AUTOR
ppłk mgr inż. Bartłomiej Terebiński
b.terebinski@akademia.mil.pl
Wydział Wojskowy, ASzWoj

BEZPIECZEŃSTWO TELEINFORMATYCZNE JAKO PODSTAWA FUNKCJONOWANIA WSPÓŁCZESNEGO PAŃSTWA

Słowa kluczowe: cyberbezpieczeństwo, infrastruktura krytyczna, broń cybernetyczna, cyberprzestępczość, cyberterroryzm, strategia cyberbezpieczeństwa

Współczesne ujęcie bezpieczeństwa teleinformatycznego państwa

Przenoszenie wszelkiej aktywności ludzkiej do sieci Internet stało się w ostatnich latach zjawiskiem powszechnym. Sprawa podłączania pojedynczych stacji roboczych do tej sieci jest już bezdyskusyjna od dawna, natomiast rutynowym działaniem zaczęło być umożliwianie zdalnego zarządzania całymi systemami sterującymi procesami produkcyjnymi, czy dostawami mediów. Nieustanny rozwój incydentów i zagrożeń naruszających bezpieczeństwo systemów komputerowych oraz użytkowników korzystających z nowoczesnych technologii informatycznych powoduje, że zachowanie bezpieczeństwa przestrzeni tworzonej przez te systemy jest obecnie jednym z istotniejszych problemów na poziomie krajowym i międzynarodowym w kontekście konieczności zapewnienia niezakłóconego funkcjonowania państw, gospodarki i społeczeństwa.

Nikt już nie poddaje w wątpliwość, że budowanie mechanizmów prewencji i ograniczanie skutków ataków elektronicznych przekłada się bezpośrednio na podniesienie poziomu szeroko rozumianego bezpieczeństwa państwa i jego obywateli. Wczesne ostrzeganie, a przede wszystkim zapobieganie takim zagrożeniom stało się priorytetem dla służb i instytucji odpowiedzialnych za tworzenie krajowego systemu bezpieczeństwa teleinformatycznego oraz zarządzanie wszelkimi działaniami w obszarze zdefiniowanym w obowiązującej doktrynie jako cyberprzestrzeń[1]. Działania mu-

[1] W Doktrynie cyberbezpieczeństwa RP definiuje się cyberprzestrzeń jako *przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie a także wysyłanie i odbieranie danych przez sieci*

szą być skoordynowane na poziomie krajowym i będą angażować zarówno administrację państwową, jak i innych zainteresowanych w postaci: podmiotów gospodarczych w różnych sektorach (w szczególności będących częścią infrastruktury krytycznej[2]), organizacji pozarządowych, instytucji naukowo-badawczych, czy wreszcie samych użytkowników cyberprzestrzeni.

Zarządzanie infrastrukturą krytyczną

W myśl zapisów ustawy o zarządzaniu kryzysowym infrastrukturę krytyczną państwa definiuje się jako *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 administracji publicznej, a także instytucji i przedsiębiorców*[3]. W praktyce są to rzeczywiste i cybernetyczne systemy, wskazane w niejawnej części dokumentu o nazwie Narodowy Program Infrastruktury Krytycznej, niezbędne do minimalnego funkcjonowania gospodarki i państwa. Każdy z tych elementów można zaliczyć do któregoś z niżej przytoczonych rodzajów systemów (Rys. 1.).

Można stwierdzić, że w wyniku rozwoju technicznego i globalnego stosowania informatycznych systemów wspomagających powszechne staje się zarządzanie ww. systemami w sposób w pełni zautomatyzowany (bez udziału lub przy minimalnym wpływie człowieka) oraz za pośrednictwem zdalnych urządzeń (a zatem wymagających medium transmisyjnego, jakim są sieci komputerowe). W ocenie autora każdy z tych obszarów ściśle związany jest z koniecznością utrzymywania dostępu do sieci teleinformatycznych i kierowania wszelkimi działaniami właśnie poprzez te sieci.

---

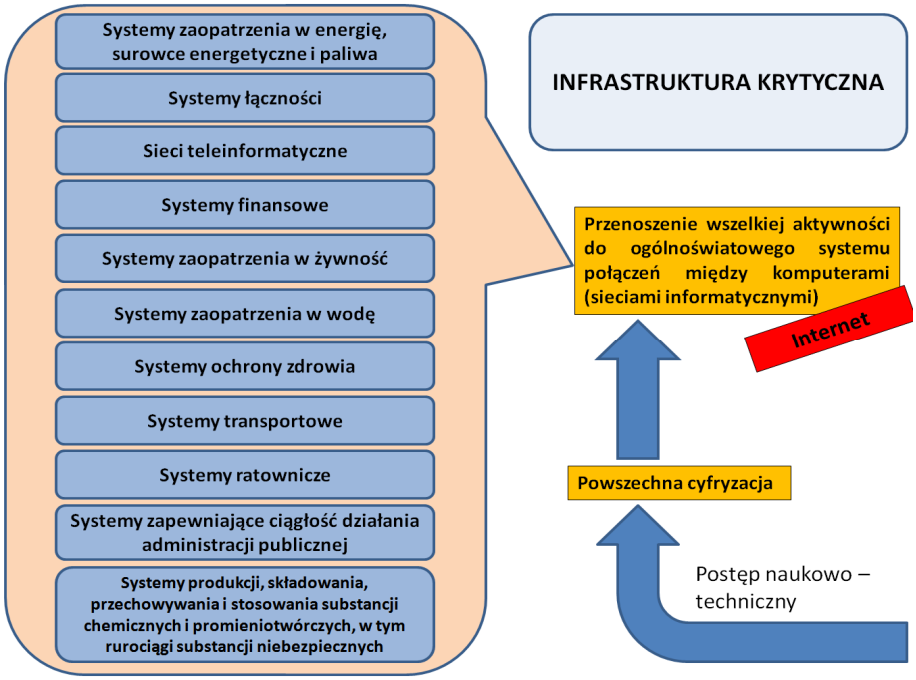
telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończenia sieci) wraz z powiązaniami między nimi oraz użytkownikami, Por. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, 2015, s. 7.

Tematykę krajowego systemu bezpieczeństwa teleinformatycznego szerzej omówiono w części końcowej artykułu, natomiast przez pojęcie bezpieczeństwa teleinformatycznego, które w dostępnej literaturze często używa się wymiennie z *cyberbezpieczeństwem* (choć zdania wobec powyższego są podzielone) rozumieć należy 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*, Tamże, s. 7.

[2] Patrz kolejny punkt artykułu.

[3] *Ustawa z dnia* 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, Dz. U. z 2017, poz. 1566, art. 3, § 2.

W zakresie obronności państwa wszelkie procesy technologiczne w zakładach produkujących broń i środki bojowe sterowane są przy pomocy zinformatyzowanych systemów. Istotna w tej dziedzinie jest również ochrona danych wrażliwych, szczególnie dotyczących prowadzonych prac konstrukcyjnych.



Źródło: opracowanie własne na podstawie *Ustawa z dnia* 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, Dz. U. z 2017 r., poz. 1566, art. 3, §2.

Rys. 1. Systemy infrastruktury krytycznej

Nieodzowna jest ochrona takich podmiotów gospodarczych państwa jak zakłady mające związek z wydobyciem surowców mineralnych o znaczeniu strategicznym dla państwa (również w pełni zautomatyzowanych). Cały sektor bankowy ściśle uzależniony jest od właściwie funkcjonującej globalnej sieci Internet. Podobne wymagania stawiane są obiektom bezpieczeństwa publicznego, a w tym elektrowniom, ciepłowniom, zakładom produkującym materiały chemiczne, liniom energetycznym i telekomunikacyjnym. W przypadku obiektów zapewniających ochronę innych ważnych interesów państwa, a w tym związanych z dystrybucją informacji (*mass media*) czy unikalną produkcją, sytuacja jest identyczna jak wyżej stwierdzono[4].

[4] Por. *Ustawa z dnia 22 sierpnia 1997r. o ochronie osób i mienia*, Dz. U. z 2017 r., poz. 2213, art.5.

Zarządzanie infrastrukturą krytyczną skupione jest na zapobieganiu zakłóceniom w jej funkcjonowaniu, przygotowaniu na sytuacje kryzysowe mogące niekorzystnie na nią wpłynąć, reagowaniu w sytuacjach zniszczenia systemów oraz ich odtwarzaniu. Szczególne miejsce, co podkreśla rolę bezpieczeństwa teleinformatycznego państwa, w obowiązującej aktualnie Strategii Bezpieczeństwa Narodowego RP[5] zajmuje tematyka zarządzania i ochrony krytycznej infrastruktury teleinformatycznej. Wskazana wyraźnie została rosnąca zależność pomiędzy poziomem bezpieczeństwa obszaru domeny cyfrowej a bezpieczeństwem ogólnym państwa. W punkcie 57 strategii uzależniono wręcz działanie całego państwa od właściwie funkcjonującego systemu teleinformatycznego RP. W związku z powyższym działania administracji państwowej skierowane są na zmniejszenie skutków naruszeń bezpieczeństwa cyberprzestrzeni, realizację spójnego systemu zarządzania cyberprzestrzenią (przede wszystkim koordynację i wymianę informacji pomiędzy podmiotami odpowiedzialnymi za ochronę tego obszaru) oraz zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w tym zakresie. Program ten dotyczy wszystkich obywateli kraju użytkujących cyberprzestrzeń zarówno w kraju, jak i poza jego granicami (np. ambasady i inne placówki dyplomatyczne, polskie kontyngenty wojskowe itp.).

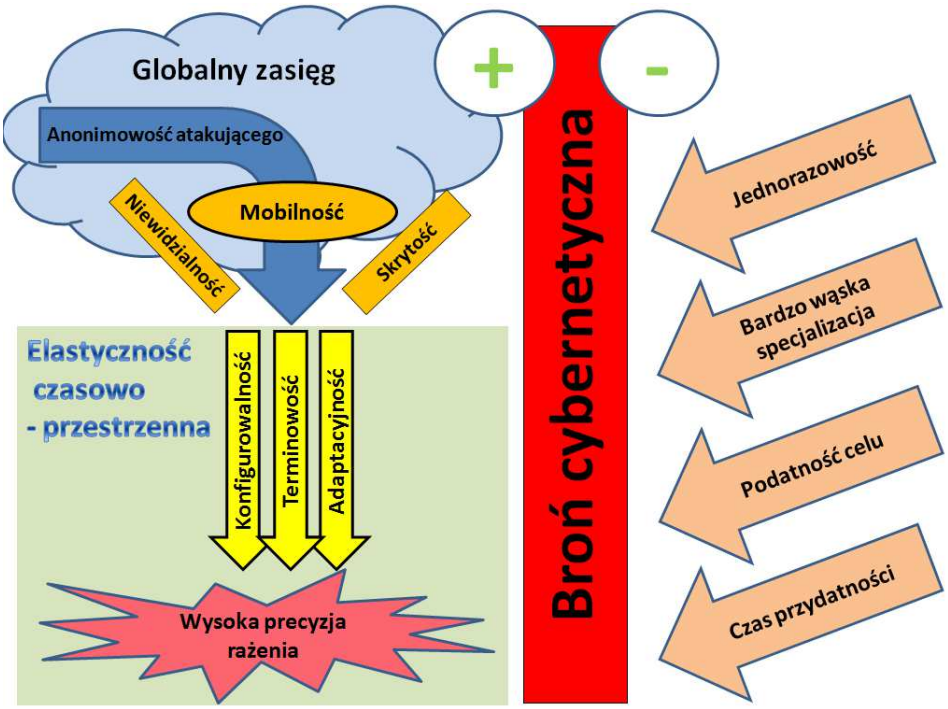
Broń elektroniczna jako narzędzie walki w cyberprzestrzeni

Cyberprzestrzeń jest środowiskiem sztucznie wytworzonym, działającym w wirtualnej rzeczywistości. Cechuje ją globalny zasięg i nieograniczone możliwości płynnego przesyłu danych niezależne od dystansu, co można uznać za dobrodziejstwo, ale również zagrożenie mające podłoże począwszy od społecznego, poprzez kryminalne, a na terrorystycznym i militarnym kończąc. W dobie społeczeństwa sieciowego, gdy coraz większa część aktywności społecznej odbywa się poprzez komunikację na skalę światową, wyłania się kolejna (po lądzie, morzu, powietrzu i kosmosie, patrząc od strony ewentualnej aktywności sił zbrojnych) przestrzeń, gdzie prowadzone będą destrukcyjne działania[6]. Narzędzia używane w tym spektrum zgodnie nazywane są w dostępnej literaturze bronią cybernetyczną[7].

[5] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa, 2014.

[6] Przestrzeń cybernetyczną jako piąty model wojny wyróżniono już na początku lat dziewięćdziesiątych w tzw. „modelu Wardena", J. Wadren, *The Enemy as System*, 1995.

[7] Do chwili obecnej w nomenklaturze wojskowej funkcjonuje pojęcie walki elektronicznej, a co za tym idzie użycie broni elektronicznej w tym spektrum. Wydarzenia i postęp technologiczny ostatnich lat oraz wyraźne odwołania w dostępnej literaturze do



Źródło: opracowanie własne na podstawie K. Dymanowski, *Broń cybernetyczna jako uzbrojenie strategiczne nowej generacji*, Kwartalnik Bellona, Rocznik XCVIII(X), nr 2 /2016 (685), s. 180-183.

Rys. 2. Cechy broni cybernetycznej

Pojęcie broni cybernetycznej (cyberbroni) jest stosunkowo nowe. W związku z powyższym istnieje wiele sprzecznych opinii ekspertów dotyczących samej definicji, klasyfikacji tego typu asortymentu oraz warunków prawnych jego użycia[8]. Na potrzeby niniejszego opracowania przyjmuje się, że jest to cybernetyczny środek walki zdolny do zadania ran lub śmierci ludziom oraz uszkadzania lub niszczenia obiektów, który obejmuje zarówno nieskomplikowane programy służące do włamywania i przeszukiwania systemów informatycznych, jak i złośliwe oprogramowanie powodujące unicestwianie infrastruktury teleinformatycznej, mogące w następstwie wywołać katastrofalne zdarzenia w świecie fizycznym. Podobnie sytuacja wygląda z klasyfikowaniem ataków z wykorzystaniem cyberbroni. Po-

przedrostka cyber- wskazuje na konieczność, wg autora opracowania, używania wymiennie nazwy broń elektroniczna – broń cybernetyczna.

[8] Por. K. Dymanowski, *Broń cybernetyczna jako uzbrojenie strategiczne nowej generacji*, Kwartalnik Bellona, Rocznik XCVIII(X), nr 2 /2016 (685), s. 178.

wszechnie stosowany jest podział na ataki z użyciem destrukcyjnego oprogramowania oraz uniemożliwiającego dostęp do zasobów (usług).

Cechą charakterystyczną niewątpliwie nowego arsenału sił zbrojnych współczesnych państw, jaką jest cyberbroń (patrz Rys. 2), jest trudność identyfikacji przeciwnika. Ze względu na nieograniczony zasięg, z którego może być przeprowadzony atak (praktycznie każde miejsce na kuli ziemskiej), nie sposób tego ataku przypisać do jakiegokolwiek konkretnego kraju (a zatem i osoby). Szybkość ograniczona jest wyłącznie przepustowością łączy transferowych znajdujących się na trasie źródło – obiekt. Daje to nieograniczone możliwości w zakresie terminu wykonania uderzenia oraz doboru miejsca prowadzenia walki. Bez wątpienia, korzystając z wysokiej elastyczności w zakresie dopasowania cyberbroni do konkretnego celu ataku przejawiającej się w łatwości zmiany jej struktury wewnętrznej (kodu programu) i zdolności przystosowania do otoczenia, daje to możliwość wykonania działań ofensywnych z niezwykle wysoką precyzją rażenia. Ponadto koszty wykonania tego typu posunięć w klasycznym ujęciu są zauważalnie niższe od użycia broni konwencjonalnej.

Wskazane jest tutaj powiedzieć również o wysoce wyspecjalizowanych a zarazem kosztownych cyberatakach na obiekty infrastruktury krytycznej państwa, kiedy istnieje potrzeba użycia tzw. kodu zerowego[9]. Koszty takiego ataku zwiększone są z powodu konieczności przygotowania zaawansowanego, inteligentnego (samouczącego się), samosterującego isamoadaptującego się oprogramowania szpiegowskiego mającego na celu zidentyfikowania luk w systemie ochrony (podatności). Pomimo faktu, że koszt *exploit* może wynieść nawet do kilkuset tysięcy dolarów i tak będzie on zdecydowanie niższy niż w przypadku użycia standardowych środków rażenia.

Differentia specifica dla ww. zalet broni cybernetycznej (Rys. 2) jest jej niepowtarzalność. Raz użyta cyberbroń musi być wycofana z użytku ze względu na jej ujawnienie (zdemaskowanie), a zatem możliwość zbudo-

[9] Kod zerowy (zero-day exploit) – program mający na celu wykorzystanie błędów w oprogramowaniu, który pojawia się na czarnym rynku przed publikacją poprawki przez producenta. Wśród wytycznych bezpieczeństwa teleinformatycznego, zwyczajem przyjętym w przypadku odkrycia nowej „dziury", jest powiadomienie producenta oprogramowania lub systemu operacyjnego i danie mu czasu na publikację poprawki. Producenci mają wówczas czas na usunięcie luk, zanim zaczną one być wykorzystywane przez cyberprzestępców (zagadnienie omówione w kolejnym rozdziale opracowania). Czasami informacja o nowej dziurze nie jest w ogóle publikowana, gdyż odkrywca sprzedaje ją cyberprzestępcom i producent dowiaduje się o niej dopiero wtedy, gdy jest ona od pewnego czasu wykorzystywana do ataków. W tych przypadkach mamy do czynienia z dziurą typu *zero-day*. Część firm z branży bezpieczeństwa stara się skupować takie informacje i oferować poprawki lub sygnatury swoim klientom z wyprzedzeniem. W niektórych przypadkach badacze publikują informację o dziurze równocześnie z powiadomieniem producenta. W takim przypadku od momentu publikacji do pojawienia się praktycznych metod ataku mija kilka dni, zwłaszcza jeśli opis podatności ma charakter teoretyczny, wikipedia.pl.

wania adekwatnych zabezpieczeń. Ograniczenia użycia związane są również z krótkim terminem jej przydatności (właściwości oprogramowania systemów informatycznych ulegają zmianie po każdej aktualizacji lub modyfikacji). Tak zwana podatność celu jest kolejnym determinantem jakości uderzenia cybernetycznego. Nieodpowiednio rozpoznane wrażliwe punkty (luki systemowe) konkretnego, fizycznego obiektu (nie tylko jego rodzaju) skutkują brakiem precyzyjności całego przedsięwzięcia. Współczesne kraje stosują już z powodzeniem od kilkunastu lat cyberbroń, czego przykładem są fakty wyeksponowane w dostępnych źródłach[10].

Podsumowując, autor opracowania skłania się do stwierdzenia, że skuteczne użycie broni cybernetycznej na szczeblu strategicznym (paraliżujące funkcjonowanie całego państwa) przy obecnym zaawansowaniu technologicznym jest raczej niemożliwe. Zdecydowanie natomiast jest to idealne narzędzie do wywiera tak zwanego efektu psychologicznego na społeczeństwo, poprzedzające klasyczny atak, co znajdzie zastosowanie we współcześnie prowadzonych działaniach hybrydowych[11].

Cyberprzestępczość a cyberterroryzm

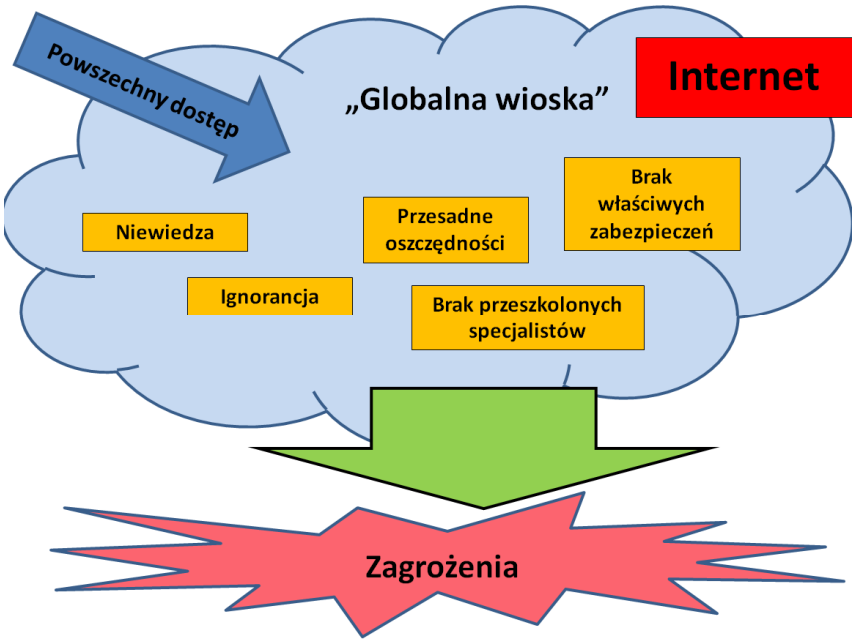
Wkroczenie w erę digitalizacji każdego obszaru życia spowodowało, że urządzenia typu komputer czy IPhone stały się nieodzownymi instrumentami pracy stosowanymi na co dzień. Dzięki możliwości natychmiastowego łączenia się i szybkiej komunikacji bariera przestrzeni i czasu ulega zatarciu, a dostępność do każdego miejsca na świecie wydaje się bezproblemowa. Globalną wioskę[12] tworzy społeczeństwo informacyjne, które opiera swoje funkcjonowanie na technologiach teleinformatycznych (przede wszystkim Internecie oraz telefonii komórkowej). Powszechność eksploatacji komputerów oraz sieci wiąże się nie tylko z korzyściami, lecz także rosnącą wrażliwością na ich szkodliwe wykorzystanie (Rys. 3.). Szybki rozwój techniki przyczynił się nie tylko do gigantycznych zmian w gospodarce światowej, lecz także do ewoluowania form łamania prawa. W praktyce każde urządzenie, program czy usługa, która powstała w celu

[10] https://en.wikipedia.org/wiki/Great_Firewall, http://large.stanford.edu/courses/2015/ph241/holloway1/, https://en.wikipedia.org/wiki/Counterelectronics_High_Power_Microwave_Advanced_Missile_Project, http://nt.interia.pl/raporty/raport-wojna-przyszlosci/lotnictwo/news-f-35-z-bronia cybernetyczna,nId,1703373 [dostęp: 01.10.2017].

[11] Wojna hybrydowa – strategia wojenna łącząca działania konwencjonalne, nieregularne, cybernetyczne oraz, w zależności od sytuacji, również inne sposoby destrukcji. Źródło: https://pl.wikipedia.org/wiki/Wojna_hybrydowa [dostęp: 05.10.2017].

[12] Globalna wioska (ang. global village) – termin wprowadzony już w 1962 przez Herberta Marshalla McLuhana w jego książce *The Gutenberg Galaxy* (Galaktyka Gutenberga), opisujący trend, w którym masowe media elektroniczne obalają bariery czasowe i przestrzenne, umożliwiając ludziom komunikację na masową skalę, https://pl.wikipedia.org/wiki/Globalna_wioska [dostęp: 10.10.2017].

ułatwienia codziennej egzystencji, mogą zostać wykorzystane przez e-przestępców[13].



Źródło: opracowanie własne na podstawie B. Biernacik, L. Kalman (red.), *Systemy i sieci teleinformatyczne SZ RP – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, ASzWoj, Warszawa, 2016, s. 278.

Rys. 3. Źródła zagrożeń w cyberprzestrzeni

Do najstarszych form wykorzystania luk w zabezpieczeniach komputerowych należy działalność hakerów[14] - osób, które dzięki indywidualnym zdolnościom i wiedzy informatycznej sabotowały zabezpieczenia elektroniczne i zdobywały dostęp do zasobów. Stąd wzięła się definicja pierwszego rodzaju e-przestępstw, czyli hakingu. Haking *jest działaniem, motywowanym przez ambicje sprawdzenia własnych umiejętności, polegającym na łamaniu zabezpieczeń komputerowych i w konsekwencji uzyskaniu dostępu do danych znajdujących się w urządzeniu*[15]. Niezależnie, czy działanie to odbywało się w granicach prawa (włącznie z informowaniem autora

[13]E-przestępca – osoba popełniająca czyn zabroniony w cyberprzestrzeni, uznany za zasadniczo społecznie szkodliwy lub społecznie niebezpieczny, konkretnie zdefiniowany i zagrożony karą na mocy prawa karnego, definicja własna na podstawie *Ustawy z dnia 6 czerwca 1997 r. Kodeks Karny*, Dz. U. z 2017 r., poz. 2204.

[14] Datowana już na połowę lat 60. XX wieku.

[15] Por. M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa, 2009, s. 98.

systemu o złamaniu jego zabezpieczeń), czy balansowało na jego granicy (stąd podział hakerów – patrz rys. 4) haking odbywa się z pobudek pozapolitycznych, bez dokonywania nieodwracalnych zniszczeń. Zupełnie innym zjawiskiem jest haktywizm[16], będący wynikiem podziału hakerów na tych, którzy uprawiają nielegalny proceder w celu osiągnięcia osobistych korzyści oraz tych, dla których potencjał cyberprzestrzeni był rozpoznawalnym miejscem do promowania konkretnych poglądów politycznych. Spojrzenie na tego typu działalność z punktu widzenia bezpieczeństwa teleinformatycznego państwa, chociaż czasami może być niewygodne w pracy instytucji publicznych, nie ma jednak istotnego wpływu na właściwe funkcjonowanie całego kraju. Zdecydowanie bardziej bezwzględną działalność wykazują haktywiści patriotyczni. Ich ataki przeciwko stronom internetowym[17] mogą przybierać groźniejsze formy, w szczególności podczas konfliktów międzynarodowych. Często cechują się głębokim fundamentalizmem[18].

Cyberprzestępczość, choć jej źródeł należy szukać w latach 80. XX wieku i ściśle wiązać z hakingiem, definicji doczekała się dopiero w 2001r.[19], kiedy określono ją jako wykorzystanie komputerów do jakiejkolwiek działalności wykraczającej poza granice prawa. W Polsce zjawisko opisano w Rządowym Programie Ochrony Cyberprzestrzeni RP[20], stwierdzając, że jest to czyn zabroniony popełniony w obszarze cyberprzestrzeni. Jego cechą charakterystyczną są aspiracje do wejścia w posiadanie wrażliwych informacji i w następstwie pozyskania określonych korzyści osobistych przez pojedyncze osoby lub zorganizowane grupy przestępcze. W tym miejscu należy zwrócić uwagę na fakt, że w ogólnym rozliczeniu zjawisko to nie może być bagatelizowane, ponieważ koszt przestępczości

[16] Termin haktywizm powstał z połączenia słów haking i aktywizm w 1996r. (grupa Cult of DeadCow).

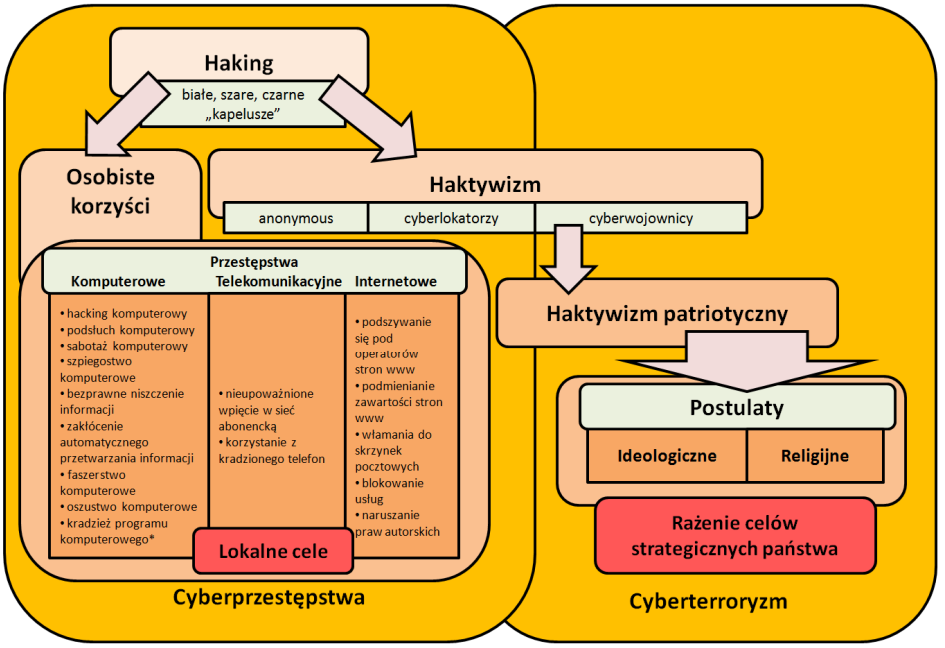
[17] DDoS (DoS) – wysyłanie do urządzenia działającego w sieci takiej ilości informacji, że nie jest on w stanie ich przetworzyć, co w konsekwencji je zablokuje, Por. M. Marczyk, M. Frączek (red.), *Wybrane aspekty bezpieczeństwa cybernetycznego SZRP*, AON, Warszawa, 2014, s. 68

[18] M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, Kwartalnik Naukowy OAP UW "e-Politikon", nr 6/2013, Ośrodek Analiz Politologicznych UW, Warszawa, 2013, s. 119-120.

[19] Konwencja Rady Europy o cyberprzestępczości, Rada Europy, Budapeszt 23.11.2001 r. Do cyberprzestępstw zaliczono: naruszenia bezpieczeństwa (haking, nielegalne uzyskanie danych), oszustwa i fałszerstwa, pornografię dziecięca, naruszenie praw autorskich. Autorzy definicji K.M. Finklea, C.A. Theohary.

[20] Klasyfikacja cyberprzestępstw wg Rządowego Zespołu Reagowania na Incydenty Komputerowe – CERT: wykorzystanie podatności w urządzeniach, próby nieuprawnionego logowania, nieuprawnione logowanie, podsłuch, naruszenie procedur bezpieczeństwa, kradzież tożsamości, podszycie się, dezinformacja, nieuprawniony dostęp do informacji, atak odmowy dostępu, błędy aplikacji WEB, skanowanie, botnet.

internetowej na świecie tylko w 2016r. został oszacowany na poziomie 445 mld dolarów[21].



*** Źródło: www.policja.pl.**
Kodeks karny: Art. 267-270, 276, 278, 287.

Źródło: opracowanie własne na podstawie M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, Kwartalnik Naukowy OAP UW "e-Politikon", nr 6/2013, Ośrodek Analiz Politologicznych UW,Warszawa, 2013, s. 110.

Rys. 4. Klasyfikacja zagrożeń w cyberprzestrzeni

W przeciwieństwie do wyżej omówionych przypadków cyberterroryzm, którego szereg wykładni znaleźć można we współczesnych publikacjach[22], jest zjawiskiem charakteryzującym się wielopłaszczyznowo rozumianymi politycznymi przesłankami. W tym kontekście cyberterroryzm przypomina haktywizm (patrz Rys. 4.), któremu również przyświeca polityczna inspiracja, jednak ta działalność ma na celu zadanie dużych strat z ofiarami

[21] W. Iszkowski, *Odpowiedzialność za bezpieczeństwo teleinformatyczne państwa*, Warszawa, 2016.

[22] Na potrzeby opracowania przyjęto następującą definicję: *cyberterroryzm to politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów, również wykorzystanie Internetu przez organizacje terrorystyczne do komunikowania się, propagandy i dezinformacji*, A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa, 2003, s. 73.

śmiertelnymi włącznie. Na „pole bitwy" w cyberprzestrzeni wytaczane są najbardziej zaawansowane sposoby niszczenia przeciwnika, w tym przede wszystkim obiekty mające kluczowe znaczenie dla bezpieczeństwa państwa. W tym rozumieniu infrastruktura krytyczna państwa będzie priorytetowym obszarem operacji. W związku z powszechną komputeryzacją każdej dziedziny życia potencjalny cyberterrorysta dysponuje szeregiem celów strategicznych, które mogłyby zostać rażone, doprowadzając do paraliżu państwa oraz szkodliwych następstw w wymiarze społecznym i gospodarczym[23].

Celem ataku będzie nie tylko dokonanie określonych zniszczeń, ale również efekt psychologiczny i propagandowy. Odnosi się to zarówno do rządu danego państwa, jak i jego obywateli poprzez wywołanie społecznego strachu. Z reguły za atakami cyberterrorystycznymi stoją wysoce zorganizowane grupy, dysponujące odpowiednimi zasobami finansowymi, często stosujące właśnie sieć Internet jako źródło werbunku w swoje szeregi. Warto podkreślić, że cyberterroryzm jest niebezpieczny nie tylko dla poszczególnych państw, ale dla całej społeczności światowej. Globalizacja sieci Internet pozwala napastnikowi na pracę z dowolnego miejsca na świecie, pomimo odległości do celu ataku. Sieć ta jest idealnym miejscem dla terrorystów ze względu na bezpłatny dostęp i szybki transfer danych, niewielką możliwość kontroli służb państwowych, anonimowość użytkownika, teoretycznie potężną ilość odbiorców, których uwagę łatwo zwrócić na różnego rodzaju forach sieciowych, dających możliwość wymiany informacji, a także poglądów politycznych.

Podsumowując, trzeba zdać sobie sprawę z faktu, że aby cyberatak był skuteczny, musi być przeprowadzony kompleksowo. Zakłócenie pracy jednego systemu, nawet stanowiącego element infrastruktury krytycznej, nie stwarza zagrożenia dla państwa jako całości. Skuteczny atak musiałby zatem obejmować wiele różnych strategicznych systemów jednocześnie. Wymagałoby to ogromnej wiedzy z różnych dziedzin techniki, w tym zastosowanie wielu typów narzędzi oraz przede wszystkim długotrwałego procesu przygotowawczego.

Kierunki rozwoju w zakresie zwiększenia cyberbezpieczeństwa państwa

Punktem wyjścia do rozważań w zakresie zwiększenia bezpieczeństwa teleinformatycznego kraju są założenia obowiązującej *Strategii bezpieczeństwa narodowego RP* z 2014 r. W myśl jej zapisów *bezpieczne*

[23] Za sztandarowy przykład ataku cyberterrorystycznego uznaje się paraliż estońskiego systemu finansowego w 2007 r.

funkcjonowanie systemu teleinformatycznego Rzeczypospolitej Polskiej jest warunkiem niezakłóconego działania całego państwa[24]. W związku z powyższym niezbędne jest określenie obszarów bezpieczeństwa właściwych systemów teleinformatycznych i zabezpieczenie możliwości transferu danych w tych systemach, a w następnej kolejności skonfigurowanie jednolitej platformy do wymiany informacji w administracji publicznej. W zakresie infrastruktury niezbędna jest modernizacja obiektów specjalnych, wprowadzanie nowoczesnych urządzeń technicznych, w tym uporządkowanie sieci w zakresie ostrzegania i alarmowania. Tworzenie mechanizmów cyberobrony konieczne jest również w Siłach Zbrojnych RP. Istotne znaczenie ma niewystarczająca wiedza użytkowników o zagrożeniach i środkach zabezpieczających.

Odpowiadając na założenia strategii bezpieczeństwa narodowego w 2016r., określono postulaty tzw. nowego podejścia[25] do problematyki cyberbezpieczeństwa, które prezentuje rys. 5.

Źródło: opracowanie własne na podstawie *Strategia cyberbezpieczeństwa RP na lata 2016-2020*, Ministerstwo Cyfryzacji, 2016, s. 6-7.

Rys. 5. Założenia strategii cyberbezpieczeństwa

[24] *Strategia bezpieczeństwa narodowego RP*, Biuro Bezpieczeństwa Narodowego, Warszawa, 2014, s.25.

[25] *Strategia cyberbezpieczeństwa RP na lata 2016-2020,* Ministerstwo Cyfryzacji, Warszawa, 2016.

Zakłada się wdrożenie krajowego systemu cyberbezpieczeństwa, który obejmował będzie całokształt przedsięwzięć niezbędnych do ustanowienia i utrzymania na zakładanym poziomie bezpieczeństwa w cyberprzestrzeni. Kompleksowe podejście do budowy tego systemu oznacza, że żaden jego element nie będzie pominięty w procedurach reagowania na zagrożenia w cyberprzestrzeni (zasoby państwowe, samorządowe, prywatne).W jego skład wejdą minister cyfryzacji oraz inni ministrowie zgodnie z zakresem kompetencji, Narodowe Centrum Cyberbezpieczeństwa, zespoły reagujące na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni (CSIRT), kierownicy instytucji objętych zakresem strategii[26]. Ze względu na zakładane zwiększenie potrzeb w zakresie specjalistów z obszaru cyberbezpieczeństwa konieczne będzie uruchomienie odpowiednich programów kształcenia, nowych kierunków studiów oraz kampanii społecznych i edukacyjno – prewencyjnych. System ma dopełnić cykl szkoleń dla organów ścigania, pracowników administracji publicznej oraz inwestowanie w personel posiadający „ponadprzeciętne kwalifikacje" (program „Złota Setka"). Podejmowany wysiłek skierowany będzie również na współpracę międzynarodową w dziedzinie cyberbezpieczeństwa oraz kooperację z ośrodkami akademickimi i naukowo-badawczymi oraz publiczno-prywatnymi odpowiedzialnymi za bezpieczeństwo teleinformatyczne, produkcję sprzętu i oprogramowania. Podobne założenia statutowe ma Europejska Agencja Cyberbezpieczeństwa – proponowana do utworzenia w najbliższym roku przez Komisję Europejską.

Przyjęte rozwiązania w zakresie zwiększenia cyberbezpieczeństwa mają na celu umożliwić zsynchronizowanie wszelkich możliwych działań dotyczących zapobiegania i zwalczania zagrożeń w tym obszarze. W założeniu pozwolą na natychmiastowe i skuteczne reagowanie na ataki wymierzone przeciwko systemom, sieciom teleinformatycznym i oferowanym przez nie usługom. Z uwagi na wzrost zagrożeń ze strony sieci publicznych, od których całkowita izolacja nie jest możliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, działanie takie wydaje się jak najbardziej pożądane i przyniesie oczekiwany efekt w nadchodzącej cybernetycznej przyszłości.

Podsumowanie

W ostatnich latach można zaobserwować wyraźny wzrost zainteresowania tematyką prowadzenia działalności w cyberprzestrzeni. Dotyczy to zarówno strony mającej w swoich założeniach statutowych zapewnienie szeroko rozumianej ochrony i utrzymanie stabilności pracy sieci teleinfor-

[26] Tamże, s. 16.

matycznych, jak i osób oraz całych organizacji, dla których ten obszar jest nowym medium do realizacji swoich destrukcyjnych celów.

Analiza przykładów cyberprzestępczości skłania do wniosku, że nie stanowi ona bezpośredniego zagrożenia bezpieczeństwa teleinformatycznego całego kraju. Z pewnością jest to wyzwanie dla organów ścigania, ale zakres tego zjawiska w kontekście funkcjonowania strategicznych urządzeń (infrastruktury krytycznej) jest dość ograniczony i z pewnością nie wiąże się z implikacjami natury politycznej lub militarnej. Z kolei wszechstronny atak cyberterrorystyczny może przygotować jedynie uporządkowana, dysponująca sporym zasobem specjalistycznego personelu oraz wystarczającymi (w domyśle dużymi) środkami finansowymi, organizacja działająca na polu międzynarodowym.

Chociaż w historii cyberataków takiego zjawiska jeszcze nie odnotowano, nie oznacza to, że nie należy podejmować wszelkich działań zapewniających możliwie skuteczną osłonę zarówno administracji i instytucji ważnych dla funkcjonowania kraju, jak i całego społeczeństwa. Natomiast bezdyskusyjną kwestią jest, że już sama świadomość złożoności problemu oraz dążenie do skoordynowania działań wielu różnych podmiotów ma kluczowe znaczenie przy realizowaniu wypracowywanej i wprowadzonej w życie strategii[27] będącej spójnym programem działań na rzecz poprawy bezpieczeństwa teleinformatycznego państwa.

Bibliografia

1. Biernacik Bartosz, Kalman Leszek*, Systemy i sieci teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polskiej – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, ASzWoj, Warszawa, 2016.

2. Bógdał-Brzezińska Anna, Gawrycki Mirosław*, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa, 2003.

3. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa, 2015.

4. Dymanowski Krzysztof, *Broń cybernetyczna jako uzbrojenie strategiczne nowej generacji*, Kwartalnik Bellona, Rocznik XCVIII(X), nr 2 /2016 (685).

5. Frączek Mariusz, Marczyk Maciej*, Wybrane aspekty bezpieczeństwa cybernetycznego Sił Zbrojnych RP*, AON, Warszawa, 2014.

6. Lakomy Marek*, Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii, Zagrożenia dla bezpieczeństwa teleinforma-*

[27] *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020*, Ministerstwo Cyfryzacji, Warszawa, 2016.

tycznego państw – przyczynek do typologii, Kwartalnik Naukowy OAP UW "e-Politikon", nr 6/2013, Ośrodek Analiz Politologicznych UW, Warszawa, 2013.

7. Lidwa Witold (red.), *Ochrona infrastruktury krytycznej*, AON, Warszawa, 2012.
8. Madej Maciej, Terlikowski Marcin (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa, 2009.
9. *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*, Dz. U. z 2010 r., nr 83, poz. 541.
10. Smolski Waldemar, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, Uniwersytet Wrocławski, Wrocław, 2015.
11. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa, 2014.
12. *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020*, Ministerstwo Cyfryzacji, Warszawa, 2016.
13. Szczepaniuk Edyta, Gawlik-Kobylińska Monika, Werner Joanna (red.), *Bezpieczny rozwój społeczeństwa informacyjnego*, ASzWoj, Warszawa, 2016.
14. *Ustawa z dnia 22 sierpnia 1997r. o ochronie osób i mienia*, Dz. U. z 2017 r., poz. 2213.
15. *Ustawa z dnia* 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, Dz. U. z 2017, poz. 1566.

Źródła internetowe

1. http://nt.interia.pl/raporty/raport-wojna-przyszlosci/lotnictwo/news-f-35-z bronia cybernetyczna,nId,1703373.
2. https://en.wikipedia.org/wiki/Counterelectronics_High_Power_Microwave_Advanced_Missile_Project.
3. https://en.wikipedia.org/wiki/Great_Firewall,http://large.stanford.edu/courses/2015/ph241/holloway1/.

IT SECURITY AS THE BASIS FOR THE FUNCTIONING OF A CONTEMPORARY COUNTRY

The paper presents issues concerning the development of IT system security, ensuring the confidentiality, integrity and availability of information in modern communication systems on the strategic level. The discussion includes implications of the malfunctioning of critical infrastructure and the wide use of modern cyber weapons, which can be observed not only on the military battlefield but also in many contemporary activities. The author analyses and classifies threats in cyberspace including electronic

crimes and terrorist acts, and finally shows developments in improving cybersecurity of a modern country.

Keywords: cybersecurity, critical infrastructure, cyber weapons, cybercrime, cyber terrorism, cybersecurity strategy