ROZDZIAŁ XXII

Sylwia Olczak
Wojskowa Akademia Techniczna

ROLA SŁUŻB SPECJALNYCH W WYKRYWANIU I PRZECIWDZIAŁANIU ZAGROŻENIOM DLA BEZPIECZEŃSTWA CYBERPRZESTRZENI RP

Wstęp

11 lipca 2016 r. Rzecznik Praw Obywatelskich zaskarżył *Ustawę antyterrorystyczną* do Trybunału Konstytucyjnego, jako niezgodną z Konstytucją, Kartą Praw Podstawowych Unii Europejskiej oraz Konwencją o ochronie praw człowieka i podstawowych wolności[1]. RPO podkreśla jednocześnie, że cel dokumentu jest jak najbardziej słuszny. Zasadne jest uporządkowanie przepisów w tym zakresie, jednak niejasność i nieprecyzyjność zapisów w ustawie powodują, że w jego ocenie, służby specjalne otrzymały duże i pozbawione kontroli uprawnienia. Budząca wiele emocji i kontrowersji ustawa stała się częścią polskiego porządku prawnego, jednak abstrahując od samego sporu wokół konkretnych jej zapisów, warto zwrócić uwagę na inne, związane z nią zagadnienie, w szerszej perspektywie. Ustawa poruszyła opinię społeczną w kontekście ograniczenia wolności na rzecz bezpieczeństwa. Benjamin Franklin powiedział: „Ci, którzy dla tymczasowego bezpieczeństwa rezygnują z podstawowych wolności, nie zasługują ani na jedno, ani na drugie”[2]. Jego słowa są często przywoływane, a w debacie publicznej zaczęto zadawać pytanie: Ile z naszej wolności jesteśmy w stanie poświecić na rzecz bezpieczeństwa? Temat ten jest wciąż aktualny i pozostanie nim ze względu na rozwój technologii informacyjnych, jednak nie powinniśmy się spodziewać jednoznacznej odpowiedzi na to pytanie. Zmiany prawne kształtują zadania i możliwości działań służb specjalnych w wykrywaniu i przeciwdziałaniu zagrożeniom dla bezpieczeństwa cyberprzestrzeni RP, zmieniając także prawa każdego użytkownika sieci teleinformatycznych. Pojawia się zatem pytanie: jaka w tym kontekście jest rola

[1] https://www.rpo.gov.pl/pl/content/rzecznik-praw-obywatelskich-skar%C5%BCy-ustaw%C4%99-antyterrorystyczn%C4%85-do-trybuna%C5%82u-konstytucyjnego (dostęp: 11.07.2016 r.).

[2] Ang.: “They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety”, http://www.brainyquote.com/quotes/quotes/b/benjaminfr136955.html (dostęp: 11.07.2016 r.).

służb specjalnych? Czy wprowadzone w Polsce rozwiązania, o których są dostępne informację[3], są wystarczające wobec pojawiających się wyzwań i zagrożeń w cyberprzestrzeni?

1. Znaczenie informacji w kształtowaniu bezpieczeństwa współczesnego państwa

Nie sposób przecenić roli informacji, jako czynnika, który w dużej mierze może okazać się decydującym o sukcesie w biznesie, nauce, polityce, a także w bezpieczeństwie jednostki, czy grupy społecznej. Wraz z rozwojem technologii rośnie zainteresowanie jej pozyskiwaniem i wykorzystywaniem, to właśnie informacja staje się współczesnym dobrem, o które wybuchają konflikty. Johnny Ryan prognozował, że: „(…) ataki informacyjne mogą się okazać największą innowacją w dziedzinie prowadzenia działań wojennych od wynalezienia prochu"[4], i jak pokazują wydarzenia na arenie międzynarodowej, miał rację. Każdy okres w dziejach ludzkości miał swoje rodzaje konfliktów i dobra, o które walczono. W czasach szybkiego rozwoju cyberprzestrzeni, w wieku informacji, uwaga zaangażowanych podmiotów jest skoncentrowana na informacji.

Wpisuje się to w koncepcję fal Alvina Toffler, który wyróżnił trzy rodzaje fal technologicznych, mających wpływ na losy świata i formę toczących się wojen[5]. Wspomnianą wojnę z wykorzystaniem nowoczesnych narzędzi technologicznych, której celem jest przejecie lub kontrolowanie informacji, poprzedziły dwie inne, związane z fazami rozwoju, w jakiej znajdowała się ludzkość. Kiedy ludzie zaczęli używać narzędzi rolniczych i osiedlali się na stałe, rozpoczęli też prowadzenie lokalnych, prostych wojen o najpotrzebniejsze dobra. Fala ta jest określana agrarną i kończy się wraz z mechanizacją i rozwojem zaawansowanych narzędzi. Po niej nastąpiła wg Tofflera druga fala technologiczna, związana z rewolucją przemysłową. Wojny lokalne znacznie zwiększyły swój zasięg, odkąd zaczęto w nich stosować broń. Narzędzia walki udoskonalano i produkowano na masową skalę. Zmieniły się też cele prowadzonych konfliktów, nie były już to najpotrzebniejsze dobra, ale przede wszystkim zdobywanie wpływów i wzbogacanie się. Kolejnym ważnym momentem było wyprodukowanie broni jądrowej. Nieporównywalnie wzrosła skala konfliktów i liczba ofiar, ale nie było i nie

[3] Należy uwzględnić, że część rozwiązań i informacji może mieć charakter niejawny, jednak na potrzeby artykułu wystarczające są dostępne informacje.

[4] J. Ryan, *Info – wojna: nowe zagrożenie, łatwość jego wykorzystania – oraz nasza rosnąca bezradność*, „Przegląd NATO", zima 2007, http://www.nato.int/docu/rewiev/2007/issuer4/polish/analysis2.html, [za:] R. Bałoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 9.

[5] A. Toffler, H. Toffler, *Wojna i antywojna. Jak przetrwać na progu XXI wieku?*, Poznań 2006, s. 41-44.

jest to narzędzie stosowane powszechnie, ze względu na ogrom zniszczenia. Samo jednak jej posiadanie znacznie zmieniło sposób postrzegania konfliktów międzynarodowych. Do powszechnego użytku weszły natomiast nowocześniejsze uzbrojenia, które rozszerzały skalę prowadzonych działań, przenosiły ja bardzo szybko nawet na inne kontynenty. Stąd wojnę XX wieku nazwano wojną mobilną[6]. Dostępność nowych technologii i wyeksploatowanie się starych metod prowadzenia działań wojennych doprowadziły do powstania nowych, w tym także niekonwencjonalnych i „hybrydowych" łączących stare elementy z nowymi[7]. W większym stopniu niż kiedykolwiek zaczęto dostrzegać znaczenie informacji. To wg Tofflera trzecia fala technologiczna. Kiedy w coraz większym stopniu społeczeństwa zaczęły przenosić swoją aktywność do cyberprzestrzeni, stało się jasne, że to tam przenosi się też strefa walki. Internet stał się miejscem pracy, nauki, rozrywki, spędzania wolnego czasu, przechowywania danych przedsiębiorstw, danych osobowych, kontaktów na skalę międzynarodową. Społeczeństwa nie potrafią normalnie funkcjonować bez dostępu do Internetu, a jeśli zostaną pozbawione także dostępu do telefonii komórkowych grozi to nawet zakłóceniem funkcjonowania państw. Ma także bardzo duży stopień oddziaływania na ludzi, może wywołać panikę[8]. Poza wywołaniem utrudnień technicznych jest to także narzędzie do wywoływania pożądanych postaw społecznych na dużą skalę. Znaczne zwiększenie się ruchu sieciowego spowodowało powstanie wojny cybernetycznej – nowej generacji wojny informacyjnej, skoncentrowanej na sieciach teleinformatycznych przeciwnika[9]. Wciąż wpisuje się w założenia wojny informacyjnej znanej od lat, ale wykorzystuje dostępne od niedawna nowoczesne narzędzia.

Zasoby informacji dostępne w sieci są nie do przecenienia, nie dziwi zatem zainteresowanie nimi zarówno ze strony podmiotów państwowych, jak i niepaństwowych. Cyberprzestrzeń stała się obszarem o charakterze strategicznym, a jednocześnie wciąż nie w pełni precyzyjnie zdefiniowanym i niedopracowanym pod względem prawnym. Jej specyfika, wiele niemierzalnych parametrów, brak ograniczeń przestrzennych sprawiają, że kwestia bezpieczeństwa tego obszaru jest dużym wyzwaniem. Dotyczy to

[6] R. Białoskórski, Tamże, s. 9.

[7] A. Gruszczak, *Hybrydowość współczesnych wojen-analiza krytyczna*, [w:] *Asymetria i hybrydowość-stare armie wobec nowych konfliktów*, BBN, Warszawa, 2011, s. 10.

[8] Potwierdza to przykład ataków na Estonię w 2007 r., które są uważane za jedne z najpoważniejszych w historii. W kraju, który jest jednym z najbardziej „internetyzowanych" na świecie kilkutygodniowe incydenty w cyberprzestrzeni i kłopoty z dostępem do sieci komórkowych i kont bankowych były trudnym doświadczeniem. Estończycy nie wpadli w panikę, ale czas cyberataków jest określany jako „wstrząsający". http://news.bbc.co.uk/2/hi/europe/6665145.stm (dostęp: 11.07.2016 r.).

[9] B. Bartoszek, *Cyberwojna-wojna XXI wieku*, http://www.eioba.pl/a/1svu/cyberwojna-wojna-xxi-wieku, (dostęp: 12.03.2016 r.).

szczególnie informacji dotyczących infrastruktury krytycznej, w przypadku których utrata dostępu, przejęcie kontroli czy uszkodzenie przez wroga może stwarzać ogromne zagrożenie dla bezpieczeństwa całego kraju[10]. Warto także zauważyć, że nawet jeśli bezpośrednio dany element w systemie bezpieczeństwa nie przechowuje wrażliwych danych w sieci, to wciąż za pomocą innych urządzeń i oprogramowań zewnętrznych może być z nią związany, a dodatkowo korzysta z działalności ludzkiej, która jest najczęściej najbardziej newralgiczna. Tym samym, można stwierdzić, że współczesne bezpieczeństwo państwa jest w dużej mierze zależne od tego, jak bezpieczna jest jego cyberprzestrzeń i informacje w niej przetwarzane.

2. Zadania służb specjalnych w systemie bezpieczeństwa cyberprzestrzeni RP – założenia i realizacja

W przygotowanych przez zespół zadaniowy Ministerstwa Cyfryzacji *Założeniach strategii cyberbezpieczeństwa RP* charakter obecnego systemu ochrony cyberprzestrzeni w Polsce określono jako „rozproszony, polegający na wzajemnym współdziałaniu odpowiedzialnych podmiotów, zarówno w sferze cywilnej, wojskowej oraz tej związanej z cyberprzestępczością"[11]. Pojawia się zatem pytanie: „Jaką rolę w tym systemie odgrywają służby specjalne odpowiedzialne za bezpieczeństwo cyberprzestrzeni"?

We wspomnianym dokumencie dotychczasowe kompetencje Agencji Bezpieczeństwa Wewnętrznego określono jako rozpoznawanie, zapobieganie i zwalczanie zagrożeń. W jej strukturze wyróżniono istotną rolę Departamentu Bezpieczeństwa Teleinformatycznego wraz z Rządowym Zespołem Reagowania na Incydenty Komputerowe: CERT.GOV.PL. W *Założeniach cyberstrategii…* rola ABW ogólnie pokrywa się z kompetencjami ustanowionymi dla tej służby i założeniami Rządowego Planu Ochrony Cyberprzestrzeni RP na lata 2011-2016[12], który dodatkowo określa Agencję wraz ze Służbą Kontrwywiadu Wojskowego „służbami ochrony cyberprzestrzeni". Zgodnie z Ustawą o ABW i AW[13], do zadań Agencji Bezpieczeństwa wewnętrznego należy m. in.: rozpoznawanie, zapobieganie i zwalczanie zagrożeń, wykrywanie szpiegostwa, ujawnienia lub wykorzystania informacji niejawnych oraz pozyskiwanie i analizowanie informacji,

[10] *Media zagraniczne i polskie informowały o domniemanych planach ataku na belgijską elektrownie atomową*, http://www.tvp.info/24571242/terrorysci-planowali-zamach-na-elektrownie-atomowa-chcieli-porwac-szefa-belgijskiego-programu-nuklearnego (dostęp:11.07.2016 r.).

[11] Założenia strategii cyberbezpieczeństwa RP, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf, (dostęp:11.07.16 r.).

[12] https://bip.mswia.gov.pl/bip/programy/19057,Rzadowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html, (dostęp: 11.07.2016 r.).

[13] Art. 5 ust. 1 pkt. 1-4 *ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

które mogą mieć znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa.

Szef ABW wraz z kadrowym zapleczem technicznym tworzy Krajowy Punkt Centralny (*Focal Point*) w ramach polityki ochrony cyberprzestrzeni NATO. Podmiotem odpowiedzialnym za koordynację reagowania na incydenty w sieciach i systemach komputerowych podłączonych do sieci rozległej NATO jest Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe umiejscowione w Wojskowym Biurze Bezpieczeństwa Łączności i Informatyki podlegającym Ministerstwu Obrony Narodowej. Szef ABW i Minister Obrony Narodowej przy współpracy z ministrem właściwym do spraw wewnętrznych są odpowiedzialni za współpracę z *NATO Cyber Defence Management Authority* – CDMA. Obie służby są odpowiedzialne za opracowanie katalogów zagrożeń i możliwych podatności oraz przedstawienie ich podmiotom administracji publicznej. Ma to ułatwiać przeciwdziałanie zagrożeniom na różnych poziomach i zunifikować podejście do cyberbezpieczeństwa.

Powołany w 2008 r., funkcjonujący w ramach ABW zespół CERT.GOV.PL miał z założenia reagować na incydenty z najwyższego możliwego poziomu – służby specjalnej zajmującej się bezpieczeństwem wewnętrznym państwa, jednak niewystarczające zasoby i braki formalnego umocowania tego CERT-u znacznie ograniczyły jego rolę. Zgodnie z przyjętą Polityką Ochrony Cyberprzestrzeni, CERT.GOV.PL miał pełnić rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym[14]. Jego najważniejszym zadaniem miało być zapewnianie i rozwijanie zdolności jednostek administracji publicznej RP do ochrony przed cyberzagrożaniami. Poprzez zapisy Polityki, przypisano mu rolę CERT-u narodowego, co zostało skrytykowane przez NIK[15], bowiem faktycznie nie pełnił on takiej funkcji. Przez wiele lat rolę CERT-u narodowego pełnił zespół CERT Polska, funkcjonujący w ramach NASK. Zgodnie z terminologią wykorzystywaną przez ENISA to właśnie on, nieformalnie był CERT-em narodowym.

CERT Polska jest zespołem reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet działającym od 1996 r. w strukturach NASK. Jest jednym z najważniejszych tego rodzaju zespołów w kraju, zaś zakres jego działania obejmuje domenę internetową „pl." oraz obsługę incydentów występujących w polskich sieciach internetowych. Do głównych zadań zespołu należy: rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci, alarmowanie użytkowników o zagrożeniach, współpraca

[14] http://www.cert.gov.pl/cer/o-nas/15,O-nas.html, (dostęp:11.07.2016 r.). Pomimo powstania CERTU Narodowego, taka informacja wciąż znajduje się na stronie.

[15] Departament Porządku i Bezpieczeństwa Wewnętrznego NIK, *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf (dostęp: 11.07.2016 r.).

z innymi zespołami CERT, prowadzenie działań zmierzających do wzrostu świadomości bezpieczeństwa teleinformatycznego, prowadzenie badań dotyczących bezpieczeństwa Internetu, testowanie produktów z dziedziny bezpieczeństwa teleinformatycznego, prace w zakresie tworzenia wzorców obsługi i rejestracji incydentów[16].

NIK raportując o stanie bezpieczeństwa cyberprzestrzeni wskazał realny problem związany z funkcjonowaniem CERT-ów na poziomie ustawodawczym i wykonawczym. Instytucja, w której taki zespół powinien funkcjonować, nie miała odpowiedniego zaplecza do prowadzenia takiej działalności, przez co jej zadania nieformalnie przejął inny zespół. CERT Polska miał korzystniejszą sytuację także ze względów finansowych. W ramach ABW system wynagrodzeń dla specjalistów z CERT wynika z regulacji prawnych, a nie kwalifikacji, zaś w NASK, gdzie CERT wspomaga jego działalność gospodarcza, takich uwarunkowań nie ma i łatwiej o środki adekwatne do specjalistycznych umiejętności. Pozwala to na pozyskanie szerszego grona eksperckiego. Dodatkowo, spośród wszystkich zespołów CERT, tylko zespół CERT.GOV.PL funkcjonował w trybie 24/7, będąc przygotowanym na sytuacje kryzysowe, wciąż jednak działając w skromnym kadrowo zespole. ABW nie miało zatem możliwości realizowania swoich zadań w zakresie ochrony cyberprzestrzeni w pełni.

Zmiany w tym układzie sił pojawiły się w ubiegłym roku. 4 lipca 2016 r. w siedzibie NASK Minister Cyfryzacji Anna Streżyńska, Krzysztof Pietraszkiewicz, prezes Związku Banków Polskich oraz Wojciech Kamieniecki, dyrektor NASK podpisali porozumienie o stworzeniu CERT-u Narodowego, czyli jednostki koordynującej zwalczanie internetowych zagrożeń w administracji państwowej oraz biznesie[17]. Nowo powstały CERT Narodowy jest częścią Narodowego Centrum Cyberbezpieczeństwa[18], który również niedawno powstał w NASK. Będzie łączył działania środowiska naukowego, biznesowego i administracji publicznej. Do tej pory w ramach CERT-u Narodowego współpracę biznesową rozpoczęto np. z Credit Agricole, PKO BP, T-Mobile, Energa SA i innymi[19]. Z uwagi na nakładanie się w wielu aspektach działań tych sektorów w cyberprzestrzeni, ich współpraca na rzecz bezpieczeństwa jest bardzo ważna i konieczna. W zakresie prowadzonych działań, dotychczasowa rola CERT Polska nie zmieni się, wciąż będzie prowadzić szeroko pojęte działania analityczne, ale nie będzie już pełnić roli CERT-u o charakterze narodowym. Powołanie

[16] Ibidem.

[17] https://www.cert.pl/tag/nask/, (dostęp 12.07.2016 r.).

[18] NCC działa w trybie 24/7, jest to centrum szybkiego reagowania, koordynowania działań i wymiany informacji, https://mc.gov.pl/aktualnosci/cert-narodowy, (dostęp:12.07.2016 r.).

[19] http://businessinsider.com.pl/wiadomosci/cyberbezpieczenstwo-polski-powstal-cert-narodowy/str16te, (dostęp: 12.07.2016 r.).

CERT-u Narodowego rozwiązuje część ważnych problemów wskazanych przez NIK, choć na razie teoretycznie. Faktyczna działalność tej instytucji pozwoli na całościową ocenę tej zmiany.

Interesującą inicjatywą wspólną podjętą przez ABW i zespół CERT Polska jest stworzenie systemu wczesnego ostrzegania o zagrożenia internetowych – ARAKIS-GOV24. System wykrywa anomalie, które mogą wskazywać na atak. Instalowany w jednostkach administracji państwowej ma wspierać wczesne wykrywanie incydentów w sieci, szczególnie na styku sieci wewnętrznych i Internetu[20]. Jak podaje NIK[21], ze względu na braki finansowe, dobrowolność udziału i instalowanie sond wyłącznie w instytucjach publicznych przyczyniły się do znacznego ograniczenia zasięgu systemu. Tym samym, ARAKIS-GOV24 nie mógł działać w pełni swoich możliwości, ale jego powstanie i dotychczasowa, choć ograniczona działalność pozwala na pozytywną ocenę.

W *Polityce Ochrony Cyberprzestrzeni i Założeniach Strategii Cyberbezpieczeństwa* nie pojawia się wzmianka o drugiej ze służb specjalnych, nazywanej razem z ABW „służbą ochrony cyberprzestrzeni" – SKW. W Rządowym Programie Ochrony Cyberprzestrzeni jej zadania są przedstawiane w części wspólnej z zadaniami ABW. Obie służby mają przedstawić podmiotom administracji publicznej opracowane katalogi zagrożeń i podatności, uczestniczyć w tworzeniu wytycznych dotyczących systemów zarządzania bezpieczeństwem informacji. Na właściwych dla siebie obszarach, SKW i ABW prowadzą działania, których ogólnym celem jest rozpoznawanie, zapobieganie i zwalczanie zagrożeń, z wykorzystaniem dostępnych dla nich sił i środków. Ich rola jest kluczowa, bowiem ze względu na swoją specyfikę, poza zespołami CERT, najszybciej mogą wykrywać anomalie w systemach, także na poziomie inwigilacji grup i jednostek. SKW realizuje zadania wynikające z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych w odniesieniu do MON i jednostek podległych oraz ataszatów obrony w placówkach zagranicznych – w zakresie bezpieczeństwa osobowego oraz bezpieczeństwa przemysłowego[22]. Zwalcza cyberszpiegostwo i cyberterroryzm. SKW dokonuje także certyfikacji urządzeń i narzędzi służących do realizacji zabezpieczenia teleinformatycznego, szkoleń specjalistycznych dla administratorów systemów teleinformatycznych i inspektorów bezpieczeństwa teleinformatycznego. Służba Kontrwywiadu Wojskowego zgodnie z decyzją byłego szefa MON,

[20] W 2014 r. CERT.GOV.PL zarejestrował 4681 incydentów dotyczących oprogramowania złośliwego działającego na stacjach roboczych, podłączonych do sieci teleinformatycznej jednostek administracji publicznej, W sumie, zarejestrowanych zostało aż 12017 zgłoszeń, z których 7498 zakwalifikowano, jako incydenty, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html, s.6, (dostęp: 12.07.2016 r.).

[21] *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Ibidem, s. 15.

[22] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, sap.sejm.gov.pl (dostęp: 12.07.2016 r.).

Tomasza Siemoniaka, pełni także rolę koordynatora Systemu Reagowania na Incydenty Komputerowe w Siłach Zbrojnych RP. Zapewne ze względu na specyfikę służby, nie znajdziemy wielu transparentnych przykładów jej działalności, czy projektów, warto jednak zauważyć, że niemożliwość ich wskazania świadczy o znaczeniu tej służby dla bezpieczeństwa cyberprzestrzeni. Interesującym zagadnieniem są kontrowersje, jakie wzbudził zakończony w sądzie konflikt pomiędzy SKW a Fundacją Panoptykon, w którym to Służba przegrała sprawę w NSA. Przedmiotem sporu był wniosek Fundacji o udostępnienie informacji publicznej dotyczącej częstości sięgania po dane telekomunikacyjne i internetowe przez Służbę Kontrwywiadu Wojskowego. Według Fundacji, SKW jako jedyna ze służb odmówiła udzielenia takich informacji. Argumentacja Służby nie przekonała NSA. Zgodnie z ogłoszonym wyrokiem, taka informacja jest publiczna. Jak podaje Panoptykon, wciąż trwa spór o udostępnienie tych informacji, sama Fundacja zaś nie po raz pierwszy wysuwa zarzuty przeciwko działaniom SKW. Pojawia się zatem pytanie o przyczyny przyjęcia takiej postawy przez SKW, kiedy pozostałe służby ich nie praktykują? W obliczu emocjonującego społeczeństwo sporu o zbyt duże uprawnienia służb w zakresie inwigilacji obywateli, takie informacje działają niekorzystnie na wizerunek służb specjalnych.

Obie służby w obecnym systemie mają kluczowe znaczenie dla wykrywania i reagowania na zagrożenia w cyberprzestrzeni, a szczególnie ich współpraca. Wciąż jednak dyskusję wzbudza przydzielenie zadań związanych z ochroną cyberprzestrzeni dwóm służbom, które oprócz tego realizują też inne zadania, a znaczenie incydentów w sieci wzrasta. Czy dysponują odpowiednimi siłami i środkami? Wśród wielu głosów coraz częściej przebijają się opinie, o konieczności utworzenia odrębnej służby, zajmującej się wyłącznie bezpieczeństwem cyberprzestrzeni, czy dostosowaniem form działania służb do zmieniającej się rzeczywistości. Staje się to trudnym wyzwaniem dla odpowiedzialnych za tworzenie i funkcjonowanie systemu ochrony cyberprzestrzeni. Zgodnie z Krajowymi Ramami Polityki Cyberbezpieczeństwa RP na lata 2017-2022, w obecnym kształcie zadań poszczególnych służb konieczne będą zmiany, zgodnie z wytycznymi unijnej Dyrektywy NIS[23].

3. Służby specjalne wobec wyzwań i zagrożeń dla bezpieczeństwa cyberprzestrzeni RP – próba oceny i perspektywa zmian

W odpowiedzi na rozwój zagrożeń w sieci i krytyczne oceny niektórych dotychczasowych działań na rzecz bezpieczeństwa cyberprzestrzeni, w ostatnich miesiącach widać wzmożenie działań na tej płaszczyźnie, także

[23]Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022, MC, Warszawa 2017

w ramach zadań służb specjalnych. Wspomniany Raport Najwyższej Izby Kontroli porusza wiele istotnych problemów, które rzutowały negatywnie na cały obraz realizacji zadań z zakresu ochrony cyberprzestrzeni. Wśród zarzutów na pierwszy plan wysuwają się dotyczące kształtu całego systemu. Dokument wskazuje na brak odpowiednich struktur, ram prawnych, procedur oraz rozproszone i nieskoordynowane działania. Najostrzejsza krytyka dotknęła Ministerstwo Administracji i Cyfryzacji[24] oraz Ministerstwo Spraw Wewnętrznych. Brak odpowiednich działań ze strony tych dwóch ośrodków decyzyjnych, spowodował szereg niedociągnięć na niższych szczeblach, m.in. w Urzędzie Komunikacji Elektronicznej, ABW czy RCB[25]. W ocenie NIK, kierownictwo ABW realizowało zadania związane z zapobieganiem i reagowaniem na incydenty przy pomocy systemu ARAKIS.GOV i Zespołu CERT.GOV.PL, ale aktywność Agencji podlegała ograniczeniom ze względu na ograniczone zasoby. Jej działalność była oceniona w raporcie pozytywnie, choć zauważony został brak porozumienia pomiędzy poszczególnymi jednostkami[26]. Na tle negatywnie ocenianych działań Ministerstw, pozytywnie uwidaczniają się dokonania ABW przy współpracy z NASK, choć wielokrotnie podkreślane są ich ograniczone możliwości. Powołany niedawno CERT Narodowy realizuje część wytycznych NIK-u, jednak problem jest znacznie szerszy, stąd też wzmożone prace nad Strategią Cyberbezpieczeństwa[27].

W lutym 2016 r. opublikowano i poddano pod publiczną debatę z założenia do niej. Okazało się, że również one wzbudzają duże kontrowersje. Do Ministerstwa Cyfryzacji wpłynęło wiele uwag dotyczących Założeń[28], z których część dotyczy kompetencji ABW. Choć bezpośrednio Agencji dotyczy kilka zapisów, koncentrujących się na zmianach ustawowych, a głównie na wskazaniu w ustawie, że ABW ma pełnić funkcję rządowego zespołu reagowania na incydenty[29], to w szerszym znaczeniu, dotyczy zdecydowanie większej liczby zagadnień. Jedna z kwestii dotyczy postulowanego w Założeniach monitorowania punktów wymiany ruchu internetowego, jako naruszenia prawa do prywatności i narzędzia do pozyskiwania informacji dla służb. Stało się to

[24] Obecnie znowu są to dwa oddzielne Ministerstwa, raport dotyczył funkcjonowania Ministerstwa Administracji i Cyfryzacji. Aktualnie zadania te realizuje Ministerstwo Cyfryzacji.

[25] *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Ibidem, s. 9.

[26] W skrajnych przypadkach nie dochodziło nawet do wymiany informacji i dublowania się działań, jako przykład wskazane zostały prace nad niekompletną „Polityką ochrony cyberprzestrzeni RP".

[27] Najnowszy opublikowany dokument o tym charakterze to Krajowe Ramy Polityki Cyberbezpieczeństwa, które mają spełniać wymagania związane z implementacją Dyrektywy NIS. W tworzeniu dokumentu brali także udział przedstawiciele ABW.

[28] http://www.cyberdefence24.pl/323172,do-resortu-cyfryzacji-wplynelo-69-opinii-o-zalozeniach-strategii-cyberbezpieczenstwa-dla-rp, (dostęp: 12.07.2016 r.).

[29] *Założenia strategii cyberbezpieczeństwa RP*, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf, s. 30, (dostęp:11.07.16 r.).

przedmiotem politycznych dyskusji, w nawiązaniu do wejścia w życie *Ustawy antyterrorystycznej*. W obu przypadkach kontrowersje wzbudza domniemana inwigilacja obywateli przez służby, bez jakiejkolwiek kontroli odpowiednich organów. W uwagach do Założeń zaznaczono, że część proponowanych zmian jest wyrażona nieprecyzyjnie, stąd może rodzić obawy o ochronę danych osobowych obywateli. Analogicznie jest w przypadku zawartych w ustawie jako kompetencja ABW testów penetracyjnych w obiektach infrastruktury krytycznej. Z perspektywy użytkowników jest to zapis niejasny, poruszający istotną rolę obiektów prywatnych w infrastrukturze krytycznej i uprawnień służb w kontekście inwigilacji obywateli. Z całą pewnością wprowadzane rozwiązania mające na celu poprawę stanu bezpieczeństwa cyberprzestrzeni nie powinny budować kontrowersji wokół atmosfery niejasności, nawet jeśli są zasadne i konieczne. Ministerstwo Cyfryzacji odnosi się do tych uwag tłumacząc niektóre niejasności, jednak wciąż pojawiają się głosy krytyki. Płaszczyzna ochrony korespondencji użytkowników sieci budzi wiele emocji nawiązując do zagadnienia poświęcania części swojej prywatności na rzecz bezpieczeństwa. Generuje to ryzyko braku akceptacji społecznej, co może powodować trudności we wprowadzaniu nowych rozwiązań[30]. Krytycznie mówi się o nieuprawnionym wykorzystywaniu takich danych, z drugiej strony zaś podkreśla się, jak wiele informacji przekazują sami użytkownicy korzystając z portali społecznościowych, czy chmur obliczeniowych, mających serwery poza europejskim systemem prawnym. Niewątpliwie jest to kolejne wyzwanie, przed którym stajemy tworząc ramy prawne bezpieczeństwa cyberprzestrzeni w Polsce i będąc użytkownikami sieci.

Opublikowane w marcu 2017 r. Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022 określają priorytety polskiej polityki w tym zakresie, wynikające zarówno z krytycznych uwag zawartych we wspomnianym raporcie NIK, jak i dynamicznie zmieniającym się zapotrzebowaniem. Zadaniem tego dokumentu jest wskazanie "(...) ramowych działań, mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni[31]. Kolejnym krokiem będą zatem szczegółowe plany wdrażania rozwiązań z Krajowych Ram, na niższych poziomach i w różnego rodzaju organizacjach, od których zależy skuteczność całego procesu zmian w kształtowaniu bezpieczeństwa informacyjnego.

[30] Jest to jedno z ryzyk zdefiniowane przez *Doktrynę Cyberbezpieczeństwa*.

[31] KRPC RP, https://mc.gov.pl/files/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf, (dostęp: 16.06.2017 r.)

Ważnym krokiem w kierunku wprowadzenia zmian w działaniach na rzecz bezpieczeństwa cyberprzestrzeni było stworzenie *Doktryny Cyberbezpieczeństwa*. Dokument opublikowany w 2015 r. definiuje środowisko bezpieczeństwa w cyberprzestrzeni za pomocą wyzwań i zagrożeń[32]. Jako wyzwania, Doktryna wskazuje ryzyka i szanse. W obszarze ryzyka znalazły się zdiagnozowane też w naszym obecnym systemie nieuregulowane lub niewłaściwie uregulowane relacje między poszczególnymi podmiotami w systemie. Nieprecyzyjna określona odpowiedzialność i niejasny zakres kompetencji dotknął także służby specjalne. Wiąże się z tym także wiele luk prawnych, zarówno na poziomie prawa krajowego jak i europejskiego. Dynamicznie zmieniające się zjawiska w sieci nie mają często odzwierciedlenia w systemie prawnym, brakuje dla nich odpowiednich uregulowań, co znacznie utrudnia ściganie przestępstw w sieci. Dotyczy to także wykorzystywania np. serwerów poza granicami Polski, a tym samym poza jej jurysdykcją, jak również korzystania z usług operatorów międzynarodowych. Jako ryzyko zakwalifikowano też wykorzystanie zinformatyzowanych systemów na potrzeby bezpieczeństwa narodowego. Dotyczy to szczególnie infrastruktury krytycznej, czego doświadczył np. Iran w 2010 r. Odkryty wtedy w systemie robak komputerowy Stuxnet wykorzystywał luki w systemie operacyjnym Windows do szpiegowania i ataków na systemy przemysłowe firmy Siemens, które były wykorzystywane w irańskim programie atomowym. Stuxnet zainstalował się na 16 tysiącach komputerach. Władze Izraela nie odniosły się do pojawiających się zarzutów, ale wyniki śledztwa dziennikarskiego przeprowadzonego w 2011 roku przez redakcję „New York Timesa" sugerowały, że robak powstał i był testowany właśnie w Izraelu[33]. Problem ten może dotknąć także inne państwa, bowiem wykorzystywanie oprogramowania i urządzeń produkowanych przez prywatne firmy jest normalną praktyką. Nawet przy zwiększonych środkach ostrożności w przypadku takich zamówień, wciąż istnieje zagrożenie szpiegostwa przemysłowego i wykorzystania zdobytych informacji przeciwko podmiotom państwowym. Wśród szans, Doktryna wyróżnia możliwości rozwoju potencjału naukowego, co jest zauważalne w przypadku działań NASK-u i zespołów CERT oraz rozwijanych studiach nad kryptologią i cyberbezpieczeństwem.

Jednym z najpoważniejszych zagrożeń, z jakim mierzą się służby specjalne jest cyberszpiegostwo, również określone jako istotne zagrożenie w Doktrynie Cyberbezpieczeństwa. W lipcu 2016 r. Ministerstwo Obrony Narodowej stało się celem takiego ataku, choć jego autentyczność wciąż stoi pod dużym znakiem zapytania[34]. Intranet MON-u miał zostać zaatakowany

[32] *Doktryna Cyberbezpieczeństwa RP*, BBN, Warszawa 2015.

[33] http://di.com.pl/stuxnet-iran-nie-byl-jedynym-celem-52298, (dostęp: 16.07.2016 r.).

[34] https://niebezpiecznik.pl/post/mon-zhackowany-pravyy-sector-twierdzi-ze-wykradl-dane-z-intranetu-ministerstwa-obrony-narodowej/, (dostęp:19.07.2016 r.).

przez organizację podającą się za ukraiński Pravy Sector. Początkowo z komunikatów Ministerstwa wynikało, że to próba manipulacji i do żadnego ataku nie doszło, jednak pojawiają się także informacje, że do ataku doszło faktycznie, przez prywatnego maila jednego z pracowników, ale uzyskane informacje są nieznaczące. Poruszyło to po raz kolejny krytyczne opinie wobec SKW, jako odpowiedzialnych za bezpieczeństwo wewnętrzne sieci MON.

Obok szpiegostwa w sieci coraz większą rolę odgrywa przestępczość finansowa. Cyberprzestępcy za pomocą narzędzi śledzących, zawirusowanych maili i innych uzyskują dostęp do kont bankowych. Dotyczy to zarówno indywidualnych użytkowników, jak i firm czy instytucji publicznych. W 2015 r. ABW poinformowała Komisję Nadzoru Finansowego o możliwych atakach na jej infrastrukturę teleinformatyczną, do których finalnie nie doszło, być może właśnie dzięki wczesnemu wykryciu takiego ryzyka.

Poza zagrożeniem związanym z pozyskaniem i wykorzystaniem informacji przez podmioty nieuprawnione, co ma szczególne znaczenie dla administracji publicznej, należy wspomnieć też o wykorzystaniu sieci przez organizacje terrorystyczne i grupy przestępcze w celu dotarcia do jak największej grupy ludzi, co stanowi duże zagrożenie dla obywateli i całego systemu. Państwo Islamskie korzysta z sieci TOR, serwisów SIGAINT, Ruggedinbox i Mail2Tor, żeby zamieszczać propagandowe informacje na innych stronach. Sprawnie też szyfrują maile tworzą własne aplikacje[35]. Do kontaktu z nowymi, potencjalnymi członkami wykorzystywane są portale społecznościowe, takie jak Facebook, czy Twitter, pomimo walki z takimi zachowaniami przez administrację portali. Co ciekawe, do walki z ISIS w sieci przyłączyli się także hakerzy z grupy Anonymous[36]. To duże wyzwanie dla polskich służb specjalnych, które muszą pozyskać specjalistów od sieci społecznościowych, by skutecznie wykrywać tego typu zagrożenia.

Służby specjalne muszą nadążać za zmianami w cyberprzestrzeni. Obserwując problemy, z jakimi boryka się zarówno ABW, SKW jak i ogólnie cały system, zasadne jest stwierdzenie, że tak nie jest. Raport NIK nie pozostawia wątpliwości, że problemy zaczynają się już na etapie podstaw prawnych i podziału kompetencji. Dodatkowo, dynamiczny rozwój zagrożeń znacznie wyprzedza podejmowane działania. Warto jednak zaznaczyć, że problemy te nie wynikają ze specyfiki samych służb, ale z braku odpowiednich działań na wyższych poziomach zarządzaniach. Braki odpowiednich regulacji prawnych oraz zasobów nie mogą wpływać korzystnie na działania służb ochrony cyberprzestrzeni. W perspektywie możliwych zmian rysuje się wyodrębnienie oddzielnej służby, która przejmie ten typ działań i będzie do nich wyspecjalizowana. Z całą pewnością konieczny jest rozwój zespołów CERT oraz wprowa-

[35] http://www.cyberdefence24.pl/365903,terrorysci-uzywaja-metod-cyberprzestepcow-do-szerzenia-propagandy, (dostęp: 18.07.2016 r.).

[36] http://www.spidersweb.pl/2016/02/isis-twitter.html, (dostęp: 18.07.2016 r.).

dzanie sprawdzonych już rozwiązań do większej liczby jednostek administracji publicznej. Warto także zaznaczyć konieczność wprowadzenia elementów myślenia biznesowego o cyberprzestrzeni i jej bezpieczeństwie. Kluczowe wydaje się pozyskanie wykwalifikowanych specjalistów do pracy nad nią, jednak nie jest to możliwe, jeśli bezpieczeństwo cyberprzestrzeni pozostanie traktowane jako zwykła część administracji publicznej, na takim samym poziomie wynagrodzenia. Bez wprowadzenia niezbędnych zmian na poziomie legislacyjnym, organizacyjnym, a także samego podejścia do ochrony cyberprzestrzeni, płaszczyzna ta może stać się słabym punktem bezpieczeństwa państwa.

Podsumowanie

Z punktu widzenia założeń i swoich kompetencji ABW i SKW są kluczowymi organami w wykrywaniu i przeciwdziałaniu zagrożeniom dla bezpieczeństwa cyberprzestrzeni RP. Praktyka i aktualna sytuacja pokazują jednak, że pomimo dużego zapotrzebowania na ich skuteczne działania w tym zakresie, ich rola jest ograniczana przez nieprecyzyjne rozwiązania prawne, brak spójnych rozwiązań na wyższych szczeblach i ograniczone zasoby. Służby te i będące w ich strukturach komórki zajmujące się bezpieczeństwem cyberprzestrzeni, ze względu na swoją specyfikę mogą wykrywać zagrożenia w początkowych stadiach, ale wiele rozwiązań administracji państwowej nie nadąża za zmianami w sieci. Obserwując obecną sytuację można zatem stwierdzić, że mimo wielu solidnych kroków naprzód kwestia ta pozostanie nierozwiązana dopóki na cele związane z bezpieczeństwem cyberprzestrzeni nie zostanie przekazanych więcej sił i środków, a sam system nie zostanie poprawiony i pozbawiony błędów kompetencyjnych. Bezpieczeństwo cyberprzestrzeni zgodnie z oczekiwaniami i zapotrzebowaniem staje się priorytetem, a co za tym idzie, wymaga większego zaangażowania.

Bibliografia

Pozycje zwarte

1. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011.
2. Gruszczak A., *Hybrydowość współczesnych wojen-analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, BBN, Warszawa, 2011.
3. Ryan J., *Info – wojna: nowe zagrożenie, łatwość jego wykorzystania – oraz nasza rosnąca bezradność*, „Przegląd NATO", zima 2007, http://www.nato.int/docu/rewiev/2007/issuer4/polish/analysis2.html, [za:]

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011.
4. Toffler A., Toffler H., *Wojna i antywojna*. *Jak przetrwać na progu XXI wieku?*, Poznań 2006.

Akty prawne

5. *Doktryna Cyberbezpieczeństwa RP*, BBN, Warszawa 2015.
6. *Krajowe Ramy Polityki Cyberprzestrzeni RP na lata 2017-2022, Warszawa 2017.*
7. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Warszawa 2010.
8. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, Warszawa 2002.

Strony internetowe

9. www.mc.gov.pl (dostęp:11.07.16 r.).
10. www.di.com.pl (dostęp: 16.07.2016 r.).
11. www.cyberdefence24.pl (dostęp: 18.07.2016 r.).
12. www.spidersweb.pl (dostęp: 18.07.2016 r.).
13. www.niebezpiecznik.pl (dostęp:19.07.2016 r.).
14. www.bip.mswia.gov.pl (dostęp: 11.07.2016 r.).
15. www.nik.gov.pl (dostęp: 11.07.2016 r.).
16. www.news.bbc.co.uk (dostęp: 11.07.2016 r.).
17. www.tvp.info (dostęp:11.07.2016 r.).
18. www.rpo.gov.pl (dostęp: 11.07.2016 r.).
19. www.eioba.pl (dostęp: 12.03.2016 r.).
20. www.cert.gov.pl (dostęp: 12.07.2016 r.).
21. www.cyberdefence24.pl (dostęp: 12.07.2016 r.).
22. www.cert.pl (dostęp 12.07.2016 r.).
23. www.businessinsider.com.pl (dostęp: 12.07.2016 r.).

Liczba znaków ze spacjami: 36 310