiązań w dziedzinie cyberbezpieczeństwa, tak aby być gotowym na nowe zagrożenia;
- państwo powinno zabezpieczyć właściwe środki budżetowe zapewniające utrzymanie wysokiego potencjału ludzkiego, niezbędnego do ochrony systemów i sieci teleinformatycznych administracji wewnętrznej. Proces budowania systemu cyberbezpieczeństwa nie może być dłużej traktowany jako niskobudżetowy, a zabezpieczenie środków na wynagrodzenia jest jego najważniejszym elementem i celem.

W odniesieniu do zdefiniowanych wyzwań i problemów, określono niniejsze działania bazujące na wzajemnej współpracy:

- w sektorze komercyjnym i środowisku naukowym najważniejszym okazuje się być potencjał wiedzy i kompetencji, mogący wesprzeć państwo. Niedostatek kadr oraz braki budżetowe można wyrównywać rozwijając formuły i modele współpracy z biznesem, administracją i jednostkami naukowymi (uczelnie wyższe). Dlatego też współpraca – oparta na synergii celów, zaufaniu, przejrzystości i przekonaniu o potrzebie zintegrowania działań na rzecz budowy cyberbezpieczeństwa – jest najważniejszą rekomendacją CYBERSEC PL 2016;
- rząd powinien utrzymywać kontakty z ekspertami. Jedną z form przepływu wiedzy i platformą dialogu może być CYBERSEC PL;

[255] *Ibidem*, 8-9.

- potencjał przemysłu wymaga stałej rozbudowy. Zatem przykładem wsparcia instytucjonalnego mogą być np. grupy robocze w NATO. Sojusz Północnoatlantycki definiuje problem do rozwiązania i zaprasza do współpracy podmioty prywatne. Dzięki takiej praktyce wzrasta potencjał wiedzy firm. Również UE prowadzi grupy robocze związane z bezpieczeństwem cybernetycznym, zajmujące się podobnymi konsultacjami;
- strategiczne programy rozwojowe i modernizacyjne, np. program modernizacji Sił Zbrojnych RP powinien obejmować także oprogramowanie, tym samym angażować potencjał narodowy;
- współpraca jednostek naukowych z biznesem powinna być katalizatorem przemiany oferty edukacyjnej, mając na celu kształcenie specjalistów odpowiednich dla potrzeb rynku. Przedsięwzięcie to powinno mieć charakter przemiany długoterminowej.

W kontekście przyszłości funkcjonowania polskiej cyberprzestrzeni, rozumiejąc zachodzące w niej procesy oraz wynikające zagrożenia godzące w bezpieczeństwo państwa, na konferencji CYBERSEC PL 2016 ustalono kilka zagadnień związanych z cyberedukacją. Są to:

- konieczność budowania świadomości społeczeństwa, przy podkreśleniu, że cyberprzestrzeń jest elementem dobra narodowego i gospodarki narodowej, w której wypracowywana jest znacząca część produktu krajowego brutto kraju. Dzięki systemom teleinformatycznym realizowane są podstawowe potrzeby obywateli. Najistotniejszy kapitał ludzki konieczny do budowania cyberbezpieczeństwa kraju stanowi zatem ogół społeczeństwa;
- oprócz higieny korzystania z Internetu, ważne jest to, aby program nauczania bardziej koncentrował się na tzw. przedmiotach STEM (ang. *Science, Technology, Engineering, Mathematics* – Nauka, Technologia, Inżynieria, Matematyka). Dzięki temu oczekuje się, że wzrośnie również zainteresowanie kontynuacją kształcenia na tych specjalnościach;
- potrzeba założenia „zespołów łowców", składających się z cyberspecjalistów o najwyższych kwalifikacjach, potrafiących skojarzyć wybrane elementy i tworzyć innowacyjną całość systemu;
- konieczność wspierania programów naukowych prowadzonych w jednostkach naukowych i centrach naukowych działających we współpracy z firmami komercyjnymi[256].

Ostatnią z poruszanych na konferencji CYBERSEC PL 2016 ścieżek tematycznych był panel dyskusyjny – „Biznes". Uwzględniając szeroki zasób możliwości, które stwarza użytkowanie cyberprzestrzeni stwierdzono, że

[256] *Ibidem*, s. 10-13.

z powodzeniem możne ona również być wykorzystywana w zakresie np. inwestycji biznesowych lub ubezpieczeń, zapewniając podmiotom i klientom większy poziom komfortu podczas obsługi. Z tego powodu, dyskusje prelegentów konferencji skupione były wokół inicjatyw podejmowanych w obszarze bezpieczeństwa cybernetycznego w Polsce, problematyki zarządzania ryzykiem cybernetycznym z perspektywy ubezpieczyciela czy ubezpieczenia konsekwencji ataku cybernetycznego. Analizując poruszaną tematykę, opracowano następujące rekomendacje do wdrożenia w Polsce:

- ważnym wydaje się, że rozwój rynku cyberubezpieczeń jest istotny także z punktu widzenia bezpieczeństwa infrastruktury krytycznej, a tym samym bezpieczeństwa narodowego. Cyberpolisy mogą znacznie przyczynić się do podniesienia jego poziomu;
- w ramach procesu ubezpieczania podmiotów, prowadzone są działania weryfikujące poziom cyberbezpieczeństwa. Między innymi polega to na wskazywaniu elementów wymagających poprawy oraz przekazywaniu rekomendacji konkretnych rozwiązań. Zastosowanie elementów związanych z podejściem proaktywnym (co może obniżyć składkę lub być warunkiem ubezpieczenia) przyczynia się do podniesienia poziomu cyberbezpieczeństwa;
- należy rozważyć zmianę aktów prawnych dotyczących zamówień publicznych i włączenie ich w katalog cyberubezpieczenia;
- z punktu widzenia operatorów infrastruktury krytycznej, w sytuacji braku obowiązkowego przeprowadzania audytów zewnętrznych, dodatkowy audyt przeprowadzony przez ubezpieczyciela (wraz z rekomendacjami), może posiadać dużą wartość dodaną[257].

Obecnie jednym z najważniejszych dokumentów, realizujących długookresową oraz średniookresową strategię rozwoju państwa jest „Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022" (SRSBN RP), przyjęta przez Radę Ministrów w drodze uchwały w dniu 9 kwietnia 2013 r. Należy zauważyć, że SRSBN RP jest jedną z dziewięciu komplementarnych, zintegrowanych strategii rozwoju, które opracowano w oparciu o współczesne wyzwania postawione przed Polską w aspekcie szeroko rozumianego bezpieczeństwa narodowego. Wypełniając postulaty dokumentów o charakterze nadrzędnym w SRSBN RP, akcent strategiczny położony jest na tworzenie zintegrowanego systemu bezpieczeństwa narodowego, opartego na sojuszniczych i bilateralnych zabezpieczeniach oraz stopniowo rozbudowywanym własnym potencjale cywilno-militarnym. Za **cel główny** SRSBN RP uznano wzmocnienie efektywności i spójności systemu bezpieczeństwa narodowego, rozumianego jako synergia wysiłków poszczególnych organów, instytucji i służb państwowych od-

[257] *Ibidem*, s. 14.

powiedzialnych za bezpieczeństwo państwa do identyfikacji i eliminacji źródeł, przejawów oraz skutków zagrożeń bezpieczeństwa narodowego[258].

W dokumencie zawarto też zalecenie odnoszące się do zwiększenia poziomu bezpieczeństwa cybernetycznego. Jest nim pogłębienie współpracy z organizacjami międzynarodowymi, takimi jak NATO oraz UE. Konieczność zwiększenia poziomu bezpieczeństwa wynika z problemu, jakimi są cyberataki w coraz większym stopniu zagrażające bezpieczeństwu czy stabilności obszaru euroatlantyckiego. W dobie rozwoju technologicznego i swobodnego dostępu do sieci internetowej (w tym do mediów społecznościowych), trzeba podkreślić, że niektóre państwa dysponują możliwościami oraz środkami do przeprowadzenia ataków cybernetycznych (z dowolnego miejsca na świecie, godzące w dowolnie wybrany cel), których poziom byłby porównywalny do konwencjonalnych ataków zbrojnych. Z uwagi na to – zarówno w NATO, jak i UE – podniesiono rangę cyberbezpieczeństwa do stopnia rozpatrywanego przez najwyższe gremia polityczne. O bezpieczeństwie informatycznej infrastruktury krytycznej obydwu tych organizacji decyduje ich najsłabsze ogniwo. Stwarza to konieczność spełnienia standardów i wymagań przez infrastrukturę krajową ich państw członkowskich. Wobec określonego w SRSBN RP problemu, opracowano zespół głównych działań, które należy wdrożyć. Zaliczają się do nich:

- wspieranie inicjatyw na rzecz wzmocnienia roli i zdolności NATO oraz UE w zakresie polityki bezpieczeństwa cybernetycznego oraz wyposażenie obydwu organizacji w instrumenty udzielania pomocy państwom członkowskim (w szczególności średnim i małym) narażonym na ataki cybernetyczne;
- wspieranie działań na rzecz uwzględnienia obrony cybernetycznej w bieżących pracach planistycznych NATO;
- wzmocnienie współpracy pomiędzy NATO oraz UE w obszarze bezpieczeństwa cybernetycznego, w tym w szczególności w zakresie ochrony infrastruktury krytycznej sektorów cywilnych, takich jak: łączność, energetyka, transport lub finanse;
- aktywny udział Rzeczpospolitej Polskiej w budowie i funkcjonowaniu unijnych i sojuszniczych elementów struktur cyberobrony;
- udoskonalanie zasad i mechanizmów współpracy wewnątrz- i międzyresortowej (w tym pomiędzy Agencją Bezpieczeństwa Wewnętrznego oraz Ministerstwem Obrony Narodowej);
- uwzględnienie w „Polityce bezpieczeństwa cyberprzestrzeni Rzeczpospolitej Polskiej" nowych elementów wynikających z prac NATO

[258] *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022 –przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r.*, BBN, Warszawa 2013.

i UE nad polityką bezpieczeństwa cybernetycznego[259].

Inicjatywą promowaną i rozwijaną przez SRSBN RP w kontekście zapewnienia cyberbezpieczeństwa jest „System Reagowania na Incydenty Komputerowe MON" (SRnIK MON). Dokument ten został przyjęty przez Komitet Rady Ministrów ds. Cyfryzacji w dniu 28 listopada 2012 roku. SRnIK powołano na zasadzie analogii wobec funkcjonującego dla administracji rządowej w sferze cywilnej CERT.GOV.PL, lecz jego głównymi zadaniami są:

- zapewnienie realizacji i koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych resortu obrony narodowej;
- współpraca w obszarze przeciwdziałania atakom cybernetycznym z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz CERT POLSKA.

Dynamiczny rozwój sieci teleinformatycznych resortu obrony narodowej o różnych klauzulach oraz coraz szersze wykorzystywanie ich do przesyłania danych, jak również do dowodzenia i zarządzania, w naturalny sposób spowodował konieczność zagwarantowania bezpieczeństwa dla funkcjonowania samych sieci oraz przesyłanych w nich informacji. Wzrost zagrożeń w obszarze cyberprzestrzeni wymaga dostosowywania i ciągłego rozwijania istniejących już struktur systemu reagowania. Dlatego jednym z podstawowych zadań realizowanych w najbliższych latach, w założeniu „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022", będzie kontynuowanie procesu rozbudowy powołanego w ramach SRnIK zespołu MIL-CERT i pozyskanie nowych kompetencji pozwalających na realizację zawansowanych technologicznie funkcji; w tym informatyki śledczej i aktywnej odpowiedzi na ataki cybernetyczne. Będzie się to odbywać w sposób powiązany z rozwojem Rządowego Zespołu Reagowania na Incydenty Komputerowe oraz budową kompetencji strategicznej koordynacji w Ministerstwie Administracji i Cyfryzacji, właściwym dla działów łączność i informatyzacja. W związku z tym, określono główne działania strategiczne, polegające na:

- dalszym rozszerzaniu współpracy z innymi zespołami narodowymi i organizacjami konsolidującymi międzynarodowe struktury CERT, w tym nowo powstałym zespołem CERT UE;
- ustanowieniu Krajowego Systemu Reagowania na Incydenty Komputerowe pozwalającego na podjęcie szybkiej reakcji na zagrożenia z sieci Internet;
- posiadaniu przez Agencję Bezpieczeństwa Wewnętrznego oraz resort obrony narodowej silnych, wyposażonych w zaawansowane techno-

[259] *Ibidem*, s. 42-43.

logie zespołów reagowania, w tym zespołów szybkiego reagowania (ang. *Rapid Reaction Team*). Ich przeznaczeniem będzie usprawnienie realizowanego zakresu współpracy międzynarodowej oraz możliwość osiągania nowych zdolności operacyjnych z obszaru zadań reagowania na incydenty bezpieczeństwa teleinformatycznego oraz dowodzenia i kierowania w cyberprzestrzeni[260].

Spośród dokumentów o charakterze prawnym należy wskazać, iż Rada Ministrów przyjęła „Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022"[261] (KRPC RP), które jako strategiczny cel określają osiągniecie wysokiego poziomu bezpieczeństwa cyberprzestrzeni państwa.

Dokument KRPC RP prezentuje strategiczne podejście administracji rządowej do kwestii obejmującej zakres szeroko rozumianego cyberbezpieczeństwa. Został on opracowany przez grupę składającą się z przedstawicieli kilku resortów, takich jak: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa oraz Biura Bezpieczeństwa Narodowego.

W KRPC RP wskazano, że jego głównymi założeniami jest określenie ramowych działań, mających na celu uzyskanie wysokiego poziomu niepodatności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty zachodzące w cyberprzestrzeni. Ponadto, proponowane kierunki rozwoju na szczeblu strategicznym mają znacząco wpływać na zwiększenie skuteczności organów ścigania oraz wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni.

Krajowe Ramy Polityki Cyberbezpieczeństwa zawierają w szczególności:

- określone cele w zakresie bezpieczeństwa teleinformatycznego;
- główne podmioty zaangażowane we wdrażanie krajowych ram polityki ochrony w zakresie bezpieczeństwa teleinformatycznego;
- ramy zarządzania służące realizacji celów krajowych, a także ramy polityki ochrony w zakresie bezpieczeństwa teleinformatycznego;
- kwestie związane z potrzebą zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy między sektorami publicznym i prywatnym;

[260] *Ibidem*, s. 86-87.

[261] *Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Ministerstwo Cyfryzacji, Warszawa 2017.

- zasady oceny ryzyka;
- podejście do programów dotyczących cyberbezpieczeństwa – edukacyjnych, informacyjnych i szkoleniowych;
- działania dotyczące planów badawczo-rozwojowych (B+R) w zakresie bezpieczeństwa teleinformatycznego;
- zasady współpracy międzynarodowej w zakresie cyberbezpieczeństwa.

Zgodnie z dokumentem KRPC RP przyjęto wizję, że w 2022 r. Polska będzie krajem bardziej odpornym na cyberataki oraz zagrożenia wynikające z przestrzeni cybernetycznej. Równocześnie, dzięki synergii działań wewnętrznych i międzynarodowych, cyberprzestrzeń Rzeczypospolitej Polskiej ma stanowić bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa. Dodatkowo ma pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy jednoczesnym poszanowaniu praw oraz wolności obywateli.

KRPC RP wskazują na zawarty w nich cel główny oraz wynikające z niego cele szczegółowe. Jako cel główny założono wysoki priorytet zapewnienia znacznego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych. Wyznaczono również cztery cele szczegółowe:

- pierwszy cel szczegółowy – określa osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa;
- drugi cel szczegółowy – definiuje wzmocnienie zdolności Rzeczpospolitej Polskiej do przeciwdziałania cyberzagrożeniom;
- trzeci cel szczegółowy – dotyczy sukcesywnego zwiększania potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni;
- czwarty cel szczegółowy – dotyczy budowy silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Każdy z przedstawionych celów szczegółowych został dokładnie opisany i zaprezentowany poprzez wskazanie konkretnych, fizycznych działań zmierzających bezpośrednio do jego osiągnięcia. W zakresie pierwszego celu szczegółowego wymieniono:

- dostosowanie aktów prawnych do potrzeb i wyzwań w obszarze cyberbezpieczeństwa (wskazano na konieczność rozbudowy krajowego systemu cyberbezpieczeństwa wymagającego przeglądu i zmian aktów prawnych, a także monitorowanie zachodzących tam zjawisk);

- udoskonalenie struktury krajowego systemu cyberbezpieczeństwa, wskazując na konieczność określenia zakresu odpowiedzialności podmiotu koordynującego krajowy system cyberbezpieczeństwa. Dodatkowo należy opracować zakres obowiązków i uprawnień uczestników systemu oraz sposobów oddziaływania koordynatora na uczestników systemu. Zwrócono także uwagę na konieczność określenia kompetencji organów właściwych, odpowiedzialnych za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe;
- zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni Rzeczpospolitej Polskiej, poprzez organizowanie i przeprowadzanie treningów i ćwiczeń o zróżnicowanym zasięgu terytorialnym;
- zwiększenie poziomu bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej. W tym celu oczekuje się podjęcia działań wspierających budowanie zdolności oraz kompetencji w zakresie cyberbezpieczeństwa pośród operatorów usług kluczowych, infrastruktury krytycznej, a także dostawców usług cyfrowych;
- opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych;
- wypracowanie oraz wdrożenie na poziomie krajowym systemu zarządzania ryzykiem;
- zapewnienie bezpiecznego łańcucha dostaw, poprzez ocenę i certyfikację produktów;
- zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni o ryzyku wynikającym z cyberzagrożeń.

W ramach realizacji drugiego celu szczegółowego, wobec wyzwania w postaci wzmocnienia zdolności do przeciwdziałania cyberzagrożeniom, wskazano na poniższe działania, mianowicie:

- zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym;
- osiągnięcie zdolności do prowadzenia pełnego zakresu działań o charakterze wojskowym w cyberprzestrzeni;
- podwyższenie zdolności w zakresie analizy zagrożeń na poziomie krajowym;
- zbudowanie systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego;
- wykonywanie audytów i testów bezpieczeństwa.

W zakresie trzeciego celu szczegółowego, odnoszącego się do zwiększania potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni, wskazano na następujące aspekty:

- potrzebę rozbudowy zasobów przemysłowych i technologicznych na cele cyberbezpieczeństwa;
- zbudowanie zasad współpracy między sektorami – publicznym i prywatnym;
- stymulowanie badań i rozwoju (B+R) w zakresie bezpieczeństwa systemów teleinformatycznych;
- zwiększanie kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni;
- stworzenie warunków dla obywateli do bezpiecznego korzystania z cyberprzestrzeni.

W odniesieniu do czwartego celu szczegółowego, dotyczącego zbudowania silnej pozycji międzynarodowej Rzeczpospolitej Polskiej w obszarze cyberbezpieczeństwa, wskazano na:

- aktywną współpracę międzynarodową na poziomie strategiczno-politycznym;
- aktywną współpracę międzynarodową na poziomie operacyjnym i technicznym.

Dokument określa także kwestię zarządzania Krajowymi Ramami Polityki Cyberbezpieczeństwa wskazując, że są uchwalane na okres 5 lat. Koordynatorem wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji. Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument ten podlega przeglądowi pod względem osiągniętych efektów. W założeniu, wyniki przeglądu zostaną przedstawione Radzie Ministrów. Wobec dokonanego przeglądu, minister właściwy do spraw informatyzacji jest zobowiązany opracować nową propozycję działań korygujących lub projekt dokumentu na kolejny pięcioletni okres. Jednocześnie, w dokumencie zastrzeżono, że w przypadku wystąpienia uzasadnionych okoliczności, Krajowe Ramy Polityki Cyberbezpieczeństwa mogą być aktualizowane w innych terminach.

Kolejnym dokumentem odnoszącym się do bezpieczeństwa cyberprzestrzeni RP jest „Strategia cyberbezpieczeństwa RP zaplanowana na lata 2017-2022" (SC RP)[262]. Dokument ten został wprowadzony uchwałą Rady Ministrów, co spowodowało, że powyższa dokument w sposób bezpośredni oddziałuje na podmioty administracji rządowej. Należy także podkreślić, iż dokument ten jest zbieżny z unijną dyrektywą[263] dotyczącą utrzymania

[262] *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Ministerstwo Cyfryzacji, Warszawa 2017.

[263] *Dyrektywa Parlamentu i Rady Unii Europejskiej w sprawie środków na rzecz wysokiego*

wysokiego, wspólnego poziomu bezpieczeństwa cyberprzestrzeni. Z uwagi na fakt, iż jest to przepis prawa powszechnie obowiązującego, wpływa on także na inne podmioty władzy publicznej, np. na przedsiębiorców oraz obywateli. Celem analizowanej strategii jest wskazanie ramowych działań zmierzających do uzyskania wysokiego poziomu zabezpieczenia poszczególnych systemów teleinformatycznych, podmiotów dostarczających usługi cyfrowe. Obejmuje też kwestię ochrony całokształtu administracji publicznej przed incydentami w sferze cyberprzestrzeni. Założenia strategiczne mają wywołać następstwo oddziaływania w postaci zwiększonej efektywności działań organów ścigania i wymiaru sprawiedliwości podczas wykrywania oraz zwalczania przestępczości o charakterze terrorystycznym oraz szpiegowskim dokonywanych w sieci.

W SC RP zaplanowaną na lata 2017-2022 można wyróżnić zawarty w niej ogólny zarys problematyki, mianowicie:

- wskazanie na cele w zakresie bezpieczeństwa teleinformatycznego;
- główne podmioty realizujące wdrażanie strategii w zakresie bezpieczeństwa teleinformatycznego;
- wskazanie ram zarządzania, których celem jest realizacja krajowej strategii w zakresie bezpieczeństwa teleinformatycznego;
- potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego zdarzeniem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym;
- zasady podejścia do oceny ryzyka;
- kierunki działań programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa;
- działania odnoszące się do planów badawczo-rozwojowych (B+R) w zakresie bezpieczeństwa teleinformatycznego;
- zasady współpracy międzynarodowej w zakresie cyberbezpieczeństwa[264].

Kolejnym dokumentem prawno-strategicznym w aspekcie podniesienia poziomu bezpieczeństwa informacyjnego jest wspomniana już „Doktryna cyberbezpieczeństwa RP”[265] (DC RP). Jest to akt o specyfice koncepcyjnej oraz wykonawczej w odniesieniu do „Strategii Bezpieczeństwa Narodowego RP”. Określa on w szczególności cele w dziedzinie cyberbezpieczeństwa, opisuje wnikliwie środowisko, wymieniając zagrożenia, ryzyka i szanse oraz przedstawia rekomendacje w kwestii najważniejszych zadań,

wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE z dnia 19.07.2016 r, Nr L 194/1).

[264] *Ibidem*, s. 7.

[265] *Doktryna cyberbezpieczeństwa Rzeczypospolitej…*, *op. cit.*

jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa. Celem doktryny jest zapewnienie bezpiecznego funkcjonowania RP w cyberprzestrzeni. Odnosi się to w szczególności do adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych (zwłaszcza teleinformatycznej infrastruktury krytycznej państwa) oraz kluczowych dla funkcjonowania całego społeczeństwa prywatnych podmiotów gospodarczych. Względem tych ostatnich szczególne znaczenie stanowi sektor finansowy, energetyczny i ochrony zdrowia[266].

Na poziomie strategicznym to Rada Ministrów jest odpowiedzialna za koordynację działań w zakresie cyberbezpieczeństwa. Jednocześnie, należy podkreślić, że postulaty zawarte w DC RP dotyczą ob.:

- wprowadzenia określonych rozwiązań formalno-prawnych;
- określenia mechanizmów współpracy i wzajemnego oddziaływania sektora publicznego i prywatnego;
- inwestycji w narodowe rozwiązania w zakresie cyberbezpieczeństwa;
- racjonalnego wykorzystania potencjału obywatelskiego na rzecz obrony oraz ochrony państwa w cyberprzestrzeni.

W „Doktrynie cyberbezpieczeństwa RP" nadmieniono, że wymogiem niezbędnym jest, by proces kształtowania się polskiego systemu cyberbezpieczeństwa przebiegał w zgodzie z dokumentami Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego, jak i innymi inicjatywami międzynarodowymi w taki sposób, żeby był wewnętrznie spójny oraz kompatybilny z systemami państw sojuszniczych i organizacji międzynarodowych[267].

Następnym dokumentem, istotnym z punktu widzenia zapewnienia cyberbezpieczeństwa w RP, jest wspomniana we wcześniejszej części pracy „Polityka Ochrony Cyberprzestrzeni RP"[268]. Zgodnie z tym dokumentem, określono cel strategiczny, którym jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej. Jednocześnie, dokument ten wskazuje, że kontrolowanie i realizacja tak zdefiniowanego celu są realizowane poprzez stworzenie ram organizacyjno-prawnych a także systemu skutecznej koordynacji i wymiany informacji pomiędzy jego użytkownikami.

Celami szczegółowymi „Polityki Ochrony Cyberprzestrzeni RP" są:

- zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa;
- zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze

[266] *Ibidem*, s. 9.
[267] *Ibidem*, s. 17.
[268] *Polityka ochrony cyberprzestrzeni...*, *op. cit.*

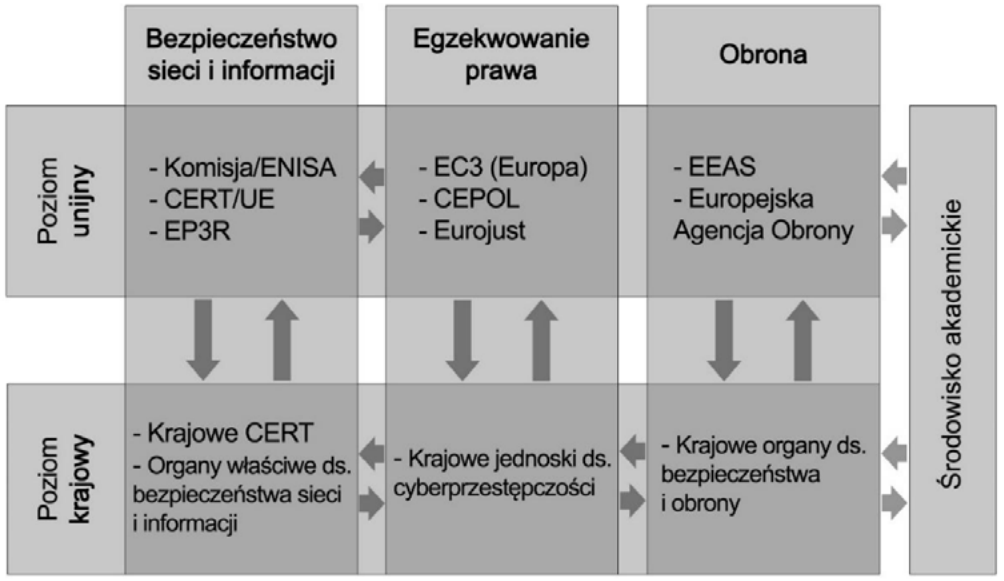
strony cyberprzestrzeni;
- zmniejszenie skutków zdarzeń skierowanych w bezpieczeństwo teleinformatyczne;
- określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni;
- utworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz opracowanie dla podmiotów niepublicznych wytycznych w tym zakresie;
- utworzenie stabilnego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni;
- zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni[269].

6.1.2. Strategiczne założenia cyberbezpieczeństwa Unii Europejskiej w kontekście wykorzystania mediów społecznościowych

Unia Europejska uznaje zagrożenia występujące w cyberprzestrzeni za jeden z czynników mogących istotnie oddziaływać na bezpieczeństwo narodowe. W „Europejskiej strategii bezpieczeństwa”[270] podkreślono rangę cyberbezpieczeństwa wskazując, że nowoczesne gospodarki zależą w dużym stopniu nie tylko od infrastruktury krytycznej, łączności czy energii, ale także od sieci Internet. Przestępczość internetowa uznana została za nowy a zarazem ważny problem, do którego musi się odnieść Wspólnota Europejska. Ataki kierowane na prywatne bądź rządowe systemy informatyczne krajów członkowskich nadały tej przestępczości nowy wymiar, jako potencjalnej broni – ekonomicznej, wojskowej i politycznej.

Chcąc zrozumieć relacje pomiędzy systemem unijnym a krajowym dotyczącym odpowiedzialności za cyberbezpieczeństwo można odnieść do rysunku 14.

[269] *Ibidem*, s. 6-7.
[270] *Europejska strategia bezpieczeństwa. Bezpieczna Europa w lepszym świecie*, Urząd Publikacji Unii Europejskiej, Luksemburg 2009, s. 13.



Rysunek 14. Relacje między filarami odpowiedzialnymi za cyberbezpieczeństwo, egzekwowanie prawa oraz cyberobronę na poziomie krajowym i Unii Europejskiej
Źródło: opracowanie własne na podstawie Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, Komisja Europejska, Bruksela 2013, s. 21.

Można wyróżnić w nim dwie główne płaszczyzny – krajową i unijną, na których realizowane są działania z zakresu zapewnienia cyberbezpieczeństwa, zdolności do cyberobrony oraz wymiaru sprawiedliwości w przypadku niedostosowania się do narzuconych wymogów. Ustanowiono, że wymienione poziomy będą rozpatrywane, jak również wspierane przez trzy filary: w aspekcie bezpieczeństwa sieci i informacji, egzekwowania prawa, obrony. W tym celu, konieczne jest powołanie odpowiednich instytucji oraz komórek, których misją będzie wypełnienie obszaru określonego przez filary.

Państwa członkowskie w odniesieniu do działań krajowych powinny posiadać, bądź utworzyć w wyniku strategii, struktury przeznaczone do działań w zakresie odporności cybernetycznej, cyberprzestępczości i obrony, takie jak: Krajowe CERT, właściwe organy ds. bezpieczeństwa sieci i informacji, krajowe jednostki ds. cyberprzestępczości, krajowe organy ds. bezpieczeństwa i obrony. Dzięki planowanym strukturom organizacyjnym powinny też osiągnąć stopień zdolności wymagany do celów reagowania na zaistniałe incydenty cybernetyczne. Zważając na fakt, że na kilka podmiotów mogą zostać nałożone obowiązki o charakterze operacyjnym – dotyczące różniących się od siebie kwestii bezpieczeństwa cybernetycznego, a także biorąc pod uwagę wzrost znaczenia udziału sektora prywatnego

– na poziomie krajowym należy zapewnić optymalną koordynację z udziałem różnych ministerstw. Na państwa członkowskie Unii Europejskiej nałożono obowiązek, aby w swoich krajowych strategiach cyberbezpieczeństwa określiły funkcje poszczególnych podmiotów krajowych. Wymiana informacji między podmiotami krajowymi oraz między nimi a sektorem prywatnym powinna być wspierana i promowana. Takie działanie miałoby na celu umożliwienie państwom członkowskim i sektorowi prywatnemu posiadanie świadomości i wiedzy o zagrożeniach oraz większe zrozumienie nowych tendencji i technik wykorzystywanych zarówno do przeprowadzania cyberataków, jak i do szybszego reagowania na przeciwdziałanie im. Dzięki ustanowieniu krajowych planów współpracy w zakresie bezpieczeństwa sieci i informacji, które miałyby być wykorzystywane w przypadku incydentów cybernetycznych, państwa członkowskie powinny być w stanie dokonać wyraźnego podziału ról i obowiązków oraz zapewnić optymalność podejmowanych działań[271].

W odniesieniu do poziomu unijnego, podobnie jak w krajowym, został powołany szereg podmiotów i organizacji, zajmujących się kwestiami bezpieczeństwa cybernetycznego, wspieranego na trzech, wspomnianych wcześniej filarach. Aspektami bezpieczeństwa sieci i informacji zajmują się organy, takie jak: Europejska Agencja Bezpieczeństwa Sieci i Informacji (ang. *European Network and Information Security Agency* – ENISA), CERT UE, EP3R (ang. *European Public Private Partnership for Resilience*) oraz inne sieci właściwych w tym filarze organów. Za egzekwowanie prawa odpowiadają: Europol, Europejskie Centrum ds. Walki z Cyberprzestępczością (ang. *European Cyber-crime Centre* – EC3), Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (ang. *European Union Agency for Law Enforcement Training* – CEPOL) i Eurojust. Zwierzchnictwo nad obroną sprawują: Służba zewnętrzna *Unii Europejskiej (*ang. *European External Action Service* – EEAS), jak i Europejska Agencja Obrony (E*uropean Defence Agency* – EAO). Trzy z wymienionych agencji, do których zaliczają się: ENISA, Europol (EC3) i EAO, posiadają rady zarządzające, gdzie reprezentowane są państwa członkowskie. Owe rady stanowią platformy odpowiedzialne za proces koordynacji na poziomie Unii Europejskiej. ENISA, Europol/EC3 i EAO będą zachęcane do nawiązywania wzajemnej współpracy w dziedzinach, w których wspólnie prowadzą działania, zwłaszcza w zakresie analiz tendencji, oceny zagrożeń, szkoleń i wymiany najlepszych praktyk. Powinny one ze sobą współpracować, zachowując jednocześnie swoją odrębność. Podmioty te wraz z CERT-UE, Komisją Europejską i państwami członkowskimi mają za zadanie wspierać rozwój obdarzonej zaufaniem grupy ekspertów technicznych i ekspertów ds. polityki w tej dzie-

[271] *Wspólny komunikat do Parlamentu…*, *op. cit.*, s. 21.

dzinie. Do celów koordynacji w dziedzinie obronności można wykorzystać personel wojskowy wydzielony do zadań w zakresie UE oraz działający w ramach EAO zespół projektowy ds. obrony cybernetycznej. W pracach Rady Programowej Europolu/EC3 uczestniczyć mają między innymi: Eurojust, CEPOL, państwa członkowskie, ENISA i Komisja Europejska. Powinny one mieć możliwość dzielenia się wiedzą ekspercką oraz bycia gwarantem tego, że działania EC3 będą prowadzone na zasadach współpracy partnerskiej, przy uznaniu znaczenia dodatkowej wiedzy specjalistycznej oraz z poszanowaniem mandatów wszystkich zainteresowanych stron. Nowy mandat ENISA powinien umożliwić wzmocnienie jej powiązań z Europolem i z zainteresowanymi stronami z branży[272].

Najważniejszym dokumentem strategicznym dotyczącym bezpieczeństwa cyberprzestrzeni Unii Europejskiej jest „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej" (SBC UE). W szerokim zakresie reguluje on rozwiązania organizacyjne na poziomie wspólnoty unijnej. Celem tych rozwiązań jest uzyskanie wysokiego gwarantu bezpieczeństwa sieci i informacji. Określa ona przede wszystkim podstawowe, unijne zasady bezpieczeństwa cybernetycznego. Stanowią one ważny czynnik warunkujący przyjęte w tym zakresie rozwiązania organizacyjne i organizacyjno-prawne. Do tych zasad należy zaliczyć następujące twierdzenia i postulaty zawarte w dokumencie:

- podstawowe unijne wartości mają zastosowanie w cyfrowym świecie tak samo, jak w świecie fizycznym (przyjęte normy obowiązują również w cyberprzestrzeni);
- ochrona podstawowych praw, danych osobowych, wolności wypowiedzi i prywatności;
- dostęp dla wszystkich cyberprzestrzeni UE;
- efektywne i demokratyczne zarządzanie wielostronne (cyberprzestrzeni nie kontroluje jeden podmiot);
- wspólna odpowiedzialność za gwarantowanie cyberbezpieczeństwa (wszystkich organów publicznych oraz sektora prywatnego).

Unia Europejska określiła także w SBC UE pięć strategicznych priorytetów w zakresie bezpieczeństwa cybernetycznego, do których ujednolicono poniższe zagadnienia:

- ustanowienie spójnej międzynarodowej polityki w obszarze cyberprzestrzeni dla UE oraz promowanie podstawowych wartości unijnych;
- rozbudowa zasobów technologicznych i przemysłowych na potrzeby bezpieczeństwa cybernetycznego;

[272] *Ibidem*, s. 22.

- tworzenie polityki obronnej oraz rozbudowa zdolności w obszarze bezpieczeństwa cybernetycznego z uwzględnieniem wspólnej polityki bezpieczeństwa i obrony;
- radykalne ograniczenie cyberprzestępczości;
- osiągnięcie odporności na zagrożenia cybernetyczne[273].

Jednym z istotnych działań podjętych w ramach realizacji ostatniego z wymienionych wyżej celów strategicznych było ustanowienie w 2004 roku Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ang. T*he European Union Agency for Network and Information Security* – ENISA). Stanowi ona ośrodek wiedzy specjalistycznej dotyczącej cyberbezpieczeństwa w Europie, z siedzibą w Atenach. Zadaniem ENISA jest świadczenie pomocy na rzecz UE oraz krajów członkowskich w zakresie zapobiegania problemom dotyczącym bezpieczeństwa informacji, jak również w zakresie ich wykrywania i reagowania na nie. ENISA udziela praktycznych porad oraz proponuje rozwiązania problemów zarówno dla sektora publicznego, jak i prywatnego w państwach Unii Europejskiej, a także w samych instytucjach unijnych. Działania ENISA obejmują następujące czynności:

- organizowanie ogólnoeuropejskich ćwiczeń, które przygotowywać mają do reagowania w przypadku zaistnienia sytuacji kryzysowej;
- udział w opracowywaniu krajowych strategii bezpieczeństwa cybernetycznego;
- wspieranie współpracy pomiędzy zespołami reagowania na zagrożenia komputerowe oraz rozwój umiejętności[274].

Dodatkowo ENISA publikuje sprawozdania oraz badania odnoszące się do zagadnienia bezpieczeństwa cybernetycznego, w zakresie:

- identyfikowania zagrożeń cybernetycznych;
- identyfikacji elektronicznej oraz usług zaufania w cyfrowym środowisku;
- technologii wykorzystywanych do ochrony prywatności, a także zapewniania prywatności w przypadku stosowania nowych technologii;
- ochrony danych;
- bezpieczeństwa danych przechowywanych w chmurze.

Można zatem stwierdzić, że ENISA uczestniczy w szeroko pojmowanym zakresie działań związanym bezpośrednio z kształtowaniem się prawa oraz polityki unijnej w dziedzinie bezpieczeństwa cyberprzestrzeni. W ten sposób przyczynia się także do wzrostu gospodarczego na rynku Unii Europejskiej. Szczegółowy sposób działania Europejskiej Agencji do spraw

[273] *Wspólny komunikat do Parlamentu…*, *op. cit.*, s. 4-5.
[274] *Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA). Informacje ogólne*, online – https://europa.eu/european-union/about-eu/agencies/enisa_pl [dostęp: 07.09.2017].

Bezpieczeństwa Sieci i Informacji zawierany jest w rocznym programie prac, który opracowany jest corocznie po odbyciu konsultacji. Dodatkowo ENISA ściśle współpracuje z wieloma organizacjami zarówno z sektora publicznego, jak i prywatnego. Współpraca ta odbywa się na następujących płaszczyznach:

- wiedzy fachowej – nawiązującej do przewidywania nowych wyzwań z zakresu bezpieczeństwa informacji i sieci, wspieranie Europy w radzeniu sobie z takimi wyzwaniami, dzięki reagowaniu na zmiany zachodzące w świecie cyfrowym;
- strategii – ukierunkowanej na pomoc państwom członkowskim oraz instytucjom unijnym w kreowaniu i wdrażaniu strategii koniecznej do spełnienia regulacyjnych i prawnych wymogów krajowego bezpieczeństwa informacyjnego;
- zdolności – bazującej na wspieraniu Europy w tworzeniu nowoczesnych sieci oraz zdolności w obszarze bezpieczeństwa cybernetycznego;
- społeczeństwa – w odniesieniu do kreowania współpracy pomiędzy krajami członkowskimi a systemami bezpieczeństwa informacyjnego.

ENISA współpracuje z innymi organizacjami międzynarodowymi, takimi jak Europejskie Centrum ds. Walki z Cyberprzestępczością oraz Europol, w zakresie komunikacji i badań naukowych. Wspomaga ona również unijne agencje w zakresie bezpieczeństwa cybernetycznego.

Główną grupą docelową Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji są rządu krajów UE oraz instytucje UE. Agencja pracuje także na rzecz: sektora technologii komunikacyjnych i informacyjnych (firmy informatyczne, dostawcy usług internetowych, telekomunikacja), przedsiębiorstw, środowisk akademickich, specjalistów do spraw bezpieczeństwa informacji i sieci, takich jak zespoły CERT oraz ogółu społeczeństwa[275].

Jedną z ważnych inicjatyw rozwijanych przez ENISA jest Europejskie partnerstwo publiczno-prywatne na rzecz odporności (ang. *European Public Private Partnership for Resilience* – EP3R). Platforma ta zainicjowała działania oraz intensywniejszą współpracę pomiędzy sektorem publicznym i prywatnym dotyczącą identyfikacji kluczowych zasobów, funkcji, środków, jak również podstawowych wymogów w odniesieniu do odporności cybernetycznej. EP3R stało się także platformą współpracy i rozwijania mechanizmów reagowania na zakłócenia łączności elektronicznej o szerokim zasięgu[276].

[275] *Ibidem.*
[276] *Wspólny komunikat do Parlamentu...*, *op. cit.*, s. 7.

Wsparcie finansowe kluczowej infrastruktury cyberprzestrzeni oraz połączenie zdolności państw członkowskich w obszarze bezpieczeństwa informacji i sieci zapewnić ma powołany instrument o nazwie – *Łącząc Europę* (ang. *Connecting Europe Facility* – CEF)[277].

W ramach rozwijania współpracy między państwami członkowskimi Unii Europejskiej a sektorem prywatnym organizowane są także ćwiczenia dotyczące bezpieczeństwa cybernetycznego na poziomie całej UE. Pierwsze tego rodzaju ćwiczenia przeprowadzono w roku 2010 (pk. *Cyber Europe-2010*). W kolejnym roku przeprowadzone zostały ćwiczenia, w których wspólnie uczestniczyli przedstawiciele krajów członkowskich UE oraz Stanów Zjednoczonych (pk. *CyberAtlantic-2011*).

Kolejnym istotnym elementem unijnego systemu zapobiegania zagrożeniom cybernetycznym jest zespół CERT-EU. Jest on zespołem reagowania na incydenty komputerowe świadczącym usługi dla instytucji, organów i agencji Unii Europejskiej. CERT-EU powstał w dniu 11 października 2012 roku. Zakres jego zadań jest tożsamy z zakresem zespołów CERT.GOV.PL czy innych krajowych zespołów CERT[278].

Omawiając rozwiązania organizacyjne w zakresie cyberbezpieczeństwa funkcjonujące w Unii Europejskiej należy zwrócić szczególną uwagę na to, że w procesie gwarantowania tego bezpieczeństwa uczestniczą nie tylko wyspecjalizowane instytucje wspólnotowe, ale także najważniejsze organy Unii Europejskiej, jak: Komisja Europejska, Rada Europejska czy Parlament Europejski. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej" precyzyjnie określa zadania poszczególnych podmiotów unijnych w tym zakresie oraz ich wzajemne relacje.

Najważniejszym dokumentem prawnym regulującym problematykę cyberbezpieczeństwa na poziomie unijnym jest wspomniana już Dyrektywa Parlamentu Europejskiego i Rady Europejskiej w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[279]. Głównym celem tego dokumentu jest wprowadzenie środków, dzięki którym możliwe będzie – „osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego" (zgodnie z art. 1 dyrektywy NIS – (*Network and Information Systems Directive* [280]). Aby cel ten stał się możliwy do zrealizowania dokonano następujących działań:

---

[277] *Ibidem*, s. 8.
[278] *CERT-UE for the EU institutions, bodies and agencies*,
online – https://cert.europa.eu/cert/plainedition/en/cert_about.html
[dostęp: 07.09.2017].
[279] *Dyrektywa Parlamentu i Rady Unii Europejskiej*, *op. cit*.
[280] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.

- ustanowiono obowiązki wobec wszystkich państw członkowskich odnoszące się do przyjęcia krajowych strategii w zakresie bezpieczeństwa systemów i sieci informatycznych;
- utworzono grupę współpracy, by wspierać oraz ułatwiać współpracę strategiczną oraz wymianę informacji pomiędzy państwami członkowskimi Unii Europejskiej oraz rozwijać pośród nich pewność i zaufanie;
- utworzono sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (ang. *Computer Security Incident Response Team* – CSIRT), by przyczyniać się do rozwoju pewności i zaufania pomiędzy państwami członkowskimi oraz promować skuteczną i szybką współpracę operacyjną;
- ustanowiono wymogi odnoszące się do bezpieczeństwa oraz zgłaszania incydentów dla dostawców usług cyfrowych i operatorów usług kluczowych;
- ustanowiono obowiązki dla krajów członkowskich odnoszące się do wyznaczania kompetentnych organów krajowych, pojedynczych punktów kontaktowych i CSIRT mających zadania wiążące się z bezpieczeństwem systemów oraz sieci teleinformatycznych.

6.1.3. Strategiczne założenia cyberbezpieczeństwa NATO w kontekście wykorzystania mediów społecznościowych

Analiza podatności na zagrożenia pochodzące z cyberprzestrzeni jest jednym z najważniejszych wyzwań, które podejmowane są w pracach planistycznych i projektowych NATO dotyczących rozwijania strategii obrony i bezpieczeństwa państw członkowskich[281]. Należy zauważyć, że problematyka bezpieczeństwa cyberprzestrzeni jest dla Sojuszu Północnoatlantyckiego dosyć nowa. Jeszcze w latach 90. ubiegłego stulecia na forum NATO nie dyskutowano na temat żadnych zagadnień związanych z cyberzagrożeniami. Sytuacja ta uległa zmianie dopiero po dokonaniu cyberataku przez hakerów z Serbii, który został wymierzony w systemy decydujące o sprawnym funkcjonowaniu NATO. Sprawcy włamali się na strony internetowe Sojuszu Północnoatlantyckiego w odwecie za interwencję sił sojuszniczych w byłej Jugosławii (Operacja Allied Force z 1999 roku). Ich działania ukie-

w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE 19.7.2016 L 194/1). Szerzej nt. inicjatywy NIS w dalszej części pracy.

[281] J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Difin, Warszawa 2014, s. 212.

runkowane były na obniżenie prestiżu NATO jako instytucji bezpieczeństwa i utratę poparcia społecznego dla działań Sojuszu. Po zbombardowaniu przez sojusznicze siły ambasady chińskiej w Belgradzie do cyberataku przyłączyli się hakerzy z Chin. Opisane działania wymierzone w bezpieczeństwo Sojuszu unaoczniły jego decydentom, że u progu XXI wieku cyberprzestrzeń stała się ważnym obszarem bezpieczeństwa[282]. Wskutek opisanego ataku, NATO wdrożyło program cyberobrony oraz reagowania na zagrożenia, których źródłem jest cyberprzestrzeń (koncepcję w tym zakresie przedstawiono jednak dopiero w 2002 roku na szczycie w Pradze)[283].

W kolejnych latach temat dotyczący cyberzagrożeń pozostawał na forum NATO w aspekcie problematyki związanej ze światowym terroryzmem. Sytuacja ta uległa zmianie dopiero po ataku cybernetycznym na Estonię, który przeprowadzony w został w 2007 roku przez grupę „Nasi" powiązaną z Rosją. Był to pierwszy w historii zmasowany cyberatak skierowany przeciw bezpieczeństwu suwerennego państwa. W jego ramach rosyjscy hakerzy unieruchomili na kilka dni działanie stron estońskich instytucji publicznych, a później także należących do sektora prywatnego. Choć realne straty nie okazały się bardzo duże, to jednak sprawcom ataku udało się osiągnąć spektakularny efekt psychologiczny. Zarówno Estonia, jak i inne państwa NATO przekonały się wówczas, że odpowiednio przygotowany atak cybernetyczny jest w stanie skutecznie oddziaływać na funkcjonowanie państwa. Władze w Tallinie rozważały powołanie się na artykuł 5 Traktatu Waszyngtońskiego, zrezygnowano jednak z tego pomysłu z uwagi na brak istniejących w tym zakresie procedur postępowania, a także sprzeciw części członków Sojuszu Północnoatlantyckiego. Wiele państw członkowskich NATO udostępniło jednak Estończykom swoje zespoły CERT oraz udzieliło pomocy technicznej i sprzętowej[284].

Współcześnie, w kontekście cyberzagrożeń, NATO wskazuje przede wszystkim na problem szpiegostwa. Państwa należące do Sojuszu Północnoatlantyckiego wymieniają między sobą szereg informacji, które objęte są najwyższym priorytetem ochrony, równocześnie jednak stają się celem ataków pochodzących z różnych grup hakerów. Strony internetowe NATO atakowane są także przez cyberaktywistów, których działania ukierunkowane były na ośmieszenie NATO, a także utraty przez nią wizerunku gwaranta bezpieczeństwa. Ostatecznie zauważyć należy, że NATO zostało narażone także na szkodliwą działalność wewnątrz organizacji. Wszystkie te

[282] A. Kozłowski, *NATO wobec wyzwań i zagrożeń w cyberprzestrzeni*, „Biuletyn OPINIE FAE" 2016, nr 7, s. 2.
[283] R. Czulda, *Atak w wirtualu*, „Polska Zbrojna" 2013, nr 11(811), s. 26.
[284] A. Kozłowski, *NATO wobec wyzwań*…, *op. cit.*, s. 3.

okoliczności sprawiają, że problematyka zagrożeń cyberprzestrzeni jest dla Traktatu Północnoatlantyckiego nadal szczególnie ważna[285].

Pierwsze kompleksowe regulacje NATO w zakresie cyberbezpieczeństwa przyjęte zostały na szczycie w Pradze, który odbył się w 2002 roku. Przyjęto wówczas istotny dla tej problematyki dokument, czyli „Program Obrony Cybernetycznej" (ang. *The Cyber Defence Program)* oraz powołano zespół[286], którego działania skupione są na wysokiej zdolności do reagowania na incydenty komputerowe (ang. *NATO Computer Incident Response Capability* – NCIRC)[287].

Inicjatorami tych działań byli przede wszystkim Amerykanie. O przyjęcie rozwiązań ukierunkowanych na zabezpieczenie cyberprzestrzeni NATO apelował zarówno ówczesny prezydent Stanów Zjednoczonych – George W. Bush, jak i sekretarz obrony tego państwa – Donald Rumsfeld. Zadaniem zespołu NCIRC stało się wykrywanie i unieszkodliwianie złośliwego oprogramowania w systemach i sieciach NATO (można zauważyć, że charakter pracy oraz funkcje tego zespołu zbliżone były do działalności zespołów CERT). *The Cyber Defence Program* był zaś wszechstronnym planem ukierunkowanym na usprawnienie zdolności NATO w zakresie obrony przed cyberatakami[288].

Skutkiem ataku cybernetycznego w Estonii było podjęcie decyzji o zapoczątkowaniu przez państwa NATO aktywnych działań zmierzających do przeciwdziałania i zapobiegania zagrożeniom tego rodzaju. W konsekwencji na początku 2008 roku przyjęto dokument o nazwie „Strategia Obrony Cybernetycznej" (ang. *The Policy on Cyber Defence*)[289]. W maju tego samego roku w Brukseli szefowie Sztabów Generalnych Estonii, Litwy, Łotwy, Niemiec, Hiszpanii, Włoch i Słowacji przez Sojusznicze Dowództwo podpisali dokument dotyczący *Transformacji memorandum w sprawie utworzenia Centrum Kompetencyjnego ds. Obrony Teleinformatycznej* (ang. *The Concept for Cooperative Cyber Defense Centre of Excellence* – CCD-COE)[290] w Tallinie. Pięć miesięcy później Centrum zyskało od Rady Północnoatlantyckiej akredytację jako *The NATO Centre of Excellence*, a także sta-

[285] J. Dereń, A. Rabiak, *NATO a aspekty…*, *op. cit.*, s. 213.
[286] Opisany w dalszej części pracy.
[287] *Zapobieganie i zwalczanie terroryzmu. Cyberterroryzm*, online – http://www.msz.gov.pl/pl/polityka_zagraniczna/polityka_bezpieczenstwa/zwalczanie_terrory-zmu_miedzynarodowego/zapobieganie_i_zwalczanie_terroryzmu/page_30058?printMode=true [dostęp: 08.09.2017].
[288] A. Kozłowski, *NATO wobec wyzwań…*, *op. cit*., s. 2-3.
[289] *Cyber defence*, online – http://www.nato.int/cps/en/natohq/topics_78170.htm [dostęp: 08.09.2017].
[290] *NATO Cooperative Cyber Defence Centre of Excellence*, online – https://ccdcoe.org/ [dostęp: 08.09.2017].

tus *The International Military Organization*. W 2008 roku utworzono także Radę NATO ds. Zarządzania Cyberobroną (ang. *The Cyber Defence Management Board* – CDMB*)*[291].

Kolejne regulacje z zakresu cyberbezpieczeństwa włączone zostały do „Koncepcji Strategicznej NATO" przyjętej w listopadzie 2010 roku. W dokumencie tym zagrożenia cybernetyczne uznano za jedne z podstawowych zagrożeń środowiska bezpieczeństwa Sojuszu Północnoatlantyckiego. Zwrócono uwagę, iż ataki tego rodzaju stają się coraz lepiej zorganizowane oraz coraz bardziej dotkliwe dla administracji rządowych, biznesu, gospodarki, a potencjalnie również dla transportu, sieci dostaw i innej infrastruktury krytycznej. Podkreślono, że ataki cybernetyczne osiągnąć mogą poziom, którego przekroczenie zagraża dobrobytowi, stabilności oraz bezpieczeństwu poszczególnych państw przynależnych do NATO oraz całej Wspólnoty Euroatlantyckiej. W analizowanym dokumencie, jako potencjalne źródło ataków wskazano obce służby wywiadowcze i siły wojskowe oraz zorganizowane grupy terrorystyczne, ekstremistyczne i przestępcze[292].

W kontekście powyższego stanowiska, Sojusz Północnoatlantycki w „Koncepcji strategicznej NATO" przyjął odpowiedzialność za obronę swoich członków również w zakresie cyberzagrożeń. W dokumencie tym została zawarta deklaracja, zgodnie z którą NATO gwarantuje, że Sojusz Północnoatlantycki dysponować będzie pełnym zakresem zdolności koniecznych do odstraszania oraz obrony przed jakimkolwiek zagrożeniem dla bezpieczeństwa jego państw członkowskich. Środkiem do osiągnięcia tego celu są m.in.:

- stałe rozwijanie możliwości wykrywania, zapobiegania i obrony przez atakami cybernetycznymi a co za tym idzie również nieustanne uświadamianie społeczności o konsekwencjach, które za sobą pociągają;
- odtwarzanie zdolności po wystąpieniu ataków cybernetycznych, w tym przy wykorzystaniu procesu planowania NATO na rzecz poprawy i koordynacji narodowych zdolności w obszarze obrony cybernetycznej.

Ponadto w koncepcji strategicznej zadeklarowano włączenie instytucji NATO do scentralizowanego systemu ochrony cybernetycznej oraz zintegrowanie systemu monitorowania, reagowania i ostrzegania cybernetycznego Sojuszu Północnoatlantycki z państwami członkowskimi[293].

[291] A. Kozłowski, *NATO wobec wyzwań…*, *op. cit*., s. 3.
[292] M. Adamczuk, *Ewolucja strategii i metod…*, *op. cit.*, s. 211-214.
[293] *Ibidem,* s. 208.

W 2011 roku ministrowie obrony państw członkowskich Sojuszu Północnoatlantyckiego przyjęli „Politykę NATO w obszarze cyberobrony" (ang. *The NATO Policy on Cyber Defence*) wraz z planem jej realizacji (ang. *The Cyber Defence Action Plan*). Celem obydwu, wymienionych dokumentów było zwiększenie operacyjnych oraz politycznych zdolności Sojuszu Północnoatlantyckiego oraz pomocy dla jego członków. Głównymi elementami przyjętej polityki uczyniono:

- uświadomienie decydentom, że zagwarantowanie cyberobrony jest konieczne z perspektywy wypełniania przez NATO misji obrony kolektywnej i zarządzania kryzysowego;
- ochronę i zwalczanie zagrożeń dla krytycznych systemów państw członkowskich oraz całego NATO;
- zaimplementowanie rozwiązań mających na celu wzmocnienie cyberobrony;
- centralizację ochrony sieci Sojuszu Północnoatlantyckiego;
- wspomaganie państw członkowskich w procesie osiągania minimalnego wymagalnego poziomu cyberobrony, który zapewniać będzie zmniejszenie podatności infrastruktury krytycznej na cyberataki;
- współpracę z międzynarodowymi organizacjami, sektorem prywatnym oraz przedstawicielami świata nauki[294].

W celu zaimplementowania powyższych postanowień, Rada NATO ds. Zarządzania Cyberobroną podpisała protokół ustaleń z przedstawicielami państw członkowskich Sojuszu. Na tej podstawie przedkładają oni Radzie Północnoatlantyckiej coroczne raporty z postępów we wdrażaniu uzgodnionych zaleceń. Potwierdzeniem znaczenia bezpieczeństwa cyberprzestrzeni dla NATO było także zwiększenie wydatków Sojuszu Północnoatlantyckiego na ten cel. Już w kolejnym roku po przyjęciu polityki w zakresie cyberobrony, wydatki na ten cel wyniosły niemal 60 mln euro. Środki przeznaczone zostały przede wszystkim na wzmocnienie zdolności zespołu NCIRC, dzięki zainstalowaniu dodatkowych sensorów mających za zadanie wykrywać zagrożenia dla serwerów i sieci NATO. Dodatkowo powołano do życia zespół mający za zadanie wyłącznie tworzenie ocen zagrożeń[295].

W 2013 r. odbyło się pierwsze spotkanie szefów resortów obrony państw NATO, które w całości poświęcono zagadnieniom cyberbezpieczeństwa. Podstawowym wnioskiem wyciągniętym z obrad była decyzja o konieczności wzmocnienia bezpieczeństwa wszystkich sieci używanych w NATO. Okoliczności te są bez wątpienia przejawem wzrostu znaczenia roli cyberbezpieczeństwa w obszarze dotyczącym kwestii bezpieczeństwa Sojuszu Północnoatlantyckiego.

[294] A. Kozłowski, *NATO wobec wyzwań…*, *op. cit.*, s. 5.
[295] *Ibidem*, s. 5.

W 2014 roku przyjęto inny ważny dokument NATO z zakresu cyberbezpieczeństwa – „Wzmocnioną Politykę Cyberobrony" (ang. *Enhanced Cyber Defense Policy*). Uwzględniono w nim m.in. potwierdzenie Sojuszu Północnoatlantyckiego dotyczącego tego, iż istniejące reguły prawa międzynarodowego obowiązują także w świecie wirtualnym. Podkreślono także, że ataki cybernetyczne powodować mogą zniszczenia porównywalne do zniszczeń będących skutkiem konwencjonalnych działań. W konsekwencji państwa Sojuszu Północnoatlantyckiego stanęły na stanowisku, że wymienione cyberataki uzasadniać mogą powołanie się na Artykuł 5[296] Traktatu Waszyngtońskiego[297]. W opisywanym dokumencie zwrócono również uwagę, że za obronę własnych systemów teleinformatycznych odpowiadają same państwa członkowskie, zaś NATO odpowiedzialne jest za obronę swoich sieci. Kolejnym efektem obrad prowadzonych na szczycie w 2014 roku było przyjęcie „Programu Partnerstwa z Sektorem Przemysłu Cybernetycznego" (ang. *NATO Industry Cyber Partnership*). Była to pierwsza inicjatywa Organizacji Paktu Północnoatlantyckiego zawiązania współpracy z podmiotami sektora prywatnego. Głównym zadaniem programu była poprawa cyberobrony łańcucha dostaw oprogramowania i sprzętu komputerowego, prowadzenie wzajemnych szkoleń oraz wymiana informacji i dobrych praktyk.

Współcześnie można mówić już o wieloobszarowej, zintegrowanej obronie cyberprzestrzeni Sojuszu Północnoatlantyckiego. Jednym z obszarów, w których NATO doskonali zdolności organizacyjne, proceduralne oraz zdolności dotyczące interoperacyjności i wymogów standaryzacyjnych są ćwiczenia w zakresie cyberochrony[298]. Udział w tego rodzaju manewrach biorą kraje członkowskie oraz kraje partnerskie, służby specjalne, formacje wojskowe czy niezależni obserwatorzy. Realizując wieloetapowe zadania, zespoły odpowiedzialne za wykrywanie i zwalczanie cyberzagrożeń podnoszą swoje kompetencje w tej dziedzinie oraz nawiązują międzynarodowe kontakty[299]. Do najbardziej znanych operacji przeprowadzanych w środowisku wirtualnym należą *Locked Shields* oraz *Cyber Coalition.* Ich scenariusze opierają się na symulowaniu konfliktu w cyberprzestrzeni przez dwie drużyny. Każda z nich dysponuje jedynie ogólnodostępnymi, standardowymi narzędziami, bez możliwości przygotowania wcześniej

[296] Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. 2000 nr 87 poz. 970).
[297] Szerzej w dalszej części pracy.
[298] J. Dereń, *Asymetryczność wyzwaniem dla bezpieczeństwa XXI wieku* [w:] *Biblioteka Wiedzy o Bezpieczeństwie. Metodologia badań bezpieczeństwa narodowego*. *Tom III*, red. P. Sienkiewicz, M. Marszałek, H. Świeboda, Akademia Obrony Narodowej, Warszawa 2012, s. 115.
[299] J. Dereń, A. Rabiak, *NATO a aspekty*…, *op. cit.,* s. 215.

specjalistycznej cyberobrony. Ćwiczenia te mają pomóc Sojuszowi Północnoatlantyckiemu w sprawdzeniu strategii, doktryn oraz mechanizmów reagowania w przypadku zaistnienia kryzysu. Służą one także wzmacnianiu współpracy między członkami NATO. Ćwiczenia przygotowywane są w oparciu o doświadczenia cyberataków na Estonię. Należy dodać, że Sojusz Północnoatlantycki zmierza do coraz głębszego integrowania ćwiczeń konwencjonalnych (wojsk lądowych, marynarki, sił powietrznych) oraz ćwiczeń w obszarze cyberprzestrzeni[300].

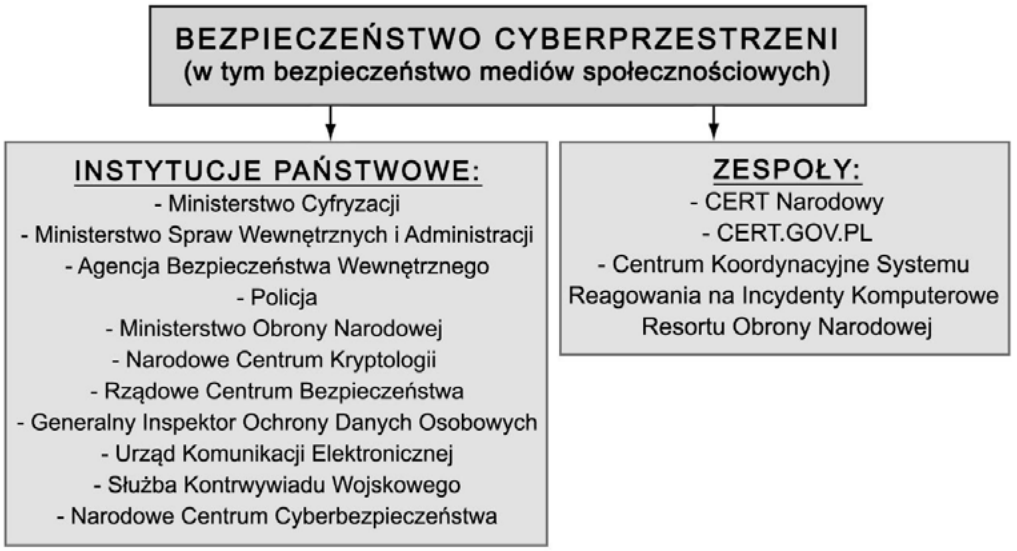
Cyberbezpieczeństwo jest również ważnym elementem rozwijanej przez NATO koncepcji tzw. *Smart Defense*. Pierwszym projektem z tego obszaru był „Wielonarodowy rozwój zdolności cyberobronnych" (ang. *The Multinational Cyber Defense Capability Development*). Celem podjętych działań było usprawnienie wymiany informacji technicznych i promowanie świadomości zagrożeń w cyberprzestrzeni. W ramach drugiego projektu zatytułowanego „Platforma wymiany informacji o zagrożeniach w cyberprzestrzeni" (ang. *The Malware Information Sharing Platform*) podjęto działania ukierunkowane na umożliwienie państwom Sojuszu Północnoatlantyckiego wymiany informacji dotyczących charakterystyki technicznej złośliwych programów bez konieczności przekazywania danych w szczegółach o metodyce prowadzonych z ich wykorzystaniem ataków. W ramach *Smart Defense* prowadzono także działania o charakterze edukacyjnym i szkoleniowym.

6.2. Instytucje i zespoły odpowiadające za bezpieczeństwo w cyberprzestrzeni

6.2.1. Narodowe instytucje i zespoły odpowiadające za bezpieczeństwo w cyberprzestrzeni

Z punktu widzenia problematyki szeroko rozumianego bezpieczeństwa narodowego, można wskazać instytucje (organy państwowe) oraz zespoły wpływające na zachowanie wysokiego poziomu w obszarze bezpieczeństwa cyberprzestrzeni RP (rysunek 15).

[300] A. Kozłowski, *NATO wobec wyzwań…*, *op. cit.*, s. 6.



Rysunek 15. Instytucje państwowe oraz zespoły realizujące zadania bezpieczeństwa cyberprzestrzeni RP
Źródło: opracowanie własne.

Do instytucji państwowych zajmujących się bezpieczeństwem cyberprzestrzeni RP należą:

- **Ministerstwo Cyfryzacji** (MC) – odpowiadające za takie obszary, jak: telekomunikacja, informatyzacja oraz społeczeństwo informacyjne[301];
- **Ministerstwo Spraw Wewnętrznych i Administracji** (MSWiA) – dopowiada za takie działy, jak: ochrona bezpieczeństwa i porządku publicznego, zarządzanie kryzysowe, obrona cywilna, czy też ochrona granicy państwa. Organ ten sprawuje nadzór nad takimi formacjami, jak np. Policja, Straż Graniczna, Państwowa Straż Pożarna, Biuro Ochrony Rządu. Dlatego też obszar ochrony bezpieczeństwa i porządku publicznego jest rozumiany przede wszystkim jako wszelkiego rodzaju działania związane ze ściganiem przestępczości w cyberprzestrzeni;
- **Agencja Bezpieczeństwa Wewnętrznego** (ABW) – do głównych zadań agencji należy w szczególności rozpoznawanie, zapobieganie oraz zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa, a także obronność. ABW realizuje zadania służby ochrony państwa oraz krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych. Od lipca 2016 roku do zadań ABW należy również rozpoznawanie, zapobieganie i wykrywanie zagrożeń mają-

[301] https://mc.gov.pl/o-nas [dostęp: 29.08.2017].

cych wpływ na bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa: systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej (art. 5, pkt. 1–5 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)[302].

- **Policja** – jest umundurowaną i uzbrojoną formacją przeznaczoną do ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego. Jednym z głównych obszarów ścigania przestępstw jest obszar przestępczości w cyberprzestrzeni. Zaznaczenia wymaga, że od 2014 roku w Policji powoływane są specjalne wydziały do walki z cyberprzestępczością. W jej ramach funkcjonuje Biuro do Walki z Cyberprzestępczością, które w szczególności[303]:
  - nadzoruje, koordynuje i wspiera ukierunkowane na zwalczanie cyberprzestępczości działania prowadzone przez komendy wojewódzkie Policji w zakresie czynności operacyjno-rozpoznawczych oraz współdziałania z Centralnym Biurem Śledczym (CBŚ) Policji w tym zakresie;
  - prowadzi czynności operacyjno-rozpoznawcze pozostające we właściwości CBŚ;
  - inicjuje i prowadzi współpracę z organami administracji rządowej, sądami, prokuraturami, instytucjami państwowymi, a także podmiotami prywatnymi w zakresie zadań pozostających we właściwości CBŚ;
  - prowadzi współpracę międzynarodową oraz współdziała z Biurem Międzynarodowej Współpracy Policji,
  - prowadzi całodobową służbę mającą na celu koordynowanie działań Policji w zakresie zagrożeń przestępstwami w sieci Internet, ich zwalczania oraz współdziałania jednostek organizacyjnych Policji z krajowymi i zagranicznymi organami oraz podmiotami pozapolicyjnymi;
  - prowadzi konsultacje techniczne, inicjuje i wspiera badania oraz projekty, a także współpracuje z podmiotami krajowymi i zagranicznymi, zmierzając do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z cyberprzestępczością;

[302] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r. nr 29, poz. 154).
[303] http://www.policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html [dostęp: 29.08.2017].

- **Ministerstwo Obrony Narodowej** (MON) – kluczowym dokumentem opisującym podejście Ministerstwa Obrony Narodowej do problematyki cyberbezpieczeństwa jest analizowana wcześniej „Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022", która jako jeden z celów określa przeciwdziałanie i zwalczanie negatywnych zjawisk w cyberprzestrzeni. W ramach MON działają zespoły odpowiedzialne za incydenty komputerowe, tj. System Reagowania na Incydenty Komputerowe – RON. Realizuje on zadania w zakresie koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych Resortu Obrony Narodowej[304]. Warto również zwrócić uwagę na zadania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni. Jest upoważniony do[305]:
  - koordynowania przedsięwzięć przewidzianych dla MON w sprawach bezpieczeństwa cyberprzestrzeni, w odniesieniu do wszystkich komórek organizacyjnych MON i jednostek organizacyjnych resortu obrony narodowej, z wyłączeniem zadań zastrzeżonych dla pełnomocników do spraw ochrony informacji niejawnych określonych odrębnymi przepisami;
  - inicjowania oraz wspierania działań komórek organizacyjnych MON i jednostek organizacyjnych resortu obrony narodowej w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni resortu obrony narodowej;
  - sprawowania nadzoru nad realizacją zadań wynikających z aktów prawnych, polityk i programów rządowych dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni;
  - współpracy ze Służbą Kontrwywiadu Wojskowego w zakresie kreowania spójnego, jednolitego i efektywnego systemu zarządzania bezpieczeństwem cyberprzestrzeni resortu obrony narodowej;
  - ustanowienia (z zachowaniem warunków bezpieczeństwa informacji oraz kompetencji komórek organizacyjnych MON i jednostek organizacyjnych resortu obrony narodowej), spójnego, współdzielonego systemu informacyjnego o bieżącym stanie oraz zagrożeniach cyberprzestrzeni;
- **Narodowe Centrum Kryptologii** (NCK) – zajmuje się w szczególności badaniami i wdrażaniem rozwiązań kryptograficznych na potrzeby administracji publicznej i wojska;

[304] http://srnik.wp.mil.pl/pl/index.html [28.08.2017].

[305] Decyzja Nr 38/MON Ministra Obrony Narodowej z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni (Dz.Urz. MON z 2012 r., poz. 52, pkt. 3, ppkt. 1-5).

- **Rządowe Centrum Bezpieczeństwa** (RCB) – pełni ważną rolę w obszarze zarządzania kryzysowego i ochrony infrastruktury krytycznej. Podstawą prawną jego działań jest ustawa o zarządzaniu kryzysowym (art. 3 ustawy o zarządzaniu kryzysowym)[306]. Uściślenia wymaga, że infrastruktura sieci teleinformatycznych i łączności uznawana jest za krytyczną dla funkcjonowania państwa. Do podstawowych zadań Rządowego Centrum Bezpieczeństwa należy analiza zagrożeń oraz opracowywanie rozwiązań mających zastosowanie w sytuacjach kryzysowych, a także koordynowanie przepływu informacji o istniejących zagrożeniach[307];
- **Urząd Ochrony Danych Osobowych** (UODO) – pełni rolę organu dbającego o ochronę danych osobowych w kraju, jak również harmonizację przepisów krajowych z regulacjami Unii Europejskiej. Uściślenia wymaga, że w ten sposób odgrywa rolę w kwestii danych osobowych przetwarzanych przez przedsiębiorców telekomunikacyjnych;
- **Urząd Komunikacji Elektronicznej** (UKE) – pełni on rolę swoistego regulatora rynku telekomunikacyjnego oraz pocztowego. Organ ten w kontekście bezpieczeństwa w cyberprzestrzeni zapewnia właściwą implementację prawa telekomunikacyjnego[308];
- **Służba Kontrwywiadu Wojskowego** (SKW) – dokonuje certyfikacji środków ochrony elektromagnetycznej, certyfikacji urządzeń i narzędzi kryptograficznych, certyfikacji urządzeń i narzędzi służących do realizacji zabezpieczenia teleinformatycznego, szkoleń specjalistycznych dla administratorów systemów teleinformatycznych i inspektorów bezpieczeństwa teleinformatycznego[309];
- **Narodowe Centrum Cyberbezpieczeństwa** (NCC) – jego kluczowym zadaniem jest koordynacja działań państwa w walce ze zjawiskiem cyberterroryzmu. Centrum to działa w układzie pełnozmianowym (24 h/dobę), co zdecydowanie umożliwia skuteczną i zarazem szybką reakcję na potencjalne zagrożenia w postaci ataków w sieci. Omawiana jednostka działa w strukturach Naukowej i Akademickiej Sieci Komputerowej. Ponadto w jej skład wchodzą cztery piony: badawczo-rozwojowy, operacyjny, szkoleniowy oraz analityczny. NCC będzie jednostką nadzorującą bezpieczeństwo cyberprzestrzeni w Polsce. Będzie się ono zajmowało także: przygotowywaniem planów ewentualnościowych, organizowaniem szkoleń, a także ćwiczeń

[306] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.
[307] http://rcb.gov.pl/o-rcb/ [dostęp: 29.08.2017].
[308] https://www.uke.gov.pl/kompetencje-972 [dostęp: 29.08.2017].
[309] http://www.skw.gov.pl/zadania.html [dostęp: 29.08.2017].

dla osób odpowiadających za bezpieczeństwo administracji państwowej oraz wdrożeniem minimalnych wymagań bezpieczeństwa dla poszczególnych instytucji państwowych[310].

Oprócz organów w polskim systemie prawnym istnieją i funkcjonują zespoły, sprawujące opiekę nad obszarem cyberbezpieczeństwa. Wśród nich możemy wyróżnić:

- CERT.GOV.PL – zespół działający w ramach Agencji Bezpieczeństwa Wewnętrznego, odpowiedzialny za ochronę systemu administracji państwowej[311];
- Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej (CK SRnIK) – zwane także wojskowym CERT-em, do którego głównych zadań należą: koordynacja procesu reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych resortu MON; prowadzenie działalności profilaktycznej, przez opracowanie zaleceń zapobiegających występowaniu incydentów; analiza informacji o zdarzeniach oraz tworzenie na ich podstawie raportów; udział w grupach roboczych NATO zajmujących się problematyką cyberochrony[312];
- CERT[313] Narodowy – jego głównym zadaniem jest szybkie reagowanie na incydenty zachodzące w cyberprzestrzeni. W ramach tej jednostki dyżury pełnią specjaliści z zakresu energetyki, bankowości czy też telekomunikacji. Ich zadaniem jest wymienianie się informacjami na temat zagrożeń w sieci, a także – w razie konieczności – podejmowanie decyzji w przedmiocie działań zmierzających do zwalczania zjawiska przestępczości w Internecie;
- CERT – działające w ramach poszczególnych operatorów telekomunikacyjnych, tj. CERT Polska oraz CERT Orange Polska.

Omawiając instytucje państwowe oraz zespoły, których zadaniem jest zachowanie wysokiego poziomu bezpieczeństwa w cyberprzestrzeni, konieczne jest poruszenie wspomnianej już problematyki **dyrektywy NIS** (ang. *Network and Information Security Directive*)[314], obejmującej wymogi cyberbezpieczeństwa dla firm z kluczowych sektorów gospodarki. Dyrek-

[310] B. Józefiak, *Na bazie CERT Polska rusza Narodowe Centrum Cyberbezpieczeństwa*, online – http://www.cyberdefence24.pl/398863,na-bazie-cert-polska-rusza-narodowe-centrum-cyberbezpieczenstwa

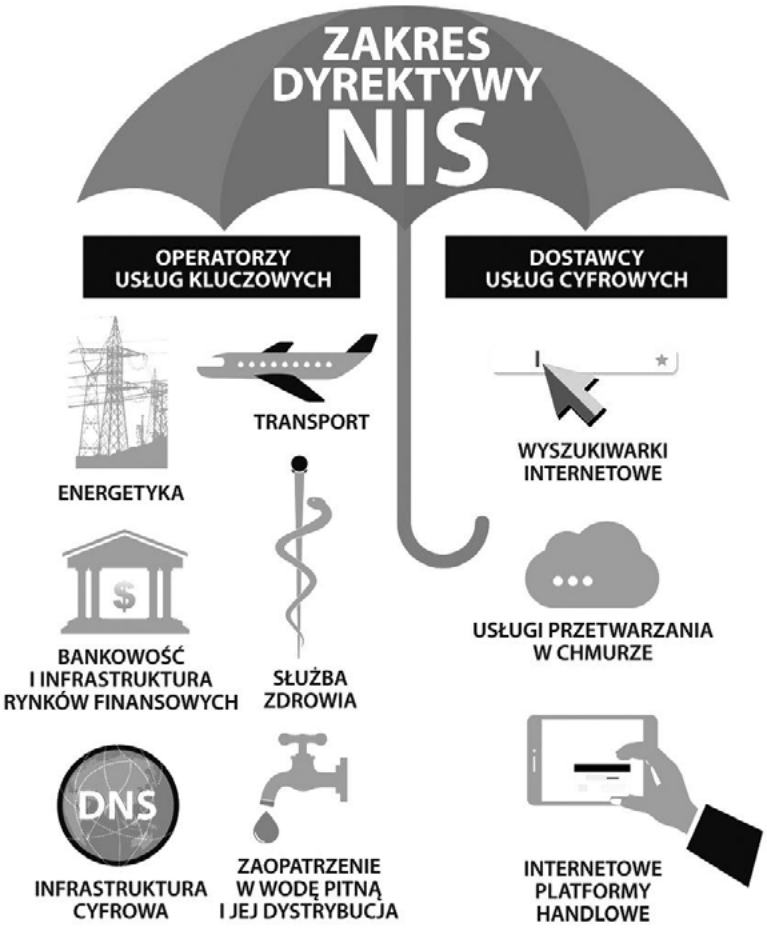
[311] M. Młotek, M. Siedlarz, *Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 4, s. 158-165.

[312] T. Dąbrowski, T. Strycharek, *Rola i zadania polskiego CERT-u wojskowego*, WBBŁiI, Warszawa 2016, s. 7.

[313] Nazwa CERT zespołu pochodzi od akronimu anglojęzycznego – ang. *Computer Emergency Response Team*.

[314] *Dyrektywa Parlamentu i Rady…*, *op. cit.*

tywa NIS wskazuje na obowiązki z zakresu bezpieczeństwa, jakim podlegają operatorzy m.in. takich usług, jak: energetyka, finanse czy też opieka zdrowotna, czyli podmiotów odpowiedzialnych za bezpieczeństwo narodowe, a także dostawców usług cyfrowych: internetowe platformy handlowe, wyszukiwarki, usługi przetwarzania w chmurze (rysunek 16). Działania takie służą poszerzeniu współpracy państw członkowskich w zakresie cyberbezpieczeństwa.



Rysunek 16. Zakres dyrektywy NIS
Źródło: opracowanie własne.

Wdrożenie dyrektywy ma obejmować kompleksowe podejście na poziomie Unii Europejskiej, obejmujące wymagania dotyczące budownictwa i planowania wspólnych minimalnych zdolności, wymianę informacji, współpracę oraz wspólne wymogi w ramach bezpieczeństwa dla operatorów usług kluczowych i dostawców usług cyfrowych.

Cele dyrektywy NIS muszą zostać osiągnięte przy pomocy:

- ustanowienia obowiązków dla państw członkowskich dotyczących przyjęcia krajowej strategii cyberbezpieczeństwa;
- utworzenia sieci Zespołów Reagowania na incydenty bezpieczeństwa komputerowego tzw. CSIRT;
- utworzenia grupy współpracy zapewniającej strategiczną kooperację, jak również wymianę informacji;
- sprecyzowania wymogów dotyczących bezpieczeństwa sieci i informacji, jak również zgłaszania incydentów;
- ustanowienia obowiązków, które dotyczą wyznaczania przez państwa członkowskie organów krajowych, punktów kontaktowych oraz CSIRT, którym powierzone zostaną zadania związane z cyberbezpieczeństwem.

Dyrektywa NIS dzieli prawa i obowiązki związane z cyberbezpieczeństwem pomiędzy dwa podmioty – prawne i publiczne. Akt ten ma za zadanie osiągnięcie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii Europejskiej poprzez ustalenie przekazu informacji o pojawiających się zagrożeniach pomiędzy państwami UE oraz podmiotami sektora krytycznego. Ważne jest również unormowanie standardów ochrony.

Istotną rolę we wdrążaniu dyrektywy NIS będzie pełnić, opisana we wcześniejszej części pracy, Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA). Jej rolą, w tym zakresie, jest koordynowanie współpracy między państwami członkowskimi w obszarze cyberbezpieczeństwa. Co ważne, państwa członkowskie zobligowane są zapewnić, aby operatorzy usług kluczowych, a także dostawcy usług cyfrowych, zgłaszali właściwemu organowi krajowemu lub do CSIRT incydenty dotyczące bezpieczeństwa, zaistniałe w ich sieciach informatycznych. Organy krajowe powinny także dysponować takimi narzędziami, aby móc zweryfikować, czy podmioty przestrzegają realizacji obowiązków, o których mowa w Dyrektywie NIS[315]

Należy zauważyć, że od momentu obowiązywania dyrektywy (sierpień 2016 roku) państwa członkowskie mają 21 miesięcy na implementację jej założeń do przepisów prawa krajowego. Dodatkowo obliguje ich okres pół roku, służący zaprezentowaniu dostawców kluczowych usług. Obecnie trudno jest stwierdzić, czy wdrożenie dyrektywy w ustawodawstwo faktycznie będzie efektywne i wpłynie na wzrost cyberbezpieczeństwa. Nie ulega jednak wątpliwości, że działania podejmowane przez UE są prawidłowe i konieczne. Wydaje się jednak, że rozmiar wyzwań związanych z cyberbezpieczeństwem oraz wzrost zagrożeń, przewyższają możliwości

[315] *Ibidem.*

legislacyjne zarówno w skali krajowej, jak i na poziomie międzynarodowym.

6.2.2. Instytucje i zespoły NATO odpowiadające za bezpieczeństwo w cyberprzestrzeni

Podejmując zagadnienie dotyczące organów państwowych oraz zespołów odpowiadających za bezpieczeństwo w cyberprzestrzeni należy poruszyć kwestie odnoszące się do NATO. Sojusz Północnoatlantycki, będący instytucją wchodzącą w skład systemu bezpieczeństwa międzynarodowego, posiada w swoich strukturach wyspecjalizowane jednostki, których zadaniem jest nadzorowanie ochrony transmisji danych. Wśród nich można wyróżnić:

- **Zespół Reagowania na Incydenty Komputerowe NATO** (ang. *NATO Computer Incident Response Capability* – NCIRC) – to podstawowa instytucja NATO działająca w obszarze cyberbezpieczeństwa (na najniższym szczeblu). Zajmuje się ona wykrywaniem oraz zwalczaniem złośliwych programów, a także informowaniem o pojawiających się w sieciach NATO nowych rodzajach zagrożeń;
- **Rada NATO ds. Zarządzania Cyberobroną** (ang. *NATO Cyber Defence* Management *Board* – CDMB) – jest podmiotem odpowiedzialnym za koordynację cyberobrony Paktu Północnoatlantyckiego oraz powiązanych z nim organizacji. W jego skład wchodzą specjaliści z zakresu planowania technicznego i operacyjnego odpowiedzialni za cyberobronę. Rada zajmuje się także wspieraniem państw członkowskich w zakresie prac nad ulepszaniem narodowych systemów bezpieczeństwa cyberprzestrzeni;
- **DPPCRF** (ang. *Defense Policy and Planning Committee in Reinforced Format*) – instytucja stworzona w celu koordynowania i nadzorowania prac CDMB;
- **Centrum Doskonalenia Obrony przed Cyberatakami** (ang. *Cooperative Cyber Defence Centre of Excellence* – CCDCoE) – instytucja współpracująca z NATO, która uzyskała akredytację Sojuszu w strukturze sił NATO. Stanowi ona forum wymiany informacji, edukacji, konsultacji, szkoleń, badań oraz wdrażania projektów pozwalających sprawnie i szybko zabezpieczać systemy teleinformatyczne. Nie jest finansowana z budżetu NATO, lecz sponsorowana bezpośrednio przez kraje członkowskie. Kraje zapewniające środki na jej działanie premiowane są w zakresie korzystania z zasobów CCDCoE. Pełni ona funkcję *think-tank*-u[316] Sojuszu Północnoatlantycki w zakresie inter-

[316] ***Think-tank*** (zbiornik myśli) – „to niezależny komitet doradczy o charakterze organiza-

dyscyplinarnych badań dotyczących bezpieczeństwa;

- **CERT** (ang. *Computer Emergency Response Teams*) – są to organizacje działające w poszczególnych państwach członkowskich, zajmujące się nadzorowaniem ruchu internetowego oraz natychmiastowym reagowaniem w przypadku pojawienia się zagrożenia, w obszarze wykonywanych działań podejmują one współpracę z NATO;
- **Grupa Szybkiego Reagowania w Cyberprzestrzeni** (ang. *Rapid Reaction Team* – RRT) – to zespół powołany w celu udzielania pomocy technicznej przy atakach oraz przy przywracaniu prawidłowego funkcjonowania systemów teleinformatycznych. RRT wykorzystywane są do wsparcia członka Sojuszu Północnoatlantycki, który stał się ofiarą cyberataku. Odgrywają one także istotną rolę polityczną, będąc świadectwem tego, że Organizacja Paktu Północnoatlantyckiego jest solidarna z zaatakowanymi członkami oraz przychodzi im z pomocą w przypadku cyberataku. Problemem związanym z funkcjonowaniem RRT jest konieczność ich szybkiego przemieszczania oraz zapoznawania się z zaatakowanymi sieciami (co wynika z tempa samych cyberataków);
- **Komitet Cyberobrony** (ang. *Cyber Defense Committee* – CDC) – jego zadaniem jest ogólne zarządzanie polityką bezpieczeństwa Sojuszu Północnoatlantycki w cyberprzestrzeni, a także sprawdzanie i kierowanie procesem wdrażania rekomendacji polityki cyberobrony NATO (ang. *Cyber Defense Policy* – CDP) przez państwa członkowskie[317].

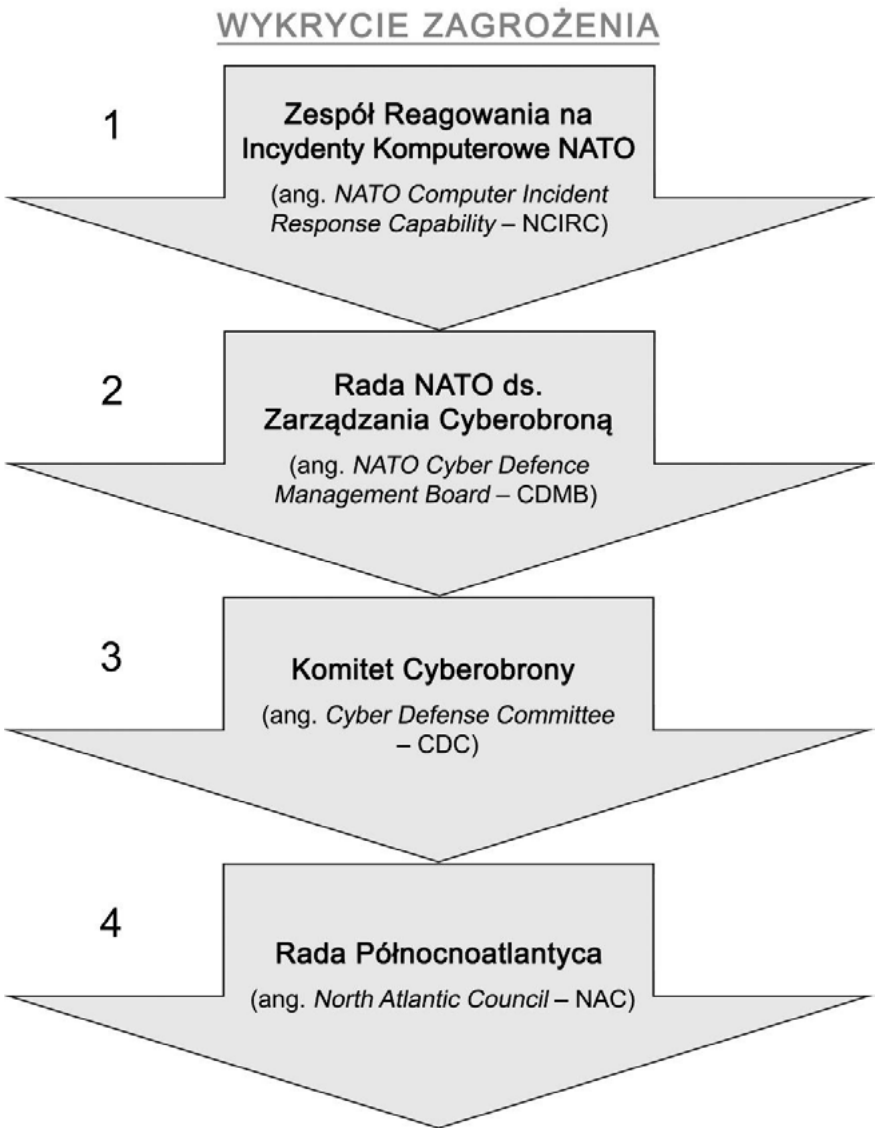
Czteroetapowy schemat reagowania na zagrożenia cybernetyczne przez NATO opiera się na ustalonej hierarchii – rysunek 17.

W pierwszej kolejności zagrożenie zostaje wykryte przez Zespół Reagowania na Incydenty Komputerowe NATO. W kolejnym etapie (jeśli zagrożenie może mieć znaczenie polityczne) informacje przekazywane są do Rady NATO ds. Zarządzania Cyberobroną oraz do Komitetu Cyberobrony. Na końcu trafiają one do Rady Północnoatlantyckiej (ang. *North Atlantic Council* – NAC), jako najważniejszego organu decyzyjnego w NATO.

---

cji non-profit (nie skupionej na zysku), zajmujący się badaniami i analizami dotyczącymi spraw publicznych"
https://pl.wikiquote.org/wiki/Think_tank [dostęp: 30.01.2019].

[317] J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa…*, *op. cit.*, s. 215-216, A. Kozłowski, *NATO wobec wyzwań…*, *op. cit.*, s. 7.



Rysunek 17. Czteroetapowy schemat reagowania na zagrożenia cybernetyczne przez NATO

Źródło: opracowanie własne na podstawie
A. Kozłowski, *NATO wobec wyzwań…*, *op. cit.*, s. 8.

Fundamentem funkcjonowania NATO jest artykuł 5. Traktatu Waszyngtońskiego, stanowiący, iż „Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi, to każda z nich (…) udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie, jak i w porozumieniu z innymi Stronami, działania, jakie uzna za konieczne, łącznie z użyciem

siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego”[318]. W obliczu rosnącego znaczenia cyberzagrożeń istotną kwestią stało się rozstrzygniecie, czy artykuł ten stosowany może być w przypadku ataku cybernetycznego na jedno z państw Sojuszu Północnoatlantyckiego. W obliczu eskalacji ataków cybernetycznych godzących w członków Sojuszu NATO (np. cyberatak w Estonii z 2007 roku) kwestie te zostały zainicjowane w 2010 roku w „Strategicznej koncepcji NATO”, gdzie odnajdujemy odniesienie do tej problematyki „Ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej. Mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne”[319]. W tym samym dokumencie stwierdzono, że NATO w takiej sytuacji będzie „rozwijać dalej (…) możliwości zapobiegania, wykrywania, obrony przed atakami cybernetycznymi oraz odtwarzania zdolności po nich, w tym wykorzystując proces planowania NATO na rzecz wzmocnienia i koordynacji narodowych zdolności w dziedzinie obrony cybernetycznej, włączając instytucje NATO w scentralizowany system ochrony cybernetycznej oraz integrując system monitorowania, ostrzegania i reagowania cybernetycznego NATO z państwami członkowskimi”[320].

Aspekt wspólnej pomocy członkom Sojuszu Północnoatlantyckiego, w kontekście artykułu 5. Traktatu Waszyngtońskiego, został uregulowany podczas Szczytu NATO w Walii (w Newport), który odbył się 4-5 września 2014 r. Ustalono wtedy, że Rada Północnoatlantycka będzie każdorazowo podejmować decyzje o zastosowaniu art. 5 Traktatu Waszyngtońskiego, na podstawie analizy danego przypadku. Pod uwagę będą brane takie czynniki cyberataku, jak:

- **zasięg** – zastosowanie art. 5 Traktatu Waszyngtońskiego uzależnione będzie prawdopodobnie od tego, czy celem stało się jedno czy kilka państw NATO oraz jak wiele sektorów padło ofiarą działań cyberprzestępców;
- **czas trwania** – czy cały atak przeprowadzony został w obrębie jednej doby czy też stanowi on wielodniową sekwencję wyniszczających działań podejmowanych w cyberprzestrzeni NATO lub państwa

[318] Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r.
[319] *Koncepcja Strategiczna NATO z 2010 r.*, s. 206.
[320] *Ibidem*, s. 208.

członkowskiego;
- **skutki** – czy rezultatem cyberataku są szkody dotyczące: mienia, zdrowia i życia ludzkiego;
- **atrybucja** – czy za cyberatakiem stoi podmiot państwowy, czy też grupa niepowiązana z żadnym państwem, co do zasady Sojusz Północnoatlantycki reagował będzie jedynie w pierwszym wypadku[321].

Biorąc pod uwagę opisane wyżej kryteria, przyjąć można, że w praktyce powoływanie się na artykuł 5 Traktatu Waszyngtońskiego, nie będzie zjawiskiem częstym. Dotychczasowe doświadczenia przeprowadzonych cyberataków wskazują, że tego typu działania zwykle nie spełniają równocześnie kryteriów zasięgu, czasu trwania i skutków, zaś powiązanie atakujących z konkretnym państwem jest procesem trudnym i czasochłonnym. W praktyce jedynie w niewielu przypadkach udało się dowieść, że taki związek miał miejsce. Jako przykład podać można raport firmy Madiant dotyczący chińskiej jednostki szpiegowskiej 61398. Tu jednak zauważyć należy, że przygotowanie tego raportu zajęło specjalistom ponad dwa lata. Czas ten jest zdecydowanie za długi w kontekście rozważania zastosowania artykułu 5. Traktatu Waszyngtońskiego. Mimo opisanych okoliczności, nie można umniejszać roli deklaracji złożonej na koniec szczytu w Walii. Jej znaczenie – nawet jeśli w praktyce okaże się niewielkie – ma jednak także wymiar polityczny oraz odstraszający dla potencjalnych agresorów.

Znacznie mniej kontrowersyjna, a także bardziej doniosła praktycznie jest problematyka stosowania w przypadku cyberzagrożeń art. 4 Traktatu Waszyngtońskiego. Przepis ten daje sojuszniczym państwom możliwość konsultowania się zawsze, gdy w opinii któregokolwiek z nich dochodzi do zagrożenia jego integralności terytorialnej, niezależności politycznej lub bezpieczeństwa. Ta regulacja prawna może być podstawą takich użytecznych działań, jak wsparcie zaatakowanego państwa przez wysłanie zespołów CERT czy Grup Szybkiego Reagowania w Cyberprzestrzeni (RRT)[322].

Podsumowując rozważania dotyczące kwestii NATO zauważyć należy przede wszystkim ewolucję, jaka zaszła w obszarze podejścia NATO do problematyki zagrożeń w cyberprzestrzeni. Jeszcze niespełna dwie dekady temu, Sojusz Północnoatlantycki był całkowicie nieprzygotowany zarówno do odpierania cyberataków na własne systemy teleinformatyczne, jak i do udzielania w tym zakresie wsparcia państwom członkowskim. Kraje Organizacji Traktatu Północnoatlantyckiego przekonały się o tym po ataku serbskich hakerów w 1999 roku. Sytuacja ta pozwoliła na przeprowadzenie działań prewencyjnych – zwiększano potencjał obrony przed cyberzagrożeniami NATO w postaci stworzenia systemu instytucji NATO odpowia-

[321] A. Kozłowski, *NATO wobec wyzwań…*, *op. cit.*, s. 9.
[322] *Ibidem*, s. 10.

dających za cyberbezpieczeństwo Sojuszu Północnoatlantyckiego, z możliwością skorzystania z artykułu 5. Traktatu Waszyngtońskiego.

6.3. Uogólnienia i wnioski

Zapewnienie bezpieczeństwa cybernetycznego należy rozumieć jako proces długotrwały oraz bardzo złożony. Jego sukcesywne wdrażanie ma wpływ nie tylko na prawidłowe i nieprzerwane funkcjonowanie kluczowych elementów, takich jak infrastruktura krytyczna państwa, ale gwarantuje bezpieczny dostęp dla użytkowników Internetu do mediów społecznościowych. W Rzeczpospolitej Polskiej, w ujęciu strategicznym, najważniejszymi dokumentami kładącymi szczególny nacisk na aspekty związane z cyberbezpieczeństwem są: „Strategia bezpieczeństwa narodowego RP" oraz „Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022". Zawierają one wielowariantowe podejście do kwestii zapewnienia bezpiecznego korzystania z cyberprzestrzeni, również w kontekście mediów społecznościowych, od szczebla władzy centralnej do władzy regionalnej. Oprócz tego, ważną rolę pełnią opracowane na konferencji CYBERSEC PL 2016 rekomendacje dla Polski, podczas której rozważano możliwości, jakie oferuje przestrzeń cybernetyczna: państwu, Siłom Zbrojnym RP, sferze biznesowej oraz zastanawiano się, jakie działania trzeba będzie podjąć w przyszłości, by użytkowanie jej było bezpieczne i sprawne. Ponadto, należy zauważyć, że kwestia bezpieczeństwa polskiej cyberprzestrzeni jest rozwijana w aktach prawnych, takich jak: „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022", „Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej zaplanowaną na lata 2017-2022" i „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej".

Unia Europejska wdrożyła szereg rozwiązań organizacyjno-prawnych ukierunkowanych na poprawę bezpieczeństwa cyberprzestrzeni. Ramy działań określone zostały w dokumentach strategicznych. Na mocy dyrektywy NIS ustanowiono zaś wiele rozwiązań, które czynić mają państwa członkowskie i instytucje Wspólnoty Europejskiej mniej podatnymi na cyberzagrożenia. Należy do nich priorytetowy cel, jakim jest określenie obowiązków z zakresu cyberbezpieczeństwa, którymi mają podlegać operatorzy kluczowych usług, czyli np. infrastruktury krytycznej lub opieki medycznej. Powołano specjalistyczne instytucje realizujące zadania w tym zakresie. Ponadto, dyrektywa NIS zobowiązuje każde państwo członkowskie UE do wyznaczenia organu w celu ochrony bezpieczeństwa cybernetycznego i z jego pomocą opracowania odpowiedniej strategii Wiele uwagi zarówno w unijnych dokumentach strategicznych, jak i aktach prawnych

poświęcono właściwej integracji mechanizmów działających w poszczególnych państwach członkowskich z mechanizmami na poziomie wspólnotowym. Dodatkowo Unia Europejska (podobnie jak NATO) organizuje ćwiczenia w zakresie cyberobrony, które pomagają zwiększyć umiejętności reagowania w warunkach realnego zagrożenia.

Organizacja Traktatu Północnoatlantyckiego szczególną uwagę zwraca na problem szpiegostwa komputerowego, które mogłoby zostać nielegalnie wykorzystane przeciwko państwom członkowskim Sojuszu Północnoatlantyckiego, tym samym godząc w pozycję NATO jako gwaranta bezpieczeństwa. Pierwszą regulacją prawną, w ujęciu strategicznym, wydaną w celu ochrony systemów przed cyberszpiegostwem był „Program Obrony Cybernetycznej" (wraz z odpowiednimi komórkami wspomagającymi), którego działania skupione zostały wokół wysokiej zdolności do reagowania na incydenty komputerowe. Zakres wykonywanej działalności jest również bardzo zbliżony do zadań CERT. Kolejne dokumenty prawne rozszerzały, koordynowały i wspierały rozwój oraz wieloaspektowe podejście do kwestii cyberbezpieczeństwa, jak również cyberobrony na rzecz NATO i jego państw członkowskich. Należą do nich „Strategia Obrony Cybernetycznej" czy „Wzmocniona Polityka Cyberobrony". Oprócz aspektów prawnych, ważną kwestią mającą na celu zwiększenie świadomości społeczeństwa o wadze cyberzagrożeń jest rozwijana koncepcja *Smart Defense*, która w założeniu powinna przygotować państwa członkowskie na reagowanie w przypadku wysyłania do ich systemów m.in. złośliwego oprogramowania. Całokształt działań podejmowanych przez Sojusz Północnoatlantycki w kontekście szeroko rozumianego cyberbezpieczeństwa ma być archiwizowany w postaci corocznych raportów.

Ważnym aspektem pracy było wytypowanie, scharakteryzowanie i sklasyfikowanie instytucji i zespołów odpowiadających za bezpieczeństwo w cyberprzestrzeni za pomocą mediów społecznościowych. Instytucje i zespoły podzielono na dwie grupy: narodowe oraz działające na rzecz NATO. W odniesieniu do instytucji i zespołów narodowych należy wskazać na takich partycypantów, jak: Ministerstwa – Cyfryzacji, Bezpieczeństwa Wewnętrznego oraz Obrony Narodowej. Poza nimi za cyberprzestrzeń odpowiadają także: Policja, Narodowe Centrum Kryptologii, Rządowe Centrum Bezpieczeństwa, Generalny Inspektor Ochrony Danych Osobowych, Urząd Komunikacji Elektronicznej, Służba Kontrwywiadu Wojskowego, jak i Narodowe Centrum Cyberbezpieczeństwa. Do zespołów, których kompetencje dotyczą bezpieczeństwa cyberprzestrzeni, należą: CERT Narodowy, CERT.GOV.PL, a także Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe Resortu Ministerstwa Obrony Narodowej.

W ramach NATO, wyróżnić można 8 podmiotów odpowiadających za cyberbezpieczeństwo Sojuszu Północnoatlantyckiego. Należą do nich: Ze-

spół Reagowania na Incydenty Komputerowe NATO, Rada NATO ds. Zarządzania Cyberobroną, DPPCRF, Centrum Doskonalenia Obrony przed Cyberatakami, CERT, Grupa Szybkiego Reagowania w Cyberprzestrzeni oraz Komitet Cyberobrony. Omawiając działania NATO, wskazano na czteroetapowy proces reagowania na zagrożenia cybernetyczne przez NATO, który został stworzony w celu efektywnego przeciwdziałania tego typu zagrożeniom. Uwagę skupiono także na aspektach związanych z artykułem 5 Traktatu Waszyngtońskiego, dotyczących podjęcia przez Sojusz Północnoatlantycki przeciwdziałań w przypadku cyberataku. Ustalono, że w takim przypadku pod uwagę będą brane takie czynniki, jak: zasięg, czas trwania agresji, skutki oraz atrybucja. Z uwagi na ryzyko niespełnienia wszystkich warunków, współczesne cyberataki nie powinny wywoływać częstych reakcji NATO w analizowanym obszarze.

ROZDZIAŁ 7.
Aspekty prawne wykorzystania mediów społecznościowych

7.1. Przestępstwa z wykorzystaniem mediów społecznościowych

Przestępstwa oraz czyny zakazane z wykorzystaniem mediów społecznościowych w cyberprzestrzeni należy postrzegać jako akty przestępczości komputerowej. W polskim systemie prawnym nie ma jednoznacznej definicji przestępczości komputerowej. Zdaniem K. Jakubskiego „w szerokim rozumieniu przestępczość komputerowa obejmuje wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer. Należy tu zaznaczyć, iż będą to zarówno czyny popełniane przy użyciu elektronicznych systemów przetwarzania danych (komputer jako narzędzie do popełnienia przestępstwa), jak i skierowane przeciwko takiemu systemowi”[323]. Inny uczony – M. Sowa określa przestępstwa (internetowe) jako „przestępstwa, w przypadku których usługi sieciowe (możliwości oferowane przez Internet) umożliwiły lub co najmniej ułatwiły sprawcy realizację zamierzonego czynu przestępnego albo jego poszczególnych stadiów. Innymi słowy, o przestępczości internetowej mówimy wtedy, gdy bez użycia sieci do popełnienia określonego czynu dojść by nie mogło lub jego dokonanie byłoby znacznie bardziej utrudnione”[324].

Należy dodatkowo stwierdzić, że nie jest ważne, jaką definicję pojęcia przestępstwa internetowego przyjmiemy. Będą to czyny zakazane i skierowane przeciwko systemowi komputerowemu (w sytuacji, gdy komputer

[323] K. Jakubski, *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo” 1996, nr 12, s. 34.
[324] M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo” 2002, nr 4, s. 62.

jest celem ataku), jak i czyny dokonane przy użyciu komputera (w sytuacji, gdy komputer jest narzędziem ataku).

Podziału przestępstw komputerowych po raz pierwszy dokonał Peter Sommer[325], wyróżniając cztery związane z nimi zjawiska[326]:

- **przestępstwa niemożliwe do wykonania poza środowiskiem komputerowym** – za które uważa się: manipulacje dokonywane za pomocą komputera na zbiorach danych, oprogramowaniu, kradzież materiałów eksploatacyjnych systemów komputerowych (papier, taśmy do drukarek itp.), *hacking* (nieuprawnione wejście do systemów komputerowych) oraz zamachy dokonywane na urządzeniach systemów informatycznych oraz ich kradzież;
- **przestępstwa, których dokonanie ułatwia użycie komputera** – do których należą: oszustwa (fikcyjne transakcje finansowe, manipulowanie danymi wejściowymi i ich fałszowanie), fałszerstwa, kradzież tożsamości (używanie cudzego nazwiska), kradzieże informacji czy podsłuch, a także rozpowszechnianie w sieciach komputerowych treści i ideologii zakazanych przez prawo np. pornografia dziecięca;
- **przestępstwa dokonywane przy biernym stosowaniu komputerów** – dotyczące oszustw i wyrządzania szkód w interesach prawnych i gospodarczych;
- **przestępstwa popełniane z wykorzystaniem komputerów przez profesjonalnych przestępców** – można zaliczyć do nich trzy rodzaje przestępstw: dotyczące naruszenia ochrony danych (np. tajemnicy urzędowej, bankowej, zawodowej, danych osobowych); przestępstwa gospodarcze z użyciem komputerów, takie jak: manipulacje i malwersacje komputerowe (np. nieuprawnione użycie kart bankomatowych), manipulowanie stanem kont bankowych czy nadużycia telekomunikacyjne, takie jak sabotaż i szantaż komputerowy; hacking komputerowy; szpiegostwo komputerowe; kradzież oprogramowania i inne metody piractwa związane z produktami przemysłu komputerowego. Trzecią grupę przestępstw popełnianych z wykorzystaniem komputerów stanowią – inne formy przestępstw. Należą do nich: upowszechnianie za pomocą komputerów informacji rasistowskich, pornograficznych czy pozwalających na użycie przemocy; użycie techniki komputerowej w tradycyjnych rodzajach przestępstw[327].

[325] Były hacker o pseudonimie Hugon Cornwall, późniejszy prawnik.

[326] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych,* Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008, s. 560.

[327] U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka,* „Przegląd Policyjny" 1995, nr 3, s. 6–34.

Inną literaturową propozycja typologii przestępstw komputerowych obrazuje rysunek 18.

Rysunek 18. Typologia przestępstw komputerowych
Źródło: opracowanie własne na podstawie B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Kantor Wydawniczy Zakamycze, Zakamycze 2000, s. 33.

Typologia ta wyszczególnia:

- **nielegalne rozpowszechnianie** – w kontekście popełnianych przestępstw komputerowych może oznaczać m.in. rozpowszechnianie i wysyłanie złośliwego oprogramowania (np. koń trojański) bądź wirusów (np. typu makro) do urządzeń technicznych bez wiedzy lub autoryzacji przez jego użytkownika;
- **sabotaż** – to czyn opierający się na działaniach prowadzących do uszkadzania, niszczenia, zmieniania lub usuwania danych o charakterze informacyjnym, które posiadają szczególnie ważne znaczenie np. w aspekcie bezpieczeństwa funkcjonowania infrastruktury krytycznej, administracji rządowej bądź obronności państwa. Sabotaż komputerowy może trwale uszkodzić lub nawet uniemożliwić przetwarzanie danych;
- **oszustwa komputerowe** – są to przede wszystkim przestępstwa o charakterze gospodarczym, często również godzące w sferę biznesową, do których należą fikcyjne transakcje finansowe, manipulowanie i fałszowanie danych wejściowych;

- **niszczenie danych lub programów** – to świadoma aktywność bazująca na niszczeniu, szkodzeniu, usuwaniu bądź zmienianiu oryginalnego formatu danych lub programów przez użytkowników nieuprawionych do prowadzenia tego rodzaju działalności;
- **podsłuch** – zamierzone działanie polegające na przechwytywaniu przez niepożądane osoby (hakerów) informacji i danych, które są przesyłane np. poprzez lokalne sieci, również użyciu sieci bezprzewodowej, takiej jak Wi-Fi. Posłuch komputerowy wykorzystywany przez hakerów jest nielegalny, jednak pierwotnie miał w uzasadniony sposób służyć administratorom sieci do diagnozowania i analizy problemów związanych z wydajnością łącza;
- **fałszerstwa** – spośród fałszerstw komputerowych można wyróżnić fałszerstwo dokumentów (w którym to oprogramowanie i peryferia komputera stanowią narzędzie do zafałszowania dokumentów w klasycznej postaci) oraz fałszerstwo dokumentów elektronicznych (ten rodzaj przestępstwa polega na dokonywaniu zmian, modyfikacji w utworzonych i przyjętych dokumentach elektronicznych – mogą to być np. księgi handlowe i podatkowe, ewidencje magazynowe, kartoteki pojazdów itp.)[328];
- **szpiegostwo** – to nielegalna forma aktywności o charakterze wywiadowczym. W kontekście użytkowania cyberprzestrzeni, szpiegostwo komputerowe opiera się na pozyskiwaniu danych oraz informacji, będących tajemnicą i przekazywanie ich w różnych formach wywiadowi przy jednoczesnej dbałości o zachowanie anonimowości cyberszpiega;
- **włamanie do systemu** – to działanie mające na celu dokonanie impersonacji, czyli zabiegu polegającego na podszywaniu się pod uprawnionego użytkownika przy użyciu np. specjalnej aplikacji internetowej wspierającej proces pozyskania jego sieciowej tożsamości;
- **nielegalne używanie/użytkowanie** – może zaliczać się do niego używanie komputera jako narzędzia planowania oraz kontroli dowolnego rodzaju przestępczości. Przykładem nielegalnego użytkowania jest ***superzapping***, czyli bezprawne wykorzystywanie programów użytkowych przez zmiany, zniszczenie lub ujawnienie danych.

Oprócz przestępstw, określonych w aktach prawnych, możemy wyróżnić nasilające się zachowania antyspołeczne charakterystyczne dla forów dyskusyjnych i innych miejsc w Internecie, w których prowadzi się dysku-

[328] *Fałszerstwo komputerowe*, online – http://cyberprzestepczosc.info/falszerstwo-komputerowe/ [dostęp: 14.09.2017].

sje. Praktyki takie charakteryzują się formami działalności z przewagą aktywności oraz pobudzania wyraźnej agresji i wrogości. Ich symptomami są: dążenie do szkodzenia innym osobom, okrucieństwo, brak wrażliwości moralnej oraz stosowanie przemocy. Jednym z tego typu negatywnych praktyk jest **trolling** (inaczej **trollowanie**). Działania te można zdefiniować jako „antyspołeczne zachowanie charakterystyczne dla internetowych grup, forów dyskusyjnych, czatów i sieci społecznościowych, polegające na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych przekazów"[329]. Polega ono na umyślnym wpływaniu na innych użytkowników cyberprzestrzeni, zebranych najczęściej na forach, lub innych miejscach dyskusji w sieci, w celu ich ośmieszenia lub obrażenia (w konsekwencji wywołania kłótni) poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych informacji czy też poprzez stosowanie różnego typu **zabiegów erystycznych**. Istotą takiego działania jest upublicznianie kontrowersyjnej wiadomości jako przynęty[330]. Należy także stwierdzić, że trollowanie powoduje łamanie zasad netykiety[331] i w efekcie powoduje dezorganizowanie miejsca, gdzie prowadzona jest dyskusja np. fora internetowego, poprzez skupienie uwagi na osobie trollującej.

Należy także nadmienić, że rozwój technologii informacyjnych/informatycznych stwarza dobre warunki dla prowadzenia działalności przestępczej. Pojawiające się nowe rozwiązania z jednej strony wspomagają procesy podejmowania decyzji na różnych szczeblach zarządzania organizacją, natomiast z drugiej strony niosą ze sobą jakościowo nowe niebezpieczeństwa. Zagrożenia te mogą naruszać zasoby: osobowe, materialne, finansowe, informacyjne[332], w tym także te dotyczące państwa i wpływające na jego bezpieczeństwo. W tym kontekście, na podstawie badań naukowych, można stwierdzić, że istotnym współczesnym zagrożeniem jest cyberterroryzm. Stanowi on najbardziej nieprzewidywalny sposób oddziaływania zorganizowanych grup na funkcjonowanie i stabilność struktur państwowych. Jednym z celów takiej przestępczej działalności jest infrastruktura krytyczna, której uszkodzenie lub zniszczenie może spowodować osłabienie zdolności obronnej oraz bezpieczeństwa państwa. Jej podstawowymi elementami są: telekomunikacja, system bankowy i finansowy,

[329] *Doktryna Bezpieczeństwa Informacyjnego…*, *op. cit*.
[330] P. Wallace, *Psychologia Internetu*, Rebis, Poznań 2003, s. 136.
[331] **Netykieta** – etymologia słowa odnosi się do dwóch wyrazów – *net* (sieć) i etykieta. Jest to niesformalizowany zbiór zasad przyzwoitego zachowania się (między innymi z dużym poziomem kultury osobistej) podczas kontaktu między innymi za pomocą mediów społecznościowych.
[332] A. Żebrowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000, s. 65.

system energetyczny, produkcja, magazynowanie oraz transport gazu ziemnego i ropy naftowej, transport, system zaopatrzenia w wodę, służby ratownicze oraz ciągłość funkcjonowania władzy i służb publicznych[333].

Mając na uwadze bezpieczeństwo państwa, w literaturze przedmiotu funkcjonuje pojęcie – **przestępstwa przeciwko bezpieczeństwu powszechnemu**. Są one odrębną kategorią czynów zabronionych. Do tego typu przestępstw komputerowych możemy zaliczyć: sprowadzenie zagrożenia dla życia lub zdrowia wielu osób, zamach terrorystyczny na statek morski lub powietrzny, nieumyślne zakłócenie automatycznego przetwarzania informacji skutkujące zaistnieniem niebezpieczeństwa powszechnego. Zasadniczo mają one chronić systemy informatyczne najważniejszych instytucji życia publicznego, takich jak: szpitale, stacje kolejowe, lotniska, obiekty wojskowe itp.

Analizując różnorodność klasyfikacji nielegalnych czynów popełnianych za pośrednictwem i w środowisku cyberprzestrzeni, można zauważyć, że zachodzące w niej przejawy działalności przestępczej posiadają pewne wspólne cechy. Zaliczają się do nich:

- duża „ciemna" liczba incydentów – dotyczy przestępstw komputerowych, do których doszło w wyniku niewyjaśnionych okoliczności;
- niskie prawdopodobieństwo wykrycia sprawcy – tylko w nielicznych przypadkach udało się zdemaskować tożsamość cyberprzestępcy lub gangu (np. pseudonim) prowadzącego nielegalną działalność w przestrzeni cybernetycznej;
- niechęć względem informowania policji o zaistniałym zdarzeniu – nawiązuje przede wszystkim do braku świadomości społeczeństwa na temat skali i możliwego niebezpieczeństwa, jakie niosą za sobą cyberprzestępstwa. Stąd też atakowane instytucje lub osoby prywatne wolą unikać informowania służb porządku publicznego o ich zajściu;
- lekceważenie przez pokrzywdzonych środków bezpieczeństwa – może wynikać z braku posiadania odpowiednich środków (np. finansowych) do wdrożenia systemów ochrony przed cyberzagrożeniami, jak również z przekonania, że kolejne ataki o charakterze przestępczym nie będą mieć miejsca.

Ze względu na powyższy podział, trudnym jest oszacowanie rozmiarów i tendencji przestępczości komputerowej. Jednakże każdy z odnotowanych incydentów posiada wspólną specyfikę. Sieć internetowa, za pomocą której dochodzi do najliczniejszych cyberataków, stanowi medium, wykorzystywane do takich niepożądanych działań, jak: oszustwa, prostytucja, promo-

[333] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, s. 168.

wanie przemocy, ekstremizmy polityczne, elektroniczne „pranie pieniędzy", przestępcze wymuszenia, sabotaż, szpiegostwo, łamanie praw autorskich, a czasami nawet naruszanie nietykalności osobistej czy zabójstwa (na przykład ingerencja w dane informatyczne dotyczące leczenia pacjentów – zmiana leku lub jego dawki może stać się przyczyną śmierci). Jeszcze do niedawna w krajach Europy Zachodniej rzadko prowadzone były badania dotyczące wpływu nowoczesnych technologii przetwarzania informacji na działania przestępcze. Jednakże, jak wynika ze współczesnych policyjnych statystyk, prowadzonych m.in. w Polsce, nastąpiła zmiana i zainteresowanie tą tematyka wzrasta.

W polskim systemie prawnym przepisy związane z przestępczością komputerową nie są ujednolicone w jednym akcie normatywnym. Przestępstwa są ujęte w układzie systemowym i mogą one zostać podzielone na dwie grupy główne:

- przestępstwa ujęte w przepisach części szczególnej Kodeksu karnego[334] (dalej k.k.);
- przestępstwa uregulowane w ramach przepisów karnych poszczególnych ustaw.

Można zauważyć, że część przestępstw komputerowych regulowana jest przez kodeks karny. W rozdziale XVII dotyczącym przestępstw przeciwko Rzeczypospolitej Polskiej uporządkowane zostały na przykład kwestie dotyczące szpiegostwa komputerowego. Jedną z jego form jest szpiegostwo komputerowe, które polega na zdobywaniu danych zawartych na komputerowych nośnikach informacji. Z reguły ma to na celu pozyskanie istotnych informacji dotyczących nowoczesnych technologii oraz danych dotyczących sił zbrojnych. Na mocy art. 130 § 3 k.k. czyn taki zagrożony jest karą pozbawienia wolności od sześciu miesięcy do ośmiu lat. Karalne jest również szpiegostwo na rzecz państwa sojuszniczego.

Następną, wyodrębnioną w kodeksie karnym grupą przestępstw są przestępstwa przeciw ochronie informacji. Należą one do szczególnie często występujących. Do grupy tych przestępstw zaliczamy: *hacking*, nieuprawnione przechwytywanie informacji (podsłuch), niszczenie informacji, sabotaż komputerowy. Zgodnie z art. 267 § 2 k.k. karze podlega każdy, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym. Ustawodawca nie wskazał konkretnych urządzeń, których wykorzystanie jest karalne. Oznacza to, że przepis ten obejmuje również komputer wyposażony w odpowiednie oprogramowanie. Zazwyczaj sprawcy stosują tego typu urządzenia, tak aby pozyskać poufne infor-

[334] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553, art. 267 z późn. zm.).

macje umożliwiające dalsze przestępstwa, np. zdobycie danych dotyczących kart kredytowych[335].

7.2. Agresorzy i naruszyciele prawa w aspekcie wykorzystania mediów społecznościowych oraz metody ich działalności

Jednym z powszechnie stosowanych naruszeń prawa w cyberprzestrzeni, związanym z mediami społecznościowymi, jest trolling. Osoby, które dokonują trollowania nazywamy **trollami**. Do ich charakterystycznych cech możemy zaliczyć: bezgraniczne podporządkowanie się jakiejś idei, udawanie nieznajomości tematu, nagminne zadawanie tych samych pytań, celowe wyrażanie zdania różniącego się od zdania grupy, chętne używanie argumentów *ad personam*, skrajną megalomanię i pogardę w stosunku do innych osób, nazywanie innych dyskutantów trollami, wprowadzanie zamieszania w stosunku do własnej osoby, przedstawianie siebie jako ofiary, próby utrudniania innym wypowiedzi, rozpoczynanie wypowiedzi stale od tego samego zwrotu (np. pogardliwego powitania), zmienianie własnych danych, tworzenie multikont, w celu udawania poparcia dla siebie w dyskusji[336].

Działalność trolli jest zazwyczaj mało szkodliwa społecznie, ale może ona przybierać bardziej radykalną – groźną dla społeczeństwa postać, jeżeli ich działania: przybierają formę zorganizowaną, dokonują się w czasie sytuacji kryzysowej, zawierają założony przekaz ideologiczny. W takim przypadku trolle utrudniają prowadzenie pracy niezależnym serwisom informacyjnym poprzez dużą ilość krytycznych wpisów na wielu możliwych stronach i kontach (komentarze pod artykułem, forum, w serwisach społecznościowych).

Literatura przedmiotu przewiduje kilka klasyfikacji trolli. Jedną z propozycji jest stanowisko NATO, zawarte w raporcie Dowództwa Strategicznego USA (StratCom – *NATO Strategic Communications Centre of Excellence*), gdzie rozróżnia się ich dwa rodzaje:

- **troll klasyczny** – to osoba próbująca sprowokować emocjonalną reakcję użytkownika, wywołać szok, doprowadzić do wściekłości, wzbudzić strach lub poczucie zagrożenia. Jest nią także osoba, która próbuje skierować na siebie uwagę poprzez sabotowanie zasad korzystania z serwisu (np. mnożenie wątków na forach albo wklejanie

[335] M. Nowak, *Cybernetyczne przestępstwa…*, *op. cit.*
[336] T. Grabowski, *Metody walki informacyjnej…*, *op. cit.*, s. 35.

wbrew regulaminowi ogromnych partii skopiowanego tekstu). Jego działania nie są podyktowane żadnymi ideologiami czy wierzeniami ani też przejęte prawdą czy fałszywością rozpowszechnianych informacji. Wprowadzana przez niego treść ma za zadanie prowokować i wywoływać u innych gwałtowne, emocjonalne negatywne reakcje;
- **troll hybrydowy** – to osoba wynajęta, działająca pod kierunkiem i na zlecenie państwa bądź instytucji państwowej, propagująca konkretną zleconą ideologię. Taka aktywność związana jest zazwyczaj z dodatkową działalnością, np. dezinformacją, powodowaniem kontrowersji itd.[337].

Dodatkowo można wyróżnić kilka innych typów trolli, które występują w przestrzeni informacyjnej mediów społecznościowych. Należą do nich:
- **troll „obwiń o wszystko amerykański spisek"** – rozpowszechnia tezę, że wszystko jest winą Stanów Zjednoczonych. Teksty „spiskowego" trolla są bardzo rozbudowane, zazwyczaj zawierają długi i logiczny wywód z szeroką argumentacją. Po bliższym zapoznaniu okazuje się jednak, że logika ta jest pozorna, a wynik wywodu jest zawsze ten sam – winne są Stany Zjednoczone. Znakiem rozpoznawczym tego typu trolla jest objętość wpisów, tzn. są one znacznie dłuższej treści niż w innych przypadkach;
- **troll „bikini"** – nazwa tego typu trolla pochodzi od zdjęcia profilowego lub avataru[338]. Zazwyczaj jako ikona pojawia się atrakcyjna kobieta ubrana w strój plażowy. Przekaz tego agresora cechuje naiwność i uproszczona wizją świata. Poddaje on do publicznej dyskusji tematy, w których zawiera pytania, np. „Czy naprawdę tylko Rosja jest taka zła? Może powinniśmy spojrzeć na to co robią USA?" Świat chyba nie jest taki prosty? Trolle typu „bikini" mają według ekspertów wyjątkowe zdolności do adaptacji w sieci i często trudno ich rozpoznać. Pomimo niewielkiej objętości, naiwności i banalności, ich wpisy mają bardzo duży wpływ na społeczność internetową;
- **troll agresywny** – to typ najbardziej zbliżony do klasycznego trolla, publikuje tylko agresywne i silnie ekspresyjne wpisy i nietrudno rozpoznać stanowisko, którego broni. Jego działanie polega na wywoływaniu lęku i strachu wśród czytelników i tym samym wyzwoleniu emocjonalnej reakcji. W odróżnieniu od trolla klasycznego, który reaguje na polemikę, tak aby jak najbardziej przedłużyć konflikt i sprowokować szerszą grupę do reakcji, hybrydowy troll typu agresywne-

[337] *Internet trolling as a tool of hybrid warfare: The case of Latvia – Results of the study*, StratCom, Riga 2016, s. 10.
[338] **Avatar** (inaczej **awatar**) – stanowi tożsamość w sieci. Występuje często w postaci ikony, dopasowanej do danej osoby, lub grupy osób.

go charakteryzuje się niską reaktywnością. Spowodowane jest to prawdopodobnie barierą językową i obawą przed dekonspiracją;

- **troll „wikipedyjny"** – to specyficzny rodzaj trolla, który przekopiowuje informacje z portalu Wikipedia (lub innych źródeł, takich jak np. blogi historyczne), nie stosując komentarzy o nasyceniu emocjonalnym. Przeklejane informacje są przeważnie zgodne z prawdą, ale pozbawione kontekstu zdaniowego, prowadząc często do błędnych wniosków. W praktyce polega to na tym, że np. pod artykułami o agresji wojskowej Rosji przekopiowywane są ze źródeł otwartych fragmentów tekstów o interwencjach wojskowych USA – lecz bez wskazania przyczyn, kontekstu, polityki innych państw w tym samym okresie itd. W efekcie powoduje to niepełność informacji, a przez to zafałszowany odbiór.
- **troll „załącznikowy"** – przekazywane przez tego typu trolle wiadomości są zwięzłe. Zawsze posiadają załączony link, który jest zachętą dla czytelnika. Prowadzi on np. na rosyjski serwis informacyjny, nagranie z YouTube zawierające fragment programu informacyjnego lub amatorsko wyprodukowany klip propagandowy. Co ważne, hybrydowy troll nigdy nie przekierowuje do płatnych serwisów czy stron zawierających wirusy. Jego zadanie polega na wskazaniu treści o charakterze politycznym innym internautom. Zdefiniowanie tego typu trolla jest utrudnione, ponieważ jego wpisy pozbawione są specyficznego stylu[339].

Inne źródło – encyklopedia internetowa, klasyfikuje trolle na 81 typów, wśród których możemy wyróżnić: wygadany, zły klaun, prowokator, egocentryk, buntownik bez pojęcia, hyrhu-hyrhu czy wędkarz[340].

Jedna z klasyfikacji, opracowana metodą wniosków arbitralnych[341], na podstawie rozkładów statystycznych populacji użytkowników została przeprowadzona w oparciu o próbę badawczą – 234 876 posty z 45 grup dyskusyjnych. Z liczby tej zostało wybranych 10% najciekawszych z nich. Wyniki tej analizy dzielą trolle internetowe na następujące typy: zwyczajny, zagrodowy i maniakalny[342], których charakterystki przedstawiono poniżej:

- **troll zwyczajny** – charakteryzują go proste formy wypowiedzi, zawierające na ogół nieskładne złożenia przypadkowo dobranych wy-

[339] *Ibidem*, s. 32; T. Grabowski, *op. cit.*, s. 48-49

[340] v. *Wielka Ilustrowana Encyklopedia Internetowa Mike'a Reeda*,
online – http://trole.joemonster.org/index.php [dostęp: 13.08.2017].

[341] W.J. Plauchowski, A. Bujacz, P. Haładziński, L. Kaczmarek (red.), *Nowoczesne metody badawcze…*, *op. cit.*, s. 122.

[342] J. Wesołowski, *Klasyfikacja gatunkowa trolli sieciowych, dokonana na podstawie obserwacji grup dyskusyjnych w hierarchii PL*, *s.l./s.n.*, 2002.

razów, brak stosowania estetyki edycyjnej wypowiedzi, przejawiającej się m.in. błędami w zapisach, bezpodstawnym stosowaniu dużych i małych liter, braku lub nadużywaniu znaków interpunkcyjnych – w tym także wykrzykników itd. Cechą charakterystyczną jego działalności w sieci jest także stosowanie dużej ilości wulgaryzmów;

- **troll zagrodowy** – jest on zbliżony do trolla zwyczajnego z zasadniczą różnicą. Celem ataków agresora są konkretne osoby lub grupy osób, przy wykazaniu znajomości zasad panujących w mediach społecznościowych, w których odbywa się jego działalność. W większości przypadków atakowane są przez niego osoby, które na teren grupy dyskusyjną wchodzą nieproszone, dodatkowo łamiąc zasady netykiety. Poza tym stosuje on, drogą naśladowania, dużo skrótowców np. NTG, ROTFL[343]. Cechą wyróżniająca jest także to, że jego zachowanie jest bardzo brutalne;
- **troll maniakalny** – jego działalność wyróżnia się dużym poziomem agresji oraz natychmiastową „regeneracją" objawiającą się tym, że w przypadku niepowodzenia jego działalności jest on zdolny do szybkiego powrotu do dyskusji i dalszej szkodliwej działalności. Po trzecie odznacza się obroną haseł i postów, do których jest przywiązany[344].

Wcześniej cytowane w pracy opracowanie – projekt „Narodowej doktryny bezpieczeństwa informacyjnego" przewiduje pojęcie – tzw. **dobre trolle**. Nazywa się nimi takich użytkowników cyberprzestrzeni państwa, których działalność skupiona jest na samoorganizacji społeczeństwa obywatelskiego przez samokształcenie, a także podnoszenie świadomości o zagrożeniach i wspieranie obywatelskiego potencjału przeciwdziałania[345].

Kolejnymi agresorami, działającymi w przestrzeni internetowej, związanymi z trollami są hejterzy oraz flamerzy. **Hejterem** (etymologia pochodzi od słowa ang. *hate* – nienawiść, nienawidzić) nazywamy osobę, która wyraża się agresywnie, często prowokując kłótnie. Cechą charakterystyczną odróżniającą jest to, że celami ich ataków są zazwyczaj osoby publiczne. Można zatem stwierdzić, że hejterstwo[346] to „forma dewiacyjnych zacho-

[343] NTG (ang. *not this group*) – oznaczający: nie ta grupa; ROTFL (ang. *Rolling On The Floor Laughing*) – onzaczający: „zwijanie" się ze śmiechu.

[344] J. Wesołowski, *Klasyfikacja gatunkowa trolli…*, *op. cit.*

[345] *Doktryna Bezpieczeństwa Informacyjnego…*, *op. cit*., s. 10.

[346] Innymi terminami pojawiającymi się w różnego rodzaju publikacjach na określenie tego samego zjawiska są także – „hejt", „hejting", „hejtowanie", „hejtować" i inne, w których morfemem jest człon – „hejt". M. Juza M., *Hejterstwo w komunikacji internetowej: charakterystyka zjawiska, przyczyny i sposoby przeciwdziałania*, „Profilaktyka Społeczna i Resocjalizacja" 2015, nr 25, s. 29.

wań podczas publicznych dyskusji internetowych. Polega ono na używaniu obelżywego języka, pogardliwej ocenie różnych zjawisk, znieważaniu zarówno rozmówców, jak i różnych innych podmiotów oraz na wyrażaniu agresji i nienawiści pod ich adresem”[347]. Komentarze hejterów nie niosą żadnym merytorycznych treści, poza agresją wobec innych użytkowników lub ich całe grupy.

Flamerzy (etymologia pochodzi od wyrazu ang. *flame* – prowokować kłótnie) to kolejna grupa użytkowników cyberprzestrzeni, których działanie skupione jest na obrażaniu innych współużytkowników, za pomocą inwektyw i obelg, często używając w tym celu wulgaryzmów. Innymi agresorami w cyberprzestrzeni są **grieferzy**, których działalność polega na powtarzającym się trapieniu konkretnego człowieka, np. przez nękanie go groźbami czy wyzwiskami. Ich działalność jest bardzo niebezpieczna, ponieważ takie praktyki mogą doprowadzić ofiary do desperackich czynów np. samobójstwa. Bardzo niebezpieczni są także **ranterzy**. Traktują oni siebie z powagą, co odróżnia ich od trolli zazwyczaj działających dla zabawy. Zazwyczaj są oni inicjatorami dysput, pouczając pozostałych użytkowników. Cechą charakterystyczną ich działalności jest używanie słów, takich jak: prawda, kłamstwo, zło, zdrada itp. – nasyconych bardzo emocjonalnie oraz wykazujących przekonania polityczne czy społeczne.

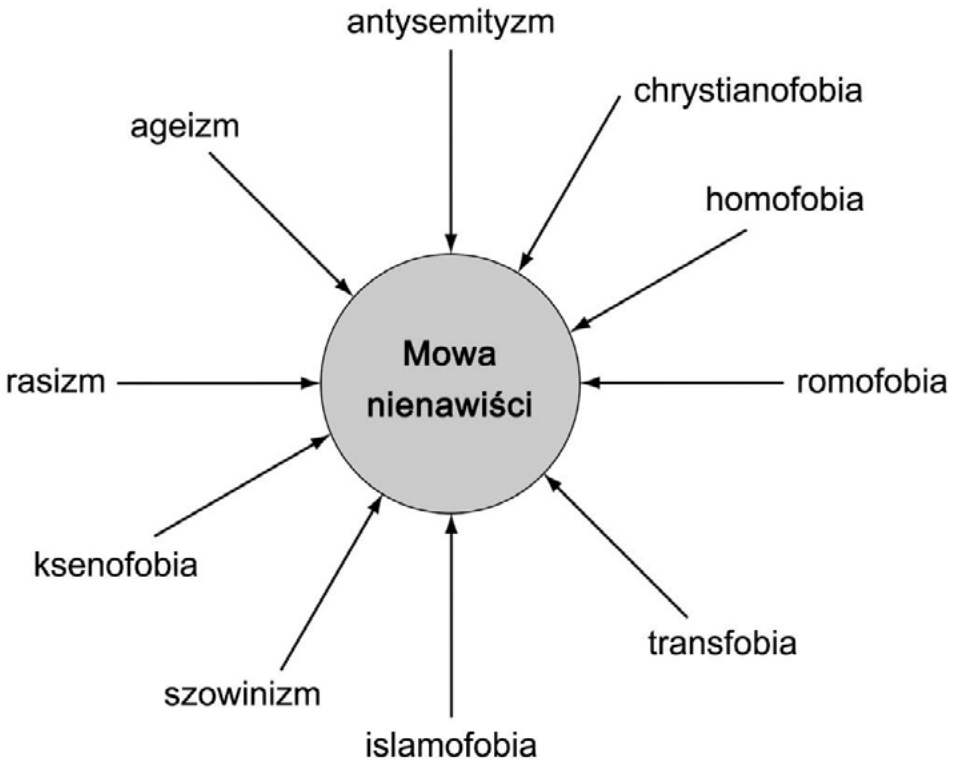
Jedną z używanych przez hejterów i flamerów metod jest tzw. **mowa nienawiści** (ang. *hate speech*). Polega ona na takim używaniu języka, aby rozbudzić, rozpowszechnić czy usprawiedliwić nienawiść i dyskryminację, jak również przemoc wobec konkretnych osób, grup osób, przedstawicieli mniejszości czy jakiegokolwiek innego podmiotu danej wypowiedzi. Jest ona zbiorem różnych negatywnych form zachowań antyspołecznych, w większości fobii (strachu, lęku) oraz niektórych tzw. izmów.

Na rysunku 19 wyróżniono dziesięć głównych składowych mowy nienawiści, do których należą:

- antyseityzm – niechęć i uprzedzenie do Żydów, głównie bazująca na przesądach;
- christianofobia – lęk lub nienawiść odczuwane w stosunku do chrześcijan;
- homofobia – uprzedzenia wobec osób nieheteroseksualnych;
- romofobia – dyskryminacja, niechęć oraz nieuzasadniony lęk wobec Romów;
- transfobia (inaczej: transuprzedzenia i transmizogynia – dyskryminacja osób transpłciowych (transseksualnych, transwestytycznych, transgenderowych);
- islamofobia – strach i dyskryminowanie osób przynależących do gru-

[347] *Ibidem*, s. 29.

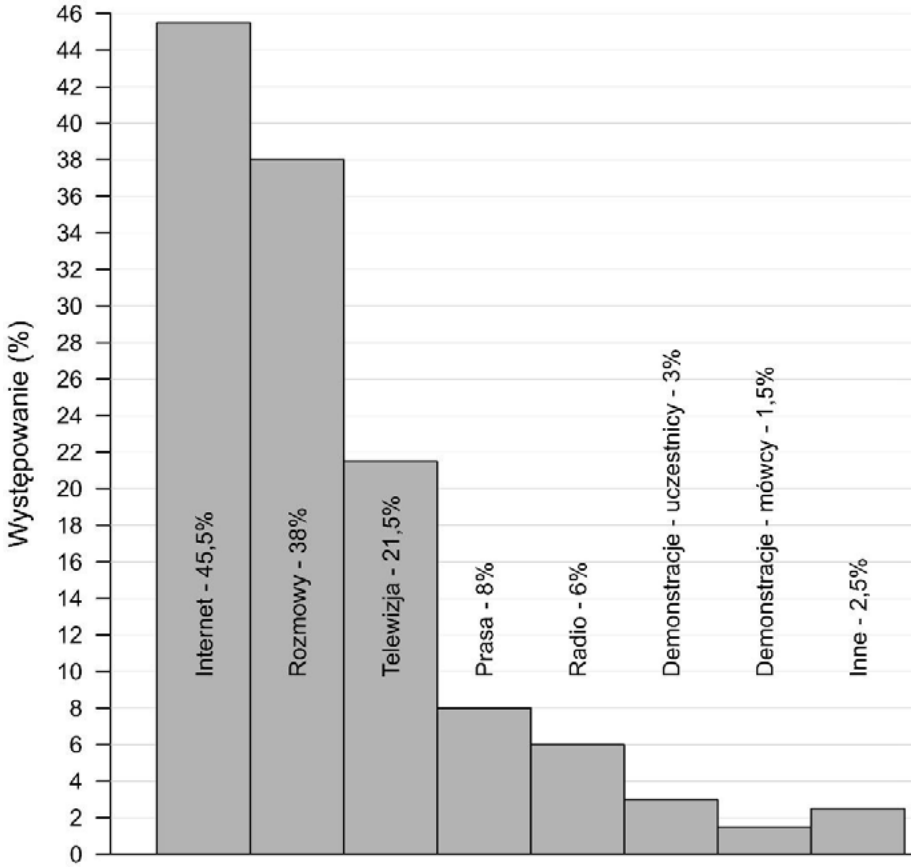
py muzułmanów – wyznawców islamu;
- szowinizm – w pierwszym znaczeniu – przypisywanie szczególnie wysokiej wartości lub przyznawanie uprzywilejowanej pozycji własnej płci, rasie lub grupie, w drugim znaczeniu – to skrajny nacjonalizm wyrażający się ślepym uwielbieniem dla własnego narodu i w nienawiści oraz pogardzie dla innych[348].
- ksenofobia – to wrogi stosunek do cudzoziemców i cudzoziemszczyzny;
- rasizm – przekonanie, iż osoby innej rasy są gorsze;
- ageizm – uprzedzenia i stereotypy dotyczące wieku, zachowania dyskryminujące ze względu ma wiek.



Rysunek 19. Składowe mowy nienawiści
Źródło: opracowanie własne.

Podejmując temat mediów społecznościowych należy zauważyć, że mowa nienawiści jest często spotykana i propagowana w mediach społecznościowych, co zilustrowano na rysunku 20.

[348] *Słownik Języka Polskiego PWN*, online – https://sjp.pl/szowinizm [dostęp: 15.08.2017].



Rysunek 20. Media stosujące mowę nienawiści

Źródło: opracowanie własne na podstawie W. Soral, *Mowa nienawiści. Definicja, przyczyny, skutki, skala zjawiska*, Centrum Badań nad Uprzedzeniami UW, Warszawa 2017, s. 19.

Wyniki przeprowadzonych badań dowodzą, że największym medium, w którym występuje i proliferowana jest mowa nienawiści jest sieć Internet (45,5% – z czego 29% to dorośli, natomiast 62% stanowi młodzież). Kolejne media w którym wykorzystywane jest to zjawisko to: telewizja (21,5%), prasa (8%) oraz radio (6%)[349].

Akceptacja mowy nienawiści w wymiarze społecznym prowadzi do utrwalania się stereotypów, uprzedzeń i powoduje ona mniejszą akceptację przedstawicieli hejtowanych grup społecznych. Może ona także prowadzić do tzw. przestępstw z nienawiści (ang. *hate crimes*).

Mowa nienawiści przyjmuje różne formy i dlatego istnieje trudność w jednoznacznym jej określeniu. Obecnie nie ma uniwersalnej definicji mowy nienawiści, ale powstało kilka prób jej określenia, które przedsta-

[349] W. Soral, *Mowa nienawiści. Definicje, przyczyny, skutki, skala zjawiska*, Centrum Badań nad Uprzedzeniami UW, Warszawa 2017, s. 19.

wiono poniżej. Jedną z nich proponuje Rada Europy (RE). Według niej mowa nienawiści obejmuje wszelkie formy wypowiedzi, które szerzą, propagują czy usprawiedliwiają nienawiść rasową, ksenofobię, antysemityzm oraz inne formy nienawiści bazujące na nietolerancji, m.in.: nietolerancję wyrażającą się w agresywnym nacjonalizmie i etnocentryzmie, dyskryminację i wrogość wobec mniejszości, imigrantów i ludzi o imigranckim pochodzeniu. W jednym z opracowań Rady Europy zdefiniowany jest termin – rasistowski i ksenofobiczny materiał, który oznacza każdy materiał, obraz lub jakąkolwiek inną ilustrację idei lub teorii, która zaleca, promuje albo nawołuje do nienawiści, dyskryminacji lub przemocy wobec osoby lub grupy osób ze względu na rasę, kolor skóry, wyznanie, pochodzenie albo przynależność narodową lub etniczną, jeśli są wykorzystywane jako pretekst do któregokolwiek z tych czynników. Rada Europy zwraca także uwagę, że rozwój mowy nienawiści ma ścisły związek z rozwojem mediów społecznościowych[350].

Unia Europejska określa czyny, które popełniane są na tle rasistowskim lub ksenofobicznym i podlegają one sankcjom karnym, jako przestępstwa kryminalne. Są to:

- publiczne nawoływanie do przemocy lub nienawiści skierowanej przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, pochodzenia, wyznawanej religii lub światopoglądu albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy;
- publiczne rozpowszechnianie lub rozprowadzanie tekstów, obrazów lub innych materiałów zawierających treści rasistowskie i ksenofobiczne;
- publiczne aprobowanie, negowanie lub rażące pomniejszanie zbrodni ludobójstwa, zbrodni przeciwko ludzkości oraz zbrodni wojennych w rozumieniu art. 6, 7 i 8 statutu Międzynarodowego Trybunału Karnego[351] oraz zbrodni określonych w art. 6 Karty Międzynarodowego Trybunału Wojskowego załączonej do Porozumienia międzynarodowego w przedmiocie ścigania i karania głównych przestępców wojennych Osi Europejskiej, podpisanego w Londynie dnia 8 sierpnia 1945 r.[352], jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko takiej grupie lub jej członków;
- publiczne aprobowanie, negowanie lub rażące pomniejszanie zbrodni

[350] *Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "hate speech"*, Rada Europy, Strasburg 1997, s. 107.

[351] Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r.(Dz.U. 2003 nr 78 poz. 708).

[352] Porozumienie międzynarodowe w przedmiocie ścigania i karania głównych przestępców wojennych Osi Europejskiej, podpisanego w Londynie dnia 8 sierpnia 1945 r. (Dz.U. z 1947 r. poz. 367).

określonych w art. 6 Karty Międzynarodowego Trybunału Wojskowego załączonej do porozumienia londyńskiego z dnia 8 sierpnia 1945 r., a skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi[353].

Należy podkreślić, że w publikacjach UE nie występuje termin mowa nienawiści, a inny – czyny popełniane na tle rasistowskim i ksenofobicznym. Należy zatem uznać je za tożsame.

Analizując mowę nienawiści, w kontekście prawa należy także dokonać pewnych rozgraniczeń, tzn. należy odróżnić *hate speech* od *hate crime*, tzn. mowę nienawiści od przestępstw popełnianych na tym tle, m.in. aktów fizycznej przemocy, pobić, gwałtów i zabójstw. Mowa nienawiści może towarzyszyć i zwykle towarzyszy *hate crime*, jednak nieobowiązkowo. Pomimo powiązania przemocy werbalnej z przemocą fizyczną, nie powinno się mylić tych dwóch zjawisk. Trzeba jednak odróżniać szerszą kategorię, jaką jest mowa nienawiści, od karalnych w danym kraju form publicznej agresji werbalnej oraz pozawerbalnej, których przykładami są: ikonografia transparentów i ulotek, rysunki i karykatury w pismach itp. W tej kwestii przykładem może być kłamstwo oświęcimskie, *Auschwitzlüge*, karalne na mocy Ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz.U. 1998 nr 155 poz. 1016 z późn. zm.).

Biorąc pod uwagę techniczne uwarunkowania komputera, można wysnuć wniosek, że urządzenie to posiadające dostęp (przewodowy oraz bezprzewodowy) do innych komputerów jest szczególnie narażone na wszelkiego rodzaju cyberataki. Ich głównym celem jest dążenie do zniszczenia działającego na nim oprogramowania, kradzież różnego rodzaju dóbr bądź destrukcja danych i wykorzystanie ich mocy obliczeniowej do groźniejszych w skutkach incydentów w cyberprzestrzeni. Taktyka i sposoby działań przestępców komputerowych w obecnych czasach są bardzo zróżnicowane. Jedną z propozycji jest poniższa typologia:

- **hakerzy** (ang. *hackers*) – zazwyczaj się reprezentowani przez ludzi młodych, wykształconych, niejednokrotnie działających w sformalizowanych grupach, nawet o charakterze międzynarodowym, dzielących się doświadczeniem i narzędziami. Uważani są oni za najbardziej

[353] Decyzja ramowa Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych (Dz.Urz. UE L 328/55 z dnia 6.12.2008, art. 1, pkt. 1a–d).

niebezpiecznych, z uwagi na to, że ich działania skupione są na łamaniu zabezpieczeń systemów komputerowych. Hakerzy uchodzą także za miłośników informatyki a wywołane przez nich incydenty najczęściej mają charakter poznawczy, nie destrukcyjny;
- **krakerzy** (ang. *crackers*) – podobnie jak hakerzy dokonują nielegalnych cyberataków, lecz skupiają się wokół złamania zabezpieczeń programów komputerowych w celu ich użycia w sposób nieautoryzowany przez właściwego użytkownika;
- **wandale** – ich aktywność w sieci jest skoncentrowana *stricte* na niszczeniu danych informatycznych, systemów komputerowych. Ich działalność motywowana jest zazwyczaj pragnieniem zemsty, podążają za emocjami i w przeciwieństwie do hakerów są zdecydowanie nastawieni na destrukcyjne oddziaływanie w cyberprzestrzeni;
- **pospolici przestępcy** – sprzęt komputerowy i sieć służy im do dokonywania różnego rodzaju przestępstw, bodźcem ich działania może być chęć zysku lub motywy polityczne;
- ***phreaker*** – był zjawiskiem częstym, jeszcze zanim upowszechniono komputery osobiste. Polega on na łamaniu zabezpieczeń telefonicznych i uzyskiwaniu możliwości połączeń, odbywanych na koszt innego abonenta;
- **piraci komputerowi** – są to osoby rozpowszechniające oprogramowanie, których zabezpieczenia zostały złamane przez *crackerów*. Aktualnie skala tego zjawiska jest bardzo duża;
- **carderzy** (ang. *carding*) – to nowa i nietypowa forma działalności przestępczej, która polega na kradzieży numerów kart kredytowych lub ich fałszowaniu[354].

7.3. Uogólnienia i wnioski

Analizując zakres przestępstw komputerowych, dokonywanych przy użyciu mediów społecznościowych ustalono, że w polskim systemie prawnym brak jest jednoznacznej definicji tych czynów, a próby jej zdefiniowania nie są ostre. Jednakże uogólniając można stwierdzić, że zawsze będą to czyny zabronione, skierowane przeciwko systemowi komputerowemu (w przypadku, gdy komputer jest celem ataku), jak i czyny dokonane przy użyciu komputera (w przypadku, gdy komputer jest narzędziem ataku). W literaturze istnieje kilka typologii przestępstw komputerowych. Jeden

[354] *Przestępstwa komputerowe – zarys problematyki*, online – http://kryminalistyka.org.pl/artykuly/przestepstwa-komputerowe-zarys-problematyki/#_ftnref7 [dostęp: 15.09.2017].

z prekursorów – Peter Sommer – wyróżnił cztery zjawiska związane z przestępstwami komputerowymi. Należą do nich przestępstwa: niemożliwe do wykonania poza środowiskiem komputerowym, których dokonanie ułatwia użycie komputera, dokonywane przy biernym stosowaniu komputerów oraz popełniane z wykorzystaniem komputerów przez profesjonalnych przestępców. Inna, bardziej współczesna typologia dzieli je na: nielegalne rozpowszechnianie, sabotaż, oszustwa komputerowe, niszczenie danych lub programów, podsłuch, fałszerstwa, szpiegostwo, włamanie do systemu, nielegalne używanie/użytkowanie. Zauważono także, że wyodrębnił się sposób antyspołecznego zachowania w mediach społecznościowych, jakim jest trolling, polegający na zamierzonym działaniu w cyberprzestrzeni. W aspekcie globalnym – w odniesieniu do bezpieczeństwa państwa – podniesiono problem przestępstw przeciwko bezpieczeństwu powszechnemu. Do tej grupy zaliczamy przestępstwa komputerowe skierowane przeciwko życiu i zdrowiu wielu osób, a także zamach terrorystyczny na statek morski lub powietrzny oraz nieumyślne zakłócenie automatycznego przetwarzania informacji prowadzące do zaistnienia niebezpieczeństwa powszechnego. Celem takich ataków mogą być elementy infrastruktury krytycznej państwa lub inne ważne elementy wpływające na bezpieczeństwo narodowe. Zauważono, że w polskim systemie prawnym przepisy dotyczące przestępczości komputerowej nie są ujednolicone w jednym akcie normatywnym. Można dokonać klasyfikacji dzieląc je na dwa typy przestępstw ujęte w przepisach części szczególnej kodeksu karnego oraz uregulowane w ramach przepisów karnych poszczególnych ustaw.

Oprócz przestępstw komputerowych, zwrócono także uwagę na agresorów oraz naruszycieli prawa, a także przedstawiono metody ich działalności, realizowanej za pomocą mediów społecznościowych. Wśród tych agresorów – trolli – zgodnie z nomenklaturą NATO można wyróżnić ich dwa rodzaje – trolli klasycznych i hybrydowych. W odniesieniu do drugich z nich – hybrydowych – wskazano na możliwość ich neutralizacji, skorzystawszy z czteroetapowego algorytmu. Składa się on z następujących po sobie faz: rozpoznania, sprawdzenia, oznaczenia oraz ignorancji hybrydowego trolla. Należy zwrócić uwagę, że literatura przedmiotu uogólnia kilka typów trolli, takich jak: „obwiń o wszystko amerykański spisek", „bikini", a także trolli: agresywnych, „wikipedyjnych" i „załącznikowych". Badania naukowe prowadzone metodą wniosków arbitralnych wykazały inny podział trolli na: zwyczajnych, zagrodowych i maniakalnych. Oprócz złych praktyk realizowanych przez tego typu agresorów cyberprzestrzeni, wyróżniono tzw. dobre trolle. Są nimi ci użytkownicy cyberprzestrzeni, których działalność skupiona jest na samokształceniu, podnoszeniu świadomości o zagrożeniach oraz wspieraniu społeczeństwa. Oprócz trolli, któ-

rym poświęcono dużo uwagi w cyberprzestrzeni, aktywnymi działaczami są także: hejterzy, flamerzy, grieferzy oraz ranterzy. Można stwierdzić, że ich działalność pochodzi od trollingu, a ich aktywność za pomocą mediów społecznościowych ma cechy destrukcyjne. Jedną z metod stosowanych przez wymienionych agresorów cyberprzestrzeni jest mowa nienawiści. Polega ona na szerzeniu nienawiści, jej usprawiedliwianiu oraz dyskryminacji różnych warstw społecznych (np. muzułmanów, osób nieheteroseksualnych oraz innych mniejszości). Analizując te treści zauważono reakcję Unii Europejskiej na problemy związane z mową nienawiści. Określone zostały czyny, podlegające sankcjom karnym, jako przestępstwa kryminalne. Jednakże analizując te aspekty należy rozgraniczyć mowę nienawiści od przestępstw (w kontekście fizycznym) na tym tle. W takim przypadku należy wskazać na kategorię szerszą, jaką jest mowa nienawiści w stosunku do przestępstw o charakterze kryminalnym

ZAKOŃCZENIE

Na podstawie przeanalizowanych zagadnień można stwierdzić, że bezpieczeństwo informacyjne oraz cyberbezpieczeństwo to ważne elementy wpływające na bezpieczeństwo narodowe. Zgodnie z typologią, podzielono je na cztery główne filary – bezpieczeństwo: militarne, informacyjne, finansowo-ekonomiczne oraz polityczno-społeczne. Taki funkcjonalny podział można odnieść także do cyberprzestrzeni, w tym także CRP. Bezpieczeństwo informacyjne stanowi zatem część bezpieczeństwa narodowego, rozumianego w ten sposób, że wpływa znacząco na bezpieczeństwo państwa, spełniając przy tym warunki: utrzymania wysokiego poziomu bezpieczeństwa; strategicznych zasobów państwa; aktualności informacji, jakie dostarczane są do organów władzy państwowej, pozostaje niezakłócony przepływ informacji w państwie, co przekłada się na właściwe i stabilne funkcjonowanie elementów tworzących krytyczną infrastrukturę państwa. W aspekcie tych czynników należy mieć na uwadze, że zachowanie poziomu bezpieczeństwa dotyczy zarówno działań zamierzonych, jak i niezamierzonych ze strony agresorów korzystających z cyberprzestrzeni.

Zestawione w pracy modele walki informacyjnej w przestrzeni cybernetycznej wskazują przede wszystkim na wieloaspektowość oraz wielowariantowość prowadzonych w niej działań. Stanowią teoretyczne założenia wykorzystania cyberprzestrzeni do osiągania zamierzonych celów, najczęściej za pomocą aktów cybernetycznych. Zatem nie może być ona rozumiana jako jednolity, wirtualny obszar, pozwalający na określony zespół wykonywanych w niej czynności. Należy podkreślić, że opracowane i opisane wyżej modele nie są ze sobą w żaden sposób powiązane lub posiadają wyłącznie kilka wspólnych cech. Wskazuje to na zróżnicowane spojrzenie na środowisko cybernetyczne i wojny informacyjne, dające duże możliwości wpływania na zachodzące w niej procesy. Jednym z czynników zorientowanych na złożoność cyberprzestrzeni jest jej podział na warstwy, zgodnie z modelem walki sieciowej według Libickiego. Koncepcja ta zwraca szczególną uwagę na fakt, że żadna z wymienionych warstw nie może istnieć bez urządzeń elektronicznych. Teoria dekapitacji według Wardena zakłada, iż największe oddziaływanie na przeciwnika jest możliwe przy trafnie określonym środku ciężkości (ang. *Centre of Gravity* – CoG) przy użyciu charak-

terystyk cyberprzestrzeni, przenikających wszystkie zdefiniowane kręgi. Rosyjskie modele wojny informacyjnej uwzględniają podział technologiczny na Wschód (Rosja) i Zachód (Stany Zjednoczone) oraz wartości narodowe i kulturowe, które mają kluczowe znaczenie dla dalszego rozwoju praktycznych działań prowadzonych w przestrzeni cybernetycznej. Dodatkowo wyróżniają one nie tylko zachodzące w niej procesy wymierzone w społeczeństwo, ale także narzędzia, czyli wszelkie środki bezpośrednio oddziałujące na daną zbiorowość ludzi po zorientowaniu zespołu działań. Aby proces ten przebiegał zgodnie z określonymi standardami, dokonano ustalenia łańcucha zarządzania, skupionego wyłącznie na procesach informacyjnych.

Dokonując ewaluacji zagrożeń bezpieczeństwa narodowego w cyberprzestrzeni skorzystano z wieloaspektowego i wielowymiarowego podejścia. Podejmując to zagadnienie uznano, że w pierwszej kolejności należy zdefiniować obiekty państwowe, które stając się celami ataków cybernetycznych, mogłyby wywołać znaczące niestabilności bezpieczeństwa narodowego. Do systemów tych należą: ważne obiekty wojskowe, systemy przedsiębiorstw oraz wchodzące w skład infrastruktury krytycznej państwa. Krótkoterminowa perspektywa wyantycypowała 5 podstawowych zagrożeń w cyberprzestrzeni, do których należą: Internet rzeczy, zwiększenie się aktywności cyberterrorystów oraz rozwój Darknetu, wzrost napięcia międzynarodowego związanego z cyberatakami oraz intensyfikacja prac legislacyjnych w obszarze cyberbezpieczeństwa.

Analizując wpływ mediów społecznościowych, w kontekście kształtowania cyberbezpieczeństwa narodowego, należy podkreślić ich cechy: możliwość szerokiego wykorzystania, łatwy dostęp (niezwiązany z nakładem finansowym); możliwość umieszczania treści w czasie rzeczywistym, w sposób dwukierunkowy – od i do nadawcy. Dodatkowo wykazano ich cechy w stosunku do tradycyjnych mediów, takie jak: zasięg, dostęp, użytkowanie, natychmiastowość oraz trwałość. Jako wyróżnik *social media* wskazano na ich dialogowość, polegającą na możliwości współkomunikowania się – sprzężenia zwrotnego pomiędzy nadawcą, a odbiorcą. Jest ona dodatkowo wspomagana multimedialnością, odziaływującą na większość zmysłów ludzkich. Wśród mechanizmów (sposobów) wykorzystania mediów społecznościowych w cyberprzestrzeni narodowej wyróżniono trzy ich grupy: operacje psychologiczne, dezinformację i propagandę oraz *fake news* i post-prawdę. W ramach operacji psychologicznych, prowadzonych w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika należało rozróżnić je od wojny psychologicznej w cyberprzestrzeni, wykazując jej długofalowe i agresywne oddziaływanie środkami politycznymi, propagandowymi, dyplomatycznymi, kulturalnymi i emocjonalnymi. Skie-

rowane są one na świadomość, psychikę oraz morale ludności cywilnej i sił zbrojnych.

Unia Europejska wdrożyła szereg rozwiązań organizacyjno-prawnych ukierunkowanych na poprawę bezpieczeństwa cyberprzestrzeni. Ramy działań określone zostały w dokumentach strategicznych. Na mocy dyrektywy NIS ustanowiono zaś wiele rozwiązań, które czynić mają państwa członkowskie i instytucje Wspólnoty Europejskiej mniej podatnymi na cyberzagrożenia. Należy do nich priorytetowy cel, jakim jest określenie obowiązków z zakresu cyberbezpieczeństwa, którymi mają podlegać operatorzy kluczowych usług, czyli np. infrastruktury krytycznej lub opieki medycznej. Powołano specjalistyczne instytucje realizujące zadania w tym zakresie. Ponadto, dyrektywa NIS zobowiązuje każde państwo członkowskie UE do wyznaczenia organu w celu ochrony bezpieczeństwa cybernetycznego i z jego pomocą opracowania odpowiedniej strategii. Wiele uwagi zarówno w unijnych dokumentach strategicznych, jak i aktach prawnych, poświęcono właściwej integracji mechanizmów działających w poszczególnych państwach członkowskich z mechanizmami na poziomie wspólnotowym. Dodatkowo Unia Europejska (podobnie jak NATO) organizuje ćwiczenia w zakresie cyberobrony, które pomagają zwiększyć umiejętności reagowania w warunkach realnego zagrożenia. Organizacja Traktatu Północnoatlantyckiego szczególną uwagę zwraca na problem szpiegostwa komputerowego, które mogłoby zostać nielegalnie wykorzystane przeciwko państwom członkowskim Sojuszu Północnoatlantyckiego, tym samym godząc w pozycję NATO jako gwaranta bezpieczeństwa. Pierwszą regulacją prawną, w ujęciu strategicznym, wydaną w celu ochrony systemów przed cyberszpiegostwem był „Program Obrony Cybernetycznej" (wraz z odpowiednimi komórkami wspomagającymi), którego działania skupiono wokół wysokiej zdolności do reagowania na incydenty komputerowe. Zakres wykonywanej działalności jest również bardzo zbliżony do zadań CERT. Kolejne dokumenty prawne rozszerzały, koordynowały i wspierały rozwój oraz wieloaspektowe podejście do kwestii cyberbezpieczeństwa, jak również cyberobrony na rzecz NATO i jego państw członkowskich. Należą do nich „Strategia Obrony Cybernetycznej" czy „Wzmocniona Polityka Cyberobrony". Oprócz aspektów prawnych, ważną kwestią mającą na celu zwiększenie świadomości społeczeństwa o wadze cyberzagrożeń jest rozwijana koncepcja *Smart Defense*, która w założeniu powinna przygotować państwa członkowskie na reagowanie w przypadku wysyłania do ich systemów m.in. złośliwego oprogramowania. Całokształt działań podejmowanych przez Sojusz Północnoatlantycki, w kontekście szeroko rozumianego cyberbezpieczeństwa ma być archiwizowany w postaci corocznych raportów. W ramach NATO, wyróżnić można 8 podmiotów odpowiadających za cyberbezpieczeństwo Sojuszu Północnoatlantyckiego. Należą do nich: Ze-

spół Reagowania na Incydenty Komputerowe NATO, Radę NATO ds. Zarządzania Cyberobroną, DPPCRF, Centrum Doskonalenia Obrony przed Cyberatakami, CERT, Grupa Szybkiego Reagowania w Cyberprzestrzeni oraz Komitet Cyberobrony. Omawiając działania NATO wskazano na czteroetapowy proces reagowania na zagrożenia cybernetyczne przez NATO, który został stworzony w celu efektywnego przeciwdziałania tego typu zagrożeniom. Uwagę skupiono także na aspektach związanych z artykułem 5. Traktatu Waszyngtońskiego, związanego z podjęciem przez Sojusz Północnoatlantycki przeciwdziałań w przypadku cyberataku. Ustalono, że w takim przypadku pod uwagę będą brane takie czynniki, jak: zasięg, czas trwania agresji, skutki oraz atrybucja. Z uwagi na niespełnienie wszystkich warunków, współczesne cyberataki nie powinny wywoływać częstego oddziaływania NATO.

Podejmując rozważania dotyczące przestępstw komputerowych, dokonywanych przy użyciu mediów społecznościowych ustalono, że w polskim systemie prawnym brak jest jednoznacznej definicji tych czynów, a próby jej zdefiniowania nie są ostre. Jednakże uogólniając można stwierdzić, że zawsze będą to czyny zabronione, skierowane przeciwko systemowi komputerowemu (w przypadku, gdy komputer jest celem ataku), jak i czyny dokonane przy użyciu komputera (w przypadku, gdy komputer jest narzędziem ataku). W literaturze istnieje kilka typologii przestępstw komputerowych. Jedne z prekursorów – Peter Sommer – wyróżnił cztery związane z nimi zjawiska. Należą do nich przestępstwa: niemożliwe do wykonania poza środowiskiem komputerowym, których dokonanie ułatwia użycie komputera, dokonywane przy biernym stosowaniu komputerów oraz popełniane z wykorzystaniem komputerów przez profesjonalnych przestępców. Oprócz przestępstw komputerowych, zwrócono także uwagę na agresorów oraz naruszycieli prawa, a także przedstawiono metody ich działalności, realizowanej za pomocą mediów społecznościowych. Jedną z metod stosowanych przez wymienionych agresorów cyberprzestrzeni jest mowa nienawiści. Analizując te treści zauważono reakcję Unii Europejskiej na problemy związane z tym negatywnym zjawiskiem społecznym.

Przedstawiając treści zawarte w pracy uznano, że właściwym będzie poprzedzenie ich charakterystyką i podstawowymi pojęciami związanymi z cyberbezpieczeństwem. Stwierdzono, że będzie to stanowiło wprowadzenie do zagadnienia, pozwalające na uporządkowanie wiedzy w obszarze badań. Poza tym takie podejście przyczyniło się do stworzenia podstawowej siatki pojęciowej. Tak zebrany rezerwuar pojęciowy może zostać wykorzystany do kolejnych opracowań, których treści odnosić się będą do cyberbezpieczeństwa.

Reasumując, należy stwierdzić, że zaprezentowane treści nie wyczerpują w pełni złożoności całego zagadnienia cyberbezpieczeństwa, jednak-

że zawierają najważniejsze aspekty i problemy dotyczące poruszanej tematyki. Co ważne, w odniesieniu do dynamiki zmian zagrożeń cybernetycznych, opracowanie zawiera aktualną wiedzę w tym obszarze. Dlatego też tworzy ona asumpt do poszerzenia problematyki książki, poprzez aktualizowanie zamieszczonych w pracy treści.

Bibliografia

Wydawnictwa zwarte

Arnold M.T., *A Comparative Analysis of Rootkit Detection Techniques*, University of Houston, Clear Lake 2011.

Ash B.R., *Information Theory*, Dover Publications, Inc., New York 1990.

Bezpieczeństwo teleinformatyczne państwa, red. M. Madej, M. Terlikowski, PISM, Warszawa 2009.

Bolter J.D., *Człowiek Turinga,* PIW, Warszawa 1990.

Bógdał-Brzezińska A., Gawrycki F.M., *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.

Bógdał-Brzezińska A., Gawrycki F.M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.

Brzeski R., *Wojna informacyjna – wojna nowej generacji*, Wydawnictwo Antyk Marcin Dybowski, Komorów 2014.

Ciborowski L., *Walka informacyjna*, Adam Marszałek, Toruń 1999.

Clarke R., Knake R., *Cyber War: the next threat to national security and what to do about it*, Harper-Collins Publishers, New York 2010.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, OSW, Warszawa 2014.

Dąbrowski T., Strycharek T., *Rola i zadania polskiego CERT-u wojskowego*, WBBŁiI, Warszawa 2016.

Denning E.D., *Walka informacyjna i bezpieczeństwo informacyjne*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002.

Dziubek I., *Antyterrorystyczne przygotowanie żołnierzy wojsk lądowych. Wybrane problemy*, AON, Warszawa 2010.

Dziubek I., *Edukacja obronna w Polsce*, Zysk i S-ka, Poznań 2013.

Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kantor Wydawniczy Zakamycze, Zakamycze 2000.

Gawliczek P., Pawłowski J., *Zagrożenia symetryczne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2003.

Gibson W., *Neuromancer*, (przeł.) P.W. Cholewa, Katowice 2009.

Gibson W., *Neuromancer*, Ace Books, New York 1984.

Golicyn A., *New Lies For Old, Londyn*, The Bodley Head, 1984.

Gręboszz M., Siuda D., Szymański G., *Social Media Marketing*, Wydawnictwo Politechniki Łódzkiej, Łódź 2016.

Gruza E., Goc M., Moszczyński J., *Kryminalistyka – czyli rzecz o metodach śledczych,* Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008.

Gustowski W., *Komunikacja w mediach społecznościowych*, Novae Res – Wydawnictwo Innowacyjne, Gdynia 2012.

Hartmann G.F., *The Relations of Nations*, Macmillan Publishing Co., Inc., London 1978.
Internet trolling as a tool of hybrid warfare: The case of Latvia – Results of the study, StratCom, Riga 2016.
Jędrzejewski M., *Analiza systemowa zjawiska infoterroryzmu*, AON, Warszawa 2002.
Krepinevich A., *Cyber warfare: a "nuclear option"?*, Center for Strategic and Budgetary Assessments 2012.
Kurtz H., *Media Circus – The Trouble with America's Newspapers*, New York 1993.
Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
Lakomy M., *Demokracja 2.0. Interakcja polityczna w nowych mediach*, Wydawnictwo WAM, Kraków 2013.
Lenczowski J., *Soviet Disinformation: An Overview, Background*, no. 465, The Heritage Foundation, Waszyngton DC 1985.
Libicki C.M., *Cyberdeterrence and cyberwar*, RAND Corporation 2009.
Libicki C.M., *What is Information Warfare?*, National Defense University, Center for Advanced Concepts and Technology, Washington D.C. 1995.
Liedel K., *Zarządzanie informacją w walce z terroryzmem*, Trio, Warszawa 2010.
Michalewski E., *Podstawy metody analizy diagnostycznej i projektowania systemów zarządzania (metoda DIANA)*, IBS PAN, Seria: Badania Systemowe, t. 34, Warszawa 2004.
Michalewski E., *Wspomagane komputerowo diagnoza i projektowanie systemów informacyjnych zarządzania,* Wyższa Szkoła Informatyki Stosowanej i Zarządzania, Seria: Manografie, Warszawa 2008.
Modrzejewski A., *Operacje informacyjne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2014.
Modrzejewski Z., *Operacje informacyjne*, Akademia Obrony Narodowej, Warszawa 2014.
Mynarski S., *Elementy teorii systemów i cybernetyki*, PWE, Warszawa 1979.
Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011.
Pepłoński A., *Wojna o tajemnice*, Wydawnictwo Literackie, Kraków 2011.
Podraza A., Potakowski P., Wiak K., *Cyberterroryzm zagrożeniem XXI wieku*, Difin, Warszawa 2013.
Rheingold H., *The virtual community. Homesteading on the electric fronter*, Addison-Wesley, Reading MA, 1993.
Schwartau W., *Information Warfare: Chaos on the Electronic Superhighway* 1st, Thunder's Mouth Press, New York 1994.
Skudrzyk A., *Homo videns – nowe media a język młodego pokolenia*, Uniwersytet Śląski, Katowice 2017.
Soral W., *Mowa nienawiści. Definicja, przyczyny, skutki, skala zjawiska*, Centrum Badań nad Uprzedzeniami UW, Warszawa 2017.
Szpyra R., *Operacje informacyjne państwa w działaniach sił powietrznych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002.
Tofller A., Toffler H., *War and anti-war: survival at the dawn of the 21st century*, Boston 1993.
Wallace P., *Psychologia Internetu*, Rebis, Poznań 2003.
Weimann G., *Cyberterrorism. How real is the threat?*, United States Institute of Peace, Special Report 119, December 2004.
Wesołowski J., *Klasyfikacja gatunkowa trolli sieciowych, dokonana na podstawie obserwacji grup dyskusyjnych w hierarchii PL*, *s.l./s.n.*, 2002.
Wojnarowski J., *Gotowość systemu bezpieczeństwa narodowego*, Wydawnictwo, Warszawa 2010.
Wrzosek M., *Dezinformacja jako komponent operacji informacyjnych*, Warszawa 2005.

Żebrowski A., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000.
Żebrowski A., *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016.

Rozdziały w wydawnictwach zwartych

Bielawski R., Ziółkowska A., *Media społecznościowe, a kształtowanie bezpieczeństwa państwa* [w:] *Człowiek a technologia cyfrowa – przegląd aktualnych doniesień*, red. P. Szymczyk, K. Maciąg, Wydawnictwo Naukowe TYGIEL, Lublin 2018.
Cebrowski K.A., Garstka J.J., *Network Centric Warfare, Its Origin and Future* [w:] *Proceedings of the Naval Institute* 124:1, January 1998.
Dereń J., *Asymetryczność wyzwaniem dla bezpieczeństwa XXI wieku* [w:] *Biblioteka Wiedzy o Bezpieczeństwie. Metodologia badań bezpieczeństwa narodowego*. *Tom III*, red. P. Sienkiewicz, M. Marszałek, H. Świeboda, Akademia Obrony Narodowej, Warszawa 2012.
Dereń J., Rabiak A., *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Difin, Warszawa 2014.
Fabjaniak-Czerniak K., *Internetowe media społecznościowe jako narzędzie public relations* [w:] *Zarządzanie w sytuacjach kryzysowych niepewności,* red. K. Kubiak, Warszawa 2012.
Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu* [w:] *Bezpieczeństwo narodowe* II – 2012*,* nr 22, BBN, Warszawa 2012.
Kaznowski D., *Social media – społeczny wymiar Internetu* [w:] *E-marketing. Współczesne trendy. Pakiet startowy*, red. J. Królewski, P. Sala, PWN, Warszawa 2016.
Orzechowski M., *Koncepcja walki informacyjnej jako element bezpieczeństwa Federacji Rosyjskiej. Wojna w Donbasie jako study case zastosowania elementów walki informacyjnej* [w:] *Polska – Rosja, Polityka bezpieczeństwa Federacji Rosyjskiej*, red. M. Kaszub, M. Minkin, Wydawnictwo UPH, Siedlce 2016.
Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.
Sienkiewicz P., *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?,* red. L.H. Haber, T. 1, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003.
Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, [w:] *„Rodzinna Europa". Europejska myśl polityczno-prawna u progu XXI wieku,* H. Malewski, Henryk, P. Fiktus, M. Marsza (red.), E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2015.

Wydawnictwa ciągłe

Adamczuk M., *Ewolucja strategii i metod działania islamskich ugrupowań terrorystycznych i ich wpływ na bezpieczeństwo Polski*, „Bezpieczeństwo Narodowe", nr 19, Biuro Bezpieczeństwa Narodowego, Warszawa 2011.

Adamczuk M., Liedel K., *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

Aleksandrowicz R.T., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15.

Arquilla J., Ronfeldt D., *Cyberwar is coming!*, „Comaparative Strategy" 1993.

Bielawski R., Radomska A., *Selected models of information warfare in cyberspace*, „Security and Defence Quarterly" 2017, nr 1(14).

Czeszejko S., *Działania w środowisku elektronicznym a świadomość sytuacyjna pola walki*, „Journal of KONBiN" 2011, nr 18.

Czulda R., *Atak w wirtualu*, „Polska Zbrojna" 2013, nr 11(811).

Dugin A., *Gieopolitika postmodierna*, (przeł) P. Sieradzan, „Geopolityka" 2009, nr 1(2).

Grabowski T., *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016)*, „Horyzonty Polityki" 2016, nr 7 (20).

Grenda B., *Sieciocentryczne zarządzanie siłami powietrznymi,* „Journal of KONBiN" 2011, nr 3(19).

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

Hanna R., Rohm A., Crittenden L.V., *We're All connectwd: The Power of the socal media ekosystem*, „Business Horizons" 2011, vol. 54, no. 3.

Jakubski K., *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo" 1996, nr 12.

Juza M., *Hejterstwo w komunikacji internetowej: charakterystyka zjawiska, przyczyny i sposoby przeciwdziałania*, „Profilaktyka Społeczna i Resocjalizacja" 2015, nr 25.

Kacała T., *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, 2(24).

Kaczyńska K., *Koncepcja neo-eurazjatyzmu Aleksandra Dugina*, „Nowy Prometeusz" 2013, nr 5.

Kozłowski A., *NATO wobec wyzwań i zagrożeń w cyberprzestrzeni*, „Biuletyn OPINIE FAE" 2016, nr 7.

Krok E., *Media społecznościowe elementem systemu zarządzania wiedzą w firmie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2011, nr 656.

Lachow I., Richardson C., *Terrorist use of the internet. The real story*, „Joint Force Quartely" 2007, no. 45.

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

Marzec M., *Media w procesie komunikowania politycznego – władza, wpływ a może symbioza?*, „Palimpsest" 2010, nr 1.

Matusitz J., *Cyberterrorism: how can American foreign policy by strenghtenedet in the information age?*, „American Foreign Policy Interests" 2005, vol. 27, no. 2.

Mąka D., Sienkiewicz P., *Sieciocentryczna infrastruktura procesów decyzyjnych*, „Zeszyty Naukowe AON" 2009, nr 2.

Michalewski E., *Analiza systemów sieciocentrycznych*, Polskie Stowarzyszenie Zarządzania Wiedzą, „Seria: Studia i Materiały" 2010, nr 32.

Młotek M., Siedlarz M., *Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 4.

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Cyberkłopoty i Pułapki Sieci" 2010, nr 4(113).
Scheffs W., *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, „Journal of KONBiN" 2011, nr 3(19).
Sieber U., *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka,* „Przegląd Policyjny" 1995, nr 3.
Sowa M., *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo" 2002, nr 4.
Szews P., *Medialny fanpage – szanse i zagrożenia*, „Media i Społeczeństwo" 2015, nr 5.
Świech A., *Rewolucja dokonana – czym jest cyberpunk?*, „Ha!art" 2002, nr 2/3.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.
Weimann G., *Cyberterrorism: the sum of all fears?*, „Studies in Conflict and Terrorism" 2005, vol. 28, no. 2.
Wrzosek M., *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2(87).

Encyklopedie, słowniki

Deacon R., *Spyclopaedia*, Futura, Londyn 1989.
Encyclopedia PWN, online https://encyklopedia.pwn.pl/encyklopedia/wojna%20psychologiczna.html [dostęp: 11.08.2017].
Encyclopedia PWN, online – https://encyklopedia.pwn.pl/haslo/propaganda;3962718.html [dostęp: 11.08.2017].
Encyclopedia PWN, online – https://encyklopedia.pwn.pl/haslo/wojna-psychologiczna;3997505.html [dostęp: 11.08.2017].
Encyklopedia Gazety Prawnej, online – http://www.gazetaprawna.pl/encyklopedia/prawo/hasla/332774,haker.html [dostęp: 02.07.2017].
Encyklopedia Zarządzania, online – https://mfiles.pl/pl/index.php/Ryzyko [dostęp: 11.07.2017].
Bennett M.R., *Espionage: An Encyclopedia of Spies and Secrets*, Virgin Books, Londyn 2002.
Słownik Języka Polskiego PWN, online – http://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915 [dostęp: 19.04.2017].
Słownik Języka Polskiego PWN, online – http://sjp.pwn.pl/sjp/cybernetyka;2553914 [dostęp: 03.05.2017].
Słownik Języka Polskiego PWN, online – http://sjp.pwn.pl/slowniki/dez%20.html [dostęp: 19.08.2017].
Słownik Języka Polskiego PWN, online – https://sjp.pl/bloger [dostęp: 19.08.2017].
Słownik Języka Polskiego PWN, online – https://sjp.pl/cyberatak [dostęp: 29.06.2017].
Słownik Języka Polskiego PWN, online – https://sjp.pl/szowinizm [dostęp: 15.08.2017].
Słownik Języka Polskiego PWN, online – https://sjp.pwn.pl/szukaj/dezinformacja.html [dostęp: 25.08.2017].
DOD Dictionary of Military and Associated Terms, As of March 2017.

Analizy, ekspertyzy, komunikaty, programy, raporty, rekomendacje i strategie

Concept for Future Joint Operations, Joint Chiefs of Staff, 1997.

CYBERSEC PL 2016. Rekomendacje, Polskie Forum Cyberbezpieczeństwa, Warszawa 2016.

DOD & Joint Staff – CJCSI 3210.01 [w:] *FM 100-6 Information Operations*, Headquarters, Department of the Army, 1996.

Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej, 6 grudnia 2016, nr 646.

Doktryna Bezpieczeństwa Informacyjnego RP – projekt, BBN, Warszawa 2015.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015.

Europejska strategia bezpieczeństwa. Bezpieczna Europa w lepszym świecie, Urząd Publikacji Unii Europejskiej, Luksemburg 2009.

Friedrichs G., Schaff A. (red.), *Mikroelektronika i społeczeństwo. Na dobre czy na złe?* Raport Klubu Rzymskiego, Książka i Wiedza, Warszawa 1987.

IBM ISS Managed Security Services, March 31, 2009.

International Strategy for Cyberspace. Prosperity, Secirity, and Openess in a Networked World, May 2011.

Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013.

Joint Publication 3-13, *Joint Doctrine for Command and Control Warfare (C2W)*, 9 October 1998.

Joint Publication 3-13.2, Psychological Operations, 07 January 2010.

Katalog zagrożeń, CERT.GOV.PL, 2017.

Koncepcja Strategiczna NATO z 2010 r.

Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji, Warszawa 2017.

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku, CERT.GOV.PL, Warszawa 2016.

Raport: „Fake news z perspektywy polskich dziennikarzy" – wyniki badań, Public Dialog, 2017.

Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "hate speech", Rada Europy, Strasburg 1997.

Regulamin działań Wojsk Lądowych, DWLąd, Warszawa 2002.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa 2014.

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017.

Strategia Obronności Rzeczpospolitej Polskiej, Warszawa 2009.

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022 – przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r., BBN, Warszawa 2013.

The National Strategy to Secure Cyberspace February 2003.

University of Arizona Cybersecurity Framework, ver. 004, 8/29/2016.

Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, Komisja Europejska, Bruksela 2013.

Akty prawne

Dyrektywa Parlamentu i Rady Unii Europejskiej w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE z dnia 19.07.2016 r, Nr L 194/1).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE 19.7.2016 L 194/1).

Decyzja ramowa Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych (Dz.Urz. UE L 328/55 z dnia 6.12.2008, art. 1, pkt. 1a–d).

Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. 2000 nr 87 poz. 970).

Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r.(Dz.U. 2003 nr 78 poz. 708).

Porozumienie międzynarodowe w przedmiocie ścigania i karania głównych przestępców wojennych Osi Europejskiej, podpisanego w Londynie dnia 8 sierpnia 1945 r. (Dz.U. z 1947 r. poz. 367).

Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2011 r. nr 222 z późn. zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm.).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r. nr 29, poz. 154).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553, art. 267 z późn. zm.).

Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 1967 r. nr 44, poz. 220).

Decyzja Nr 38/MON Ministra Obrony Narodowej z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni (Dz.Urz. MON z 2012 r., poz. 52, pkt. 3, ppkt. 1–5).

Inne

Cebrowski K.A., *Network Centric Warfare*, *An Emerging Military Response to the Information Age.* Command and Control Research and Technology Symposium, Naval War Collage, Newport, RI, June 2003.

Garstka J.J., *Theory and practise of Network Centric Warfare*, Materiały z konferencji „Conference Documentation from Network Centric Warfare Conference", London, 10-11th September 2001.

Kośla R., *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*. Wystąpienie na konferencji w Bemowie, 29 listopada 2002.

PN-ISO/IEC 27005:2010 Zarządzanie ryzykiem w bezpieczeństwie informacji; PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN, Warszawa 2013.

Storch T., *Cyberbezpieczeństwo – fundament bezpiecznego społeczeństwa w dobie internetu*, TwC Next, Microsoft, 9 marca 2012 r., s. 4. Dokument udostępniony w sieci na licencji

Źródła internetowe

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA). Informacje ogólne, online – https://europa.eu/european-union/about-eu/agencies/enisa_pl [dostęp: 07.09.2017].

Aleksandrowicz T., *Wojna informacyjna. Dlaczego Zachód przegrywa z Rosją?*, online – https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-wojna-informacyjna-dlaczego-zachod-przegrywa-z-rosja

Atak hakerów na PLL LOT, online – http://www.polskieradio.pl/69/273/Artykul/1465337,Atak-hakerow-na-PLL-LOT-celem-ataku-system-naziemny-lotniska-bez-wplywu-na-system-rezerwacji [dostęp: 14.07.2017].

Boty i sieci typu „bot" — rosnące zagrożenie, online – https://pl.norton.com/botnet [dostęp: 07.07.2017].

CERT-UE for the EU institutions, bodies and agencies, online – https://cert.europa.eu/cert/plainedition/en/cert_about.html [dostęp: 07.09.2017].

Co to jest atak DDoS i jak się przed nim chronić?, Dataspace 2017, https://dataspace.pl/assets/ddos_broszura_web.pdf [dostęp: 31.01.2019].

Cyber defence, online – http://www.nato.int/cps/en/natohq/topics_78170.htm [dostęp: 08.09.2017].

Cyberbezpieczeństwo. Wyzwania i zagrożenia w 2017 roku, 2017, online – http://aspolska.pl/cybe rbezpieczenstwo-wyzwania-i-zagrozenia-w-2017-roku/ [dostęp: 06.07.2017].

Demchak Ch., *Cybered Conflict vs. Cyberwar*, http://www.acus.org/new_atlanticist/cybered-con-fl ict-vs-cyber-war [dostęp: 30.06.2017].

Dobranowska-Wittels M., *Decydująca rola źródeł informacji dla sytuacji politycznej na przykładzie Ukrainy*, online – http://www.kirkland.edu.pl/ru/2012-12-19-12-21-29/83-biblioteka/315-piddub [dostęp: 19.08.2017].

Fałszerstwo komputerowe, online – http://cyberprzestepczosc.info/falszerstwo-komputerowe/ [dostęp: 14.09.2017].

Gełzakowski W., *ISO 27005 Analiza ryzyka*, https://www.centrum-doskonalenia.pl/wdrozenie-i-certyfikacja-iso/normy-iso/iso-27005-analiza-ryzyka/ [dostęp: 31.01.2019].

Gladwell M., C. Shirky, *From Innovation to Revolution. Do Social Media Make Protests Possible?*, online – https://www.foreignaffairs.com/articles/2011-01-19/innovation-revolution [dostęp: 28.08.2017].

http://networkeddigital.com/2010/05/10/podzial-i-klasyfikacja-social-media/ [dostęp: 28.08.2017].

http://rcb.gov.pl/o-rcb/ [dostęp: 29.08.2017].

http://srnik.wp.mil.pl/pl/index.html [28.08.2017].

http://www.policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html [dostęp: 29.08.2017].

http://www.skw.gov.pl/zadania.html [dostęp: 29.08.2017].

https://cybersecforum.eu/pl/nas-czeka-obszarze-cyberbezpieczenstwa-2017-r-publikujemy-prognozy-ekspertow/ [dostęp: 31.01.2019].

https://marketingwsieci.pl/slownik-e-marketingu/ppc-pay-per-click/ [dostęp: 30.01.2019].
https://mc.gov.pl/o-nas [dostęp: 29.08.2017].
https://pl.wikiquote.org/wiki/Think_tank [dostęp: 30.01.2019].
https://plblog.kaspersky.com/botnet/6302/ [dostęp: 03.07.2017].
https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted [dostęp: 03.07.2017].
https://www.uke.gov.pl/kompetencje-972 [dostęp: 29.08.2017].
Infrastruktura krytyczna, Rządowe Centrum Bezpieczeństwa, online – http://rcb.gov.pl/infrastruktura-krytyczna/ [dostęp: 11.07.2017].
Józefiak B., *Na bazie CERT Polska rusza Narodowe Centrum Cyberbezpieczeństwa*, online – http://www.cyberdefence24.pl/398863,na-bazie-cert-polska-rusza-narodowe-centrum-cyberbezpieczenstwa
Kaznowski D., *Podział i klasyfikacja social media, Networked Digital Ag*e, online – http://networkeddigital.com/2010/05/10/podzial-i-klasyfikacja-social-media/ [dostęp: 28.08.2017].
Krautz W., *Piąty wymiar walki, czyli logiczne konsekwencje modelu Wardena*, online – http://xportal.pl/?p=2110 [dostęp: 28.06.2017].
Krytyczna infrastruktura zagrożona cyberatakami, online – http://di.com.pl/krytyczna-infrastruktura-zagrozona-cyberatakami-54699 [dostęp: 15.07.2017].
Liczba cyberataków na firmy w Polsce rośnie znacznie szybciej niż na świecie, 2016, online – https://www.pwc.pl/pl/media/2016/2016-01-12-liczba-cyberatakow-na-firmy-w-polsce-rosnie.html [dostęp: 10.07.2016].
Liedel K., *Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego*, online – http://www.liedel.pl/?p=13 [dostęp: 27.06.2017].
Łuczyńska A., *Jak radzić sobie z fake news?*, Fundacja Szkoła z Klasą, 2017, s. 1–2 (CC-BY-SA 3.0), https://migracje.ceo.org.pl/sites/migracje.ceo.org.pl/files/10_wskazowek_fake_news.pdf
Ministerstwo Cyfryzacji, online – https://mac.gov.pl/dzialania/krmc-dopinanie-projektow-przed-koncem-roku [dostęp: 29.06.2017].
Muczyński R., *Największy cyberatak w historii?*, online – http://www.nowastrategia.org.pl/najwiekszy-cyberatak-w-historii/ [dostęp: 15.07.2017].
NATO Cooperative Cyber Defence Centre of Excellence, online – https://ccdcoe.org/ [dostęp: 08.09.2017].
Nazario J., *Two Weeks of Conficker Data and 12 Million Nodes*, 2009, online – https://www.arbornetworks.com/blog/asert/two-weeks-of-conflicker-data/ [dostęp: 05.07.2017].
Pięć wyzwań cyberbezpieczeństwa w 2017 roku, online – http://www.cyberdefence24.pl/52003 9,piec-wyzwan-cyberbezpieczenstwa-w-2017-roku [dostęp: 09.07.2017].
Przestępstwa komputerowe – zarys problematyki, online – http://kryminalistyka.org.pl/artykuly/przestepstwa-komputerowe-zarys-problematyki/#_ftnref7 [dostęp: 15.09.2017].
Rhodes A., *Do you have Conficker? Find out in your OpenDNS account*, 2009, online – https://umbrella.cisco.com/blog/blog/2009/04/02/do-you-have-conficker-find-out-in-your-opendns-account/ [dostęp: 05.07.2017].

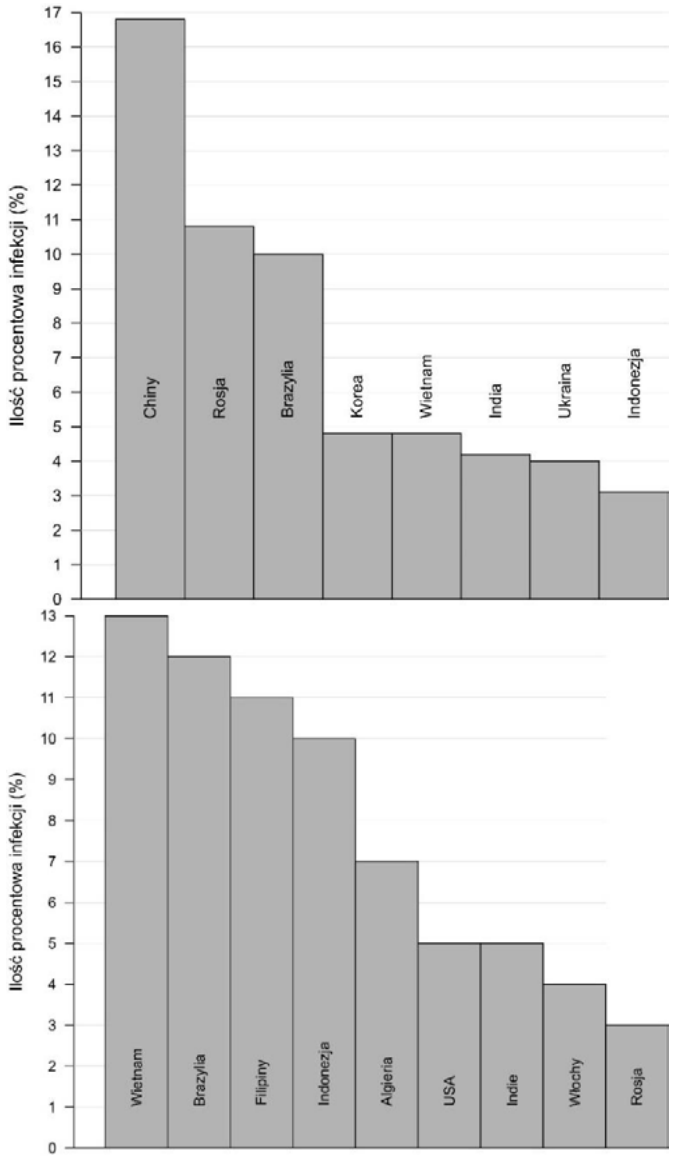
Rhodes A., *Do you have Conficker? Find out in your OpenDNS account*, 2009, online – https://umbrela.cisco.com/blog/blog/2009/04/02/do-you-have-conficker-find-out-in-your-opendns-account/ [dostęp: 05.07.2017].
Roszmann M., Wilczewska K., *Internet jako nowoczesne medium komunikacji w społeczeństwie*, online – http://kneb.wpit.am.gdynia.pl/?p=513 [dostęp: 28.08.2017].
Rudke M., *Cyberatak: Będzie więcej ataków na banki i ich klientów*, online – http://www.rp.pl/Banki/302059917-Cyberatak-Bedzie-wiecej-atakow-na-banki-i-ich-klientow.html [dostęp: 14.07.2017].
Szurmiński Ł., *Pojęcie propagandy*, 2016, online – http://www.id.uw.edu.pl/~lukasz.szurm /Anatomia%20propagandy/2.%20Poj%C4%99ie%20propagandy.pdf [dostęp: 25.08.2017].
Warden J., *The Enemy as System*, Maxwell 1995, online – http://www.airpower.maxwell.af.mil /airchronicles/apj/apj95/spr95_files/warden.htm [dostęp: 23.04.2017].
Wielka Ilustrowana Encyklopedia Internetowa Mike'a Reeda, online – http://trole.joemonster.org/index.php [dostęp: 13.08.2017].
Wilczewska K., *Internet jako nowoczesne medium komunikacji w społeczeństwie*, online – http://kneb.wpit.am.gdynia.pl/?p=513 [dostęp: 28.08.2017].
Willsher K., *French fighter planes grounded by computer virus*, 2009, online – http://www.telegr aph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html [dostęp: 05.07.2017].
Woźniak K., *Informacja*, https://mfiles.pl/pl/index.php/Informacja [dostęp: 28.01.2019].
Zapobieganie i zwalczanie terroryzmu. Cyberterroryzm, online – http://www.msz.gov.pl/pl/polityka_zagraniczna/polityka_bezpieczenstwa/zwalczanie_terroryzmu_miedzynarodowego/zapobieganie_i_zwalczanie_terroryzmu/page_30058?printMode=true [dostęp: 08.09.2017].
ZeuS – P2P+DGA variant – mapping out and understanding the threat, 2012, online – https://www.cert.pl/news/single/zeus-wariant-p2pdga-analiza-nowego-zagrozenia/ [dostęp: 05.07.2017].
ZeuS – P2P+DGA variant – mapping out and understanding the threat, 2012, online – https://www.cert.pl/news/single/zeus-wariant-p2pdga-analiza-nowego-zagrozenia/ [dostęp: 05.07.2017].
Войны и их классификация, online – http://voina-i-mir.ru/article/109 [dostęp: 25.08.2017].

Spis rysunków

Spis tabel

Załączniki

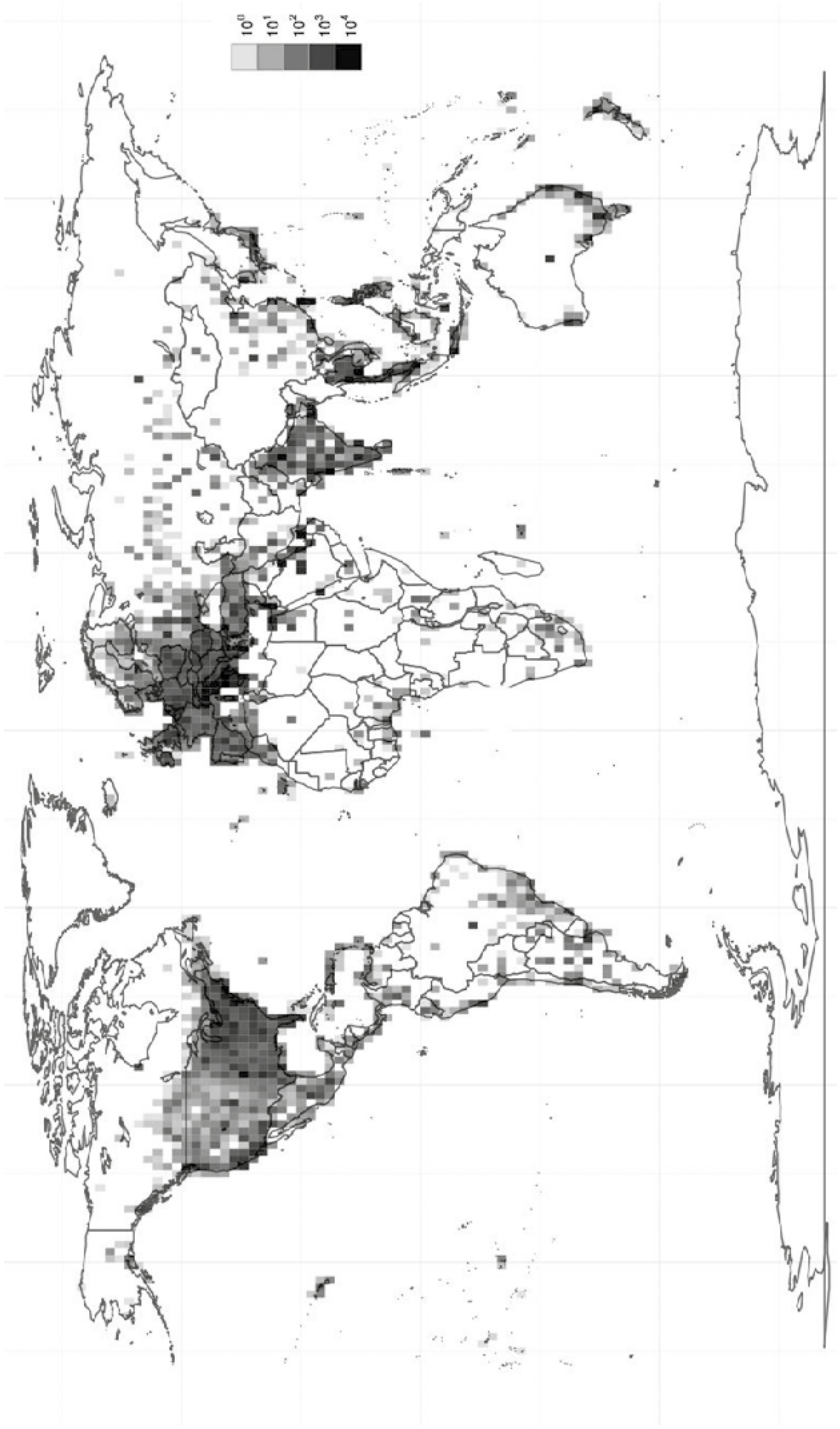
Załącznik 1 – Infekcja systemów komputerowych przez botnet Conficker



Infekcja systemów komputerowych (%) państw przez botnet Conficker w a) marcu 2009 roku , b) kwietniu 2010 roku

Źródło: opracowanie własne na podstawie *IBM ISS Managed Security Services, March 31, 2009*, A. Rhodes, *Do you have Conficker? Find out in your OpenDNS account*, 2009, online – https://umbrella.cisco.com/blog/blog/2009/04/02/do-you-have-conficker-find-out-in-your-opendns-account/ [dostęp: 05.07.2017].

Załącznik nr 2 – Światowa skala infekcji botnetem Zeus



Zagęczczenie infekcji botnetem GameOver Zeus (GOZ) w skali światowej
Źródło: opracowanie własne na podstawie *ZeuS – P2P+DGA variant – mapping out and understanding the threat*, 2012, online –https://www.cert.pl/news/single/zeus-wariant-p2pdga-analiza-nowego-zagrozenia/ [dostęp: 05.07.2017].

Załącznik 3 – Algorytm obliczania ryzyka aktywu oraz ryzyka szczątkowego

Ryzyko aktywu można obliczyć według poniższego wzoru:

$$R_a=E(W_a \times P_{wz})$$

gdzie:
R_a – ryzyko aktywu
W_a – wpływ (skutek) zmaterializowania się zagrożenia (uzależniony od istotności aktywu, jego zagrożeń, podatności), rozumiany jako:

$$W_a =S_p((W_p + W_i +W_d)*LZ*W_{pd})$$

gdzie:
S_p – suma wg podatności
W_p – wpływ zagrożenia na poufność
W_i – wpływ zagrożenia na integralność
W_d – wpływ zagrożenia na dostępność
LZ – liczebność zasobu/ilość miejsc przetwarzania
W_{pd} – wpływ liczebności na podatność

Ryzyko szczątkowe można obliczyć z poniższej zależności:

$$R_{sa}=W_{sa} \times P_{wz}$$

gdzie:
Rs_a – ryzyko szczątkowe
W_{sa} – wpływ (skutek) zmaterializowania się zagrożenia (uzależniony od istotności aktywu, jego zagrożeń, podatności oraz zastosowanych zabezpieczeń)

$$W_a=S_p((W_p/Z_p + W_i/Z_i +W_d/Z_d)*LZ*W_{pd})$$

gdzie:
Z_p – poziom zabezpieczeń przed wpływem zagrożenia na poufność
Z_i – poziom zabezpieczeń przed wpływem zagrożenia na integralność
Z_d – poziom zabezpieczeń przed wpływem zagrożenia na dostępność.

O Autorach

ppłk dr inż. Radosław BIELAWSKI – absolwent Wojskowej Akademii Technicznej, Akademii Obrony Narodowej oraz Prywatnej Wyższej Szkoły Businessu, Administracji i Technik Komputerowych w Warszawie. Zastępca Dyrektora Instytutu Podstaw Bezpieczeństwa Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej. Redaktor naczelny czasopisma naukowego „Security and Defence Quarterly". Ekspert Narodowego Centrum Badań i Rozwoju Programu Operacyjnego Inteligentny Rozwój (POIR). Autor kilku monografii naukowych, prac badawczo-naukowych oraz ponad 30 artykułów naukowych z zakresu bezpieczeństwa.

płk nawig. dr hab. Bogdan GRENDA – absolwent Wyższej Oficerskiej Szkoły Lotniczej. Ukończył studia podyplomowe „Dowódczo-Sztabowe" w Akademii Obrony Narodowej oraz Logistykę w Uniwersytecie Ekonomicznym w Poznaniu. W 2006 r. uzyskał stopień doktora nauk wojskowych w specjalności Siły Powietrzne. Od 2015 r. doktor habilitowany w dziedzinie nauk społecznych w dyscyplinie nauki o obronności. Uczestnik ćwiczeń narodowych i międzynarodowych oraz kursów specjalistycznych. Pełnił służbę w 62 Pułku Lotnictwa Myśliwskiego w Poznaniu, Zarządzie Dowodzenia i Łączności Dowództwa Wojsk Lotniczych i Obrony Powietrznej w Warszawie, Centrum Operacji Powietrznych w Warszawie oraz Zarządzie Operacji SP Dowództwa Sił Powietrznych w Warszawie. W latach 2007-2010 zastępca dowódcy w 6 Bazie Lotniczej w Dęblinie. Od 2010 r. pracuje w Akademii Obrony Narodowej. Od 2018 r. pełni obowiązki Dziekana Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej.

ISBN 978-83-66187-36-8 (PDF)