Tomasz Szewczyk
Maciej Pyznar

Ochrona infrastruktury krytycznej a zagrożenia asymetryczne

Termin zagrożenia asymetryczne już od dłuższego czasu funkcjonuje zarówno w teorii stosunków międzynarodowych, jak i w nauce o bezpieczeństwie. Należy podkreślić, że istnieje wiele koncepcji związanych z definiowaniem powyższego terminu oraz jego klasyfikacji. Dla potrzeb tego artykułu zagrożenie asymetryczne zdefiniowane zostanie jako działanie podmiotu, przede wszystkim pozapaństwowego, który wykorzystuje niekonwencjonalne z punktu widzenia swego przeciwnika środki i techniki. Jako zagrożenia asymetryczne wyróżnić możemy m.in.: terroryzm międzynarodowy, użycie przez podmioty pozapaństwowe broni masowego rażenia oraz wrogie zastosowanie technologii informatycznych (cyberterroryzm)[1].

Ochrona infrastruktury krytycznej

W wyniku zdarzeń spowodowanych przez siły natury lub będących konsekwencją działań człowieka infrastruktura krytyczna może ulec zniszczeniu, uszkodzeniu, a jej działanie zakłóceniu, w związku z czym zagrożone może być życie i mienie. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państw.

Infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli, a jej ochrona jest jednym z priorytetów stojących przed państwem polskim. Istota zadań związanych z infrastrukturą krytyczną sprowadza się nie tylko do zapewnienia jej ochrony, ale również do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki.

Infrastruktura krytyczna oraz jej ochrona to pojęcia stosunkowo nowe. Po raz pierwszy pojawiły się w oficjalnych dokumentach państwowych w USA wraz z dyrektywą prezydenta Billa Clintona z 22 maja 1998 r. w sprawie ochrony infrastruktury krytycznej. Dyrektywa ta wskazywała na konieczność wzrostu wrażliwości Stanów Zjednoczonych na ewentualne ataki terrorystyczne, ze zwróceniem szczególnej uwagi na bezpieczeństwo infrastruktury krytycznej. Tego typu infrastrukturę zdefiniowano jako rzeczywiste i cybernetyczne systemy niezbędne do funkcjonowania gospodarki i państwa w minimalnym zakresie. Wśród tych systemów wymieniono m.in.: system telekomunikacyjny, energetyczny, transportowy, bankowy i finansowy. Co znamienne, podkreślono, iż w celu efektywnej ochrony infrastruktury krytycznej zachodzi konieczność ścisłej współpracy z sektorem prywatnym (wg danych Departamentu Bezpieczeństwa Narodowego USA, operatorami lub właścicielami około 85% infrastruktury krytycznej są podmioty prywatne) w ramach partnerstwa publiczno-prywatnego. Od tego czasu zagadnienia ochrony infrastruktury krytycznej były systematycznie rozwijane, a Amerykanie stali się światowymi liderami w tej dziedzinie.

---

[1] Definicja została zaczerpnięta z książki M. Madeja – *Zagrożenia asymetryczne bezpieczeństwa państwa obszaru transatlantyckiego,* PISM, Warszawa 2007, która w sposób kompleksowy opisuje zagadnienie, przedstawiając jego wieloaspektowość.

W polskim prawodawstwie pojęcie infrastruktury krytycznej nie było obecne. Brakowało definicji w dokumencie rangi ustawy lub rozporządzenia. Jednakże brak jednoznacznych przepisów definiujących tego typu infrastrukturę i jej ochronę nie oznaczał, że w ogóle jej nie było, lub że nie była ona chroniona.

W Polsce dostrzegano konieczność ochrony niektórych składników infrastruktury państwa. Już w 1997 r. przyjęto ustawę o ochronie osób i mienia, w której wskazano obszary, obiekty, urządzenia i środki transportu, mające znaczenie dla obronności, gospodarki, bezpieczeństwa publicznego i innych ważnych interesów państwa, które miały być obowiązkowo chronione przez specjalne, uzbrojone formacje lub odpowiednie zabezpieczenie techniczne.

W ramach ochrony obowiązkowej, kierownik jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w ewidencji albo upoważniona przez niego osoba, zobowiązany zostaje do opracowania oraz uzgodnienia z właściwym terytorialnie komendantem wojewódzkim policji planu ochrony tych obszarów, obiektów i urządzeń. Dodatkowo, w 2003 roku, przyjęto rozporządzenie Rady Ministrów w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, które regulowało sprawę ochrony tych obiektów w warunkach pozapokojowych. Natomiast podstawy do zdefiniowania i zapewnienia odpowiedniej ochrony krytycznej infrastruktury teleinformatycznej zawarto w ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Należy podkreślić, że polska administracja miała styczność z pojęciem infrastruktury krytycznej podczas uczestnictwa w pracach toczących się zarówno na forum Paktu Północnoatlantyckiego, jak i Unii Europejskiej[2)].

Można zatem wnioskować, iż dotychczasowy stan prawny zawierał przepisy dotyczące ochrony tego typu infrastruktury. Dążąc do pełniejszego jej zabezpieczenia, w ślad za innymi krajami oraz instytucjami UE, w administracji polskiej rozpoczęto prace nad stworzeniem programu, w który, poza administracją, zaangażowani byliby właściciele oraz posiadacze obiektów, instalacji lub urządzeń infrastruktury krytycznej. Konieczność stworzenia systemu ochrony tej infrastruktury wynika z dwóch powodów. Po pierwsze, rozproszone działania podejmowane przez administrację publiczną, mające na celu ochronę infrastruktury krytycznej muszą zostać poddane procesowi koordynacji. Po drugie, w działania z zakresu ochrony tej infrastruktury należy zaangażować podmioty, które nią zarządzają, poprzez intensyfikację współpracy sektora prywatnego i publicznego w tym zakresie. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno podmiotów prywatnych, jak i odpowiedzialnej za funkcjonowanie państwa administracji państwowej. Aktywny, oparty na warunkach partnerskich, udział prywatnych i państwowych właścicieli oraz posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej w tworzonym systemie pozwoli na stabilne jej funkcjonowanie.

Omawiany typ infrastruktury jest szczególnie podatny na zagrożenia. W przeszłości elementy tworzące obecną infrastrukturę krytyczną funkcjonowały jako niezależne lub jedynie w niewielkim stopniu zależne systemy. Obecnie, w dobie postępującej globalizacji i rozwoju technologicznego, poszczególne obiekty są coraz bardziej współ-

[2)] Obecnie trwa proces nowelizacji *Ustawy o zarządzaniu kryzysowym* pod kątem dostosowania polskich przepisów do *Dyrektywy z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (2008/114/WE).*

zależne nie tylko w wymiarze jednego państwa, ale i w skali regionalnej, europejskiej, a nawet światowej. Postęp, poza oczywistymi korzyściami, spowodował równoczesne zwiększenie podatności tego rodzaju obiektów na potencjalne zagrożenia. Pojawiły się nowe rodzaje niebezpieczeństw, wcześniej nie znane. W efekcie, istniejąca sieć powiązań powoduje, że uszkodzenie lub utrata części infrastruktury krytycznej w jednym systemie spowoduje straty i uszkodzenia w innych. Zależność sprawnego funkcjonowania państwa i bezpieczeństwa obywateli od kluczowych systemów i usług, a tym samym konieczność ochrony infrastruktury, wchodzącej w skład tych systemów, jest zagadnieniem szerszym i nie może opierać się wyłącznie na ochronie fizycznej obiektu. Dlatego właśnie ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3)] wprowadziła do polskiego prawodawstwa pojęcie infrastruktury krytycznej. Zgodnie z definicją zaproponowaną w tej ustawie, za infrastrukturę krytyczną uważa się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje i usługi, kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje takie systemy, jak:

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

Ochrona infrastruktury krytycznej (OIK) to zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia infrastruktury krytycznej w przypadku zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. W wyniku zeszłorocznej nowelizacji ustawy o zarządzaniu kryzysowym (art. 3 ust. 3 ustawy) definicja OIK otrzymała następujące brzmienie: [...] *wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania 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*. Zmiana definicji miała na celu dostosowanie polskiego stanu prawnego do przepisów unijnych.

W poszczególnych systemach, o których mówi ustawa, infrastruktura krytyczna zostanie wyłoniona na podstawie określonych kryteriów. Kryteria[4)] te podzielone są na dwie grupy:

1) kryteria sektorowe (systemowe), charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może

[3)] Dz. U. z 2007 r., nr 89, poz. 590 z późn. zm.

[4)] Kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, spełniające przedstawione powyżej założenia, zostały w dniu 18 grudnia 2009 r. zatwierdzone przez Dyrektora RCB. Ich wykaz został opatrzony klauzulą „zastrzeżone".

spowodować zaliczenie do elementów infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów IK;
2) kryteria przekrojowe, opisujące parametry odnoszące się do skutków zniszczenia lub zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi.

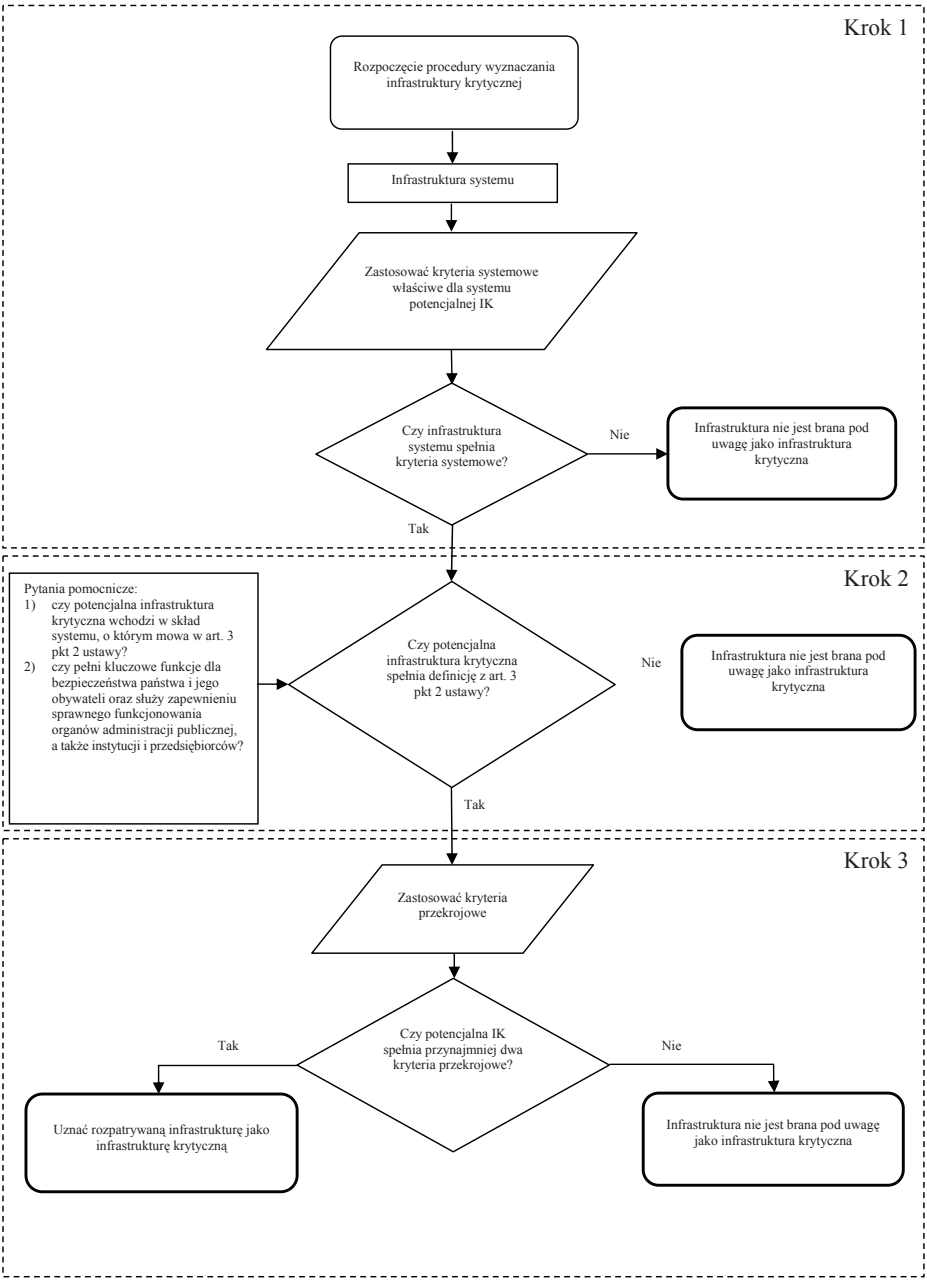
Aby obiekt, urządzenie, instalacja lub usługa mogły być zakwalifikowane jako IK, zgodnie z przyjętą metodyką muszą być zrealizowane wszystkie trzy niżej przedstawione kroki:
1) w kroku pierwszym – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK w danym systemie, do infrastruktury systemu należy zastosować kryteria sektorowe (systemowe), właściwe dla danego systemu IK;
2) w kroku drugim – w celu sprawdzenia, czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, do infrastruktury wyłonionej w drodze spełnienia pierwszego kroku należy zastosować definicję zawartą w art. 3 pkt. 2 ustawy;
3) w kroku trzecim – w celu wskazania, jakie będą skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK, do infrastruktury wyłonionej w drodze spełnienia kroku pierwszego i drugiego należy zastosować kryteria przekrojowe (należy wybrać kryteria najlepiej odzwierciedlające charakterystykę systemu), przy czym aby wypełnić krok trzeci, potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe.

Proces postępowania podczas wyznaczania infrastruktury krytycznej przedstawia algorytm na rysunku 1.

Jak przedstawiono powyżej, decydujące znaczenie dla wskazania obiektów, instalacji, urządzeń lub usług IK ma spełnienie kryteriów przekrojowych. Położenie akcentu na skutki zniszczenia lub zaprzestania funkcjonowania IK, mające bezpośredni związek z powiązaniem z sytuacją kryzysową, ma głębokie uzasadnienie w rozumieniu jej jako pełniącej kluczową funkcję dla państwa jako całości i jego obywateli.

Kryteria, o których była mowa wyżej, będą stanowić element Narodowego Programu Ochrony Infrastruktury Krytycznej[5)] i podobnie jak on będą podlegały systematycznej aktualizacji. Można będzie zatem wykorzystać mechanizm do „regulacji" kryteriów w taki sposób, aby objęły one większą lub mniejszą liczbę elementów IK. Założeniem jest, by w przyszłości, po opracowaniu narzędzi, które w miarodajny sposób pozwalałyby na ocenę skutków zniszczenia lub zaprzestania funkcjonowania IK (Rządowe Centrum Bezpieczeństwa pracuje nad ich przygotowaniem) w ogóle zrezygnować z kryteriów sektorowych (systemowych). W efekcie, kryteria przekrojowe stosowane byłyby do dowolnie wybranej infrastruktury systemu lub do jakiejkolwiek krajowej infrastruktury.

[5)] Zgodnie z art. 5 b ustawy o zarządzaniu kryzysowym na program składają się następujące elementy:
1. Narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury.
2. Wykaz ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy, o których mowa w ustawie o zarządzaniu kryzysowym.
3. Szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej.



Rys. 1 – Proces postępowania podczas wyznaczania infrastruktury krytycznej.

Jedną z kluczowych zmian wprowadzonych do ustawy o zarządzaniu kryzysowym nowelizacją z 2009 r. jest podkreślenie roli Szefa Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym, również w odniesieniu do infrastruktury krytycznej. Ograny administracji publicznej oraz posiadacze takiej infrastruktury zobowiązani zostali do przekazywania Szefowi ABW będących w ich posiadaniu informacji na temat zagrożeń terrorystycznych w stosunku do niej. Jednocześnie Szef ABW może udzielać zaleceń zagrożonym podmiotom, pomocnych w przeciwdziałaniu zagrożeniom.

Zgodnie z przyjętą przez Rządowe Centrum Bezpieczeństwa filozofią, ochronę infrastruktury krytycznej należy rozumieć jako sumę:

1) ochrony fizycznej,
2) ochrony technicznej,
3) ochrony osobowej,
4) ochrony teleinformatycznej,
5) ochrony prawnej,
6) planów odtwarzania.

W przedstawionym powyżej podziale ochrona fizyczna jest najbardziej znanym i rozpowszechnionym elementem OIK. Dotyczy jej nawet konkretna ustawa o ochronie osób i mienia. Na ochronę fizyczną składają się: ochrona osób, rozumiana jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej oraz ochrona 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. Ochrona fizyczna realizowana jest przez pracowników ochrony, którzy „fizycznie" bronią dostępu do obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej (IK). Pozostałe elementy ochrony IK nie są już tak rozpowszechnione i wymagają krótkiego wyjaśnienia.

Ochrona techniczna to zespół przedsięwzięć związanych z budową i eksploatacją obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, w tym również techniczne środki ochrony, mające na celu minimalizację ryzyka zakłócenia w funkcjonowaniu IK. Oznacza to, że techniczna ochrona infrastruktury krytycznej dotyczy nadzoru nad zgodnością konstrukcji budynków, urządzeń, instalacji i usług z obowiązującymi normami (np. budowlanymi) oraz innymi przepisami (np. przeciwpożarowymi), co ma zagwarantować bezpieczne użytkowanie IK. Jest to również wymienione w ustawie o ochronie osób i mienia zabezpieczenie techniczne obiektu, czyli wykorzystanie do ochrony obiektów płotów, barier, systemów telewizji przemysłowej, systemów dostępowych i tym podobnych środków.

Przez ochronę osobową należy rozumieć zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka będącego ewentualnym skutkiem działań pracowników oraz usługodawców, którzy poprzez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu. Oznacza to, iż właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej chronią ją, zarówno poddając weryfikacji kwalifikacje pracowników, jak i dokonując sprawdzenia, czy dana osoba gwarantuje świadczenie pracy na wymaganym poziomie (także uczciwości) Tego typu weryfikacja to najczęściej kontakt z byłym pracodawcą lub wysłanie zapytania do rejestru skazanych. Następnie proces weryfikacji i obserwacji pracownika jest kontynuowany. Podobne sprawdzenie powinno dotyczyć również pracowników firm świadczących usługi na rzecz operatora IK.

Zależność infrastruktury krytycznej od informatycznych narzędzi zarządzania i kierowania nie ulega wątpliwości. Dlatego istotnym elementem jej ochrony jest ochrona teleinformatyczna. Przez ochronę teleinformatyczną należy rozumieć zespół przedsięwzięć i ich procedur mających na celu minimalizację zakłóceń w funkcjonowaniu IK związanych z wykorzystaniem do użytkowania tego typu infrastruktury systemów i sieci teleinformatycznych. Oznacza to ochronę przed atakami hakerskimi i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom[6)].

Ochrona prawna jest pojęciem nowym, związanym z kształtem współczesnej gospodarki rynkowej, w której pojawiają się zagrożenia ze strony innych podmiotów gospodarczych państwowych lub prywatnych, których działania mogą prowadzić do zakłócenia funkcjonowania IK. Stąd też przez ochronę prawną infrastruktury krytycznej należy rozumieć zespół przedsięwzięć, mających na celu minimalizację ryzyka związanego z działalnością innych podmiotów gospodarczych, państwowych lub prywatnych, których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług IK. Mamy tu na myśli zastosowanie narzędzi prawnych (ustaw) niedopuszczających, poprzez możliwość kontroli i ewentualnego blokowania lub ograniczania decyzji zarządów, do np. wrogiego przejęcia, fuzji czy też sprzedaży niektórych elementów infrastruktury, której efektem mogą być zakłócenia jej w funkcjonowaniu.

Podsumowanie

Jak widać, powyższa koncepcja ochrony zaproponowana przez RCB jest kompleksowa i ukierunkowana na przeciwdziałanie wszelkim rodzajom zagrożeń, w tym zagrożeniom asymetrycznym. W tym obszarze, oprócz ochrony fizycznej, szczególnie istotne znaczenie ma ochrona osobowa i teleinformatyczna.

ABSTRACT

The aim of the article is to describe undertaken by the polish administration in the sphere of critical infrastructure protection, which are targeted At creating a comprehensive critical infrastructure protection system of the most important elements of the national infrastructure. The above mentioned actions ensure proper functioning of the state and enterprises in case of asymmetric threats. They require a coordinated interaction between the central and local governments, but also with the private sector.

[6)] Należy podkreślić, iż obecnie trwają prace nad przygotowaniem Rządowego Programu Ochrony Cyberprzetrzeni, który przedstawi kompleksowe działania polskiego rządu w tym obszarze.