# BEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ W ŚWIETLE NOWYCH ZAGROŻEŃ

**Ryszard Radziejewski**

Wojskowa Akademia Techniczna

**Streszczenie.** W artykule przedstawiono akty prawne regulujące ochronę infrastruktury krytycznej, a także obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa w świetle nowych zagrożeń dla infrastruktury, zwłaszcza terroryzmu i cyberterroryzmu.

Bezpieczeństwo jest jedną z najważniejszych potrzeb człowieka, w piramidzie Maslowa wymienianą za potrzebami fizjologicznymi, a przed potrzebą afiliacji, szacunku i samorealizacji. Nic dziwnego, że od zarania dziejów człowiek stara się zapewnić je sobie na wszelkie sposoby, dbając o nie samemu lub powierzając to innym, w tym państwu. To państwo opracowuje stosowne akty prawne, na mocy których tworzy wyspecjalizowane instytucje (wojsko, policja, wymiar sprawiedliwości), a tam, gdzie „majestat" państwa jest niekoniecznie potrzebny (lub nie warto go narażać na szwank – vide działalność amerykańskiej firmy Blackwater w Iraku czy Afganistanie), scedowuje to także na komercyjne firmy ochrony osób i mienia. Czy te instytucje, a zwłaszcza firmy komercyjne, są dziś w stanie sprostać zagrożeniom dla bezpieczeństwa narodowego?

We współczesnym rozumieniu bezpieczeństwa narodowego przyjmuje się, że zagrożeniem dla niego będzie „…taki splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w którym z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju wewnętrznego bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych – w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej itp."[1] Wydawać by się mogło, że dziś żadna z tych form przemocy nam nie zagraża, jednak czy takim „splotem zdarzeń", który powinien budzić niepokój o bezpieczeństwo, nie jest nasz aktywny udział w światowej wojnie z terroryzmem? Warto zwrócić uwagę, że wśród wielu cech zagrożeń „bezwzględnie dominującą cechą charakterystyczną zagrożenia bezpieczeństwa

[1] S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, Akademia Obrony Narodowej, Warszawa 1994, s. 61.

globalnego, międzynarodowego i narodowego jest **zagrożenie terrorystyczne**" i, na co rzadko zwraca się uwagę, „**stan organizacji bezpieczeństwa narodowego i międzynarodowego**"[2].

Tym dwóm zagrożeniom należy poświęcić szczególną uwagę, bowiem w świadomości społecznej zagrożenie terroryzmem jest postrzegane jako umiarkowane, o czym „…świadczy też fakt, iż zdecydowana większość respondentów (72%) deklaruje, że osobiście nie obawia się ataków terrorystycznych. Obawy w tym zakresie deklaruje jedna czwarta badanych (25%), przy czym jedynie co szesnasty (6%) twierdzi, że bardzo się obawia takich ataków"[3]. Natomiast organizację bezpieczeństwa narodowego postrzegamy przez pryzmat naszej przynależności do NATO i Unii Europejskiej, co jest wielkim błędem. Sama przynależność do tych organizacji nie wystarczy, ponieważ – jak to ujął J. Nowak-Jeziorański – „Powszechnym, przyjętym kryterium bezpieczeństwa jest własny potencjał obronny połączony z układami sojuszniczymi, zapewniającymi skuteczne odstraszanie potencjalnego napastnika"[4].

Tak więc „Oczekiwanie albo liczenie na to, że bezpieczeństwo będzie efektem jednorazowego działania (np. założenia instalacji alarmowej, wygrania wojny itp.) (także przystąpienia do NATO i UE – przypis autora), darem losu, szczęścia czy Boga (Fryderyk II Wielki – Pan Bóg jest po stronie silniejszych batalionów), jest nie tylko błędne, ale wręcz samobójcze"[5]. Zwłaszcza że „Przechodząc do doświadczeń Polski w zakresie współdziałania z innymi państwami w tworzeniu bezpieczeństwa narodowego, a ściślej do doświadczeń z «liczenia» na gwarancje i pomoc innych państw lub opierania swego bezpieczeństwa na sojusznikach można stwierdzić, iż Polska ma w tym zakresie doświadczenia bogate, ale – niestety – wszystkie katastrofalne"[6].

Czy te „katastrofalne" doświadczenia czegoś nas nauczyły? Czy w sytuacji realnego zagrożenia tegoż bezpieczeństwa nie okazałoby się, że – jak zwykle – mądry Polak po szkodzie? Niestety, analizując rodzaje współczesnych zagrożeń oraz „stan organizacji bezpieczeństwa narodowego" (to nie współczesne zagrożenie, to stan chroniczny naszej „dbałości", lub raczej jej braku, o bezpieczeństwo), można powiedzieć, że nie uczymy się na błędach. Jednym z przykładów jest „Ogromna liczba przepisów, czyli inflacja prawa, to wciąż pierwsza z głównych bolączek polskiej legislacji. Drugą jest jej jakość. Jedna wynika z drugiej, a obie układają się w błędne koło: przepisy są złe, więc się je szybko i często «poprawia», efektem są kolejne

---

2 *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, red. nauk. R. Jakubczak, J. Flis, Bellona, Warszawa 2006, s. 103 i 106.

3 *Rola instytucji rządowych i samorządowych w zakresie informowania obywateli o zagrożeniach terrorystycznych*, komunikat z badań BS/163/2010, CBOS, grudzień 2010.

4 J. Nowak-Jeziorański, *Polska z bliska*, Kraków 2003, s. 127.

5 *Obrona Narodowa w tworzeniu bezpieczeństwa III RP. Podręcznik dla studentek i studentów*, red. nauk. R. Jakubczak, Dom Wydawniczy Bellona, Warszawa 2004, s. 60.

6 *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, op. cit., s. 69.

wadliwe regulacje i tak dalej. Do tego dochodzi złudne przeświadczenie rządzących, iż uchwalenie przepisu rozwiązuje problem"[7].

Można odnieść wrażenie, że stało się tak w przypadku ochrony obiektów „wrażliwych", niezmiernie ważnych dla bezpiecznego funkcjonowania państwa i obronności: mamy trzy akty prawne, które – wydane na przestrzeni dziesięciu lat – odnoszą się bez mała do tych samych obszarów i obiektów, nie regulując w sposób kompleksowy ich ochrony oraz nie uwzględniając zmian, jakie zaszły w tym czasie w sferze bezpieczeństwa. Pierwszy z nich, wydany w 1997 r., to ustawa o ochronie osób i mienia, w której określono **obiekty podlegające obowiązkowej ochronie**, zdefiniowane jako obszary, obiekty i urządzenia ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa, chronione przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne[8]. Drugi to rozporządzenie Rady Ministrów z 24 czerwca 2003 r.[9], określające **obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa**, ich kategorie, a także zadania w zakresie ich szczególnej ochrony oraz właściwości organów w tych sprawach. Trzecim aktem jest ustawa o zarządzaniu kryzysowym, w której zdefiniowano **infrastrukturę krytyczną** 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 organów administracji publicznej, a także instytucji i przedsiębiorców"[10].

Jeśli porównamy terminy: „obiekty podlegające obowiązkowej ochronie", „obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa" oraz „infrastruktura krytyczna", to bez trudu zauważymy, że dotyczą one prawie tych samych obszarów, obiektów niezmiernie ważnych dla funkcjonowania państwa i tym samym wymagających szczególnej ochrony! Co więcej, wykazy tych obiektów (ich kwalifikowanie) sporządzane są przez **te same naczelne organy administracji państwowej**!

Zasadne jest zatem pytanie: po co wydawano kolejne akty prawne, skoro dotyczą one tej samej kategorii obiektów? Zdaniem autora i w wielkim uproszczeniu można by powiedzieć, że w 1997 r. (wprowadzenie ustawy o ochronie osób i mienia), w czasie wielkich przemian ustrojowych oraz rosnącej przestępczości pospolitej i zorganizowanej, chciano uregulować ochronę masowo powstających firm prywatnych, a także urzędów państwowych, firm państwowych właśnie przed zagrożeniami ze strony świata przestępczego. W roku 2003 dostrzeżono, że „obiekty podlegające

---

7 I. Walencik, *Parlament i rząd tworzą coraz więcej złego prawa*, „Rzeczpospolita" z 17 stycznia 2011 r.

8 Ustawa o ochronie osób i mienia z 22 sierpnia 1997 r., DzU nr 114 z 1997 r., poz. 740.

9 Rozporządzenie Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, DzU nr 116 z 2003 r., poz. 1090.

10 Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 r., DzU nr 89 z 2007 r., poz. 590.

obowiązkowej ochronie" nie będą dostatecznie chronione na wypadek zagrożenia bezpieczeństwa państwa oraz wojny i dlatego wydano rozporządzenie Rady Ministrów, bowiem: „Zasadnicza różnica pomiędzy szczególną ochroną a obowiązkową polega na tym, że pierwsza prowadzona jest na wypadek zagrożenia bezpieczeństwa państwa i wojny, zaś obowiązkowa ochrona prowadzona jest w czasie pokoju"[11]. Natomiast ustawa o zarządzaniu kryzysowym to efekt dostosowywania naszego ustawodawstwa do wymogów unijnych – także w sferze bezpieczeństwa. Mamy więc klasyczny przykład wspomnianego złego stanowienia prawa oraz traktowania problematyki bezpieczeństwa państwa jako „resortowych królestw" (tego określenia użył, jako szef Biura Bezpieczeństwa Narodowego, Władysław Stasiak w odniesieniu do sfery bezpieczeństwa narodowego[12]), pomimo że wymaga ono kompleksowego traktowania i zaangażowania wszystkich resortów za nie odpowiedzialnych.

W efekcie należy zadać sobie pytanie, zwłaszcza w kontekście nowego rodzaju zagrożeń: **jak te obiekty są chronione?** Aby odpowiedzieć, trzeba przeanalizować definicje ochrony zawarte w tych aktach prawnych.

W ustawie o zarządzaniu kryzysowym ochronę określono jako „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie". Natomiast w ustawie o ochronie osób i mienia „ochrona mienia – działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do wstępu osób nieuprawnionych na teren chroniony".

W wielkim uproszczeniu można więc powiedzieć, że w pierwszej ustawie istotą ochrony jest zapewnienie ciągłości funkcjonowania infrastruktury poprzez zabiegi organizacyjno-techniczne, w tej drugiej – najzwyklejsza, „klasyczna" ochrona rozumiana jako: zabezpieczenie, opieka, osłona przed zniszczeniem, szkodą, skrzywdzeniem, niebezpieczeństwem; straż mająca na celu utrzymanie porządku, czuwania nad czyimś bezpieczeństwem; ochrona osobista, prezydenta, rządu; ochrona osób i mienia[13]. Realizowana przy pomocy osób i technicznych (elektronicznych i mechanicznych) środków ochrony. O takiej ochronie w ustawie o zarządzaniu kryzysowym i rozporządzeniach do niej nie ma mowy, podobnie jak w dyrektywach unijnych dotyczących ochrony infrastruktury krytycznej (jednak w „starych" państwach unijnych „klasyczna" ochrona ma nie tylko długą tradycję, ale i wypracowane oraz

[11] Z. Solejko, *Teoretyczne i praktyczne problemy ochrony infrastruktury krytycznej*, (w:) *Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, dydaktyki i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007, s. 281.

[12] A. Walentek, *Zbierać i analizować informacje*, „Życie Warszawy" z 26 sierpnia 2006 r.

[13] *Słownik języka polskiego*, Państwowe Wydawnictwo Naukowe, Warszawa 1979, t. 2, s. 437.

przestrzegane procedury – oni mogą sobie na to pozwolić). Pominięcie jej w naszej ustawie jest – zdaniem autora – błędem, chociaż trudno sobie wyobrazić, aby te obiekty, nawet jeśli nie są obiektami podlegającymi szczególnej ochronie, nie byłyby chronione przy pomocy środków technicznych i fizycznych (w rozumieniu „klasycznej" ochrony).

Natomiast w rozporządzeniu Rady Ministrów określono, iż szczególna ochrona obiektów polega na jej przygotowaniu i prowadzeniu. Przygotowanie szczególnej ochrony obiektów obejmuje prace koncepcyjne, planistyczne, organizacyjne, logistyczne, techniczne, szkoleniowe i kontrolne, zaś prowadzenie szczególnej ochrony obiektów obejmuje, między innymi: bezpośrednią ochronę fizyczną obiektów i ich zabezpieczenie techniczne; **działania obronne**, obejmujące w szczególności rozbudowę inżynieryjną terenu na podejściach i wewnątrz bronionego obiektu, system ognia broni palnej, powszechną obronę przeciwlotniczą oraz ochronę przed skażeniami. Szczególna ochrona obiektów jest prowadzona przez specjalnie tworzone w tym celu **jednostki zmilitaryzowane**, z udziałem Sił Zbrojnych Rzeczypospolitej Polskiej, Policji, Państwowej Straży Pożarnej i formacji obrony cywilnej.

Faktem jednak jest, że „obiekty jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych", a więc także jednostki wojskowe, chronią (oprócz pododdziałów ochrony i obrony oraz Oddziałów Wart Cywilnych) komercyjne firmy ochrony (co w dobie profesjonalizacji armii wydaje się rzeczą naturalną). Chronią one także „obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji publicznej lub przez niego nadzorowanych" (cytaty z rozporządzenia Rady Ministrów), bo większość z nich jest już chroniona jako obiekty podlegające obowiązkowej ochronie, a MSWiA nie ma stosownych sił i środków do ich ochrony. Zwłaszcza że udział Policji w szczególnej ochronie obiektów sprowadza się do… współdziałania, wymiany informacji, prewencyjnego zabezpieczenia, prowadzenia działań operacyjno-rozpoznawczych oraz użycia uzbrojonych oddziałów lub pododdziałów… w przypadku bezpośredniego zagrożenia obiektu lub dokonania ataku na obiekt podlegający szczególnej ochronie[14].

Można więc zaryzykować twierdzenie, że **większość obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz infrastruktury krytycznej (podobne jak te podlegające obowiązkowej ochronie) będzie/jest chroniona przez podmioty ochrony komercyjnej**! Czy zatem są one w stanie zapewnić im skuteczną ochronę? Zdecydowanie nie, bowiem zadania dla nich były określane w kontekście rosnącej przestępczości kryminalnej, inaczej też postrzegano zagrożenia dla obiektów podlegających obowiązkowej ochronie: „Jeszcze kilka lat temu ambasady, budynki rządowe i ministerstwa były uważane za miejsca względnie bezpieczne,

[14] Wytyczne ministra spraw wewnętrznych i administracji z 4 października 2007 r. w sprawie udziału Policji, Państwowej Straży Pożarnej i formacji obrony cywilnej w szczególnej ochronie obiektów.

a ich ochrona sprowadzała się jedynie do zabezpieczenia przed natarciem hałaśliwych demonstrantów. Również w przypadku obiektów takich jak bazy wojskowe, porty lotnicze, rafinerie podstawę systemu ochrony obwodowej stanowiły wysokie ogrodzenia i zasieki z drutu kolczastego, a dostępu do chronionej strefy bronił uzbrojony strażnik"[15]. Dziesięć lat później ustawodawca scedował na komercyjną ochronę – pośrednio, poprzez brak precyzyjnych zapisów w ustawie – także ochronę infrastruktury krytycznej. Nie dostrzegając przy tym, że zmienił się **charakter oraz istota zagrożeń** dla tego typu obiektów (w dalszej części pracy będzie używany wobec nich termin infrastruktura krytyczna) i nie zadając sobie pytania, czy do ich zwalczania, do przeciwdziałania im pracownicy ochrony są przygotowani!

## Zagrożenia aktami terroryzmu

Mówienie o nich w kontekście zagrożeń dla obiektów chronionych przez firmy komercyjne budzi zdziwienie: nam mieliby zagrażać terroryści? A i owszem, bowiem **terroryzm** to „ostentacyjne i maksymalistyczne (masowe, totalne, nieograniczone), celowe (tj. świadomie zamierzone) atakowanie niewinnych, postronnych (cywilnych) osób i dóbr publicznych (otoczenia) dla pośredniego (asymetrycznego, poprzez opinię publiczną) oddziaływania na rzeczywistego przeciwnika politycznego lub ideologicznego"[16].

Szczególną odmianą terroryzmu jest terroryzm samobójczy, w którym zamachowcami są samobójcy. „Dostarczają oni na ściśle określone miejsce i w określonym czasie ładunek wybuchowy i ginąc, zabijają przypadkowe lub wybrane osoby, niszczą określone budowle, a przede wszystkim sieją strach"[17]. Takim miejscem może być obiekt chroniony przez firmę komercyjną: „Nie rezygnując z prób dokonywania zamachów przeciw tradycyjnym celom, stopniowo zaczęły się one (organizacje terrorystyczne – przyp. aut.) koncentrować na atakowaniu obiektów słabiej lub w ogóle niechronionych, tzw. celów miękkich, do których zaliczają się m.in. hotele, szpitale, sklepy, bazary, mniej znane osobistości, urzędnicy niższego szczebla, turyści, odosobnione posterunki wojskowe i policyjne itp."[18] **Większość tych miękkich celów chronią właśnie komercyjne firmy ochrony**!

**Czy my w ogóle jesteśmy zagrożeni atakami terrorystycznymi?** Pytanie raczej retoryczne: bierzemy udział w światowej wojnie z terroryzmem, jesteśmy zaangażowani w wojnę w Afganistanie (wcześniej byliśmy w Iraku), a w związanych z tym licznych wypowiedziach przywódców różnego rodzaju odłamów komórek

[15] B. Kędzia, *Zabezpieczenia w dobie terroryzmu*, „Zabezpieczenia", nr 3 z 2007 r.

[16] S. Koziej, *Terroryzm międzynarodowy*, (w:) *Współczesny wymiar terroryzmu. Przeciwdziałanie zjawisku*, red. nauk. J. Gryz, R. Kwećka, Akademia Obrony Narodowej, Warszawa 2007, s. 13.

[17] M. Zimny, *Terroryzm samobójczy*, Bellona, Warszawa 2006, s. 8.

[18] J. Adamski, *Nowe technologie w służbie terrorystów*, Wydawnictwo TRIO, Warszawa 2007, s. 56.

terrorystycznych Polska jest wymieniana jako potencjalny cel ataku. I nie należy tych wypowiedzi lekceważyć: „Po 11 września 2001 roku terroryści udowodnili, że mogą uderzyć w dowolnym miejscu świata i że każdy kraj może być zagrożony. Ofiarami ich ataków mogą więc być zarówno wielkie mocarstwa, jak i niewielkie i neutralne państwa"[19]. Nie możemy też wykluczyć działań terrorystycznych rodzimych naśladowców lub ze strony grup przestępczych.

## Zagrożenia cyberterroryzmem

Odmianą terroryzmu jest **cyberterroryzm**, definiowany w rządowym programie ochrony cyberprzestrzeni RP na lata 2009-2011 jako „terroryzm wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym, stanowi kluczową i stale rosnącą postać ataków terrorystycznych"[20]. Coraz częściej padają też stwierdzenia, że w najbliższych latach każdy konflikt, nie tylko zbrojny, będzie zaczynał się od cyberataku, w którym widzi się sposób na uzyskanie przewagi nad zaatakowanym poprzez sparaliżowanie jego systemów rozpoznania i dowodzenia.

Przykładem mogą być trwające od lat próby zablokowania przez Stany Zjednoczone i Izrael irańskich badań nad bronią atomową: na drodze poczynań dyplomatycznych, poprzez blokady ekonomiczne, aż po niedwuznaczne groźby ataków militarnych. Z tymi poczynaniami zbiegły się ataki w cyberprzestrzeni: „Działanie wirusa komputerowego «Stuxnet», który zaszkodził programowi atomowemu Iranu, było przez dwa lata testowane w izraelskim laboratorium nuklearnym Dimona przez Izraelczyków i Amerykanów – napisał „New York Times"[21]. Z jakim skutkiem przebiegały te działania? „**Według najnowszych doniesień, robak Stuxnet nieustannie próbował zarazić pięć centr przemysłowych w Iranie w ciągu dziesięciu miesięcy. Najprawdopodobniej on był przyczyną infekcji irańskiego centrum wzbogacania uranu.** Według badań formy Symantec, atak przeprowadzono w trzech falach. Jego przebieg udało się prześledzić dzięki bazie danych Stuxneta, która przechowuje informacje o każdym zainfekowanym komputerze. Dzięki tym informacjom, twórcy Stuxneta wiedzą, czy odnieśli sukces"[22].

To niejedyne formy zagrożenia ze strony cyberprzestrzeni: „Niewykluczone, że w przyszłości staniemy się świadkami cybersabotażu na wielką skalę. Celem takiego typu ataków mogą stać się fabryki lub elektrownie – mówi Mikko Hypponen, szef

---

19 I. Jankowska, *Współczesny terroryzm – największe zagrożenie bezpieczeństwa człowieka*, (w:) *Zarządzanie bezpieczeństwem w Unii Europejskiej wobec globalnych zagrożeń*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów 2008, s. 90.

20 Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia.

21 *Kto wpuścił wirusa Irańczykom*, „Gazeta Wyborcza" z 17 stycznia 2011 r.

22 http://technowinki.onet.pl/wiadomosci/robak-stuxnet-precyzyjnie-wymierzony-w-przemysl-ir,1,4173483,artykul.html

laboratorium F-Secure, komentujący elektroniczny atak na elektrownię w Iranie (robak Stuxnet). – Na celowniku sabotażystów mogą się znaleźć systemy bankowe lub transportowe. Sparaliżowanie obrotu walutowego lub komunikacji z technicznego punktu widzenia jest prostsze niż atak na obiekt przemysłowy"[23]. Co więcej „…Stuxnet nie zagraża domowym komputerom, został specjalnie stworzony do ataków na systemy obsługujące fabryki. Już teraz można go pobrać za darmo z Internetu. – Zarówno grupy terrorystyczne, jak i państwa mogą nie tylko kopiować mechanizm działania Stuxneta, ale też go modyfikować, dostosowując do swoich celów – podkreśla Hypponen"[24]. I nie należy mieć złudzeń, że zarówno jedni, jak i drudzy nie pracują nad tym.

Jak na dłoni widać więc, że wszelkie obiekty infrastruktury krytycznej są zagrożone, a atak przy pomocy robaka Stuxnet „…stanowi przełom, pokazuje, że wkroczyliśmy do całkowicie nowego świata: o ile w przeszłości mieliśmy do czynienia zaledwie z cyberprzestępcami, obawiam się, że teraz nadszedł czas cyberterroryzmu, cyberbroni i cyberwojen" – powiedział Jewgienij Kasperski, współzałożyciel i dyrektor generalny Kaspersky Lab[25]. Ta ocena sytuacji jest ze wszech miar uzasadniona: „Cyberprzestępcy pokazali bowiem, że są w stanie przejąć kontrolę nad infrastrukturą krytyczną wybranego państwa – nawet nad elektrownią atomową. (…) Wykrycie Stuxneta należy potraktować jako znak ostrzegawczy, a zarazem wytyczenie kierunku, w jakim zmierzamy – cyberterroryzm nabiera realnych kształtów[26].

**Czy jesteśmy zagrożeni cyberatakami?** Przedstawione fakty chyba nie pozostawiają wątpliwości: „Z danych HP wynika, że ponad połowa firm z USA i jedna trzecia przedsiębiorstw europejskich już doświadczyła cyberataku. Znakomita większość (86-88 proc.) menedżerów tych firm potwierdza, że tego typu włamania są trudne do wykrycia, a skutki są długotrwałe"[27]. I nic nie wskazuje na to, aby w przyszłości miało być lepiej: „Akty terroryzmu, sabotaż, wykradanie prywatnych informacji o internautach, włamania do komórek – tak w opinii ekspertów od bezpieczeństwa sieciowego będzie wyglądał przyszły rok (2011 – przypis autora). Jednocześnie ostrzegają: użytkownicy są lekkomyślni i nie chronią swoich danych. Podobnie działają firmy, mimo że trzy czwarte z nich spodziewa się ataku na swoje serwery – wynika z globalnego badania Pokemon Institute dla firmy HP"[28]. Czym taka lekkomyślność może się skończyć?

„Komisja Europejska nakazała wczoraj wieczorem zawieszenie do 26 stycznia handlu emisjami $CO_2$ w Unii Europejskiej z powodu wykrycia cyberataków, których

[23] P. Kościelniak, *Idzie cyberepidemia*, „Rzeczpospolita" z 21 grudnia 2010 r.
[24] Ibidem.
[25] http://tech.wp.pl/kat,1009785,title,Poczatek-nowej-ery-cyberwojen,wid,12698822,wiadomosc.html
[26] http://tech.wp.pl/kat,1009779,title,Czy-rok-2011-bedzie-bezpieczny,wid,12984236,wiadomosc.html
[27] P. Kościelniak, *Idzie cyberepidemia*, op. cit.
[28] Ibidem.

ofiarą padły krajowe rejestry emisji dwutlenków węgla. Trwające kilka dni ataki hakerów wymierzone były w krajowe rejestry emisji dwutlenku węgla należące do Austrii, Grecji, Czech, Polski oraz Estonii. Hakerom udało się złamać zabezpieczenia rejestrów i wykraść uprawnienia do emisji, które natychmiast zostały sprzedane – podała wczoraj wieczorem KE. Uprawnienia do emisji wykradzione Czechom mają wartość 7 mln euro"[29].

Straty materialne to najmniej „bolesny" skutek cyberataków. Zniszczenie lub uszkodzenie infrastruktury krytycznej może spowodować osłabienie potencjału militarnego państwa, wywołać katastrofę ekologiczną, zagrozić sprawnemu funkcjonowaniu administracji rządowej i samorządowej. Może przynieść śmierć i kalectwo ludziom i tego należy się najbardziej obawiać. Może ktoś jednak zauważyć, że ochrona systemów teleinformatycznych nie należy do ustawowych obowiązków komercyjnych firm ochrony. Tak, ale po pierwsze, firma ochrony też może być narażona na takie ataki, po drugie – nie powinno być jej obojętne, jak ochraniany klient dba o bezpieczeństwo teleinformatyczne, bo skutki jego zaniedbań mogą uderzyć i w firmę ochrony. Tak więc wiedza na temat zagrożeń cyberatakami jest niezbędna również (a może przede wszystkim) i w firmach ochrony.

## Jak zapewnić infrastrukturze krytycznej bezpieczeństwo?

Aby odpowiedzieć na to pytanie, należy sobie uświadomić, że bezpieczeństwo infrastruktury krytycznej – zdaniem autora – należy rozpatrywać w kilku aspektach:

- bezpieczeństwo w rozumieniu klasycznej ochrony, realizowanej w głównej mierze przez komercyjne firmy ochrony;
- bezpieczeństwo w aspekcie ciągłości jej funkcjonowania i możliwości odtwarzania na wypadek jej uszkodzenia lub zniszczenia, czyli zabiegów organizacyjno-technicznych;
- bezpieczeństwo teleinformatyczne.

**Bezpieczeństwo w rozumieniu klasycznej ochrony** to pytanie o skuteczność działania komercyjnych firm ochrony. W Polsce firmy te są sytuowane jakby na obrzeżach bezpieczeństwa, traktowane „z przymrużeniem oka", lekceważone przez „mundurowe" formacje (chociaż roi się w niej od byłych „mundurowych", którzy de facto branżę tworzyli). Ta postawa, przejawiająca się w niedocenianiu roli firm ochrony w systemie bezpieczeństwa państwa, ukształtowała się w czasach tworzenia ustawy o ochronie osób i mienia i trwa do dziś, pomimo że zatrudniają one około 200 tys. osób (wobec 110 tys. policjantów!) i chronią około 4 tys. (dane szacunkowe) obiektów klasyfikowanych w ustawie o ochronie osób i mienia jako obiekty wymagające szczególnej ochrony!

[29] *Cyberataki na polskie rejestry emisji $CO_2$*, „Gazeta Wyborcza" z 2 stycznia 2011 r.

Chociażby z tego względu należy poddać wnikliwej ocenie ich skuteczność działania, a ta pozostawia wiele do życzenia, i to nie z winy tych firm! Powstawały one bowiem na przełomie transformacji ustrojowej, a zamysłem ustawodawcy, jak wspomniano, było uregulowanie ochrony firm sektora prywatnego i państwowego przed kryminalnymi zagrożeniami ze strony świata przestępczego. I tylko w takie uprawnienia je wyposażono oraz w adekwatne (nie zawsze) do tego środki. Trudno dziś oczekiwać, aby stawiły czoła współczesnym zagrożeniom, zwłaszcza że podlegają prawom rynku: „Firmy wycinają się w pień podczas przetargów na ochronę urzędów państwowych (zapewniają one trzecią część dochodów branży ochroniarskiej). – Ostatnio systematycznie wygrywają oferty dumpingowe, po 7-8 zł razem z dodatkami za godzinę pracy ochroniarza (a powinna 17,50 netto, przypis autora – www.piooim.pl) – denerwuje się Wagner"[30]. I dalej będą to czyniły, bo tam są „pewne" pieniądze, a trudno oczekiwać za takie stawki skutecznej ochrony.

Ponadto do rzadkości należą firmy, w których systematycznie szkoli się pracowników i inwestuje w nich. Trudno się dziwić przedsiębiorcom, bo to kosztuje (a nie jest obowiązkowe); trudno się dziwić klientowi firmy ochrony, że chciałby być chroniony przez profesjonalistów; dziwi jednak, że oczekuje tego, płacąc za ochronę marne grosze. W efekcie na około 200 tys. pracowników ochrony „Najwyżej 20% pracowników agencji ochrony ma naprawdę porządne kwalifikacje – mówi Janusz Raczyński, przedstawiciel organizacji International Bodyguard Association w Polsce"[31]. Nie może być inaczej, bowiem szkolenie pracowników ochrony kończy się na uzyskaniu licencji, a i z jej uzyskaniem były i są problemy: „Najwięcej problemów sprawiają zagadnienia praktyczne. Wydaje się, że firmy prowadzące kursy zbyt małą wagę przywiązują do samoobrony, technik interwencji i strzelań. Bo jeśli egzamin teoretyczny zdaje 90%, a z tej liczby tylko 50% praktyczny, to o czymś to świadczy"[32]. Nie lepiej było 10 lat później: „Nie mam prawa ani tytułu wyciągać wniosków o poziomie całej populacji pracowników ochrony na podstawie obserwacji 112 egzaminowanych osób, ale z tego, co widziałam, jest raczej źle. Gorzej, bo część tych osób (a znam je osobiście z kursów, na których prowadziłam zajęcia) jest w trakcie, albo ukończyła różne szkoły na poziomie licencjatu. (…) W sumie, w dniach 22-24 września 2009 r. w komendzie stołecznej policji do egzaminu przystąpiło 112 osób, z których egzamin zaliczyło 25, co stanowi 22%"[33].

Za taki stan rzeczy trudno winić tylko firmy ochrony komercyjnej, więcej winy leży po stronie ustawodawcy: można odnieść wrażenie, że tworząc ustawę o zarządzaniu kryzysowym, chciał tylko dostosować się (w sferze legislacyjnej) do unijnych

30 R. Omachel, W. Surmacz, *Zarobić na strachu*, „Newsweek" z 9 sierpnia 2009 r.

31 Ibidem.

32 R. Radziejewski, *Pierwszy w „Stołecznej"*, „BOS – Bezpieczeństwo – Ochrona – Systemy", nr 4/1999.

33 D. Godlewska, A. Korus, *Egzamin dla osób ubiegających się o licencję pracownika ochrony fizycznej okiem Polskiego Związku Pracodawców*, „Ochrona Mienia i Informacji", nr 6/2009.

wymogów ochrony infrastruktury krytycznej, nie kusząc się o analizę dotychczasowych form i środków ochrony takich obiektów.

**Bezpieczeństwo infrastruktury krytycznej w aspekcie ciągłości jej funkcjonowania i możliwości odtwarzania** na wypadek uszkodzenia lub zniszczenia możemy rozpatrywać poprzez pryzmat istoty działania Unii Europejskiej oraz definicji infrastruktury krytycznej, bowiem brakuje nam doświadczeń w tej dziedzinie – jesteśmy na etapie tworzenia Narodowego Programu Ochrony Infrastruktury Krytycznej, a proces kwalifikowania obszarów, obiektów dopiero się zaczyna. W tej sytuacji wskazane by było, aby Rządowe Centrum Bezpieczeństwa jasno określiło, co kryje się pod określeniem „wszelkie działania" zawartym w definicji, a następnie – wzorem Komendy Głównej Policji w odniesieniu do planów ochrony obiektów podlegających obowiązkowej ochronie – opracowało metodykę uzgadniania planów ochrony. Dziś możemy wnioskować, iż te wszelkie działania odnoszą się do zabiegów organizacyjno-technicznych zapewniających prawidłowe funkcjonowanie infrastruktury w każdych warunkach.

**Bezpieczeństwem teleinformatycznym w** obiektach (obszarach) zaliczanych do infrastruktury krytycznej zajmują się (w większym lub mniejszym stopniu) różnie nazywane i sytuowane w strukturach firm komórki bezpieczeństwa. Z punktu widzenia ustawodawcy błędem jest niewyartykułowanie ochrony „systemów łączności i sieci teleinformatycznych" (składnik infrastruktury krytycznej wymieniony w ustawie o zarządzaniu kryzysowym w art. 3), w przeciwieństwie do Komisji Unii Europejskiej, która w sprawie krytycznej infrastruktury informatycznej (ang. *critical information infrastructures*, CII) wydała komunikat, podkreślając w nim, iż „Ataki cybernetyczne osiągnęły bezprecedensowy poziom zaawansowania. Zwykłe eksperymenty stają się teraz wyspecjalizowanymi działaniami, które prowadzi się dla zysku lub z powodów politycznych. Niedawne, zakrojone na szeroką skalę ataki cybernetyczne na Estonię, Litwę i Gruzję to najszerzej opisywane przykłady ilustrujące bardziej ogólną tendencję. Duża liczba wirusów, robaków i innych rodzajów złośliwego oprogramowania, coraz częstsze występowanie botnetów i ciągły wzrost ilości spamu potwierdzają skalę tego problemu. Wysoki stopień zależności od CII, ich transgraniczne powiązania oraz współzależności z innymi infrastrukturami, a także ich słabe punkty i grożące im niebezpieczeństwa sprawiają, że konieczne jest podjęcie kwestii ich bezpieczeństwa i odporności w ujęciu systemowym, uznając je za pierwszą linię obrony w przypadku awarii i ataków"[34].

Polska nie jest „zieloną wyspą", której nie zagrażają podobne działania: „Ostatnio w CERT.GOV.PL mają pełne ręce roboty. Wrześniowy cyberatak nie był bowiem

[34] Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej *Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności*, KOM(2009) 149 wersja ostateczna.

pierwszym. W ciągu tego roku zespół udaremnił ataki na komputery pracowników administracji publicznej. Polegały one na rozsyłaniu pocztą elektroniczną złośliwego oprogramowania, które służyło do zbierania informacji, w tym transferowania poza instytucję dokumentów znalezionych na dyskach twardych lub zasobach sieciowych. Najgorzej było jednak w 2008 roku – komputery i oficjalne witryny polskich urzędów stały się celem około 500 tysięcy ataków cybernetycznych"[35].

W naszym przypadku o skuteczności przeciwdziałania cyberterroryzmowi będą decydowały „…jasne procedury postępowania, odpowiednio skonstruowane struktury organizacji odpowiedzialne za przeciwdziałanie tym zagrożeniom, dobrze przygotowani ludzie oraz odpowiednie narzędzia informatyczne"[36]. A ponadto: „Kluczem do sukcesu są ludzie. Każdy system lub podsystem powinien być zabezpieczony przez profesjonalnie przygotowany zespół administratorów, w tym kilku dysponujących wiedzą na poziomie eksperckim (odpowiedni certyfikat). Administratorzy powinni być systematycznie szkoleni na kursach krajowych i zagranicznych. Niedouczony administrator może poczynić większe szkody w systemie teleinformatycznym niż cyberterrorysta"[37].

* * *

Ochrona obszarów i obiektów, które mają istotny wpływ na bezpieczeństwo militarne i ekonomiczne państwa, powinna być „oczkiem w głowie" władzy ustawodawczej i wykonawczej. Niestety, tej problematyce poświęcają oni wiele uwagi tylko wtedy, gdy stan naszej infrastruktury krytycznej zostanie „przetestowany" na przykład przez siły natury w postaci nocnych opadów mokrego śniegu, które spowodowały uszkodzenia m.in. dwóch linii energetycznych zasilających Szczecin: „Zimne kaloryfery, kran, z którego pociekło tylko kilka kropli, głuchy telefon, milczące telewizor i radio – tak dla ponad 300 tysięcy ludzi rozpoczął się wtorkowy poranek" (…) „Wygasły ekrany bankomatów. Większość sklepów zamknięto, choć wyjątkowo fiskus zezwolił na sprzedaż bez działających kas fiskalnych"[38]. „Przez cały dzień miasto wyglądało jak opuszczone. Mały ruch, martwe światła sygnalizacyjne. Sporo policji i żandarmerii"[39]. A co by było, gdyby poziom ochrony infrastruktury krytycznej zechcieli „przetestować" na przykład terroryści?

Lepiej nie myśleć, warto za to skupić się na uporządkowaniu sytuacji prawnej ochrony infrastruktury krytycznej, która wymaga kompleksowego podejścia, sprecyzowania i uwzględnienia wszystkich jej aspektów, potraktować bezpieczeństwo jako priorytet i zagwarantować na nie pieniądze, bo bez nich możemy mówić tylko o iluzji bezpieczeństwa. Sytuacja gospodarcza kraju nie sprzyja poruszaniu wątku

35 K. Głowacki, *Straż wirtualna*, „Polska Zbrojna" z 8 listopada 2009 r.
36 W. Nowak, *Siecioobrona*, „Polska Zbrojna" z 16 sierpnia 2009 r.
37 Ibidem.
38 M. Stankiewicz, *Gwałtowny atak zimy sparaliżował Szczecin*, „Rzeczpospolita" z 9 kwietnia 2009 r.
39 A. Kraśnicki, *Szczecin przeżył ciemność*, „Gazeta Wyborcza" z 9 kwietnia 2009 r.

finansowego, ale powinniśmy na ten problem patrzeć z innej perspektywy – nie ile trzeba wydać na zbudowanie sprawnego systemu ochrony infrastruktury krytycznej, ale ile stracimy, gdy na skutek zaniedbań zostanie ona uszkodzona lub zniszczona: „Przed zarządem firmy kwestie bezpieczeństwa muszą być prezentowane w kategoriach rozsądnych wydatków w stosunku do kosztów, które mogą stać się następstwem niepodjęcia żadnych działań. W naszych czasach trzeba mówić o nich jako inwestycjach, pokazując ich wpływ na wzrost wyników"[40].

Taki punkt widzenia problemu powinien dotrzeć do świadomości nie tylko polityków i decydentów rządowych, ale także do właścicieli (operatorów) infrastruktury krytycznej, osób odpowiedzialnych za bezpieczeństwo tych obiektów – mamy zbyt wiele do stracenia, aby dalej udawać, że ten stan rzeczy może trwać dalej. Nie powinniśmy też liczyć na innych: „Polska może liczyć na pomoc sojuszników tylko wtedy, jeśli będzie chciała i mogła bronić się sama, jeśli zdobędzie własne możliwości odstraszania napastnika"[41].

Marnym pocieszeniem jest fakt, że nie tylko my mamy problem z ochroną infrastruktury krytycznej: „Trwającą od lat dyskusję w politycznych kuluarach Bonn, a później Berlina, na temat obecności militarnej USA w Europie, spotęgował niedawny raport Amerykańskiej Federacji Naukowców (FAS). Oceniono w nim, że broń atomowa, przechowywana przez USA w bazach europejskich sojuszników, jest niedostatecznie zabezpieczona, począwszy od zdezelowanych płotów, oświetlenia i «niestabilnych zabudowań», na kiepskim systemie alarmowym i niedostatecznie wyszkolonej załodze skończywszy"[42].

BIBLIOGRAFIA

1. J. Adamski, *Nowe technologie w służbie terrorystów*, Wydawnictwo TRIO, Warszawa 2007, s. 56.
2. *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, red. nauk. R. Jakubczak, J. Flis, Bellona, Warszawa 2006, s. 103 i 106.
3. *Cyberataki na polskie rejestry emisji $CO_2$*, „Gazeta Wyborcza" z 2 stycznia 2011 r.
4. P. Cywiński, *Amerykanie do domu!*, „Wprost" z 20 lipca 2008 r.
5. S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, Akademia Obrony Narodowej, Warszawa 1994, s. 61.
6. K. Głowacki, *Straż wirtualna*, „Polska Zbrojna" z 8 listopada 2009 r.
7. D. Godlewska, A. Korus, *Egzamin dla osób ubiegających się o licencję pracownika ochrony fizycznej okiem Polskiego Związku Pracodawców OCHRONA*, „Ochrona Mienia i Informacji", nr 6/2009.

40 http://www.securitystandard.pl/artykuly/51263/Nieuniknione.trzy.pytania.html.
41 J. Nowak-Jeziorański, *Polska wczoraj, dziś i jutro*, Warszawa 1999, s. 246.
42 P. Cywiński, *Amerykanie do domu!*, „Wprost" z 20 lipca 2008 r.

8. I. Jankowska, *Współczesny terroryzm – największe zagrożenie bezpieczeństwa człowieka*, (w:) *Zarządzanie bezpieczeństwem w Unii Europejskiej wobec globalnych zagrożeń*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów 2008, s. 90.
9. B. Kędzia, *Zabezpieczenia w dobie terroryzmu*, „Zabezpieczenia", nr 3 z 2007 r.
10. Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej *Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności*, KOM(2009) 149, wersja ostateczna.
11. P. Kościelniak, *Idzie cyberepidemia*, „Rzeczpospolita" z 21 grudnia 2010 r.
12. S. Koziej, *Terroryzm międzynarodowy*, (w:) *Współczesny wymiar terroryzmu. Przeciwdziałanie zjawisku*, red. nauk. J. Gryz, R. Kwećka, Akademia Obrony Narodowej, Warszawa 2007, s. 13.
13. A. Kraśnicki, *Szczecin przeżył ciemność*, „Gazeta Wyborcza" z 9 kwietnia 2009 r., *Kto wpuścił wirusa Irańczykom*, „Gazeta Wyborcza" z 17 stycznia 2011 r.
14. W. Nowak, *Siecioobrona*, „Polska Zbrojna" z 16 sierpnia 2009 r.
15. J. Nowak-Jeziorański, *Polska wczoraj, dziś i jutro*, Warszawa 1999, s. 246.
16. J. Nowak-Jeziorański, *Polska z bliska*, Kraków 2003, s. 127.
17. R. Omachel, W. Surmacz, *Zarobić na strachu*, „Newsweek" z 9 sierpnia 2009 r.
18. R. Radziejewski, *Pierwszy w „Stołecznej"*, BOS Bezpieczeństwo–Ochrona–Systemy", nr 4/1999.
19. *Rola instytucji rządowych i samorządowych w zakresie informowania obywateli o zagrożeniach terrorystycznych*, komunikat z badań BS/163/2010, CBOS, grudzień 2010.
20. *Obrona Narodowa w tworzeniu bezpieczeństwa III RP. Podręcznik dla studentek i studentów*, redakcja naukowa R. Jakubczak, Dom Wydawniczy Bellona, Warszawa 2004, s. 60.
21. Rozporządzenie Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, DzU nr 116 z 2003 r., poz. 1090.
22. Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia.
23. Z. Sobejko, *Teoretyczne i praktyczne problemy ochrony infrastruktury krytycznej*, (w:) *Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, dydaktyki i praktyki*, redakcja B. Kosowski, A. Włodarski, Warszawa 2007, s. 281.
24. *Słownik języka polskiego*, Państwowe Wydawnictwo Naukowe, Warszawa 1979, t. 2, s. 437.
25. M. Stankiewicz, *Gwałtowny atak zimy sparaliżował Szczecin*, „Rzeczpospolita" z 9 kwietnia 2009 r.
26. Ustawa o ochronie osób i mienia z 22 sierpnia 1997 r., DzU nr 114 z 1997 r., poz. 740.
27. Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 r., DzU nr 89 z 2007 r., poz. 590.
28. I. Walencik, *Parlament i rząd tworzą coraz więcej złego prawa*, „Rzeczpospolita" z 17 stycznia 2011 r.
29. A. Walentek, *Zbierać i analizować informacje*, „Życie Warszawy" z 26 sierpnia 2006 r.

30. Wytyczne ministra spraw wewnętrznych i administracji z 4 października 2007 r. w sprawie udziału Policji, Państwowej Straży Pożarnej i formacji obrony cywilnej w szczególnej ochronie obiektów.
31. M. Zimny, *Terroryzm samobójczy*, Bellona, Warszawa 2006, s. 8.

**Abstract.** The article presents the legislation, regulating protection of the high value infrastructure and facilities particularly important for the security and defense of the state – facing the new threats for the infrastructure, especially by a terrorism and cyberterrorism.