ĆWICZENIE DO WYKONANIA

Każdy zespół wybiera jeden z następujących problemów:

Wariant A: długotrwały blackout obejmujący znaczną część kraju.

Wariant B: kryzys migracyjny połączony z intensywną dezinformacją.

Etap I. Identyfikacja zagrożeń

Odpowiedz na pytania:

1. Jakie mogą być przyczyny wystąpienia zagrożenia?
2. Jakie elementy bezpieczeństwa państwa są najbardziej narażone?
3. Jakie instytucje powinny uczestniczyć w przeciwdziałaniu zagrożeniu?
4. Jakie czynniki mogą spowodować gwałtowne pogorszenie sytuacji?

Etap II. Opracowanie scenariuszy

Należy przygotować cztery możliwe scenariusze rozwoju sytuacji:

1. **Scenariusz korzystny** – zagrożenie zostaje szybko opanowane.

2. **Scenariusz umiarkowany** – zagrożenie powoduje ograniczone zakłócenia.

3. **Scenariusz niekorzystny** – zagrożenie powoduje poważne problemy w funkcjonowaniu państwa.

4. **Scenariusz ekstremalny** – następuje gwałtowne narastanie powiązanych zagrożeń i znaczne ograniczenie możliwości działania państwa.

Podział ten stanowi autorską formę ćwiczenia wykorzystującego zalecane przez Lamentowicza wielowariantowe myślenie o przyszłości.

Etap III. Projektowanie działań strategicznych

Dla każdego scenariusza należy wskazać:

- działania zapobiegawcze;
- działania przygotowawcze;
- działania podejmowane w sytuacji wystąpienia zagrożenia;
- sposób monitorowania sytuacji;
- warunki wymagające zmiany przyjętej strategii.

Etap IV. Wczesne ostrzeganie

Należy zaproponować pięć sygnałów ostrzegawczych mogących świadczyć o narastaniu zagrożenia.

Określić, które instytucje mogłyby monitorować poszczególne sygnały oraz w jaki sposób uzyskane informacje powinny wpływać na decyzje władz państwowych.

Pytania podsumowujące

1. Czy państwo może przygotować się na zagrożenie, którego przebiegu nie potrafi dokładnie przewidzieć?
2. Jakie znaczenie ma wielowariantowe planowanie strategiczne?
3. Dlaczego rozpoznawanie słabych sygnałów zagrożenia jest istotnym elementem bezpieczeństwa państwa?
4. Czy skuteczne prognozowanie może całkowicie wyeliminować ryzyko?
5. Dlaczego elastyczność strategii jest równie ważna jak jej wcześniejsze przygotowanie?

OPRACOWANIE KONCEPCJI PRZYGOTOWANIA PAŃSTWA NA ZAGROŻENIE O TRUDNYM DO PRZEWIDZENIA PRZEBIEGU

1. Podstawy teoretyczne opracowania

W. Lamentowicz w pracy „Granice strategii państwa. Efekt Tsunami” wskazuje, że współczesne państwo funkcjonuje w środowisku charakteryzującym się rosnącą złożonością, nieprzewidywalnością oraz coraz większą dynamiką zmian.

Bezpieczeństwo nie powinno być rozumiane wyłącznie jako stan braku zagrożeń, ale również jako rezultat wzajemnego oddziaływania zagrożeń i reakcji podejmowanych przez poszczególne podmioty. Autor zwraca szczególną uwagę na bezpieczeństwo człowieka, które powinno stanowić punkt odniesienia dla działań instytucji państwowych.

W kontekście analizowanych zagrożeń istotne znaczenie mają trzy podstawowe funkcje państwa wyróżnione przez Lamentowicza:

1. Funkcja adaptacyjna – dostosowywanie sposobu działania państwa do zmieniających się warunków i pojawiających się zagrożeń.

2. Funkcja regulacyjna – oddziaływanie na przebieg procesów społecznych, gospodarczych i politycznych w celu ograniczania ich negatywnych konsekwencji.

3. Funkcja innowacyjna – tworzenie nowych rozwiązań organizacyjnych, prawnych i instytucjonalnych, które zwiększają zdolność państwa do reagowania na przyszłe zagrożenia.

Lamentowicz podkreśla również niebezpieczeństwo wystąpienia Efektu Tsunami, rozumianego jako skrajna niemoc strategiczna, wynikająca z nałożenia się całkowitej nieprzewidywalności, niesterowności procesów oraz niezdolności elit do opracowania i realizacji skutecznych strategii.

W analizowanych przypadkach państwo powinno zatem przygotowywać się nie tylko na pojedyncze zagrożenia, ale również na możliwość wystąpienia ich wzajemnych powiązań i narastających konsekwencji.

WARIANT A

DŁUGOTRWAŁY BLACKOUT OBEJMUJĄCY ZNACZNĄ CZĘŚĆ KRAJU • ETAP I. IDENTYFIKACJA ZAGROŻEŃ

1. Jakie mogą być przyczyny wystąpienia zagrożenia?

Długotrwała awaria systemu elektroenergetycznego może być następstwem zarówno pojedynczego zdarzenia, jak i nałożenia się kilku niekorzystnych czynników.

Potencjalne przyczyny:

1. Awarie techniczne – uszkodzenia linii przesyłowych, stacji elektroenergetycznych, transformatorów lub elementów automatyki zabezpieczeniowej.

2. Ekstremalne zjawiska atmosferyczne – huragany, intensywne opady, powodzie i inne katastrofy naturalne powodujące rozległe uszkodzenia infrastruktury.

3. Cyberataki lub sabotaż – celowe zakłócanie działania systemów sterowania infrastrukturą energetyczną.

Potencjalne przyczyny – dalsze czynniki

4. Niekorzystne warunki pracy systemu elektroenergetycznego – poważne zakłócenia równowagi pomiędzy produkcją a zapotrzebowaniem na energię, połączone z ograniczoną zdolnością systemu do kompensowania zakłóceń.

5. Efekt kaskadowy – sytuacja, w której awaria jednego elementu systemu powoduje przeciążenia i kolejne awarie, doprowadzając do utraty zasilania na coraz większym obszarze.

Ostatnia z wymienionych przyczyn szczególnie dobrze ilustruje przedstawiony przez mechanizm narastania niekontrolowanych procesów.
Autor wskazuje, że niewielka zmiana może wywołać nieproporcjonalnie duże konsekwencje, a nakładanie się efektów kaskadowych, sieciowych i złożoności może prowadzić do narastającej destabilizacji całego systemu.

2. Jakie elementy bezpieczeństwa państwa są najbardziej narażone?

Obszar bezpieczeństwa	Możliwe konsekwencje długotrwałego blackoutu
Bezpieczeństwo energetyczne	Utrata możliwości zasilania odbiorców i ograniczenie funkcjonowania infrastruktury krytycznej.
Bezpieczeństwo społeczne	Pogorszenie warunków życia, wzrost niepewności, strachu i ryzyka wystąpienia paniki.
Bezpieczeństwo zdrowotne	Zakłócenia pracy szpitali, placówek medycznych i systemów ratownictwa.

Elementy bezpieczeństwa państwa (ciąg dalszy)

Obszar bezpieczeństwa	Możliwe konsekwencje długotrwałego blackoutu
Bezpieczeństwo ekonomiczne	Wstrzymanie produkcji, zakłócenia handlu, transportu i funkcjonowania przedsiębiorstw, problemy w dostępie do środków znajdujących się na kontach bankowych.
Bezpieczeństwo informacyjne	Awarie telekomunikacji, ograniczenie dostępu do informacji i możliwość rozpowszechniania dezinformacji.
Bezpieczeństwo publiczne	Utrudnienia w działaniach służb, awarie systemów alarmowych i wzrost ryzyka naruszeń porządku publicznego.
Bezpieczeństwo państwa jako systemu organizacyjnego	Ograniczenie zdolności administracji publicznej do koordynowania działań i podejmowania decyzji.

Najważniejszym zagrożeniem nie jest sam brak energii elektrycznej, ale możliwość utraty zdolności funkcjonowania przez kolejne, wzajemnie zależne systemy państwa.

Przykładowo:

Ciąg wydarzeń – mechanizm narastania kryzysu



1 Awaria energetyczna

- przerwy w dostawach energii elektrycznej,
- wyłączenie części infrastruktury krytycznej,
- awarie systemów zasilania rezerwowego.



2 Zakłócenia telekomunikacyjne

- przerwy w działaniu sieci komórkowych,
- niedostępność internetu,
- zakłócenia w łączności służbowej,
- ograniczony dostęp do informacji.



3 Ograniczenie koordynacji służb ratowniczych

- utrudniony kontakt między służbami,
- problemy z przekazywaniem danych o zdarzeniach,
- ograniczona możliwość współdziałania i planowania działań.



4 Utrudnienia w dostarczaniu pomocy

- utrudnienia w transporcie,
- opóźnienia w dostawach żywności, wody, paliw i leków,
- problemy z dotarciem służb na miejsce zdarzeń,
- ograniczona dostępność usług medycznych i ratunkowych.



5 Narastanie niepewności społecznej

- brak rzetelnych informacji,
- rozpowszechnianie dezinformacji,
- wzrost obaw o dostępność podstawowych potrzeb,
- panika i niepokoje społeczne,
- spadek zaufania do instytucji państwowych.



6 Zwiększenie skali kryzysu

- rozprzestrzenianie się zakłóceń na kolejne regiony,
- pogłębianie problemów gospodarczych i społecznych,
- ograniczenie zdolności funkcjonowania państwa,
- ryzyko wystąpienia dalszych, wzajemnie powiązanych zagrożeń.

NARASTANIE SKALI ZAGROŻENIA

3. Jakie instytucje powinny uczestniczyć w przeciwdziałaniu zagrożeniu?

Instytucje odpowiedzialne za bezpieczeństwo energetyczne:

- Polskie Sieci Elektroenergetyczne – monitorowanie pracy systemu przesyłowego i działania związane z przywracaniem jego stabilności.

- Operatorzy systemów dystrybucyjnych – usuwanie awarii i przywracanie zasilania odbiorcom.

- Właściwe organy administracji rządowej odpowiedzialne za energetykę – koordynacja działań na poziomie polityki państwa.

Instytucje odpowiedzialne za zarządzanie kryzysowe:

- Rządowe Centrum Bezpieczeństwa.

- Wojewodowie i wojewódzkie centra zarządzania kryzysowego.

- Starostowie, wójtowie, burmistrzowie i prezydenci miast.

- Państwowa Straż Pożarna i Policja.

- Służby medyczne i Państwowe Ratownictwo Medyczne.

- Siły Zbrojne RP – w zakresie wsparcia udzielanego zgodnie z właściwymi procedurami.

Podmioty wspierające:

Operatorzy telekomunikacyjni, przedsiębiorstwa wodociągowe, firmy transportowe, przedsiębiorstwa paliwowe, szpitale oraz organizacje społeczne i humanitarne.

Najważniejsze znaczenie ma stworzenie skutecznego mechanizmu współpracy wszystkich wymienionych podmiotów, ponieważ żadna instytucja nie będzie w stanie samodzielnie opanować wielowymiarowego kryzysu.

4. Jakie czynniki mogą spowodować gwałtowne pogorszenie sytuacji?

Do najważniejszych czynników należą:

1. Rozprzestrzenianie się awarii na kolejne obszary kraju.
2. Wyczerpanie zapasów paliwa dla generatorów awaryjnych.
3. Zakłócenie pracy systemów telekomunikacyjnych i informatycznych.
4. Przerwy w dostawach wody i funkcjonowaniu gospodarki ściekowej.
5. Narastanie dezinformacji i paniki społecznej.
6. Zakłócenia w dostawach żywności, paliw i leków.
7. Utrata sprawności koordynacyjnej administracji publicznej.

Szczególnie niebezpieczne byłoby równoczesne wystąpienie kilku wymienionych zjawisk.

ETAP II. OPRACOWANIE SCENARIUSZY

Przygotowano cztery alternatywne scenariusze rozwoju sytuacji. Podane ramy czasowe mają charakter przykładowych założeń dydaktycznych, a nie prognoz technicznych.

Scenariusz 1. Korzystny – szybkie opanowanie zagrożenia

Poważna awaria powoduje utratę zasilania na znacznym obszarze, jednak dzięki szybkiemu uruchomieniu procedur operatorów energetycznych udaje się powstrzymać rozprzestrzenianie zakłóceń.

Zasilanie najważniejszych obiektów infrastruktury krytycznej zostaje utrzymane dzięki systemom rezerwowym, a przywracanie dostaw energii następuje w ciągu kilku lub kilkunastu godzin.

Administracja publiczna skutecznie informuje społeczeństwo o sytuacji.

Rezultat: zagrożenie zostaje opanowane, a zakłócenia mają charakter przejściowy i nie prowadzą do poważnej destabilizacji państwa.

Scenariusz 2. Umiarkowany – ograniczone zakłócenia

Blackout utrzymuje się przez kilkanaście do około 24 godzin, przy czym na niektórych obszarach awaria może trwać dłużej.

Pojawiają się zakłócenia w transporcie, zaopatrzeniu i funkcjonowaniu instytucji publicznych. Część placówek medycznych korzysta z awaryjnych źródeł energii.

Sytuacja wywołuje niepokój społeczny, ale administracja publiczna zachowuje zdolność działań ratowniczych.

Rezultat: państwo ponosi straty gospodarcze i organizacyjne, lecz utrzymuje kontrolę nad sytuacją.

Scenariusz 3. Niekorzystny – poważne zakłócenia funkcjonowania państwa

Blackout utrzymuje się przez 2–3 dni i obejmuje liczne obszary kraju.

Dochodzi do przerw w funkcjonowaniu systemów wodociągowych, telekomunikacyjnych i transportowych.

Występują trudności z zaopatrzeniem ludności w żywność, wodę i paliwo.

Część instytucji publicznych ogranicza działalność. W niektórych miejscach może dochodzić do naruszeń porządku publicznego.

Rezultat: państwo zachowuje podstawową zdolność działania, jednak jego możliwości reagowania są istotnie ograniczone.

Scenariusz 4. Ekstremalny – wielowymiarowy kryzys państwa

Blackout trwa wiele dni i obejmuje znaczną część kraju.

Długotrwały brak energii powoduje narastanie powiązanych zagrożeń:

- ograniczenie dostępności wody pitnej;
- zakłócenia systemów łączności;
- problemy z funkcjonowaniem szpitali;
- przerwanie części łańcuchów dostaw;
- utrudnienia w przemieszczaniu ludności;

Scenariusz 4. Ekstremalny – konsekwencje

- wzrost napięć społecznych;

- ograniczenie zdolności administracji do koordynowania działań.

Może dojść do sytuacji, w której tempo narastania zagrożeń przekracza zdolności reagowania instytucji państwowych.

Rezultat: państwo doświadcza głębokiego kryzysu strategicznego i organizacyjnego.

Scenariusz ten może prowadzić do sytuacji zbliżonej do opisywanego przez Lamentowicza Efektu Tsunami. Nie oznacza jednak automatycznie jego wystąpienia, ponieważ warunkiem Efektu Tsunami w ścisłym znaczeniu jest całkowita niemoc strategiczna.

Scenariusz 1. Korzystny

Działania zapobiegawcze:

Systematyczne przeglądy infrastruktury energetycznej, modernizacja zabezpieczeń, zwiększanie odporności na awarie i cyberataki.

Działania przygotowawcze:

Opracowanie procedur szybkiego przywracania dostaw energii, ćwiczenia operatorów oraz testowanie zasilania rezerwowego obiektów krytycznych.

Działania po wystąpieniu zagrożenia:

Lokalizacja awarii, izolowanie uszkodzonych elementów, uruchomienie rezerw i stopniowe przywracanie zasilania.

Monitorowanie:

Bieżąca kontrola parametrów systemu elektroenergetycznego, liczby odbiorców pozbawionych energii oraz postępów prac naprawczych.

Warunki zmiany strategii:

Brak oczekiwanego postępu przywracania zasilania lub pojawienie się awarii wtórnych.

Scenariusz 2. Umiarkowany

Działania zapobiegawcze:

Zwiększanie niezależności energetycznej infrastruktury krytycznej, rozwijanie lokalnych systemów zasilania rezerwowego.

Działania przygotowawcze:

Gromadzenie zapasów paliwa, zapewnienie awaryjnej łączności oraz przygotowanie punktów pomocy dla mieszkańców.

Działania po wystąpieniu zagrożenia:

Priorytetowe zabezpieczenie placówek medycznych, wodociągów, systemów ratownictwa i innych usług niezbędnych do ochrony życia.

Monitorowanie:

Analiza dostępności energii, paliwa, wody i usług telekomunikacyjnych oraz zgłoszeń napływających do centrów zarządzania kryzysowego.

Warunki zmiany strategii:

Rozszerzenie zasięgu awarii, brak możliwości utrzymania zasilania rezerwowego lub zakłócenie funkcjonowania kolejnych usług krytycznych.

Scenariusz 3. Niekorzystny

Działania zapobiegawcze:

Budowa odporności infrastruktury krytycznej na awarie kaskadowe oraz rozwijanie zdolności współdziałania służb i przedsiębiorstw strategicznych.

Działania przygotowawcze:

Przygotowanie regionalnych planów dostaw wody, paliwa, żywności i środków medycznych. Zapewnienie alternatywnych kanałów komunikacji.

Działania po wystąpieniu zagrożenia:

Uruchomienie międzyregionalnej pomocy logistycznej, organizowanie dystrybucji podstawowych artykułów oraz priorytetowe zabezpieczanie osób wymagających szczególnej pomocy.

Monitorowanie:

Ocena stanu zapasów, funkcjonowania szpitali, dostępności transportu oraz zdolności działania administracji.

Warunki zmiany strategii:

Wystąpienie jednoczesnych zakłóceń w dostawach energii, wody i paliw lub zagrożenie ciągłości działania służb ratowniczych.

Scenariusz 4. Ekstremalny

Działania zapobiegawcze:

Tworzenie rozproszonych systemów zasilania awaryjnego, zwiększanie odporności sieci telekomunikacyjnych oraz ograniczanie uzależnienia najważniejszych funkcji państwa od pojedynczych elementów infrastruktury.

Działania przygotowawcze:

Przygotowanie awaryjnego systemu kierowania państwem, alternatywnych miejsc pracy administracji i zdecentralizowanych struktur koordynacji. Organizowanie ćwiczeń symulujących jednoczesne awarie wielu systemów.

Działania po wystąpieniu zagrożenia:

Koncentracja zasobów na ochronie życia i zdrowia ludności, utrzymaniu podstawowych funkcji państwa oraz odtwarzaniu najważniejszych systemów infrastruktury.

Monitorowanie:

Analiza zdolności funkcjonowania najważniejszych instytucji, dostępności zasobów strategicznych i skali zagrożeń społecznych.

Warunki zmiany strategii:

Utrata zdolności realizacji działań centralnie koordynowanych, załamanie systemów komunikacji lub brak możliwości zaspokojenia podstawowych potrzeb ludności.

W takim przypadku konieczne jest przejście od strategii przywracania normalnego funkcjonowania do strategii utrzymania minimalnych, niezbędnych funkcji państwa i ochrony ludności.

Pięć przykładowych sygnałów ostrzegawczych

Sygnał ostrzegawczy	Instytucje monitorujące	Znaczenie dla decyzji państwowych
1. Rosnąca liczba awarii i nietypowych zakłóceń pracy systemu elektroenergetycznego	PSE, operatorzy systemów dystrybucyjnych	Zwiększenie gotowości służb technicznych oraz przygotowanie procedur awaryjnych.

Pięć przykładowych sygnałów ostrzegawczych (ciąg dalszy)

Sygnał ostrzegawczy	Instytucje monitorujące	Znaczenie dla decyzji państwowych
2. Nasilenie nieprawidłowości i incydentów cyberbezpieczeństwa w sektorze energetycznym	Operatorzy infrastruktury, właściwe zespoły reagowania na incydenty bezpieczeństwa komputerowego	Wzmocnienie ochrony systemów sterowania i sprawdzenie możliwości utrzymania działania w trybie awaryjnym.
3. Prognozy wystąpienia ekstremalnych zjawisk pogodowych	IMGW-PIB, operatorzy infrastruktury	Podniesienie poziomu gotowości, przygotowanie ekip technicznych i zasobów naprawczych.

Pięć przykładowych sygnałów ostrzegawczych (ciąg dalszy)

Sygnał ostrzegawczy	Instytucje monitorujące	Znaczenie dla decyzji państwowych
4. Malejąca zdolność obiektów krytycznych do samodzielnego funkcjonowania	Zarządcy szpitali i infrastruktury krytycznej, właściwe centra zarządzania kryzysowego	Uruchomienie dostaw paliwa, agregatów i pomocy logistycznej.
5. Jednoczesne zakłócenia dostaw energii i usług telekomunikacyjnych	Operatorzy energetyczni, operatorzy telekomunikacyjni, centra zarządzania kryzysowego	Przejście do działań przeciwdziałających kaskadowemu rozwojowi kryzysu.

Wykorzystanie informacji ostrzegawczych

Sygnały powinny być analizowane łącznie, ponieważ pojedyncze nieprawidłowości nie muszą oznaczać nadchodzącego kryzysu.

Przykładowo wystąpienie awarii energetycznej w połączeniu z problemami telekomunikacyjnymi oraz ograniczeniem dostępności paliwa może wskazywać na rozwój kryzysu o znacznie większej skali.

Informacje powinny być przekazywane do właściwych ośrodków zarządzania kryzysowego, gdzie na podstawie potwierdzonych danych podejmowane byłyby decyzje dotyczące uruchomienia zasobów, zmiany priorytetów i modyfikacji scenariusza działania.

PODSUMOWANIE ĆWICZENIA

Odpowiedzi na pytania podsumowujące

PYTANIE 1

1. Czy państwo może przygotować się na zagrożenie, którego przebiegu nie potrafi dokładnie przewidzieć?

Tak, państwo może przygotować się na takie zagrożenie, chociaż nie jest w stanie zagwarantować pełnej skuteczności swoich działań.

Przygotowanie nie musi oznaczać dokładnego przewidywania przyszłych wydarzeń. Może polegać na tworzeniu zdolności organizacyjnych, technicznych i społecznych umożliwiających reagowanie na różne warianty rozwoju sytuacji.

Państwo powinno przede wszystkim:

PAŃSTWO WOBEC ZAGROŻEŃ

Kluczowe działania budujące odporność państwa

1



Identyfikować potencjalne zagrożenia

2



Rozpoznawać wzajemne zależności pomiędzy systemami

3



Przygotowywać alternatywne scenariusze

4



Tworzyć rezerwy zasobów

5



Rozwijać systemy wczesnego ostrzegania

6



Prowadzić ćwiczenia i symulacje

7



Doskonalić zdolność szybkiego dostosowywania strategii

Przygotowanie na niepewność – zalecenia

- identyfikować potencjalne zagrożenia;
- rozpoznawać wzajemne zależności pomiędzy systemami;
- przygotowywać alternatywne scenariusze;
- tworzyć rezerwy zasobów;
- rozwijać systemy wczesnego ostrzegania;
- prowadzić ćwiczenia i symulacje;
- doskonalić zdolność szybkiego dostosowywania strategii.

W koncepcji Lamentowicza szczególne znaczenie ma przygotowywanie się również na zdarzenia uznawane za bardzo mało prawdopodobne.

Oznacza to, że państwo nie powinno zakładać wyłącznie realizacji najbardziej prawdopodobnego scenariusza.

PYTANIE 2

2. Jakie znaczenie ma wielowariantowe planowanie strategiczne?

Wielowariantowe planowanie strategiczne polega na przygotowaniu kilku możliwych obrazów przyszłości oraz określeniu działań odpowiednich do każdego z nich.

Najważniejszą korzyścią jest ograniczenie uzależnienia państwa od jednej prognozy rozwoju sytuacji.

Jeżeli państwo przygotuje tylko jeden scenariusz, a rzeczywistość rozwinie się inaczej, przyjęta strategia może okazać się nieskuteczna.

Wielowariantowe planowanie umożliwia:

KORZYŚCI Z WIELOWARIANTOWEGO PLANOWANIA

1



Rozpoznawanie różnych kierunków rozwoju zagrożeń.

2



Identyfikowanie potencjalnych skutków pośrednich i wtórnych.

3



Przygotowanie alternatywnych sposobów reagowania.

4



Lepsze wykorzystanie ograniczonych zasobów.

5



Skrócenie czasu podejmowania decyzji w sytuacjach kryzysowych.

6



Ograniczanie ryzyka wystąpienia strategicznej bezradności.

PYTANIE 3

3. Dlaczego rozpoznawanie słabych sygnałów zagrożenia jest istotnym elementem bezpieczeństwa państwa?

Słabe sygnały to wczesne, niejednoznaczne symptomy mogące świadczyć o nadchodzącej zmianie lub zagrożeniu.

Ich znaczenie polega na tym, że pozwalają rozpocząć działania przygotowawcze jeszcze przed wystąpieniem pełnoobjawowego kryzysu.

Przykładowo:

W przypadku blackoutu słabym sygnałem może być narastająca liczba nietypowych zakłóceń pracy infrastruktury energetycznej.

W przypadku kryzysu migracyjnego połączonego z dezinformacją takim sygnałem może być skoordynowane rozpowszechnianie fałszywych informacji jeszcze przed wystąpieniem poważnych incydentów.

Słabe sygnały – działania wyprzedzające

Rozpoznawanie słabych sygnałów umożliwia:

- wcześniejsze uruchomienie procedur;
- zwiększenie gotowości instytucji;
- lepsze rozmieszczenie zasobów;
- przygotowanie ludności na możliwe zakłócenia;
- ograniczenie negatywnych konsekwencji zdarzeń.

Należy jednak pamiętać, że pojedynczy sygnał nie jest dowodem wystąpienia zagrożenia. Powinien być weryfikowany i analizowany w powiązaniu z innymi informacjami.

PYTANIE 4

4. Czy skuteczne prognozowanie może całkowicie wyeliminować ryzyko?

Nie. Nawet bardzo rozwinięte systemy prognozowania nie są w stanie całkowicie wyeliminować ryzyka.

Wynika to z charakteru współczesnego środowiska bezpieczeństwa.

Lamentowicz wskazuje na:

1. Rosnącą liczbę podmiotów i wzajemnych zależności.
2. Nieliniowy przebieg wielu procesów.
3. Występowanie zdarzeń bardzo trudnych do przewidzenia.
4. Nasilanie się procesów kaskadowych.
5. Ograniczenia ludzkiej wiedzy i zdolności decyzyjnych.

Granice prognozowania i zarządzania ryzykiem

Nawet jeśli państwo prawidłowo rozpozna potencjalne zagrożenie, nie oznacza to, że potrafi przewidzieć wszystkie jego konsekwencje.

Prognozowanie powinno więc służyć nie tyle całkowitemu wyeliminowaniu ryzyka, ile jego rozpoznawaniu, ograniczaniu i przygotowywaniu odpowiednich sposobów reagowania.

5. Dlaczego elastyczność strategii jest równie ważna jak jej wcześniejsze przygotowanie?

Elastyczność strategii oznacza zdolność do modyfikowania celów operacyjnych, priorytetów i metod działania w odpowiedzi na zmieniające się warunki.

Współczesne zagrożenia mogą rozwijać się w sposób szybki, nieliniowy i nieprzewidywalny.

Dlatego strategia skuteczna na początku kryzysu może okazać się niewystarczająca na jego dalszych etapach.

Przykład – blackout:

Początkowym celem państwa jest możliwie szybkie przywrócenie dostaw energii.

Jeżeli jednak awaria utrzymuje się przez wiele dni i pojawiają się zakłócenia w dostawach wody, paliwa i żywności, strategia musi zostać zmodyfikowana.

Wówczas priorytetem staje się zapewnienie ludności podstawowych warunków przetrwania i utrzymanie najważniejszych funkcji państwa.

WNIOSKI KOŃCOWE

Analiza obu wariantów pozwala sformułować pięć najważniejszych wniosków.

Wniosek 1. Współczesne zagrożenia bezpieczeństwa państwa mają charakter wielowymiarowy, a ich konsekwencje mogą wykraczać daleko poza obszar, w którym wystąpiło pierwotne zdarzenie.

Wniosek 2. Największe niebezpieczeństwo powstaje w sytuacji, gdy kilka zagrożeń wzajemnie wzmacnia swoje oddziaływanie, prowadząc do narastającego kryzysu.

Wniosek 3. Skuteczność strategii bezpieczeństwa zależy nie tylko od zasobów państwa, ale także od sprawności instytucjonalnej, jakości informacji, szybkości podejmowania decyzji oraz zdolności współdziałania.

Wniosek 4. Planowanie strategiczne powinno uwzględniać różne warianty przyszłości, a opracowane scenariusze muszą być systematycznie aktualizowane na podstawie informacji o zmianach zachodzących w otoczeniu państwa.

Wniosek 5. Podstawowym celem przygotowania strategicznego nie jest całkowite wyeliminowanie ryzyka, lecz ograniczanie prawdopodobieństwa wystąpienia sytuacji, w której państwo utraci zdolność do skutecznego działania.

Konkluzja

W świetle koncepcji Wojtka Lamentowicza państwo nie jest w stanie zapewnić sobie pełnej kontroli nad dynamicznym i złożonym środowiskiem bezpieczeństwa.

Może jednak rozwijać zdolność do przewidywania alternatywnych kierunków zmian, rozpoznawania wczesnych symptomów zagrożeń oraz dostosowywania działań do zmieniających się okoliczności.

Najważniejszym zadaniem strategii bezpieczeństwa państwa jest zatem nie tylko przygotowanie odpowiedzi na znane zagrożenia, ale przede wszystkim stworzenie zdolności do skutecznego działania w warunkach niepewności, nieprzewidywalności i ograniczonej sterowności procesów społecznych, gospodarczych oraz politycznych.