Arkadiusz Wochnowicz*

Cyberprzestrzeń w systemie militarnym bezpieczeństwa państwa

„Cyberprzestrzeń. Mimowolna halucynacja doświadczana każdego dnia […]. Graficzny obraz danych, wyabstrahowanych z banków każdego komputera ludzkiej domeny. Niewyobrażalna złożoność. Linie światła sięgającego nie-przestrzeni umysłu, roje i konstelacje danych. Jak światła miasta, milknące w oddali…".

William Gibson, *Neuromancer*, Warszawa 2001

Streszczenie

W artykule zostały przedstawione podstawowe pojęcia związane z bezpieczeństwem, które współcześnie uważa się za stan pewności, spokoju, zabezpieczenia oraz brak zagrożenia i ochronę przed niebezpieczeństwem, oraz z cyberprzestrzenią, która jest rozumiana jako wirtualne środowisko informacji i interakcji między ludźmi. W artykule tym pokazano również definicje pojęć odnoszących się do wartości najwyżej cenionej i chronionej przez człowieka, tj. bezpieczeństwa państwa, która jest integralną częścią polityki państwa związaną z tworzeniem i wykorzystaniem narodowego potencjału obronnego w celu zapobiegania i przeciwdziałania różnego rodzaju zagrożeniom. Pokazano znaczenie istotnych komórek Sił Zbrojnych RP jako podstawowego organu kształtowania cyberprzestrzeni w obszarze militarnym. Określono rolę i miejsce organów w Sił Zbrojnych RP gotowych do reagowania na zagrożenia systemów i sieci teleinformatycznych, których łączy cyberprzestrzeń.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo narodowe, cyberprzestrzeń, cyberbezpieczeństwo

* Dr inż. Arkadiusz Wochnowicz, wykładowca w Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej w Warszawie.

Wstęp

Współcześnie za bezpieczeństwo uważa się stan pewności, spokoju, zabezpieczenia oraz brak zagrożenia i ochronę przed niebezpieczeństwem. Obejmuje ono zaspokojenie takich potrzeb, jak: istnienie, przetrwanie, całość, niezależność, spokój, posiadanie i pewność rozwoju. Jest ona naczelną potrzeba człowieka, grup społecznych i równocześnie podstawową potrzebą państwa. Każde państwo w związku z tym stara się oddziaływać na swoje otoczenie zewnętrzne i sferę wewnętrzną, żeby usunąć lub przynajmniej oddalić występujące zagrożenia, likwidować własny lęk, obawy, niepewność i niepokój.

Obecnie w świecie globalizacji i informacji bezpieczeństwo w cyberprzestrzeni stanowi jedną z najważniejszych potrzeb, której zaspokojenie określa warunki rozwoju ludzkiej cywilizacji. Zapewnienie bezpieczeństwa kraju mieści się w związku z tym w katalogu podstawowych potrzeb i zadań Sił Zbrojnych RP, które stoją na straży granic państwa i są ich gwarantem.

Celem artykułu jest pokazanie znaczenia istotnych komórek Sił Zbrojnych RP jako podstawowego organu kształtowania cyberprzestrzeni w obszarze militarnym. Podejmując się niniejszej tematyki, kierowano się potrzebą określenia roli i miejsca organów w Sił Zbrojnych RP gotowych do reagowania na zagrożenia systemów i sieci teleinformatycznych, których łączy cyberprzestrzeń.

Autor w artykule przedstawił podstawowe pojęcia związane z cyberbezpieczeństwem najczęściej definiowanym jako „[…] całość powiązań ludzkiej działalności z udziałem ICT (Information and Communication Technology)”[1]. Przedstawia definicje pojęć odnoszących się do wartości najwyżej cenionych i chronionych przez człowieka, tj. bezpieczeństwa, bezpieczeństwa narodowego. Przedstawił organy działające na rzecz cyberbezpieczeństwa w systemie militarnym mające za zadanie ochronę państwa przed możliwymi zagrożeniami i tworzenie warunków do zapobiegania tym zagrożeniom.

1 K. Ratheeswari, *Information Communication Technology in Education*, „Journal of Applied and Advanced Research” 2018, t. 3, https://uchitelya.kz/assets/materials/2020/10/information_communication_technology_in_education.pdf [dostęp: 25.02.2023]; J. Pearson, *Information and Communications Technologies and Teacher Education in Australia*, „Technology, Pedagogy and Education” 2003, t. 12, nr 1, s. 39–58.

Definiowanie bezpieczeństwa i cyberprzestrzeni

Pojęcie „bezpieczeństwo" w literaturze jest przedstawiane wieloznacznie. Wśród wielu definicji i klasyfikacji najczęściej postrzega się je w relacjach odnoszących się do stanu zagrożenia. Celem podmiotu działającego na rzecz własnego bezpieczeństwa jest ochrona przed zagrożeniami. Ujęcie pozytywne, nieodnoszące się bezpośrednio do zagrożenia – charakteryzuje dążenie podmiotu do kształtowania pewności przetrwania i rozwoju. Współczesne definicje leksykalne określają bezpieczeństwo (łac. *sine cura*) jako „[...] stan pewności, spokoju, zabezpieczenia oraz jego poczucia i wskazują, że oznacza ono brak zagrożenia oraz ochronę przed niebezpieczeństwami"[2].

Pojęcie to koncentruje się na definiowaniu bezpieczeństwa w przeciwstawieniu do zagrożenia. Tak zdefiniowane bezpieczeństwo możemy odnieść m.in. do sfery wojny. Zapewnienie bezpieczeństwa jest wówczas równoznaczne z uniemożliwieniem agresji zbrojnej. Pojęcie szersze oznacza „[...] kształtowanie pewności przetrwania, posiadania i swobód rozwojowych podmiotu"[3]. Tak rozumiane bezpieczeństwo nie sprowadza się już jedynie do zagadnień czysto militarnych.

Jan Wojnarowski definiuje pojęcie bezpieczeństwa jako „[...] stan, który daje poczucie pewności (istnienia i przetrwania oraz warunków rozwoju i aktywności) i gwarancje jego zachowania oraz szanse na doskonalenie. Jedna z podstawowych potrzeb człowieka, sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni"[4]. Bezpieczeństwo, ponieważ jest jedną z naczelnych potrzeb człowieka oraz jednym z jego celów, jest podstawową potrzebą państw i systemów międzynarodowych.

W słowniku języka polskiego bezpieczeństwo zostało określone jako stan niezagrożenia, spokoju, pewności[5], lecz nie oddaje jego całkowitego znaczenia. Ponieważ można powiedzieć, że bezpieczeństwo coraz rzadziej oznacza brak zagrożeń. Coraz częściej na bezpieczeństwo spogląda się z punktu widzenia innych cech i wartości oraz celów, które stanowią o nim.

2 R. Zięba, *Kategorie bezpieczeństwa w nauce o stosunkach międzynarodowych* [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. D. Bobrow, E. Haliżak, R. Zięba, Warszawa 1997, s. 3.

3 Ibidem, s. 30.

4 J. Wojnarowski, *Teoretyczne podstawy podsystemu bezpieczeństwa militarnego RP*, „Myśl Wojskowa" 2004, nr 6, s. 39.

5 *Słownik języka polskiego*, red. M. Szymczak, t. 1, Warszawa 1978, s. 147.

Najstarsza formuła bezpieczeństwa – bezpieczeństwo narodowe – wywodzi się z kategorii egzystencjonalnych potrzeb i interesów społeczności tworzących państwa. Do ich zaspokajania służy aparat państwowy. Dlatego w nauce jest przyjęte utożsamianie bezpieczeństwa narodowego z bezpieczeństwem państwa.

Spośród wielu definicji bezpieczeństwa narodowego na uwagę zasługują dwie. Pierwsza określa bezpieczeństwo narodowe jako cel działania państwa i rządu do „[...] zapewnienia wewnętrznych i zewnętrznych warunków sprzyjających rozwojowi państwa, jego życiowym interesom oraz ochrony przed istniejącymi i potencjalnymi zagrożeniami”[6]. Według drugiej „[...] bezpieczeństwo narodowe [...] jest nie tylko ochroną naszego narodu i terytorium przed fizyczną napaścią, lecz również ochroną – za pomocą różnych środków – żywotnych interesów ekonomicznych i politycznych, których utrata zagroziłaby żywotnie podstawowym wartościom państwa”[7].

Analizując obszar bezpieczeństwa państw, zwraca się uwagę na jego międzynarodowy kontekst. Opisując zjawisko bezpieczeństwa, należy wymienić tu jeden z wielu czynników, który ma istotne znaczenie – czynnik militarny[8].

Czynnik militarny przez wieki odgrywał główną rolę w stosunkach między państwami, do tego stopnia, że można było utożsamiać bezpieczeństwo z brakiem bezpośredniego zagrożenia militarnego. Obecnie, wobec zwiększającego się znaczenia pozostałych czynników, nie odgrywa ono już takiej roli jak w przeszłości. Jednakże nie można zakładać, że bezpieczeństwo militarne utraciło całe znaczenie. Jakkolwiek prawne możliwości prowadzenia wojny zostały w XX wieku mocno ograniczone prawem międzynarodowym, świat nie został uwolniony od tego zjawiska.

W miarę upływu czasu zmieniają się środki i metody zachowywania bezpieczeństwa. O ile wcześniej zagrożenia miały głównie charakter wojskowy, o tyle dziś występuje różnorodność zagrożeń. Dawniej państwo wysyłało armię przeciw nadciągającej armii wroga, dziś musi dbać o bezpieczeństwo wewnętrzne obywateli, chronić ich przed zagrożeniami, np. terroryzmem i cyberterroryzmem.

Zakres pojęcia „bezpieczeństwo narodowe” jest ustalony ściśle w związku ze sposobem określania żywotnych interesów narodowych, do których można

6 J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 18.
7 Ibidem, s. 30.
8 Zob. C. Mojsiewicz, *Co wpływa na bezpieczeństwo państw* [w:] *Stosunki międzynarodowe*, red. W. Malendowski, C. Mojsiewicz, Wrocław 1998, s. 37.

zaliczyć bardziej lub mniej wymierne działania lub zachowania, m.in.: obronę, nacjonalizm, wielkość narodu, wewnętrzne i zewnętrzne interesy gospodarcze. W każdym z obszarów bezpieczeństwa narodowego – wewnętrznego lub zewnętrznego – na podstawie kryterium przedmiotowego można wyróżnić następujące, odpowiadające zidentyfikowanym postaciom zagrożeń, rodzaje bezpieczeństwa, m.in.: polityczne, militarne, gospodarcze (ekonomiczne), kulturowe, ekologiczne i społeczne.

Wraz z nadejście ery komputerów osobistych ludzkość zapragnęła czegoś więcej. Głównym celem stało się osiągnięcie komunikacji na poziomie globalnym. Odpowiedzią na te oczekiwania okazał się internet. Jako kanał komunikacyjny internet połączył rozległe środowisko komputerowe i stworzył jedną wielką sieć. Z szerszej perspektywy, środowisko komputerowe, technologie i ludzi określa się pojęciem „cyberprzestrzeń".

W literaturze przedmiotu spotkać można rozmaite jednoaspektowe ujęcia cyberprzestrzeni, często określane jako definicje.

Określenie „cyberprzestrzeń" (*cyberspace*) po raz pierwszy pojawiło się w roku 1982. Jego twórcą był William Gibson, pisarz, autor powieści z gatunku *science fiction*. Według niego cyberprzestrzeń to konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych. Graficzne odwzorowanie danych pobierane z banków wszystkich komputerów świata. Niewyobrażalna złożoność, świetlne linie przebiegające przez przestrzeń umysłu, skupiska i konstelacje danych[9].

Definicja cyberprzestrzeni składa się ze znaczeń słów: „cyber" i „przestrzeń". Cyber pochodzi od cybernetyki, nauki o systemach sterowania zapoczątkowanej przez Norberta Wienera, który zdefiniował ją jako „[...] nauka o sterowaniu i komunikacji w zwierzęciu i maszynie"[10]. Cyberprzestrzeń może być rozumiana jako przestrzeń komunikacji, gdzie sprzężenie zwrotne informacji pozwala na regulację systemów, wzajemne relacje między nimi, dynamiczny rozwój i wytyczanie szlaków. Zarówno sprzężenia zwrotne, jak i systemy sterowania, między którymi sprzężenia zachodzą, występują w całej otaczającej nas rzeczywistości[11].

9 W. Gibson, *Neuromancer*, Warszawa 2001.
10 J. Bańka, *Edukacja i czas. Wychowanie dla teraźniejszości*, Warszawa 1996.
11 M. Ostrowicki, *Wirtualne realia. Estetyka w epoce elektroniki*, Kraków 2006, s. 75.

Przemysław Maj cyberprzestrzeń określa jako sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane, sposoby i środki ich przesyłania[12].

Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj.:

– transportu;
– łączności;
– infrastruktury energetycznej;
– wodociągowej i gazowej;
– ochrony zdrowia[13].

Zasadniczym celem działania w cyberprzestrzeni jest ułatwienie użytkownikom sieci kontaktów w czasie rzeczywistym[14].

Zdaniem Pierre'a Levy'ego cyberprzestrzeń to przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie[15]. Za znamienną cechę cyberprzestrzeni uważa jej cyfrowy charakter:

– plastyczny;
– płynny;
– obliczalny z dużą dokładnością i powtarzalny w czasie rzeczywistym;
– hipertekstualny;
– interaktywny;
– wirtualny.

Według Michaela Heima cyberprzestrzeń to coś więcej niż przełom w elektronicznych mediach czy w wyglądzie komputerowego interfejsu. Cyberprzestrzeń, z jej wirtualnym środowiskiem i symulowanymi światami, stanowi metafizyczne laboratorium, narzędzie służące badaniu naszego poczucia rzeczywistości.

12 P. Maj, *Cyberterroryzm w stosunkach międzynarodowych*, „Consensus. Studenckie Zeszyty Naukowe" 2001, nr 1, s. 68.
13 *Cyberterroryzm*, https://www.gov.pl/web/mswia/msz [dostęp: 25.02.2023].
14 T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Marynarki Wojennej" 2005, R. 40, nr 6, s. 160.
15 P. Levy, *Drugi potop*, https://portal.tezeusz.pl/2004/11/27/drugi-potop-pierre-levy [dostęp: 25.02.2023].

Najważniejszą definicją dla terminu „cyberprzestrzeń" jest dyrektywa 54 National Security Presidential. Według niej pojęcie to jest rozumiane jako wirtualne środowisko informacji i interakcji między ludźmi[16].

Według dyrektywy cyberprzestrzeń wymaga nie tylko sprzętu, oprogramowania i systemów informacyjnych, lecz także ludzkich zachowań uchwyconych za pośrednictwem sieci cyfrowych. Owe interakcje to bogaty zbiór odzwierciedlający zarówno pozytywne, jak i negatywne strony ludzkiej natury, wahających się od cyber autokreacji i autoekspresji do działań przestępczych prowadzących również do aktów terrorystycznych oraz możliwych konfliktów cybernetycznych. Główne cechy cyberprzestrzeni to brak granic, dynamiczne procesy i zjawiska oraz anonimowość użytkowników.

Organy odpowiedzialne za cyberbezpieczeństwo

Zgodnie z wytycznymi dyrektywy NIS każdy kraj członkowski jest zobowiązany utworzyć krajowy zespół reagujący na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni, tzw. CSIRT (Computer Security Incident Response Team). Polska utworzyła trzy CSIRT sektorowe na poziomie krajowym:

– CSIRT NASK prowadzony przez Naukową Akademicką Sieć Komputerową;

– CSIRT MON prowadzony przez Ministerstwo Obrony Narodowej;

– CSIRT GOV prowadzony przez szefa Agencji Bezpieczeństwa Wewnętrznego.

Przepisy krajowe wdrażające dyrektywę NIS to przede wszystkim ustawa o krajowym systemie cyberbezpieczeństwa[17] wraz rozporządzeniami wykonawczymi.

Ustawa określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakres „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej".

Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług

16 Dyrektywa numer 54 National Security Presidential, https://irp.fas.org/offdocs/nspd/nspd-54.pdf [dostęp: 25.02.2023].

17 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560, z późn. zm.

kluczowych i usług cyfrowych przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Dane z wykazu operatorów usług kluczowych w zakresie niezbędnym do realizacji ich ustawowych zadań minister właściwy do spraw informatyzacji udostępnia, na wniosek, następującym podmiotom:

1) organom właściwym do spraw cyberbezpieczeństwa;
2) Policji;
3) Żandarmerii Wojskowej;
4) Straży Granicznej;
5) Centralnemu Biuru Antykorupcyjnemu;
6) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
7) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
8) sądom;
9) prokuraturze;
10) organom Krajowej Administracji Skarbowej;
11) dyrektorowi Rządowego Centrum Bezpieczeństwa;
12) Służbie Ochrony Państwa.

Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
   a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
   b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
   c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
   d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
   e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;

4) zarządzanie incydentami;

5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:

a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,

b) dbałość o aktualizację oprogramowania,

c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,

d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;

6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Ponadto operator usługi kluczowej:

1) zapewnia obsługę incydentu;

2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań;

3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny;

4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;

6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

Operator usługi kluczowej może także przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje o:

1) innych incydentach;

2) zagrożeniach cyberbezpieczeństwa;

3) dotyczące szacowania ryzyka;

4) podatnościach;

5) wykorzystywanych technologiach.

Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością, należy:

1) monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;

2) szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;

3) przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;

4) wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;

5) reagowanie na zgłoszone incydenty;

6) klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;

7) zmiana klasyfikacji incydentów poważnych i incydentów istotnych;

8) przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT;

9) przeprowadzanie, w uzasadnionych przypadkach, badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa;

10) współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej, i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;

11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego

zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;

12) przekazywanie, w terminie do 30 maja każdego roku, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;

13) wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z 26 kwietnia 2007 roku o zarządzaniu kryzysowym, dotyczącej cyberbezpieczeństwa;

14) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności:

a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności,

b) monitoruje wskaźniki zagrożeń cyberbezpieczeństwa,

c) rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,

d) prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa,

e) wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,

f) prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,

g) współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa;

15) zapewnienie możliwości dokonywania zgłoszeń i przekazywania informacji, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1, oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń;

16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA).

CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu, którego koordynacja obsługi wymaga współpracy CSIRT, oraz określają we współpracy z sektorowymi zespołami cyberbezpieczeństwa sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu.

Do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez:

1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z 26 kwietnia 2007 roku o zarządzaniu kryzysowym;

2) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, dla których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa w rozumieniu art. 5 pkt 3 ustawy z 23 sierpnia 2001 roku o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz.U. 2001, poz. 1320 oraz 2002, poz. 1571) jest Minister Obrony Narodowej.

Głównym organem działającym na rzecz cyberbezpieczeństwa, wykorzystywanego militarnie, jest Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, który został powołany przez Ministra Obrony Narodowej[18].

Do zadań Pełnomocnika należy:

1) wydawanie w imieniu Ministra Obrony Narodowej wytycznych w sprawach bezpieczeństwa cyberprzestrzeni w odniesieniu do komórek i jednostek organizacyjnych resortu obrony narodowej, z wyłączeniem zadań zastrzeżonych dla pełnomocników do spraw ochrony informacji niejawnych, określonych odrębnymi przepisami;

2) inicjowanie oraz wspieranie działań komórek i jednostek organizacyjnych resortu obrony narodowej w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni resortu obrony narodowej;

3) sprawowanie nadzoru nad realizacją zadań wynikających z aktów prawnych, polityk i programów rządowych dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni resortu obrony narodowej;

18 Decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 25 stycznia 2019 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, Dz. Urz. MON 2019, poz. 19.

4) podejmowanie działań zmierzających do wspierania spójnego, jednolitego i efektywnego systemu zarządzania bezpieczeństwem cyberprzestrzeni resortu obrony narodowej;

5) reprezentowanie:

a) resortu obrony narodowej w pracach kierowniczych gremiów (komitetów, zespołów, grup) Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej w zakresie bezpieczeństwa cyberprzestrzeni,

b) Ministra Obrony Narodowej w pracach Kolegium, o którym mowa w art. 64 ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa;

6) współpraca z zespołami eksperckimi resortu obrony narodowej wykonującymi zadania w obszarze bezpieczeństwa cyberprzestrzeni.

Pełnomocnik może w szczególności:

1) zwrócić się o przedstawienie stanowisk, informacji, dokumentów i sprawozdań okresowych lub dotyczących poszczególnych spraw albo rodzaju spraw do właściwych komórek i jednostek organizacyjnych resortu obrony narodowej;

2) oceniać oraz formułować wnioski w zakresie realizacji działań związanych z bezpieczeństwem cyberprzestrzeni;

3) zlecać przeprowadzenie badań, analiz i ekspertyz w zakresie realizowanych przez niego zadań.

Pełnomocnik, do 15 kwietnia każdego roku kalendarzowego, przygotowuje dla Ministra Obrony Narodowej, we współpracy z szefem Sztabu Generalnego Wojska Polskiego, szefem Służby Kontrwywiadu Wojskowego, pełnomocnikiem Ministra Obrony Narodowej do spraw ochrony informacji niejawnych – dyrektorem Departamentu Ochrony Informacji Niejawnych oraz dowódcą Komponentu Wojsk Obrony Cyberprzestrzeni, roczny raport o stanie bezpieczeństwa cyberprzestrzeni w resorcie obrony narodowej. Wydaje wytyczne dotyczące sposobu przygotowywania raportu o stanie bezpieczeństwa cyberprzestrzeni w resorcie obrony narodowej. Ma również możliwość podejmowania współpracy z organami administracji publicznej i organizacjami pozarządowymi oraz podmiotami krajowymi i międzynarodowymi realizującymi zadania na rzecz bezpieczeństwa cyberprzestrzeni.

Ważną rolę odgrywa również Departament Cyberbezpieczeństwa (DCyber), którego zadaniem jest:

1) definiowanie propozycji celów w obszarze cyberbezpieczeństwa w ramach procesu planowania rozwoju systemu bezpieczeństwa narodowego i udział w procesie programowania rozwoju sił zbrojnych;

2) projektowanie rozwiązań systemowych w obszarze cyberbezpieczeństwa, w tym udział w wypracowywaniu projektów aktów prawnych na szczeblu rządowym;

3) koordynowanie realizacji zadań związanych z wdrażaniem polityki krajowej i międzynarodowej resortu w obszarze cyberbezpieczeństwa, w szczególności:

a) wdrażania projektów dotyczących rozwoju zdolności resortu do prowadzenia działań w cyberprzestrzeni,

b) przedsięwzięć informacyjno-szkoleniowych oraz promocyjnych resortu dotyczących obszaru cyberbezpieczeństwa;

4) wykonywanie zadań na rzecz ministra wynikających z podporządkowania Ministrowi:

a) Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa,

b) Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni,

c) Wojskowego Instytutu Łączności im. prof. dr. hab. Janusza Groszkowskiego – Państwowego Instytutu Badawczego.

Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (ECSC) jest komórką przeznaczoną do planowania i realizacji szkolenia (kształcenia) w obszarze cyberbezpieczeństwa, teleinformatyki i IT dla resortu obrony narodowej oraz podmiotów poza nim.

Kolejnym organem działającym na rzecz cyberbezpieczeństwa jest Dowództwo Komponentu Wojsk Obrony Cyberbezpieczeństwa (DKWOC), które jednocześnie jest organizatorem wojskowego systemu telekomunikacyjnego[19]. Odpowiada ono za realizację pełnego spektrum działań w cyberprzestrzeni, w szczególności w zakresie budowy, utrzymania i ochrony infrastruktury teleinformatycznej dla potrzeb prawidłowego funkcjonowania oraz proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia sił zbrojnych. Zapewnienie prawidłowego funkcjonowania Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego, zwanego CSIRT MON.

Organem zaangażowanym w ochronę cyberprzestrzeni jest Centrum Zasobów Cyberprzestrzeni Sił Zbrojnych (CZCSZ), które jest odpowiedzialne za ogół spraw związanych z informatyzacją resortu, wsparcie procesu kierowania oraz dowodzenia bezpieczeństwem cyberprzestrzeni sił zbrojnych. Jego zadaniem

19 Decyzja Nr 109/MON Ministra Obrony Narodowej z dnia 27 lipca 2022 r. w sprawie organizatora wojskowego systemu telekomunikacyjnego, Dz. Urz. MON 2022, poz. 124.

jest zapewnienie wymaganych zasobów i usług na potrzeby bezpieczeństwa cyberprzestrzeni, rozwoju i utrzymania systemów teleinformatycznych.

Resortowe Centrum Informatyki (RCI) to kolejne ogniwo militarne działające na rzecz ochrony w cyberprzestrzeni. Odpowiada za właściwe utrzymanie systemów teleinformatycznych, w tym systemów łączności satelitarnej oraz informatycznych. Realizuje zadania Ministra Obrony Narodowej, w ramach CSIRT MON, z zakresu cyberprzestrzeni.

Zagrożenia militarne w cyberprzestrzeni

Cyberzagrożenie to wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na sieci i systemy teleinformatyczne, użytkowników takich systemów oraz inne osoby[20].

Wraz z rozwojem nowoczesnych technologii informacyjnych wzmaga się wpływ na wszelkiego rodzaju sfery aktywności człowieka, społeczeństwa oraz funkcjonowania państwa. Przyczyną tych zmian są: globalizacja, rozwijająca się gospodarka oraz przyspieszony rozwój technologii informacyjnych, którym zawdzięczamy powstanie internetu. Dzięki wysokiemu poziomowi rozwoju przyczynia się do poprawy życia społecznego, gospodarczego i militarnego.

Niestety, bardzo szybko dostrzeżono możliwości wykorzystania jej do działań o charakterze cyberprzestępczym i cyberterrorystycznym, a także stała się terenem prowadzenia cyberwojen[21].

Do najważniejszych źródeł zagrożeń sieci teleinformatycznych możemy zaliczyć:

– zakłócenia działania systemów;
– nieupoważnione wprowadzanie i kopiowanie danych;
– łamanie zabezpieczeń, co w konsekwencji prowadzi do przejęcia kontroli nad poszczególnymi elementami infrastruktury.

20 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz. Urz. UE 2019, L 151/15.

21 I. Oleksiewicz, *Cyberterroryzm jako realne zagrożenie dla Polski*, „Rocznik Bezpieczeństwa Międzynarodowego" 2019, nr 1, s. 53–67.

Cyberprzestrzeń charakteryzuje się brakiem zależności od miejsca, odległości, a także czasu i granic, ma zasięg globalny. W cyberprzestrzeni w pewnym stopniu można być anonimowym i właśnie tę anonimowość wykorzystują osoby, które pragną osiągnąć swoje cele.

Można wyróżnić kilka kategorii osób, które stanowią swoiste zagrożenie dla cyberprzestrzeni. Są to:

– cyberaktywiści – grupy osób, które prowadzą działania w celu wsparcia jakiejś idei. Propagują ją poprzez rozpowszechnianie spektakularnych działań o dość dużym zasięgu oraz zakresie i najczęściej godzą w czyjś wizerunek;

– cyberprzestępcy – pojedyncze osoby lub grupy osób, które prowadzą działania dla korzyści majątkowej lub osobistej, dokonują przeważnie klasycznych czynów przestępnych takich, jak: oszustwa, kradzieże, wyłudzenia z wykorzystaniem metod i narzędzi dostępnych w wirtualnym świecie;

– cyberterroryści – pojedyncze osoby lub grupy osób bądź organizacje polityczne prowadzące działania w cyberprzestrzeni dla wsparcia swoich egoistycznych często politycznych celów, dążą do ich osiągnięcia poprzez stosowanie różnych form zastraszania i wywoływania stanu zagrożenia. Osoby te wykorzystują cyberprzestrzeń jako narzędzie komunikacji, propagandy, gromadzenia środków finansowych oraz werbunku i prowadzenia różnych szkoleń;

– cyberszpiedzy – organizacje lub przedsiębiorstwa pracujące na rzecz biznesu lub resortów siłowych prowadzące działania w cyberprzestrzeni głównie w celu skrytego pozyskania wiedzy lub wywarcia wpływu. Wiele państw masowo wykorzystuje cyberprzestrzeń do takich celów, jest to bowiem niezwykle tania, efektywna i łatwa do ukrycia forma działalności o charakterze wywiadowczym;

– cyberżołnierze – najczęściej organizacje najemne lub oddziały wojskowe przeznaczone do prowadzenia działań zbrojnych w cyberprzestrzeni traktowanej jako arena działań wojennych.

W cyberprzestrzeni użytkownicy wymieniają informacje za pośrednictwem cybersieci i są uczestnikami cyberbezpieczeństwa.

Szkodliwe są działania:

– propagandowe;
– dezinformacyjne;
– manipulacyjne;
– przestępcze.

Głównym wymogiem dla wszystkich użytkowników cyberprzestrzeni w Unii Europejskiej, także w obszarze militarnym, jest odpowiednie zapewnienie ochrony danych osobowych.

Zgodnie z art. 13 ust. 1 i 2 RODO[22] administratorem danych osobowych jest Minister Obrony Narodowej.

Jako administrator przetwarza on dane osobowe w celu realizacji zadań ustawowych wynikających m.in. z ustawy z 14 grudnia 1995 roku o urzędzie Ministra Obrony Narodowej (Dz.U. 2019, poz. 196), uszczegółowionych w rozporządzeniu Rady Ministrów z 9 lipca 1996 roku w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz.U. 1996, nr 94, poz. 426, z późn. zm.) oraz realizuje swoje zadania m.in. na podstawie ustawy z 14 czerwca 1960 roku – Kodeks postępowania administracyjnego.

Bezpieczeństwo informacji jest bardzo ważnym zagadnieniem, tak samo jak bezpieczeństwo granic, infrastruktury czy bezpieczeństwo publiczne. Od poziomu zabezpieczeń systemu informatycznego zależy, czy informacja zostanie wykorzystana zgodnie z intencjami właściciela. Żeby warunek ten mógłby być spełniony, system informatyczny musi posiadać następujące cechy:

– poufność – oznacza, że informacja nie jest udostępniana nieupoważnionym osobom;

– integralność – oznacza, że informacja jest przedstawiana w sposób kompletny i dokładny;

– dostępność – oznacza, że informacja jest dostępna na żądanie upoważnionego podmiotu.

Zakończenie

Można stwierdzić, że w obliczu globalizacji problematyka bezpieczeństwa cyberprzestrzeni stała się jednym z priorytetowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. To szczególne środowisko, które wymaga zmian w obszarze bezpieczeństwa, a także dostosowania procedur i odpowiednich narzędzi, żeby w jak największym stopniu zminimalizować ryzyko cyberataku na posiadane zasoby. Niemniej jednak należy podkreślić, że na świecie nie ma takich rozwiązań, które mogłoby w pełni zapewnić bezpieczeństwo cyberprzestrzeni. Ważnymi działaniami podejmowanymi w obszarze cyberprzestrzeni w środowisku militarnym jest rozszerzenie dotychczasowego

22 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE 2016, L 119.

spektrum działań o przedsięwzięcia, które będą stanowić odpowiedź na nowe zagrożenia w cyberprzestrzeni oraz stale rosnące potrzeby w zakresie zapewnienia bezpieczeństwa sieci i systemów teleinformatycznych. Do działań tych z pewnością należy zaliczyć przedsięwzięcia służące zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizowaniu skutków incydentów naruszających bezpieczeństwo w cyberprzestrzeni, wzmocnieniu zdolności operacyjnych do przeciwdziałania cyberzagrożeniom oraz budowaniu u wszystkich użytkowników świadomości zagrożeń i ryzyk związanych z ich wykorzystaniem.

Bibliografia

Bezpieczeństwo państwa, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009.
Bezpieczeństwo państwa w XXI wieku, red. M. Paździor, J. Trubalska, Ł. Wojciechowski, A. Żywicka, Lublin 2018.
Bezpieczeństwo wewnętrzne państwa wybrane zagadnienia, red. S. Sulowski, M. Brzeziński, Warszawa 2009.
Cyberbezpieczeństwo jako element bezpieczeństwa państwa i ochrony prywatności obywateli, red. J. Trubalska, Ł. Wojciechowski, Lublin 2019.
Cyberbezpieczeństwo, red. C. Banasiński, M. Rojszczaka, Warszawa 2020.
Gawkowski K., *Cyberkolonializm*, Gliwice 2018.
Górka M., *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa 2014.
Hoffman T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.
Instytucjonalne podstawy bezpieczeństwa państwa w Rzeczypospolitej Polskiej, red. B. Dziemidok-Olszewska, M. Michalczuk-Wlizło, Warszawa 2018.
Kitler W., *Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Toruń 2018.
Krawiec J., *Cyberbezpieczeństwo. Podejście systemowe*, Warszawa 2019.
Marczyk M., *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" 2018, nr 1–2.
Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Warszawa 2022.
Oleksiewicz I., *Ochrona cyberprzestrzeni Unii Europejskiej*, Warszawa 2021.
Paździor M., Szmulik B., *Instytucje bezpieczeństwa narodowego*, Warszawa 2012.
Polska w systemie bezpieczeństwa międzynarodowego, red. M. Pietraś, K.A. Wojtaszczyk, Warszawa 2016.
Słownik terminów z zakresu bezpieczeństwa narodowego, wyd. 6, red. nauk. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, Warszawa 2008.
Wiśniewski B., *System bezpieczeństwa państwa*, Szczytno 2013.
Zawisza J., *Cyberprzestrzeń jako zagrożenie bezpieczeństwa państwa*, Józefów 2015.

Cyberspace in the military system of state security

Abstract

The article „Cyberspace in the military system of state security" presents the basic concepts related to security, which is nowadays considered to be a state of certainty, peace, security and lack of threat and protection against danger, and cyberspace, which is understood as a virtual environment of information and interaction between people. This article also shows the definitions of terms relating to the values most valued and protected by man, i.e. state security, which is an integral part of the state policy related to the creation and use of national defense potential to prevent and counteract various types of threats. The importance of important units of the Polish Armed Forces as the basic organ of shaping cyberspace in the military area has been shown. The role and place of bodies in the Polish Armed Forces ready to respond to threats to ICT systems and networks connected by cyberspace has been defined.

Key words: security, national security, cyberspace, cybersecurity