Robert Janczewski[1]

Współdziałanie Sił Zbrojnych RP i Policji dla zapewnienia cyberbezpieczeństwa infrastruktury krytycznej państwa w czasie działań hybrydowych prowadzonych na terenie RP

Wstęp

Stwierdzenie, że dynamiczny rozwój teleinformatyki wpływa na paradygmaty bezpieczeństwa i obronności państwa może wydawać się truizmem. Jednak wnikliwa analiza praktycznych aspektów prowadzenia działań zarówno militarnych, jak i niemilitarnych w cyberprzestrzeni lub z jej wykorzystaniem uwidocznia, że zasadne jest dokonanie rewizji dotychczasowego podejścia do utrzymywania cyberbezpieczeństwa infrastruktury krytycznej Polski.

Oddziaływanie hybrydowe na terenie Polski prowadzone jest również w czasie pokoju. Działania informacyjne łączone są z psychologicznymi. Oddziaływanie w cyberprzestrzeni[2] lub z jej wykorzystaniem na obiekty

[1] Ppłk dr inż. Robert Janczewski — doktor nauk o obronności oraz adiunktem Zakładu Bezpieczeństwa Cyberprzestrzeni Instytutu Działań Informacyjnych Wydziału Wojskowego Akademii Sztuki Wojennej. W jego obszarze zainteresowań są zagadnienia związane z cyberprzestrzenią oraz cyberbezpieczeństwem. Zainteresowania naukowe koncentruje również na procesach informacyjnych w rozpoznaniu elektronicznym, a także cyberrozpoznaniu. Swój wysiłek badawczy skupia w takich obszarach, jak: identyfikacja zmian funkcjonowania systemu rozpoznania elektronicznego w środowisku cybernetycznym, identyfikacja procesów informacyjnych zachodzących w cyberprzestrzeni, identyfikacja czynników warunkujących funkcjonowanie organizacji w cyberprzestrzeni oraz teoretyczne i praktyczne aspekty funkcjonowania organizacji wojskowej w cyberprzestrzeni oraz środowisku cybernetycznym. Naukowo zajmuje się także znaczeniem cyberprzestrzeni w działaniach hybrydowych.

Adres do korespondencji: <r.janczewski@akademia.mil.pl>.

[2] Jeden z prekursorów teorii działań hybrydowych F.G. Hoffman zauważył, że cyberprzestrzeń jest jednym z elementów katalogu obszarów oddziaływania hybrydowego. Por.: F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Virginia 2007, s. 28.

ważne dla obronności i bezpieczeństwa państwa realizowane jest z użyciem najnowszej technologii.

Złożoność cyberataków, pod względem treści i struktury, może być znacznie większa niż tych znanych z pozostałych przestrzeni operacyjnych (lądu, morza, przestrzeni powietrznej czy kosmicznej). Dobrze przygotowane cyberataki będą trudne, jak nie niemożliwe do odparcia — zaatakowany może spotkać się z nieznanymi dotychczas metodami, metodykami czy narzędziami prowadzenia cyberataku. Zastosowana cyberbroń może być profesjonalnie przygotowana jedynie do zaatakowania konkretnego nominowanego do rażenia obiektu. Działania w cyberprzestrzeni można przeprowadzać znacznie dynamicznej niż na lądzie, morzu w przestrzeni powietrznej, czy kosmicznej; w czasie quasi-rzeczywistym; z odległych od celu miejsc; przy jednoczesnym zachowaniu anonimowości. Cyberatak może mieć wysoki poziom zawiłości, może być przeprowadzony przez wiele podmiotów za pomocą dziesiątek, setek lub tysięcy komputerów połączonych przez wiele sieci rezydujących w wielu krajach. Ponadto nie bez znaczenia mogą być również indywidualne osoby — insiderzy[3]. Cyberataki na infrastrukturę krytyczną przysparzają również problemu natury prawnej. Niestety nie ma międzynarodowej definicji określającej, kiedy wrogie działania w cyberprzestrzeni są uznawane za ataki, nie mówiąc już o akcie wojny.

Biorąc pod uwagę tę mieszankę możliwości, celowe jest bardziej szczegółowe i kompleksowe podejście do zapewnienia cyberbezpieczeństwa polskiej infrastruktury krytycznej w czasie działań hybrydowych prowadzonych na terenie Rzeczypospolitej Polskiej. Jednowymiarowy, terytorialny obraz konfliktu zmienił się w wielowymiarowy, wielopoziomowy kompleks działań militarnych i niemilitarnych służących osiąganiu niejednokrotnie zróżnicowanych celów.

Anonimizacja działań w cyberprzestrzeni powoduje, że rozstrzygnięcie, czy cyberatak na polską infrastrukturę krytyczną przeprowadzony został lub jest prowadzony przez podmiot militarny czy pozamilitarny może nie być możliwe. Dlatego zapewnienie cyberbezpieczeństwa infrastruktury krytycznej Polski wymaga całościowego podejścia (ang. *comprehensive approach*), wypracowania bardziej skutecznego systemu cyberochrony i cyberobrony, a co za tym idzie współpracy Sił Zbrojnych RP (dalej jako SZ RP) i Policji.

Uwarunkowania prawne i doktrynalne

Konstytucja Rzeczypospolitej Polskiej[4] w rozdziale pierwszym pt. *Rzeczpospolita,* w art. 26 pkt 1 — *Siły Zbrojne Rzeczypospolitej Polskiej*

[3] Dobrze poinformowane, uwierzytelnione osoby, ale niegodne zaufania.

[4] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., uchwalona przez Zgromadzenie Narodowe, zatwierdzona w ogólnonarodowym referendum 25 maja 1997 r. (DzU z 1997 r., nr 78, poz. 483). Konstytucja RP weszła w życie 17 października 1997 r.

wskazuje, że SZ RP służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic. Natomiast w rozdziale piątym pt. *Prezydent Rzeczypospolitej Polskiej* art. 136 określa, że w razie bezpośredniego, zewnętrznego zagrożenia państwa prezydent Rzeczypospolitej, na wniosek prezesa Rady Ministrów, zarządza powszechną lub częściową mobilizację i użycie Sił Zbrojnych do obrony Rzeczypospolitej Polskiej.

Analiza powyższych zapisów w kontekście cyberzagrożeń skłania do sformułowania pytań. W odniesieniu do rozdziału pierwszego najważniejsze wydaje się rozstrzygnięcie: Czy cyberprzestrzeń może być wykorzystana do odebrania niepodległości? Jeśli tak, to — w jakim zakresie w czasie pokoju siły zbrojne powinny uczestniczyć w jej ochronie? Natomiast w odniesieniu do rozdziału piątego można sformułować pytania: Czy cyberataki skierowane, spoza granic państwa, na infrastrukturę krytyczną oraz inne obiekty ważne dla bezpieczeństwa i obronności państwa można uznać za bezpośrednie, zewnętrzne zagrożenie państwa? Jeśli tak to, jaki jest punkt krytyczny, w którym zasadne jest użycie Sił Zbrojnych do obrony Rzeczypospolitej Polskiej?

Artykuł 18 pkt 1 ustawy o policji[5] określa, że w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego, zwłaszcza poprzez sprowadzenie bezpośredniego zagrożenia obiektów lub urządzeń ważnych dla bezpieczeństwa lub obronności państwa, siedzib centralnych organów państwowych albo wymiaru sprawiedliwości, obiektów gospodarki lub kultury narodowej oraz przedstawicielstw dyplomatycznych i urzędów konsularnych państw obcych albo organizacji międzynarodowych, a także obiektów dozorowanych przez uzbrojoną formację ochronną utworzoną na podstawie odrębnych przepisów — jeżeli użycie oddziałów lub pododdziałów Policji okaże się lub może okazać się niewystarczające, do pomocy oddziałom i pododdziałom Policji mogą być użyte oddziały i pododdziały SZ RP .

Natomiast art. 18 pkt 4 ustawy o Policji uszczegóławia, że pomoc, o której mowa w ust. 1, może być udzielona również w formie prowadzonego samodzielnie przez oddziały i pododdziały SZ RP przeciwdziałania zagrożeniu, w przypadku gdy oddziały i pododdziały Policji nie dysponują możliwościami skutecznego przeciwdziałania tym zagrożeniom.

Analiza zapisów zawartych w powyżej przytoczonych dokumentach pozwala na wniosek, że aby działania jednego podmiotu uzupełniane były działaniami innego, konieczna i niezbędna jest wiedza na temat posiadanych przez obydwa podmioty zdolności.

Rada Ministrów RP uchwałą nr 67 z 9 kwietnia 2013 r. przyjęła Strategię rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022[6]. Według zapisów w niej zawartych w jej realizację zaangażowane będą wszystkie podmioty odpowiedzialne za umacnianie bezpieczeństwa

[5] Ustawa z 6 kwietnia 1990 r. o Policji (DzU z 1990 r., nr 30, poz. 179); dalej jako ustawa o Policji.

[6] Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022, <https://www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf>, 15 grudnia 2018 r.

narodowego, a w szczególności ministrowie, szefowie urzędów centralnych, wojewodowie, organy samorządu terytorialnego.

Strategia wskazuje podmioty odpowiedzialne za realizację strategii oraz określa ich obszary zadaniowe. Wśród nich jest minister obrony narodowej oraz minister właściwy do spraw wewnętrznych. W kontekście współpracy z Policją oraz gotowości do działań w cyberprzestrzeni do obszarów zadaniowych ministra obrony narodowej można zaliczyć:

1. doskonalenie procedur udzielania wsparcia organom administracji publicznej przez SZ RP w sytuacjach kryzysowych;
2. dostosowanie struktury organizacyjnej i dowodzenia SZ RP do wymogów środowiska bezpieczeństwa państwa;
3. koordynację planowania i realizacji zadań związanych z pozamilitarnymi przygotowaniami obronnymi państwa, w tym przedsięwzięć zabezpieczających potrzeby sił zbrojnych i wojsk sojuszniczych;
4. poprawę zdolności rozpoznania i ochrony przed zagrożeniami bezpieczeństwa państwa;
5. integrację procesów planowania obronnego i zarządzania kryzysowego poprzez zapewnienie spójności i tożsamości podejmowanych działań ujmowanych w planach zarządzania kryzysowego oraz w planach operacyjnych funkcjonowania organów administracji publicznej, planach operacyjnych użycia SZ RP;
6. integrację systemów łączności i informatycznego wsparcia procesu kierowania bezpieczeństwem narodowym oraz wymiany danych;
7. budowę resortowego zintegrowanego systemu informatycznego, wspomagającego proces decyzyjny;
8. rozwijanie zdolności do reagowania na incydenty komputerowe;
9. kształtowanie pozytywnego wizerunku i odbioru społecznego spraw dotyczących sił zbrojnych, obronności oraz zacieśniania współdziałania z organizacjami pozarządowymi i innymi podmiotami społecznymi w promocji obronności i działań na rzecz obronności.

Natomiast w kontekście współpracy z SZ RP oraz gotowości do działań w cyberprzestrzeni do obszarów zadaniowych ministra właściwego do spraw wewnętrznych można zaliczyć:

1. poprawę stanu wsparcia i zabezpieczenia potrzeb SZ RP i wojsk sojuszniczych przez podległe struktury i jednostki organizacyjne;
2. doskonalenie działań podmiotów i struktur organizacyjnych właściwych do spraw zarządzania kryzysowego i reagowania obronnego do funkcjonowania w okresie pokoju, kryzysu i w czasie wojny.

Ponadto w strategii czytamy, że aby ochrona infrastruktury krytycznej mogła być skuteczna, powinna stanowić wspólny wysiłek zarówno administracji rządowej, samorządowej, jak i operatorów oraz właścicieli. Ochrona infrastruktury krytycznej musi być zatem zadaniem jej właściciela lub operatora, natomiast rola państwa ogranicza się do funkcji koordynująco-nadzorującej. Interwencję dopuszcza się w przypadku, gdy dany element infrastruktury krytycznej nie jest dostatecznie chroniony lub gdy likwidacja skutków zaistniałej sytuacji kryzysowej przekracza możliwości danego właściciela lub operatora.

Strategia wskazuje na Narodowy Program Ochrony Infrastruktury Krytycznej jako kluczowy dokument dla tworzonego systemu ochrony infrastruktury krytycznej. Podkreśla ponadto, że integracja rozwiązań cywilnych i wojskowych w obszarze ochrony infrastruktury krytycznej wzmocni ochronę infrastruktury krytycznej.

W *Białej Księdze*[7] system bezpieczeństwa narodowego (bezpieczeństwa państwa) rozumiany jest jako całość sił (podmiotów), środków i zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana (w podsystemy i ogniwa), utrzymywana i przygotowywana. Składa się z podsystemu (systemu) kierowania i szeregu podsystemów (systemów) wykonawczych, w tym podsystemów operacyjnych (obronny i ochronne) i podsystemów wsparcia (społeczne i gospodarcze).

Prezydent RP Bronisław Komorowski w *Białej Księdze* zauważył, że „Mamy do czynienia z erupcją zagrożeń w cyberprzestrzeni. Powoduje to konieczność nowego podejścia do bezpieczeństwa narodowego”[8].

Powyższe przykłady wskazują, ze współpraca między SZ RP a Policją dla zachowania bezpieczeństwa jest regulowana zarówno przez dokumenty ustawodawcze, jak i o charakterze doktrynalnym.

Desygnat cyberbezpieczeństwa, działań hybrydowych oraz infrastruktury krytycznej

Premier RP Mateusz Morawiecki podczas exposé wygłoszonym 12 grudnia 2017 r., wśród poruszanych kwestii, zaakcentował znaczenie cyberbezpieczeństwa Polski. Stwierdził, że „Pola bitew współczesnego państwa to cyberprzestrzeń. Dlatego poważne państwo musi stawiać również na cyberbezpieczeństwo”[9]. Podczas 53. Konferencji Bezpieczeństwa w Monachium, która odbyła się w dniach 17–18 lutego 2018 r., premier RP poruszył także kwestie cyberbezpieczeństwa[10]. Będąc jeszcze wicepremierem, ministrem finansów i rozwoju Mateusz Morawiecki podczas Warsaw Security Forum 2017, które odbyło się 8–9 listopada 2017 r. w Warszawie, akcentował również znaczenie cyberbezpieczeństwa. Powiedział, że „Polska rozumie prastarą zasadę rzymską, że mogą się zmieniać rodzaje uzbrojenia, sojusze i różne inne okoliczności, ale [...] chcesz pokoju, gotuj się do wojny. Dzisiaj ta zasada obejmuje również nowy rodzaj sił zbrojnych

[7] BBN, *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013.

[8] Zob. tamże s. 5.

[9] Exposé Mateusza Morawieckiego, <https://www.premier.gov.pl/expose.html>, 22 lutego 2018 r.

[10] *Morawiecki: Silniejsza Europa oznacza Europę z lepszym sektorem obronnym*, <https://www.gazetaprawna.pl/artykuly/1105158,morawiecki-europa-sektor-obronny.html>, 22 lutego 2018 r.

— cyberbezpieczeństwo i cyberobronę”[11]. Jednocześnie zadeklarował, że Polska przeznacza coraz więcej pieniędzy na cyberbezpieczeństwo oraz dodał: „Zdajemy sobie sprawę, że we współczesnym świecie wojna ma charakter coraz bardziej hybrydowy, że mamy do czynienia z jednej strony z tradycyjnymi rodzajami broni, a z drugiej z szantażem psychologicznym, z cyberatakami, ze szpiegostwem na bardzo wysoką skalę”[12].

Nie ulega wątpliwości, że podczas oddziaływania na Polskę w cyberprzestrzeni oraz z jej wykorzystaniem wrogie podmioty swój wysiłek skupią na infrastrukturze krytycznej państwa oraz obiektach ważnych dla jego obronności i bezpieczeństwa. Z pragmatycznego punktu widzenia zapewnienie cyberbezpieczeństwa infrastruktury krytycznej RP w czasie oddziaływania hybrydowego na państwo wymaga wskazania jednoznacznie i jasno sprecyzowanego desygnatu zarówno cyberbezpieczeństwa, działań hybrydowych, jak i infrastruktury krytycznej.

Jednak, czy w Polsce podmioty kształtujące strategie i doktryny cyberbezpieczeństwa cyberbezpieczeństwo postrzegają jednomyślnie? Odpowiedź na tak postawione pytanie ułatwi analiza porównawcza przedstawionych poniżej dwóch dokumentów: Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 opracowanej przez Ministerstwo Cyfryzacji oraz Doktryny cyberbezpieczeństwa Rzeczypospolitej Polskiej opracowanej przez Biuro Bezpieczeństwa Narodowego (dalej jako BBN).

W pierwszym dokumencie pojęcia cyberbezpieczeństwo, bezpieczeństwo sieci i systemów informatycznych oraz bezpieczeństwo teleinformatyczne są tożsame i oznaczają odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne[13].

Drugi dokument wprowadza dwa rodzaje bezpieczeństwa związane z cyberprzestrzenią. Pierwsze to cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) zdefiniowane 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. Drugie, natomiast to bezpieczeństwo cyberprzestrzeni RP określone jako 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

[11] M. Jarco, *Morawiecki: Polska poważnie traktuje swoje zobowiązania obronne*, <https://www.pap.pl/aktualnosci/news%2C1157378%2Cmorawiecki-polska-powaznie-traktuje-swoje-zobowiazania-obronne.html>, 22 lutego 2018 r.

[12] Tamże.

[13] Zob.: Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017.

publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych[14].

Krytyka i analiza przedstawionych powyżej definicji wskazuje na dwa różne desygnaty cyberbezpieczeństwa. Ministerstwo Cyfryzacji utożsamia je z odpornością, natomiast BBN z procesem, a także zespołem przedsięwzięć. Można, zatem sformułować wniosek, że brak jednoznacznego, jasno sprecyzowanego desygnatu cyberbezpieczeństwa stanowi barierę w jego zapewnieniu, a prowadzenie w tym celu skutecznych działań będzie, jeśli nie niemożliwe, to na pewno utrudnione.

Analiza i krytyka literatury tej tematyki dowodzi, że również działania hybrydowe nie posiadają jednoznacznego desygnatu. Mirosław Banasik i Ryszard Parafianowicz, opierając się na wynikach swoich badań, twierdzą, że „istota działań hybrydowych polega na wielowymiarowym, jednoczesnym oddziaływaniu w sferze militarnej z zastosowaniem klasycznych i nieregularnych działań zbrojnych, w sferze informacyjnej, cybernetycznej i ekonomicznej[15]. Natomiast Łukasz Skonieczny zauważa, że w przyszłych konfliktach zbrojnych nie będzie jasnego podziału na stan wojny i pokoju oraz żołnierzy i cywilów[16].

W przypadku infrastrukturze krytycznej desygnat wskazany jest przez ustawodawcę RP. Infrastruktura krytycznej to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje następujące systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[17].

[14] BBN, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015.

[15] Zob. M. Banasik, R. Parafianowicz, *Teoria i praktyka działań hybrydowych*, „Zeszyty Naukowe AON" 2015, nr 2(99), s. 5–25.

[16] Ł. Skonieczny, *Wojna hybrydowa — wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" — wydanie specjalne, 2015, nr X, s. 39–50.

[17] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU z 2007 r.,

Powyższy katalog uwidocznia, że ze względu na wżną rolę sieci i systemów teleinformatycznych w funkcjonowaniu infrastruktury krytycznej każdy z wyodrębnionych systemów może stać się celem cyberataku.

W Katowicach w dniach 10–12 maja 2017 r. odbyła się IX edycja *Europejskiego Kongresu Gospodarczego*. Jeden z obszarów tematycznych nosił nazwę: *Cyberbezpieczeństwo infrastruktury krytycznej*. Na pierwszy rzut oka wydaje się, że nie ma nic nadzwyczajnego w takim sformułowaniu. Jednak analiza Narodowego Program Ochrony Infrastruktury Krytycznej – tekst jednolity[18] oraz załącznika do Narodowego Programu Ochrony Infrastruktury Krytycznej — Załącznik 1 — Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej[19] — dobre praktyki i rekomendacje (dalej jako Załącznik) wykazała, że w żadnym z tych kluczowych dokumentów nie ma definicji zarówno cyberprzestrzeni, jak i cyberbezpieczeństwa. W Załączniku odnajdziemy wprawdzie takie określenia, jak: cyberprzestępczość, cyberterroryzm, cyberatak, a także sformułowanie: Cyberataki na systemy IK stały się częścią konfliktów cybernetycznych cyberprzestrzeni, w tym konfliktów między państwami[20], jednak żadne z powyższych sformułowań nie zostało wyjaśnione. Czym jest wobec tego cyberprzestępczość, cyberterroryzm czy cyberatak? Czy, zatem uczestnicy Europejskiego Kongresu Gospodarczego prowadzący debatę na temat cyberbezpieczeństwa infrastruktury krytycznej, mimo że wypowiadali te same słowa mówili o tym samym? Warto w tym miejscu zwrócić uwagę na zapis „konflikt cybernetyczny cyberprzestrzeni". Czym zatem jest ów konflikt?

Nasuwa się zatem pytanie: Czy każdy czytający Narodowy Program Ochrony Infrastruktury Krytycznej rozumie cyberbezpieczeństwo tak samo, skoro pojęcie nie zostało nigdzie sprecyzowane? Odpowiedź „nie" wydaje się oczywista, jednak możliwa jest sytuacja, w której istnieje prawdopodobieństwo jednakowego pojmowania cyberbezpieczeństwa przez każdego. Niestety, bez przeprowadzenia badań, nie jest możliwe udzielenie jednoznacznej, rozstrzygającej odpowiedzi.

Aspekty współdziałania

Obecnie współdziałanie SZRP i Policji dla zapewnienia cyberbezpieczeństwa infrastruktury krytycznej państwa w czasie działań hybrydowych

nr 89 poz. 590).

[18] Zob. RCB, Narodowy Program Ochrony Infrastruktury Krytycznej, <https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-2/>, 18 lutego 2018 r.

[19] Zob. tamże.

[20] Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1 — Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej — dobre praktyki i rekomendacje, s. 72.

prowadzonych na terenie RP wymaga doprecyzowania. Praktyka wskazuje, że celowe jest wypracowanie jasnych, spójnych uregulowań. Zasadne jest również wypracowanie wydajnego dobrze funkcjonującego systemu. Nie będzie to jednak możliwe bez przeprowadzenia wspólnych międzyresortowych analiz stanu faktycznego, określenia potrzeb i opracowania optymalnych rozwiązań.

Autor niniejszego opracowania stoi na stanowisku, że charakterystyka cyberprzestrzeni warunkuje potrzebę ścisłej współpracy między SZ RP a Policją w zakresie działań w cyberprzestrzeni. Złożoność cyberataków wymaga nowego spojrzenia na podział ról w zakresie cyberrozpoznania, cyberochrony, cyberobrony, a także działań zaczepnych.

Jednoznaczny podział obszarów odpowiedzialności na wewnętrzne i zewnętrzne w przypadku działań prowadzonych w cyberprzestrzeni oraz za jej pośrednictwem wydaje się niewłaściwy. Działania hakerów prowadzone przeciwko polskiej infrastrukturze krytycznej z terytorium Polski mogą pozornie być jedynie sprawą wewnętrzną o charakterze przestępczym. W swej istocie okazać się mogą jednak częścią dużej operacji militarnej prowadzonej przez inne wrogie państwo. Ponadto działania te będą właśnie nosić znamiona działań hybrydowych, ponieważ prowadzone będą poniżej progu wojny. Co więcej, zasadne może okazać się przeprowadzenie działań ofensywnych mających na celu destrukcję źródła cyberataku lub źródeł cyberataków? W tym celu niezbędna będzie kooperacja między SZ RP oraz Policją zgodnie z posiadanymi zdolnościami.

Współdziałanie wymaga wypracowania wspólnych rozwiązań na poziomie tak technicznym, jak operacyjnym. Nie będzie ono możliwe bez kompatybilności urządzeń technicznych oraz oprogramowania (systemy operacyjne i programy użytkowe).

Właściwa skuteczna współpraca nie będzie możliwa bez zasileń informacyjnych. System wymiany informacji również wymaga wypracowania wspólnej platformy technicznej (sprzęt i oprogramowanie), procedur oraz polityki dostępu do informacji. Ponadto, co nie jest bagatelne, zapewnienia bezpieczeństwa systemów zabezpieczeń.

Zakończenie

Infrastruktura krytyczna Polski ma szczególne znaczenie dla obronności i bezpieczeństwa państwa. Dlatego w czasie oddziaływania hybrydowego na terenie RP może ona stać się dla realnego lub potencjalnego przeciwnika środkiem ciężkości, przeciwko któremu skierowane zostaną działania w cyberprzestrzeni oraz za jej pośrednictwem. Zasadne zatem jest, aby SZ RP oraz Policja podejmowały współpracę dla zapewnienia cyberbezpieczeństwa. Aby osiągnąć taki stan należy utworzyć spójny system współpracy, który będzie weryfikowany i doskonalony poprzez wspólne ćwiczenia.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, cyberatak, infrastruktura krytyczna, działania hybrydowe

Keywords: cyberspace, cybersecurity, cyber attack, critical infrastructure, hybrid operations

Streszczenie: Nowoczesna infrastruktura krytyczna uzależniona jest od teleinformatyki, a jej bezpieczeństwo zależy od bezpieczeństwa w cyberprzestrzeni. W artykule autor omawia prawne i doktrynalne uwarunkowania współdziałania między Siłami Zbrojnymi Rzeczypospolitej Polskiej a polską Policją dla zapewnienia cyberbezpieczeństwa infrastruktury krytycznej państwa w czasie działań hybrydowych prowadzonych na terytorium Polski. Autor przedstawia także istotę cyberataków oraz charakterystykę takich działań w cyberprzestrzeni oraz z jej wykorzystaniem. W artykule omówione zostały również teoretyczne i praktyczne aspekty współdziałania Sił Zbrojnych Rzeczypospolitej Polskiej z polską Policją. Niniejszy artykuł jest zaproszeniem do naukowej debaty na przedstawiony temat.

Summary: A modern critical infrastructure addicted to an Information and Communications Technology and its security depends on security in cyberspace. In the article, the author discusses the legal and the doctrinal conditions of the cooperation between the Armed Forces of the Republic of Poland and the Polish Police to provide cybersecurity of the critical infrastructure of the state during hybrid operations conducted in the territory of Poland. The author presents also the essence of cyber attacks and the characteristics of activities in and through cyberspace. The author discusses theoretical and practical aspects of cooperation between the Armed Forces of the Republic of Poland and the Police. This article is an invitation to a scientific debate on the subject presented.