PROBLEMY MECHATRONIKI
UZBROJENIE, LOTNICTWO, INŻYNIERIA BEZPIECZEŃSTWA

ISSN 2081-5891

5, 4 (18), 2014, 71-82

Analiza możliwości zapewnienia ochrony infrastruktury krytycznej przez operatorów

Ryszard RADZIEJEWSKI

Wojskowa Akademia Techniczna
ul. gen. S. Kaliskiego 2, 00-908 Warszawa
e-mail: ryszard.radziejewski@wat.edu.pl

Artykuł wpłynął do redakcji 30.07.2014. Zweryfikowaną wersję po recenzji otrzymano 14.08.2014

DOI: 10.5604/20815891.1138368

Streszczenie. W artykule dokonano analizy istoty ochrony infrastruktury krytycznej, rodzajów jej ochrony oraz możliwości ich realizacji przez operatorów tejże infrastruktury. Przedstawiono także refleksje i wnioski autora na temat miejsca i roli administracji publicznej w ochronie infrastruktury krytycznej, mające na celu poprawę jej ochrony.
Słowa kluczowe: bezpieczeństwo, infrastruktura krytyczna, ochrona fizyczna, ochrona teleinformatyczna, ochrona osobowa, ochrona techniczna, ochrona prawna, plany odtwarzania

Jeśli jesteś w stanie utrzymać wszystkie ważne strategicznie punkty na swoich drogach, możesz nie obawiać się, że wróg wkroczy.
Sun Tzu [1]

1. WSTĘP

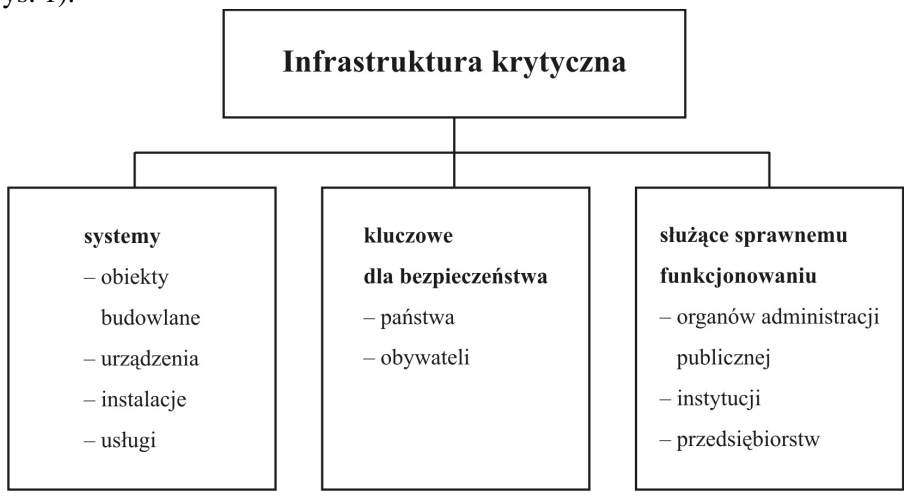
Chociaż od opublikowania traktatu [1] wybitnego chińskiego stratega na temat sztuki prowadzenia wojny upłynęły wieki, przedstawione w nim zasady nie straciły na aktualności. Są one nie tylko często cytowane współcześnie w odniesieniu do działań zbrojnych, lecz także wnikliwie analizowane i „przekładane" na konkretne sytuacje w różnych dziedzinach naszej działalności, w tym również szeroko rozumianego bezpieczeństwa narodowego. Bezpieczeństwa, które jest (a raczej być powinno) „najwyższą wartością, potrzebą narodową i priorytetowym celem działalności państwa, jednostek i grup społecznych, a jednocześnie procesem obejmującym różnorodne środki, gwarantujące trwały, wolny od zakłóceń byt i rozwój narodowy (państwa), w tym ochronę i obronę państwa jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w wartości podlegające szczególnej ochronie" [2].

Tej szczególnej ochronie podlegają także „wszystkie szczególnie ważne strategiczne punkty na drogach", które dziś – zdaniem autora – są niczym innym niż obiektami infrastruktury: **militarnej** (obronnej), **bezpieczeństwa** oraz **infrastruktury krytycznej**. Czy jest możliwe, biorąc pod uwagę nie tylko aktualny potencjał obronny naszego państwa, lecz także współczesne środki rażenia, „utrzymanie" takich strategicznie ważnych punktów w sposób gwarantujący odstraszenie potencjalnego napastnika? Odpowiedź brzmi: nie, zwłaszcza przy naszym ambiwalentnym stosunku do bezpieczeństwa narodowego [3] oraz przesadnej wierze w sojusze (sama przynależność do tych organizacji nie wystarczy, bowiem – jak ujął to J. Nowak-Jeziorański: „Polska może liczyć na pomoc sojuszników tylko wtedy, jeśli będzie chciała i mogła bronić się sama, jeśli zdobędzie własne możliwości odstraszania napastnika" [4]). Dlatego w ochronie tych strategicznie ważnych punktów powinna być zastosowana **filozofia ochrony infrastruktury krytycznej**, czyli należy dążyć do zachowania ciągłości jej działania przez tworzenie warunków do szybkiego odtwarzania na wypadek uszkodzenia lub zniszczenia.

2. ISTOTA OCHRONY INFRASTRUKTURY KRYTYCZNEJ

Infrastruktura krytyczna to „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców" [5]. Pomijając pytanie, czy o sprawne funkcjonowanie przedsiębiorców (sic!) powinniśmy się martwić, czy raczej o ich przedsiębiorstwa, **istotą** infrastruktury krytycznej można określić **środki materialne** (obiekty budowlane, urządzenia, instalacje)

oraz **usługi** kluczowe dla **bezpieczeństwa**, służące **sprawnemu funkcjonowaniu** administracji publicznej, a także instytucji i przedsiębiorstw (rys. 1).



Rys. 1. Graficzne przedstawienie definicji infrastruktury krytycznej (opracowanie własne)

Fig. 1. Graphical representation of the definition of critical infrastructure (own work)

Można więc stwierdzić, że wyznacznikiem infrastruktury krytycznej jest **bezpieczeństwo** i **sprawne funkcjonowanie**. Jak zatem w tym kontekście postrzegać jej **ochronę**, czyli „wszelkie działania zmierzające do zapewnienia **funkcjonalności** (funkcjonalny – dobrze spełniający swoją rolę [6]), **ciągłości działań** (ciągłość działania «business continuity» – strategiczna i taktyczna zdolność organizacji do przewidywania i reagowania na incydenty i zakłócenia w prowadzonej działalności w celu jej kontynuowania na akceptowalnym, zdefiniowanym poziomie [7]) i **integralności** (integralny – stanowiący całość [8]) 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" [9]?

Analizując tak sformułowaną definicję, proces budowania ochrony infrastruktury krytycznej można podzielić na cztery fazy: **zapobiegania**, a więc podejmowania wszelkich działań w odniesieniu do **środków materialnych** (obiektów budowlanych, urządzeń, instalacji), aby **zachować ciągłość świadczenia usług** (procesów zachodzących w organizacji) przez **odtwarzanie infrastruktury** (środków materialnych i usług), jeśli ta zostanie uszkodzona lub zniszczona.

W kontekście definicji infrastruktury krytycznej i jej ochrony rodzą się następujące pytania:

- O czyje bezpieczeństwo (także w odniesieniu do pewnych elementów o czyje funkcjonowanie) przede wszystkim chodzi: obywateli, instytucji, przedsiębiorstw czy państwa?
- Czy istotą systemów są one same jako środki materialne, czy też procesy w nich zachodzące, których efektem są usługi, produkty itp.? Czy istotą jest elektrownia, czy wytwarzany w niej prąd?

Prąd (tak jak wiele innych produktów, usług itp.) trafia bezpośrednio do obywatela, zaspokajając nie tylko jego potrzebę bezpieczeństwa, ale i wiele innych, ładnie ujętych w piramidzie potrzeb Masłowa. Trafia, bo to jednak państwo przez swoje struktury organizacyjne i właściwe ich funkcjonowanie zapewnia należyte działanie infrastruktury (zwłaszcza tej krytycznej) – wytwórcy i dostarczyciela wielu produktów, usług itp. Ale nie powstaną one i nie będą świadczone bez sprawnej i działającej w sposób ciągły infrastruktury. Powinna ona zatem być chroniona, a **istotą ochrony powinno być zachowanie ciągłości świadczenia usług oraz procesów zachodzących w niej – w infrastrukturze krytycznej**! Taka konstatacja jest ważna, z niej bowiem wynikają istotne pytania, jak rozłożyć akcenty, jaką przyjąć strategię działania w celu zapewnienia ochrony? Czy większy nacisk położyć na zapobieganie (a więc na „wszelkie działania"), czy na odtwarzanie? Powszechne jest przekonanie, że łatwiej jest zapobiegać niż leczyć, vide: chronić niż odtwarzać. Biorąc jednak pod uwagę rodzaje zagrożeń dla infrastruktury krytycznej oraz niewielkie możliwości przeciwdziałania im (zwłaszcza przez operatora infrastruktury), zasadniczy nacisk, zdaniem autora, należałoby położyć na zdolności do jej odtwarzania. Niemniej obowiązkiem operatora infrastruktury krytycznej jest jej ochrona, a jej rodzaje zostały określone przez ustawodawcę w „Narodowym programie ochrony infrastruktury krytycznej" (NPOIK).

3. WSZELKIE DZIAŁANIA – „CO AUTOR MIAŁ NA MYŚLI"?

Ustawodawca w definicji ochrony infrastruktury krytycznej nie określił, na czym to zapobieganie, czyli „wszelkie działania" polegają, chociaż były one już wcześniej sygnalizowane w ustawie z 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa. W niej to określono, że „pełnomocnik do spraw ochrony infrastruktury krytycznej sporządza dla zarządu spółki oraz rady nadzorczej raport o stanie ochrony infrastruktury krytycznej". Raport powinien zawierać informacje dotyczące ochrony infrastruktury krytycznej w zakresie:

1) ochrony fizycznej;
2) ochrony technicznej;
3) ochrony prawnej;
4) ochrony osobowej;

5) ochrony teleinformatycznej;
6) planów odbudowy i przywracania infrastruktury krytycznej do funkcjonowania" [10].

Uczynił to dopiero w 2013 r. w „Narodowym programie ochrony infrastruktury krytycznej", definiując „wszelkie działania" jako **rodzaje ochrony**, na którą składają się:

„1) ochrona fizyczna – zespół przedsięwzięć minimalizujących ryzyko zakłócenia funkcjonowania infrastruktury krytycznej (IK) przez osoby, które znalazły się na terenie IK w sposób nieautoryzowany. Ochrona fizyczna obejmuje ochronę osób, rozumianą jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej, ochronę mienia, czyli 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, a także techniczne środki ochrony, czyli wykorzystanie w ochronie obiektów płotów, barier, systemów telewizji przemysłowej, systemów dostępowych itp. środków;

2) ochrona techniczna – zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z technicznymi aspektami budowy i eksploatacji obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej. Ochrona techniczna IK obejmuje:

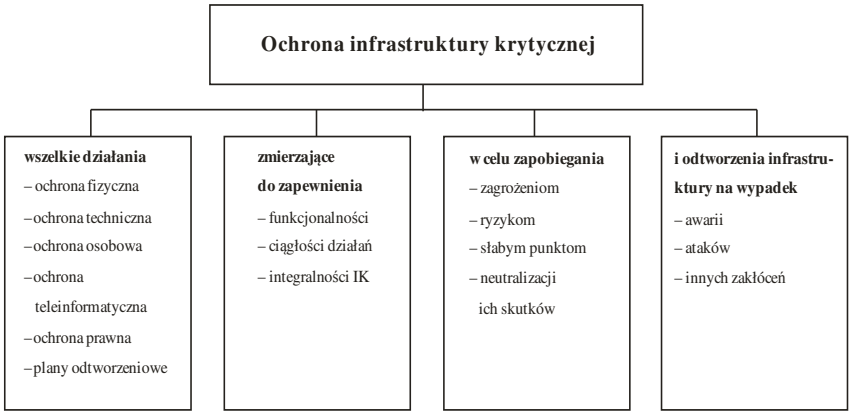
– kwestie związane ze zgodnością budynków, urządzeń, instalacji i usług z obowiązującymi przepisami i normami, np. budowlanymi, przeciwpożarowymi itp.;
– działania techniczne mające na celu zmniejszenie uzależnienia funkcjonowania IK od zewnętrznych usług;
– działania techniczne mające na celu zapewnienie ciągłości funkcjonowania IK;

3) ochrona osobowa – zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które poprzez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej mogą spowodować zakłócenia w jej funkcjonowaniu. Ochronę tę należy zatem powiązać z pracownikami oraz innymi osobami czasowo przebywającymi w obrębie IK (usługodawcy, dostawcy, goście);

4) ochrona teleinformatyczna – zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych. Oznacza to również ochronę przed cyberatakami, cyberprzestępstwami i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom;

5) ochrona prawna – zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z działalnością osób fizycznych lub przedsiębiorców (prywatnych krajowych lub zagranicznych), których działania mogą prowadzić do zakłócenia funkcjonowania obiektów, urządzeń, instalacji i usług IK. Oznacza to zastosowanie narzędzi prawnych niedopuszczających, poprzez możliwość kontroli i ewentualnego blokowania lub ograniczania decyzji zarządów, do np. wrogiego przejęcia, fuzji czy też sprzedaży niektórych elementów infrastruktury, których efektem mogą być zakłócenia w jej funkcjonowaniu;
6) plany odtwarzania, rozumianego jako odtwarzanie funkcji realizowanych przez IK" [11].

Wymienione rodzaje ochrony infrastruktury krytycznej zostały scharakteryzowane w załączniku 2 do NPOIK „Standardy służące sprawnemu funkcjonowaniu infrastruktury krytycznej – dobre praktyki i rekomendacje". Ochronę infrastruktury krytycznej w ustawowym brzmieniu można więc przedstawić graficznie (rys. 2).



Rys. 2. Graficzne przedstawienie definicji ochrony infrastruktury krytycznej (opracowanie własne)

Fig. 2. Graphical representation of the definition of critical infrastructure protection (own work)

Na podstawie analizy „wszelkich działań", czyli wymienionych rodzajów ochrony, można zadać dwa zasadnicze pytania:

1) Dlaczego ochronę fizyczną i techniczną zdefiniowano inaczej, niż jest to przyjęte w środowisku komercyjnej ochrony osób i mienia, i zawarte w ustawie o ochronie osób i mienia oraz innych dokumentach (normach itp.)?
2) Dlaczego nie przeanalizowano możliwości zapewnienia poszczególnych rodzajów ochrony przez operatora?

Odpowiedź na pytanie pierwsze: zapewne „w trosce" o uporządkowanie nazewnictwa na wzór zachodni, wprowadzając jednocześnie istotne zamieszanie, w większości (?) bowiem przypadków w organizacjach zakwalifikowanych do infrastruktury krytycznej te rodzaje ochrony realizują firmy komercyjne.

W efekcie w jednej organizacji funkcjonuje różne nazewnictwo i to nie tylko w mowie, lecz także w dokumentach, zwłaszcza w planach ochrony.

Odnośnie do drugiego pytania: najprostsza wydaje się sytuacja w **ochronie fizycznej** (tej w rozumieniu NPOIK). Można nawet pokusić się o stwierdzenie, że już funkcjonuje. W uproszczeniu – celem zabezpieczeń technicznych jest wykrycie oraz powiadomienie o naruszeniu strefy chronionej, a także uniemożliwienie lub utrudnienie przeniknięcia do tej strefy agresorowi oraz jak najdłuższe jego zatrzymanie przy pokonywanych zabezpieczeniach, aby ochrona fizyczna mogła podjąć skuteczną interwencję. Zakres tej ochrony leży w gestii operatora, który musi mieć świadomość, że:

- skuteczna ochrona musi kosztować; kryterium najniższej ceny w przetargach doprowadziło do sytuacji, w której firmy ochraniane udają, że płacą, a te ochraniające – że chronią;
- celem agresora może być nie zabór mienia, lecz jego zniszczenie, dlatego newralgiczne dla funkcjonowania organizacji części infrastruktury (np. serwerownie) muszą mieć ochronę fizyczną zdolną do natychmiastowego odparcia agresora, zwłaszcza w dobie samobójczych zamachów terrorystycznych.

Taki zamach u nas? Chyba autora poniosła fantazja. Oby… Takiej możliwości, zwłaszcza w kontekście roli i znaczenia infrastruktury krytycznej dla bezpieczeństwa państwa, nie można wykluczyć. Zasadne jest więc pytanie, czy komercyjna ochrona jest w stanie przeciwstawić się terrorystom (niekoniecznie tym z Al-Kaidy, rodzimym też), zorganizowanym grupom przestępczym, zazwyczaj bardzo dobrze wyszkolonym i wyposażonym? Odpowiedź jest tylko jedna – negatywna.

Ochrona techniczna to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z technicznymi aspektami budowy i eksploatacji obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej. Oczywiste jest, że ten temat powinien się pojawić już na desce kreślarskiej, gdy obiekty są projektowane. Gorzej, gdy pod tym kątem należy dostosować już istniejącą infrastrukturę.

Wówczas nie należy zapominać, że powinna być dostosowana również do wymagań ochrony fizycznej (tej w rozumieniu NPOIK).

Ochrona osobowa to, zdaniem autora, klasyczna ochrona kontrwywiadowcza – zadanie dla wyspecjalizowanych służb państwowych, ponieważ w dyspozycji operatora pozostają tylko… wywiadownie gospodarcze i prywatni detektywi: „Prywatni detektywi śledzili menedżera gazowego giganta na zlecenie… władz spółki. Zaczęło się od anonimu o rzekomych

nadużyciach i nieobyczajności. Liczący 90 stron dokument, który powstał pod koniec 2012 r. tylko w jednym egzemplarzu, zawiera wiele tajemnic z życia […], ówczesnego wiceprezesa Polskiego Górnictwa Naftowego i Gazownictwa (PGNiG) ds. zakupów i IT, który odszedł ze spółki w grudniu 2013 r.

Został przygotowany przez agencję detektywistyczną i firmę ochroniarską. Wynika z niego, że w okresie 14-28 grudnia 2012 r. menedżer był śledzony, a auto, którym się poruszał, monitorowane za pomocą GPS. Fotografowano też z ukrycia jego i rodzinę, sprawdzano, z kim się spotyka, prześwietlano majątek. Sprawdzono również powiązania żony i dzieci. Przygotowanie raportu kosztowało PGNiG 101 tys. zł. Dlaczego państwowy gigant gazowy zapłacił prywatnym firmom za inwigilację własnego menedżera? Zaczęło się od donosu. [...] Metody zastosowane do zweryfikowania jego treści nie wzbudziły zastrzeżeń ówczesnej prezes […]. Wątpliwości mają natomiast eksperci. Ich zdaniem, sprawdzeniem członka zarządu spółki, która ma strategiczne znaczenie dla bezpieczeństwa energetycznego państwa, powinna zajmować się Agencja Bezpieczeństwa Wewnętrznego (ABW), a nie prywatni detektywi.

To niedopuszczalne, aby takie działania zlecać na zewnątrz. Mogą one spowodować wyciek informacji, a co za tym idzie – godzić w bezpieczeństwo państwa. Dotychczas nigdy nie spotkałem się z taką sytuacją – twierdzi płk Mieczysław Tarnowski, były wiceszef ABW" [12].

Czy inni operatorzy zdobędą się na takie postępowanie i koszty, nawet w sytuacjach niebudzących takich wątpliwości? Życie dowodzi, że nie mniejszym od terrorystycznego zagrożeniem dla organizacji jest… niewłaściwy dobór kadr, zwłaszcza na kierownicze stanowiska. Najlepiej to widać (abstrahując od przytoczonego cytatu) w spółkach Skarbu Państwa, w których kryterium fachowości i kompetencji bardzo często jest zastępowane zasługami dla rządzącej partii lub prywatnymi koneksjami. Chyba nie tędy droga.

Ochrona teleinformatyczna ma na celu z jednej strony minimalizowanie ryzyka zakłócenia funkcjonowania infrastruktury związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych, z drugiej – ochronę przed zagrożeniami płynącymi z cyberprzestrzeni. Biorąc pod uwagę wyrafinowanie tych zagrożeń oraz ciągłe – mimo większej świadomości użytkowników systemów teleinformatycznych – ich lekceważenie, skuteczna ochrona teleinformatyczna wymaga opracowania jednolitych i rygorystycznie przestrzeganych procedur oraz nowoczesnych metod i środków przeciwdziałania im w obrębie całego systemu ochrony infrastruktury krytycznej, zwłaszcza w sektorach tejże infrastruktury. Ponieważ tu również występuje swoisty efekt domina (jako jedna z form niszczenia infrastruktury teleinformatycznej), ochrona ta powinna być zadaniem przede wszystkim administracji państwowej, bo operator IK nie jest w stanie jej zapewnić.

Przykładem tak rozumianej **ochrony prawnej** jest wymienione wcześniej rozporządzenie ministra skarbu ustanawiające pełnomocnika do spraw ochrony

infrastruktury krytycznej w spółkach Skarbu Państwa. Czy jest to możliwe w pozostałych sektorach infrastruktury krytycznej?

A czy operatorzy tejże sami założą sobie swoisty kaganiec potencjalnie ograniczający im swobodę prowadzenia działalności gospodarczej? Równie naiwne byłoby oczekiwanie, że dyrektor Rządowego Centrum Bezpieczeństwa, głównej przecież instytucji odpowiadającej za ochronę infrastruktury krytycznej oraz koordynującej wszelkie poczynania z tym związane, będzie złotą rybką spełniającą życzenia wszystkich podmiotów systemu ochrony tejże infrastruktury. W Rzeczypospolitej Polskiej to państwo stanowi prawo i to ono musi samo sobie zapewnić bezpieczeństwo prawne.

Plany odtwarzania funkcji realizowanych przez infrastrukturę krytyczną to, zdaniem autora, nic innego, jak zapewnienie ciągłości jej działania przez prowadzenie odpowiedniej polityki bezpieczeństwa w organizacji obejmującej obszary jako żywo pokrywające się z rodzajami ochrony wymienionymi w NPOIK. Są to obszary bezpieczeństwa:

1) organizacyjnego;
2) prawnego;
3) personalnego;
4) fizycznego i technicznego (ocena istniejących i projektowanych systemów ochrony fizycznej i technicznej; projekt modyfikacji istniejących systemów; projekt nowych systemów niezbędnych do wdrożenia w dziedzinie: ochrony fizycznej osób i mienia oraz konwojowania, kontroli dostępu, sygnalizacji napadu i włamania, sygnalizacji pożaru, telewizji dozorowej, elektroniki specjalnej);
5) informacyjnego;
6) kryzysowego (inwentaryzacja zagrożeń kryzysowych; zasady zarządzania sytuacją kryzysową; plan ciągłości działania – procedury ratunkowe, odtworzeniowe i testowania; zasady i zakres działania „zespołu szybkiego reagowania”);
7) produkcyjnego (wykaz zagrożeń ze strony kontrahentów; zasady bezpiecznej współpracy z nimi; metody zwalczania nieuczciwej konkurencji; zasady ochrony tajemnic technologicznych; sposoby przeciwdziałania kradzieżom; zasady utrzymania ciągłości produkcji; procedury kontroli jakości; zasady utrzymania właściwych warunków bhp; procedury powypadkowe) [13].

4. PODSUMOWANIE

Ten swoisty bałagan w nazewnictwie i przypisywanie operatorom infrastruktury krytycznej nadmiernych obowiązków nie musi mieć aż tak negatywnego wpływu na skuteczność jej ochrony – pod warunkiem, że jej operator weźmie sobie do serca te obowiązki.

Niekiedy jednak co innego podpowiada serce, a co innego rozum, zwłaszcza gdy ustawodawca – przez niedopracowanie problematyki ochrony infrastruktury krytycznej – wyraża swój, nazwijmy to delikatnie, lekceważący stosunek do niej (o braku kompetencji aż strach pisać!), a te „niedomówienia" wyrażają się konkretnymi kwotami.

Wielce ryzykowne, chociaż na pozór słuszne, jest pozostawienie w gestii operatora infrastruktury doboru rodzajów ochrony, o czym stanowi zapis: „Zastosowanie konkretnych rodzajów ochrony powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK. W przypadku niewielkiego ryzyka nie ma konieczności stosowania wszystkich jej rodzajów" [14]. Czy to do końca prawda? Mamy zbudować elektrownię atomową. Bez wątpienia będzie zaliczona do infrastruktury krytycznej. Jak tu szacować ryzyko wystąpienia zagrożeń? Czy w tego typu obiektach nie należy zakładać wystąpienia wszelkich możliwych zagrożeń? W japońskiej elektrowni atomowej Fukushima zakładano możliwość wystąpienia trzęsienia ziemi w okolicach elektrowni, ale nie w głębi oceanu i nie tak wielkiej fali tsunami, która spowodowała niebywałą katastrofę.

Szkoda że Rządowe Centrum Bezpieczeństwa, twórca NPOIK, nie zarekomendowało Radzie Ministrów, aby w uchwale w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022" wyartykułować te „wszelkie działania" i uregulować także ochronę obiektów podlegających obowiązkowej i szczególnej ochronie, mając świadomość, że „Doświadczenie z ochrony obiektów podlegających obowiązkowej ochronie na mocy *Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* oraz podlegających ochronie szczególnej na podstawie *Rozporządzenia Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony* wykazały konieczność uzupełnienia zakresu ochrony infrastruktury krytycznej nie tylko o ochronę fizyczną, ale również o inne elementy mające zapewnić niezakłócone jej funkcjonowanie, tzn. ochronę techniczną, osobową, teleinformatyczną i prawną" [15]. Program to program, inną moc prawną i inny wydźwięk ma jednak uchwała Rady Ministrów. Tym samym można odnieść wrażenie, że infrastruktura krytyczna jest jednak niedoceniana w systemie bezpieczeństwa narodowego.

LITERATURA

[1] Sun Tzu, *Sztuka wojny. Traktat*, Wydawnictwo Helion, s. 46, Gliwice, 2012.

[2] Pawłowski J., *System kierowania bezpieczeństwem narodowym – teoria i praktyka*, [w:] *Współczesny wymiar bezpieczeństwa. Między teorią a praktyką*, s. 56, za: W. Kitler, *Rozważania nad istotą bezpieczeństwa*

narodowego jako etap wstępny ustaleń dotyczących systemu bezpieczeństwa narodowego, materiały eksperckie do prac w ramach SPBN, Akademia Obrony Narodowej, Warszawa, 2011.
[3] Radziejewski R., *Bezpieczeństwo narodowe: między teorią a praktyką refleksji kilka*, [w:] *Interdyscyplinarny wymiar bezpieczeństwa*, pod red. nauk. M. Adamkiewicza, Wojskowa Akademia Techniczna, s. 235, Warszawa, 2012.
[4] Nowak-Jeziorański J., *Polska wczoraj, dziś i jutro*, s. 246, Warszawa, 1999.
[5] *Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 r.,* Dz.U. z 2007 r., nr 89, poz. 590.
[6] *Słownik języka polskiego*, Wydawnictwo Naukowe PWN, s. 218, Warszawa, 2008.
[7] Norma brytyjska *Zarządzanie ciągłością działania,* cz. 2: *Specyfikacja*, BS 25999-2:2007.
[8] *Słownik języka polskiego*, Wydawnictwo Naukowe PWN, s. 278, Warszawa, 2008.
[9] *Ustawa z 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym*, Dz.U. nr 131, poz. 1076.
[10] *Ustawa z 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych*, Dz.U. z 2010 r., nr 65, poz. 404.
[11] *Narodowy program ochrony infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, s. 31-32, Warszawa, 2013.
[12] *Puls Biznesu*, nr 66 z 4-6 kwietnia 2014.
[13] Ruszkowski Z., *Kompleksowa polityka bezpieczeństwa*, „BOS–Bezpieczeństwo–Ochrona–Systemy", nr 3 i 4, 1999.
[14] *Narodowy program ochrony infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, s. 32, Warszawa, 2013.
[15] Uchwała nr 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia *Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*, Monitor Polski, z 16 maja 2013 r., poz. 377, s. 73.

Analysis of Options to Ensure the Protection of Critical Infrastructure by the Operators

Ryszard RADZIEJEWSKI

Abstract. The paper analyzes the essence of critical infrastructure protection, types of protection and the possibility of their implementation by the operators of such infrastructure. Also presents the author's reflections and conclusions about the place and role of government in the protection of critical infrastructure, to improve its protection.
Keywords: safety, critical infrastructure, physical protection, protection of data communications, personal protection, technical protection, legal protection, disaster recovery plans