RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

NUMER 27 KWIECIEŃ – CZERWIEC 2019

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Alert RCB ma rok

Grzegorz Świszcz
Rządowe Centrum Bezpieczeństwa

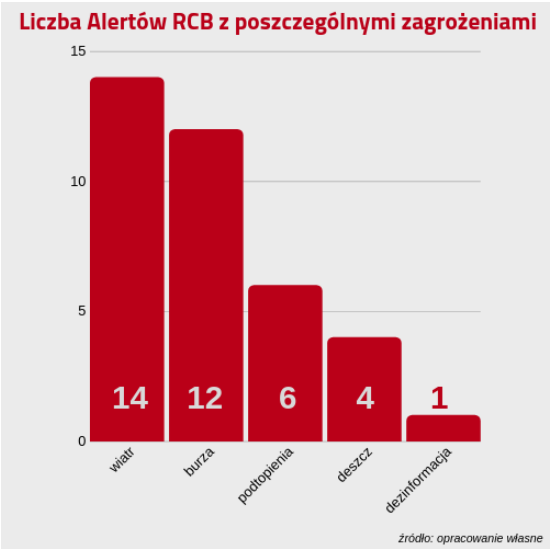
Równo rok temu powstał SMS-owy system powiadamiania ludności o zagrożeniach – Alert RCB. Przez pierwsze pół roku prowadziliśmy pilotaż, a od grudnia, po wejściu w życie nowelizacji ustawy o zarządzaniu kryzysowym, Alert RCB działa już w pełnej funkcjonalności. W tym czasie uruchomiliśmy go 23 razy. I dzięki współpracy z operatorami telefonii komórkowej, wysłaliśmy około 200 milionów SMS-ów ostrzegających przed zagrożeniem. W ciągu roku Alert RCB wszedł na stałe do świadomości społecznej i po sygnałach, które otrzymujemy można bez wątpienia stwierdzić, że jest bardzo dobrze odbierany przez większość społeczeństwa.

Alert RCB jest uruchamiany tylko w stanie wyższej konieczności, w sytuacji bezpośredniego zagrożenia życia lub zdrowia. W ciągu pierwszego roku Alert RCB wysyłaliśmy 23 razy. Najwięcej w maju br. (9 razy), gdy po intensywnych opadach deszczu na południu Polski, rzeki przekroczyły stany alarmowe, a na Wiśle przemieszczała się fala wezbraniowa. Drugim miesiącem, podczas którego uruchamialiśmy częściej niż zwykle Alert RCB był czerwiec tego roku (6 razy), gdy dni z bardzo wysokimi temperaturami były przeplatane intensywnymi burzami z bardzo silnym wiatrem.

ZAGROŻENIA POGODOWE ZDOMINOWAŁY PIERWSZY ROK ALERTU RCB

Ostrzegaliśmy przede wszystkim przed zagrożeniami pogodowymi. Tylko w jednym przypadku, 27 października 2018 roku interweniowaliśmy w przypadku dezinformacji – w związku z fałszywymi Alertami RCB w sprawie poboru mężczyzn po wprowadzeniu stanu wojennego na Ukrainie.

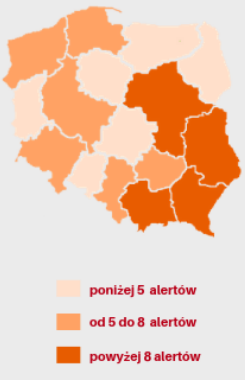
Najczęściej ostrzegaliśmy przed silnym wiatrem i burzami. W Alertach RCB informowaliśmy również o możliwych podtopieniach, będących wynikiem intensywnych opadów deszczu.



SMS-y z ostrzeżeniami wysyłaliśmy najczęściej na obszar południowo-wschodniej i centralnej Polski. Najczęściej do osób przebywających w województwie podkarpackim oraz lubelskim, małopolskim i mazowieckim. Najrzadziej Alert RCB uruchamialiśmy w województwach: opolskim oraz podlaskim, kujawsko-pomorskim i lubuskim.

Województwa, na terenie których uruchomiono Alert RCB

województwo	Alert RCB
1. podkarpackie	11
2. lubelskie	9
3. małopolskie	9
4. mazowieckie	9
5. świętokrzyskie	7
6. śląskie	6
7. dolnośląskie	5
8. pomorskie	5
9. wielkopolskie	5
10. zachodniopomorskie	5
11. łódzkie	4
12. warmińsko-mazurskie	4
13. kujawsko-pomorskie	3
14. lubuskie	3
15. podlaskie	3
16. opolskie	2



źródło: opracowanie własne

DOTYCHCZASOWE DOŚWIADCZENIA

Po roku funkcjonowania Alertu RCB nie mamy wątpliwości, że nowy system w obecnych warunkach jest najbardziej skutecznym systemem ostrzegania o zagrożeniach. Świadczy o tym około 200 milionów wysłanych SMS-ów. Otrzymujemy bardzo dużo pozytywnych reakcji od odbiorców Alertu RCB, co świadczy o tym, że chcemy dostawać SMS-owe ostrzeżenia. Oczywiście nie wszystko działa tak jakbyśmy sobie tego życzyli. Przepustowość bramek SMS u operatorów komórkowych jest nadal ograniczona, co powoduje, że Alert RCB, przy zagrożeniach obejmujących duży obszar, może być rozsyłany nawet 2-3 godziny. Zgodnie z założeniami systemu, SMS-y są wysyłane do wszystkich użytkowników telefonów komórkowych,

przebywających na zagrożonym obszarze. Jednakże, jeśli w momencie tworzenia przez operatorów bazy numerów, telefon komórkowy znajdzie się poza zasięgiem sieci, wtedy jest prawdopodobne, że ostrzeżenie nie dojdzie. Roaming krajowy stosowany przez niektórych operatorów powoduje natomiast, że niektórzy użytkownicy mogą otrzymać więcej niż jedno ostrzeżenie z różnych sieci, do których się w tym czasie zalogowali. Jesteśmy jednak w ciągłym kontakcie z operatorami komórkowymi i system jest cały czas udoskonalany, tak, żeby w przyszłości uniknąć takich sytuacji.

Mimo, że Alert RCB funkcjonuje dopiero od roku, to już istnieje w świadomości społecznej. Prowadzimy cały czas intensywną kampanię informacyjną, żeby wszyscy mieszkańcy Polski wiedzieli czym jest Alert RCB i jak na niego należy reagować. Ważne jest to, że nowy system jest powszechny, gdyż nie trzeba się do niego zapisywać, ani pobierać aplikacji. Każdy użytkownik telefonu komórkowego, jeśli będzie przebywał na zagrożonym terenie, powinien otrzymać informacje o niebezpieczeństwie. Jedyny warunek jaki musi zostać spełniony to włączony telefon i zalogowany do sieci operatora komórkowego. Sieć nie ma znaczenia, ponieważ wszyscy operatorzy są prawnie zobowiązani do przesłania SMS-a swoim abonentom na wskazany przez nas teren.

Alert RCB powstaje na podstawie informacji o zagrożeniach otrzymanych ze wszystkich odpowiedzialnych za działania antykryzysowe służb czy instytucji. W tym roku najczęściej współpracowaliśmy przy Alercie RCB z Instytutem Meteorologii i Gospodarki Wodnej, który na bieżąco przekazuje nam informacje dotyczące spodziewanych zagrożeń meteorologicznych. Alert RCB nie funkcjonowałby również bez doskonałej współpracy ze wszystkimi operatorami sieci komórkowych działających w Polsce.

Najmniejszym obszarem, na który można go wysłać jest powiat. Jednak w większości wypadków, Alert RCB jest uruchamiany na zdecydowanie większym obszarze. Osoby z zagranicznymi numerami telefonów, które przebywają na obszarze zagrożonym, otrzymują ostrzeżenie w języku angielskim. Alerty RCB mogą dostawać również Polacy przebywający za granicą, jeżeli ich życiu będzie zagrażało niebezpieczeństwo.

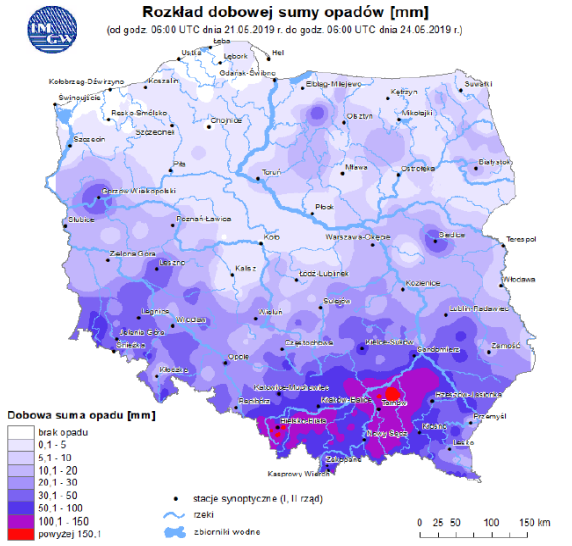
Intensywne opady deszczu w maju – podsumowanie

Ewa Michałkiewicz, Paweł Domański
Rządowe Centrum Bezpieczeństwa

W trzeciej dekadzie maja w południowej i południowo-wschodniej części kraju wystąpiły intensywne opady deszczu oraz burze. Suma opadów znacznie przekroczyła miesięczną normę, co spowodowało liczne zalania, podtopienia, uszkodzenia budynków, upraw oraz infrastruktury drogowej, szczególnie w województwach śląskim, małopolskim, podkarpackim i świętokrzyskim. Na Wiśle i Odrze utworzyły się fale wezbraniowe, które w górnej części biegu tych rzek przekroczyły stany alarmowe. Ostateczne dane dotyczące strat spowodowanych sytuacją hydro-meteorologiczną będą znane po zakończeniu prac komisji szacujących.

SYTUACJA METEOROLOGICZNA W DRUGIEJ POŁOWIE MAJA

Opady o największej intensywności wystąpiły we wtorek, środę i czwartek (21-23 maja) w województwie małopolskim, podkarpackim i śląskim. We wtorek sumy opadów lokalnie przekroczyły 100 mm na dobę (Kolbuszowa – 136 mm, Mielec – 124 mm), w środę spadło miejscami prawie 100 mm (Szczyrk – 99 mm, Bielsko-Biała – 81 mm). W czwartek, 23 maja opady były już nieco słabsze (najwyższy w Libertowie – 60 mm). W ogólnym ujęciu suma opadów przekraczała lokalnie normę dla maja nawet trzykrotnie. Za trzy omawiane doby wyniosła w Szczyrku 186 mm, w Radomyślu Wielkim 169 mm, a w Brennej 161 mm.



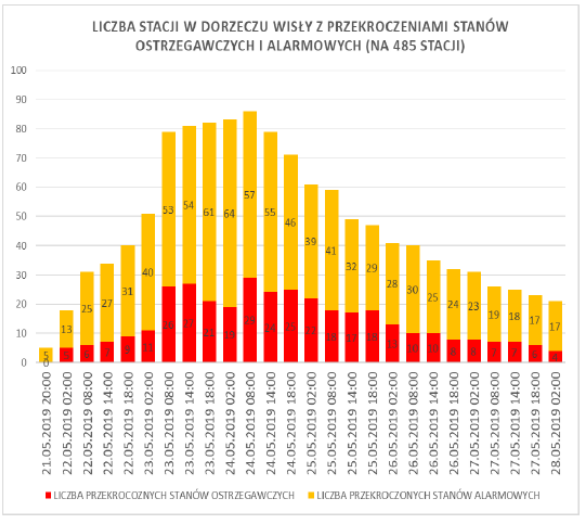
Rozkład dobowej sumy opadów od godz. 8:00 czasu lokalnego 21 maja do godz. 8:00, 24 maja. Źródło: IMGW PIB.

Opady przyczyniły się do powstania wezbrań w rzekach, które w wielu miejscach powodowały podtopienia i zalania.

SYTUACJA HYDROLOGICZNA W DORZECZU WISŁY

W górnej części dorzecza Wisły znaczne dobowe wzrosty stanów wody wystąpiły już we wtorek, 21 maja. Wystąpiło 6 przekroczeń stanu alarmowego i 25 ostrzegawczego, przy czym wezbrania były gwałtowne (w ciągu 24 h na Wisłoce w Pustkowie zaobserwowano wzrost o 487 cm). Opady trwające kolejne doby powodowały dalsze wzrosty stanów wody. 23 maja zanotowano przekroczenia stanu alarmowego na 26 stacjach, a 24 maja na 29. W kolejnych dniach wraz z ustępowaniem strefy opadów sytuacja hydrologiczna w zlewniach górnej Wisły stabilizowała się. Stany wody zaczęły opadać, a 2 czerwca na dopływach górnej Wisły układały się głównie w strefie wody średniej, lokalnie wysokiej.

W konsekwencji opadów deszczu, uformowała się fala wezbraniowa przemieszczająca się z biegiem Wisły. Na górnym odcinku rzeki notowano przekroczenia stanu alarmowego prawie wszędzie[1], zaś na odcinku środkowym jedynie powyżej Dęblina (w Zawichoście o 149 cm). W Warszawie stany wody wzrosły tylko do strefy wody wysokiej, na stacji Warszawa-Bulwary. Do przekroczenia stanu ostrzegawczego zabrakło 21 cm. Do Włocławka fala wezbraniowa dotarła 30 maja nie przekraczając stanu ostrzegawczego, w dużej mierze dzięki pracy zbiornika we Włocławku. Na dolnej Wiśle wezbranie osiągnęło stany ostrzegawcze (w Chełmnie alarmowe), zaś na odcinku ujściowym zostały lokalnie przekroczone stany alarmowe. 2 czerwca fala wezbraniowa dotarła do Zatoki Gdańskiej.



Liczba stacji w dorzeczu Wisły z przekroczeniami stanów ostrzegawczych i alarmowych. Źródło: IMGW-PIB.

WYKORZYSTANIE SYSTEMU ALERT RCB

W związku z przewidywanym zagrożeniem dla zdrowia i życia mieszkańców dyrektor RCB, po konsultacji z IMGW oraz właściwymi wojewodami, podejmował decyzje o uruchamianiu systemu Alert RCB. Między 20 a 27 maja system był wykorzystywany każdego dnia, przy czym dostosowywano obszar oraz treść ostrzeżenia do aktualnej sytuacji. Początkowo treść wiadomości dotyczyła burz oraz podtopień, następnie, wraz z normowaniem się sytuacji meteorologicznej i przemieszczaniem się wezbrania na Wiśle, ostrzegano ludność przed falą wezbraniową.

Po 27 maja zakończono wysyłanie ostrzeżeń, ponieważ sytuacja hydrologiczna na Wiśle nie stwarzała już zagrożenia. Między 20 a 27 maja operatorzy telekomunikacyjni wysłali ponad 35 milionów ostrzeżeń do użytkowników telefonów komórkowych, najwięcej 22 maja (ok. 10,5 mln SMS).

DZIAŁANIA SŁUŻB

Państwowa Straż Pożarna

Według danych KG PSP, w okresie 21-26 maja w kraju odnotowano łącznie 8 903 interwencje związane z usuwaniem skutków silnego wiatru, burz oraz intensywnych opadów deszczu. Największą liczbę zdarzeń odnotowano w woj. małopolskim – 3 344, podkarpackim – 2 555, śląskim – 1 130, świętokrzyskim – 540 oraz lubelskim – 140. Działania

[1] Najwyższy dobowy wzrost poziomu wody wystąpił w m. Czernichów-Prom (o 231 cm za dobę 23 maja), zaś stan alarmowy był przekroczony maksymalnie o 85 cm w Bieruniu Nowym i w Karsach.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

PSP polegały przede wszystkim na ewakuacji ludzi i mienia z zagrożonych obszarów, zabezpieczaniu obiektów przed oddziaływaniem nagłych przyborów wód, uszczelnianiu wałów przeciwpowodziowych, zabezpieczaniu obiektów uszkodzonych w wyniku oddziaływania trąb powietrznych i silnego wiatru oraz wypompowywaniu wody.

Podczas interwencji stwierdzono 999 wiatrołomów, 306 uszkodzeń budynków (w tym 192 budynki mieszkalne), 4 979 podtopień budynków oraz 1 044 podtopień dróg.

W działania ratownicze zaangażowanych było 47 164 ratowników oraz 13 859 pojazdów, w tym PSP – 9 383 strażaków i 3 479 pojazdów oraz OSP – 37 781 druhów i 10 380 pojazdów. Dodatkowo działania były wspierane przez 739 żołnierzy oraz 1 śmigłowiec Sił Zbrojnych RP, a także 1 śmigłowiec Straży Granicznej. Jednocześnie, w związku z przechodzeniem fali wezbraniowej na Wiśle, prowadzono działania wyprzedzające mające na celu uszczelnienie wałów.

Policja

W okresie 20-31 maja w działania związane z powodzią zaangażowanych było 4 420 policjantów wspieranych m. in. przez 1 945 pojazdów, 2 śmigłowce Black Hawk, 6 psów oraz 3 łodzie. Największe siły i środki skoncentrowano na obszarze podległym Komendzie Wojewódzkiej Policji w Krakowie (3 441 policjantów i 1 535 pojazdów).

WOJEWÓDZTWA – SKUTKI GWAŁTOWNYCH ZJAWISK ATMOSFERYCZNYCH, PODJĘTE DZIAŁANIA ORAZ STWIERDZONE STRATY

Województwo śląskie

Z powodu gwałtownych zjawisk atmosferycznych, w drugiej połowie maja w woj. śląskim odnotowano 708 zalanych budynków, w tym 578 budynków mieszkalnych i 130 innych obiektów. W m. Wilkowice (powiat bielski) nieczynny zbiornik na rzece Wilkówce stanowił zagrożenie dla okolicznych mieszkańców, ze względu na ryzyko przerwania zapory. Konieczna była ewakuacja ok. 85 osób z 35 pobliskich domów jednorodzinnych. Ze względu na brak możliwości dokonania zrzutu wody ze zbiornika, prowadzono działania mające zapobiec uszkodzeniu zbiornika przez napierającą wodę. W Bielsku-Białej odnotowano 272 zdarzenia związane z usuwaniem skutków nawalnego deszczu oraz 1 000 wyjazdów straży pożarnej. W działaniach uczestniczyli również żołnierze WOT, którzy rozkładali worki z piaskiem (łącznie wydano 4 tysiące worków). W mieście zalane zostały pomieszczenia i piwnice w 30 placówkach oświatowych.

Województwo lubelskie

W okresie 20-31 maja na terenie województwa doszło do przekroczenia stanów alarmowych na Wiśle oraz przejścia trąby powietrznej. Działania służb polegały głównie na monitorowaniu wałów i urządzeń hydrotechnicznych, uszczelnianiu wałów oraz minimalizowaniu skutków przejścia trąby powietrznej. Usuwano połamane konary drzew, udrażniano drogi dojazdowe do posesji oraz zabezpieczano plandekami uszkodzone i zerwane dachy na budynkach mieszkalnych i gospodarczych, szczególnie na terenie powiatów lubartowskiego, opolskiego oraz lubelskiego.

W związku z przejściem trąby powietrznej przez gminę Wojciechów (pow. lubelski), wojewoda lubelski 22 maja wystąpił z wnioskiem do ministra obrony narodowej o skierowanie wydzielonych sił i środków do likwidacji skutków zdarzenia. W działaniach udział wzięło 200 żołnierzy wraz z niezbędnym sprzętem. Jednocześnie zaangażowano 55 zastępów strażaków z terenu województwa.

Województwo podkarpackie

21-22 maja w wyniku intensywnych opadów deszczu (90-130 mm) i utrudnionego spływu wód z obszarów równinnych doszło do podtopień budynków, w szczególności na terenie powiatów położonych w zlewni Wisłoki, tj. mieleckiego, kolbuszowskiego i dębickiego. Najpoważniejsza sytuacja miała miejsce w gminie Wadowice Górne, gdzie doszło do przerwania dwóch grobli – w m. Izdebki oraz Wadowice Dolne na Kanale Wadowickim. W nocy z 23 na 24 maja przechodzący front atmosferyczny spowodował intensywne opady deszczu, lokalnie o charakterze burzowym (30 mm w ciągu godziny) w powiatach kolbuszowskim, ropczycko-sędziszowskim, strzyżowskim, krośnieńskim, jasielskim oraz stalowowolskim. Sytuacja ta spowodowała przekroczenia stanów alarmowych na Wisłoku oraz jego dopływach, a także liczne rozlewiska na małych ciekach wodnych. Ponadto, w wyniku spływu wód oraz intensywnych opadów deszczu, w powiecie stalowowolskim doszło do licznych podtopień. Z uwagi na konieczność użycia dodatkowych sił i środków, wojewoda podkarpacki zwrócił się do ministra obrony narodowej z wnioskiem o wsparcie działań administracji publicznej wydzielonymi silami i środkami Sił Zbrojnych RP.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

W trakcie niekorzystnej sytuacji hydrologiczno-meteorologicznej odbyło się siedem posiedzeń Wojewódzkiego Zespołu Zarządzania Kryzysowego. Z pięciu wojewódzkich magazynów przeciwpowodziowych wydano ponad 550 tys. sztuk worków oraz 700 mb rękawów przeciwpowodziowych.

W okresie 18-24 maja doszło do podtopień budynków mieszkalnych w 16 powiatach (na terenie 35 gmin) województwa. W związku z podtopieniami części mieszkalnej domostw, poszkodowane zostały 1 063 rodziny.

Województwo małopolskie

W okresie 22-26 maja odbyło się sześć posiedzeń Wojewódzkiego Zespołu Zarządzania Kryzysowego (w tym jednego, w powiecie dąbrowskim, m. Suchy Grunt). W posiedzeniach uczestniczyli między innymi premier i wicepremierzy, ministrowie, wojewodowie, członkowie WZZK, zaproszeni goście i media. W związku z niekorzystną sytuacją odnotowano 4 133 zgłoszenia. Z wojewódzkiego magazynu przeciwpowodziowego dla Małopolski wydano m.in. 228 000 worków, 26 pomp dużej wydajności i 14 zapór przeciwpowodziowych.

Województwo świętokrzyskie

23 maja zostało zwołane posiedzenie Wojewódzkiego Zespołu Zarządzenia Kryzysowego, na którym dokonano oceny zagrożenia oraz podjęto decyzję co do dalszych działań. Między innymi, w celu wsparcia samorządów podczas przeprowadzenia akcji przeciwpowodziowej, uruchomiono Wojskowe Zgrupowania Zadaniowe. Wraz ze wzrostem stanu wody w Wiśle, w wyniku przejścia fali wezbraniowej, działania zabezpieczające i monitorowanie zagrożenia prowadzone były głównie na wałach Wisły i wałach cofkowych na rzekach: Nidzica, Nida, Czarna Staszowska, Rejterówka-Kanał Strumień, Koprzywianka oraz Opatówka.

Działania w powiatach polegały przede wszystkim na wypompowywaniu wody z zalanych piwnic budynków mieszkalnych, udrażnianiu przepustów drogowych oraz wykonywaniu kanałów odwadniających na posesjach zalanych wodą i kierowaniu jej w miejsca bezpieczne. Dodatkowo zabezpieczano posesje przed ponownym zalaniem wodami opadowymi, wykorzystując do tego celu rękawy przeciwpowodziowe oraz worki z piaskiem. Ponadto, do odciętych przez wodę posesji, pontonami dostarczano żywność i wodę pitną. Intensywne działania polegające na podniesieniu korony wałów przy pomocy worków i rękawów oraz likwidacji przesiąków prowadzono wzdłuż Wisły, głównie w powiecie sandomierskim i staszowskim.

Podczas prowadzonej akcji przeciwpowodziowej z magazynów wojewody wydano 356 000 worków przeciwpowodziowych, ponad 4 000 m^2 folii ochronnej, ponad 3 000 m^2 geowłókniny i innych materiałów.

Rok funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze postanowienia i rozwiązania

Magdalena Sławińska
Rządowe Centrum Bezpieczeństwa

1 sierpnia minie rok od kiedy Prezydent RP podpisał ustawę o krajowym systemie cyberbezpieczeństwa[1]. Ustawa ta jest wdrożeniem do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS). Zobowiązuje ona państwa członkowskie do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa poprzez ustanowienie organów właściwych oraz pojedynczych punktów kontaktowych do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie krajowych strategii w zakresie cyberbezpieczeństwa.

[1] Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

Ustawa o krajowym systemie cyberbezpieczeństwa weszła w życie 28 sierpnia 2018 r., ale żeby w pełni wdrożyć Dyrektywę NIS w Polsce, potrzebne było przyjęcie dodatkowych rozporządzeń Rady Ministrów jako aktów wykonawczych[2].

Dyrektywa nakłada obowiązki służące zapewnieniu cyberbezpieczeństwa w sektorach usług, mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej państwa. Do tych sektorów zalicza się: energetykę, transport, bankowość, instytucje finansowe, sektor ochrony zdrowia, zaopatrzenie w wodę i infrastrukturę cyfrową. Ustawa wprowadziła pojęcie **systemu cyberbezpieczeństwa**, który *ma na celu zapewnienie cyberbezpieczeństwa[3] na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych, służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.* Podmioty tworzące Krajowy System Cyberbezpieczeństwa (KSC):

- Operatorzy usług kluczowych;
- Dostawcy usług cyfrowych;
- Podmioty publiczne;
- Organy właściwe;
- CSIRT poziomu krajowego,
- Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa;
- Podmioty świadczące usługi z zakresu cyberbezpieczeństwa.

Za sprawą nowego prawa pojawiły się także nowe pojęcia: incydenty (krytyczne, poważne, istotne, w podmiocie publicznym), usługi (kluczowe i cyfrowe), podatność czy zarządzanie incydentem.

Incydentem jest zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Ustawodawca wyróżnił ich kilka rodzajów. **Incydent krytyczny** – skutkuje kluczową szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych lub gospodarczych, funkcjonowania instytucji publicznych, praw i wolności obywatelskich lub zdrowia czy życia ludzi. Incydenty takie klasyfikowane są przez odpowiedni CSIRT – o których mowa będzie poniżej. **Incydent poważny** – może powodować duże obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej. **Incydent istotny** – znacząco wpływa na świadczenie usługi cyfrowej. **Incydent w podmiocie publicznym** – może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

Wystąpienie incydentu może zakłócić funkcjonowanie **usługi cyfrowej** – świadczonej drogą elektroniczną i **usługi kluczowej** – mającej zasadnicze znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. Wykaz usług kluczowych zawarty jest w Rozporządzeniu Rady Ministrów z 11 września 2018 r. *w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.*

W związku z nowymi przepisami wyodrębnia się także operatorów usługi kluczowej (załącznik nr 1 do ustawy, wykaz usług z rozporządzenia oraz nierozłączność świadczenia usługi od systemów informacyjnych) oraz nakłada na nich obowiązki, m.in.:

- prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem, wdrożenie odpowiednich środków technicznych i organizacyjnych, zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty, zarządzanie incydentami oraz stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemów informacyjnych;
- opracowanie, stosowanie i aktualizacja dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego

[2] Rozporządzenie Rady Ministrów z 31 października 2018 r. w sprawie progów uznania incydentu za poważny, Dz. U. 2018 poz. 2180; Rozporządzenie Rady Ministrów z 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Dz. U. 2018 poz. 2080; Rozporządzenie Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, Dz. U. 2018 poz. 1999; Rozporządzenie Rady Ministrów z 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa, Dz. U. 2018 poz. 1952; Rozporządzenie Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz. U. 2018 poz. 1806; Rozporządzenie Ministra Cyfryzacji z 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz. U. 2018 poz. 1780.

[3] Cyberbezpieczeństwo to odporność systemów informatycznych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzania danych lub związanych z nimi usług oferowanych przez te systemy.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

do świadczenia usługi kluczowej oraz ustanowienie nadzoru nad tą dokumentacją;
- powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa;
- zapewnienie przeprowadzenia, minimum raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego.

W przypadku wystąpienia incydentu, zgodnie z ustawą, powinna nastąpić jego obsługa. Rozumie się przez to czynności polegające na wykrywaniu, rejestrowaniu, analizowaniu, klasyfikowaniu, priorytetyzacji, podejmowaniu działań naprawczych i ograniczeniu skutków incydentu. Ustawa usankcjonowała trzy podmioty na poziomie krajowym, które zajmują się reagowaniem na incydenty komputerowe i zarządzanie nim. Zgodnie z terminologią przyjętą w dyrektywie 2016/1148 zostały one określone jako CSIRT (ang. Computer Security Incident Response Teams). W Polsce są to **CSIRT GOV, CSIRT MON, CSIRT NASK.**

CSIRT GOV czyli **Rządowy Zespół Reagowania na Incydenty Komputerowe prowadzony przez Szefa ABW** – do zadań którego należy **obsługa lub koordynacja obsługi incydentów zgłaszanych przez najistotniejsze dla ciągłości państwa jednostki sektora finansów publicznych, jednostki podległe Prezesowi Rady Ministrów i przez niego nadzorowane** (m.in. RCB, KNF, UZP, URE, PGRP), Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz podmioty objęte ustawą o zarządzaniu kryzysowym, czyli podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne wpisane są do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.

CSIRT MON to System Reagowania na Incydenty Komputerowe resortu Obrony Narodowej. Koordynuje obsługę zgłaszanych incydentów przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym.

CSIRT NASK prowadzony jest przez Naukową i Akademicką Sieć Komputerową. Obsługuje incydenty zgłaszane m.in. przez: instytuty badawcze, Polską Agencję Żeglugi Powietrznej czy osoby fizyczne.

Zespoły CSIRT zapewniają spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym – są w europejskiej sieci CSIRT oraz przekazują do innych Państw i innych Punktów Kontaktowych informacje o incydentach. Zespoły realizują te zadania poprzez współpracę pomiędzy sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem. Monitorują zagrożenia cyberbezpieczeństwa i incydenty na poziomie krajowym, szacują ryzyko z nimi związane. Mogą również wydawać komunikaty o zidentyfikowanych zagrożeniach.

CSIRT mają obowiązek informować się wzajemnie oraz Rządowe Centrum Bezpieczeństwa o incydencie krytycznym, który może spowodować wystąpienie sytuacji kryzysowej dla bezpieczeństwa lub porządku publicznego. Zespoły wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu, w ramach którego współpracują ze sobą.

Ustawa wprowadza również pojęcie **sektorowego zespołu cyberbezpieczeństwa**, a więc zespołu ustanowionego przez organ właściwy dla danego sektora lub podsektora (wymienionego w załączniku do ustawy). Zespół ten odpowiedzialny jest za obsługę lub wsparcie obsługi incydentów w swoim sektorze lub podsektorze.

Kolejnym organem ustanowionym nowym prawem jest **Zespół ds. Incydentów Krytycznych**, który pełni rolę pomocniczą w sprawach obsługi incydentów krytycznych zgłoszonych przez sieć CSIRT. W skład Zespołu wchodzą przedstawiciele Rządowego Centrum Bezpieczeństwa oraz CSIRT MON, CSIRT NASK i Szefa ABW. Kierowany jest przez dyrektora RCB.

W myśl europejskiej Dyrektywy utworzono **Pojedynczy Punkt Kontaktowy (PKK)**, który funkcjonuje przy Ministrze Cyfryzacjii jest odpowiedzialny za:

- tworzenie ram prawnych funkcjonowania obszaru cyberbezpieczeństwa RP, w tym czuwanie nad ich spójnością;
- pełnienie funkcji łącznika w celu zapewnienia współpracy z podmiotami odpowiedzialnymi za cyberbezpieczeństwo;

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

- gromadzenie i przetwarzanie informacji otrzymanych od m.in. operatorów usług kluczowych;
- kontrolowanie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymagań organizacyjnych i technicznych;
- przekazywanie, na wniosek właściwego CSIRT, zgłoszenia incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych innych państwa członkowskich UE;
- zapewnienie udziału przedstawiciela RP w Grupie Współpracy;
- zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa;
- koordynację współpracy między organami właściwymi ds. cyberbezpieczeństwa RP z odpowiednimi organami w państwach członkowskich UE;
- współpracę z innymi organami np. organami ścigania i organem właściwym do spraw ochrony danych[4].

Podmiotem odpowiedzialnym za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w RP jest Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa. Obecnie jego funkcję pełni minister Karol Okoński. Główne zadania Pełnomocnika to m.in.: analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa, opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa, wydawanie rekomendacji, a także inicjowanie krajowych ćwiczeń z zakresu cyberbezpieczeństwa. Pełnomocnik ma obowiązek przedłożyć Radzie ministrów do 31 marca każdego roku sprawozdanie za poprzedni rok kalendarzowy, zawierające informacje o prowadzonej działalności w zakresie zapewniania cyberbezpieczeństwa w kraju.

Przy Radzie Ministrów powołano **Kolegium do Spraw Cyberbezpieczeństwa**. Jest to organ opiniodawczo-doradczy w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Powołanie Kolegium miało na celu zachowanie większej spójności systemu i jego transparentność oraz nadanie zagadnieniom cyberbezpieczeństwa odpowiedniej rangi jak i umożliwienie formułowania spójnych kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa.

Opracowanie i przyjęcie **Strategii Cyberbezpieczeństwa** jest narzucone przez zapisy ustawy z 5 lipca 2018 r. (rozdział 13). Natomiast art. 90 określa termin wprowadzenia Strategii uchwałą do 31 października 2019 r. Dokument określa cele strategiczne oraz odpowiednie środki polityczne, których celem jest osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa RP. Pojawiła się również **konieczność dokonania oceny i przeglądu** w 2019 r. dotychczasowego dokumentu o charakterze strategicznym, czyli przyjętych uchwałą Nr 52/2017 Rady Ministrów z 27 kwietnia 2017 r. **Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022** oraz wynikającego z tego Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Stale zmieniające się uwarunkowania związane z bezpieczeństwem, szczególnie w cyberprzestrzeni, wymagają szybkiej i zdecydowanej reakcji organów państwa. Jak dowiadujemy się ze strony Kancelarii Prezesa Rady Ministrów: *Projektowana uchwała ma na celu ustanowienie Strategii Cyberbezpieczeństwa. Strategia ma charakter polityczno-strategiczny, natomiast na poziomie operacyjnym realizację jego zapisów zapewni szczegółowy plan działań. Plan działań opisze podmioty zaangażowane w realizację Strategii oraz środki pozwalające na jej wdrożenie. Przy opracowywaniu Strategii korzystano z dobrych praktyk i rozwiązań proponowanych przez Międzynarodowy Związek Telekomunikacyjny oraz doświadczeń innych państw*[5].

W 2018 r. NIK przeprowadziła kontrolę w zakresie zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Wyniki kontroli wykazały brak dostatecznej świadomości wśród osób pełniących funkcję organu KSC, jak istotna jest tematyka bezpieczeństwa informacji. Wykazano

[4] https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-

[5] https://bip.kprm.gov.pl/kpr/wykaz/r953654207552,Projekt-uchwaly-Rady-Ministrow-w-sprawie-Strategii-Cyberbezpieczenstwa-Rzeczypos.html.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

także brak środków finansowych, aby realizować niezbędne przedsięwzięcia oraz niedostateczną liczbę fachowców z zakresu bezpieczeństwa informacji.

DZIAŁANIA MINISTERSTWA CYFRYZACJI

Celem przygotowanej przez Ministerstwo Cyfryzacji ustawy o krajowym systemie cyberbezpieczeństwa było opracowanie uregulowań prawnych umożliwiających implementacje dyrektywy NIS oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym. Aby stało się to rzeczywistością, Pełnomocnik Rządu współpracuje z różnymi podmiotami w ukierunkowanych działaniach, np.:

- z organami właściwymi w zakresie szkoleń;
- z zespołami CSIRT w zakresie wytycznych;
- z jednostkami samorządu terytorialnego w zakresie szkoleń i e-learningu;
- z partnerami technologicznymi w zakresie wymiany informacji o nowych zagrożeniach i technologiach.

NASK-PIB dostał za zadanie przeprowadzenie działań podnoszących świadomość o cyberzagrożeniach wśród kadr administracji publicznej. Realizowane będą dwa podzadania:

1. **Budowa platformy e-learningowej (e-CTP – Cyber Training Platform) dla kadr administracji publicznej, w tym jednostek samorządu terytorialnego**.

Testy platformy mają odbywać się jesienią tego roku w chętnym do współpracy urzędzie marszałkowskim, a pełne uruchomienie platformy ma nastąpić w 2020 r. Urzędy będą sukcesywnie zapraszane do korzystania z e-learningu zgodnie z harmonogramem ustalonym przez MC. Zakłada się, że platforma będzie udostępniana czasowo dla danego urzędu. W tym czasie nie będzie dostępna dla innych. Planowane jest także uruchomienie do projektu call center wspierającego platformę.

2. **Stacjonarne szkolenia dla wybranych jednostek samorządu terytorialnego z obowiązków wynikających z ustawy o KSC.**

Celem szkoleń jest zwiększenie poziomu bezpieczeństwa w organach administracji publicznej i instytucjach samorządowych poprzez podnoszenie świadomości i budowanie kompetencji w zakresie cyberbezpieczeństwa. Zakłada się organizację czterech spotkań informacyjnych (zorganizowane poprzez cztery wybrane/chętne do współpracy urzędy marszałkowskie), które obejmą łącznie ok. czterystu pracowników urzędów na szczeblu gminy i powiatu odpowiedzialnych za cyberbezpieczeństwo. Termin realizacji to wrzesień-grudzień 2019 r. Kolejne urzędy mają dołączyć do szkoleń stacjonarnych w 2020 r.

Obydwa zadania projektu wspierane będą przez trzy zespoły NASK-PIB: Akademię NASK, IT Szkołę i CSIRT NASK. Koordynację zapewnia Departament Cyberbezpieczeństwa MC.

Następnym aspektem działań rozwijających KSC jest współpraca technologiczna. Jest ona szczególnie ważna ze względu na nawiązywane umowy dwustronne z partnerami technologicznymi i wymianę informacji (podatność, zagrożenia, narzędzia monitoringu stanu cyberbezpieczeństwa). Jednak to nie wszystkie zabiegi na rzecz budowy silnego systemu cyberbezpieczeństwa w Polsce. W ramach projektu badawczego utworzona została **Narodowa Platforma Cyfrowa**, która zakłada stworzenie prototypu kompleksowego, zintegrowanego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach cyberprzestrzeni państwa, ocenę potencjalnych skutków oraz skoordynowane reagowanie na incydenty komputerowe na poziomie krajowym. Poprzez ten projekt Minister Cyfryzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

- wymianę informacji na potrzeby współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
- generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
- zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym;
- ostrzeganie o zagrożeniach cyberbezpieczeństwa.

NASK opracowuje ponadto poradniki, które poruszają tematykę organizacji KSC, zasad zgłaszania incydentów i ochronę danych osobowych. Publikowane są również na stronach MC, a ich celem jest szerokie rozpowszechnienie wiedzy i budowanie kompetencji.

Kolejną inicjatywą jest **Partnerstwo dla Cyberbezpieczeństwa** – narzędzie dobrowolnej współpracy i wymiany doświadczeń oraz informacji o zagrożeniach cyberbezpieczeństwa i incydentach. Podstawowym założeniem partnerstwa jest: wymiana

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

informacji z zakresu cyberbezpieczeństwa, wymiana informacji o incydentach i istotnych zagrożeniach, które wykraczają (wg Partnera) poza zdarzenia wewnętrzne, zapewnienie odpowiedniej reakcji i postępowania w rozwiązywaniu problemów. W ramach uczestnictwa w programie, członkowie mogą:

- przekazywać do NASK informacje o incydentach;
- informować koordynatora programu (NASK) o zaobserwowanych zagrożeniach;
- dzielić się wiedzą z zakresu cyberbezpieczeństwa;
- zainicjować powołanie zespołu zadaniowego.

W ramach programu, na który obecnie składa się ponad pięćdziesiąt trójstronnych porozumień, podpisano siedem umów z samorządami na poziomie wojewódzkim (urzędy marszałkowskie).

Zapewnianie cyberbezpieczeństwa w Polsce i budowanie odpornego systemu to nieustanny proces. Warto zauważyć, że staje się on coraz bardziej świadomy i zaplanowany, mimo pojawiających się wyzwań i trudności. Oprócz tych wskazanych po kontroli NIK, można mówić także o braku dostatecznej liczby ekspertów na rynku, trudnościach z ujednoliceniem przepisów związanych z różnorodnością sektorów, różnych interpretacjach prawa i stawianych wymaganiach. Niemniej jednak wprowadzenie Strategii na jesieni tego roku oraz działania podjęte przez Ministerstwo Cyfryzacji mogą przyspieszyć wypracowanie odpowiednich mechanizmów zapewniających cyberbezpieczeństwo w Polsce.

Wykorzystanie podejścia usługowego przy wyłanianiu infrastruktury krytycznej

Witold Skomra

Rządowe Centrum Bezpieczeństwa

Konieczność ochrony infrastruktury krytycznej wiąże się ze zjawiskiem stopniowego uzależniania się społeczeństwa od zdobyczy cywilizacji. Proces ten prowadzi niekiedy do sytuacji, gdy zakłócenie funkcjonowania IK jest traktowane jako zagrożenie o charakterze publicznym, przy czym granice pomiędzy zadaniami realizowanymi przez administrację publiczną i sektor prywatny mogą ulegać zatarciu. Podmioty biznesowe coraz częściej bazują na danych, procesach i aplikacjach dostarczanych przez administrację, zaś administracja nie jest w stanie realizować swoich zadań bez współudziału sektora prywatnego. Jednocześnie utrzymuje się podział odpowiedzialności za skutki braku usług, od których zależy komfort życia społecznego. Przedsiębiorcy odpowiadają za bezpośrednie skutki własnej działalności i ewentualnie ponoszą koszty związane z wypłatą kar umownych. Skutki społeczne braku podstawowych dóbr i usług, zwłaszcza, gdy wiążą się z naruszeniem bezpieczeństwa publicznego, obciążają administrację publiczną.

Podstawowe urządzenia i instytucje, niezbędne do funkcjonowania gospodarki i społeczeństwa, noszą encyklopedyczną nazwę „infrastruktura", zaś ta infrastruktura, której dysfunkcja powoduje naruszenie bezpieczeństwa publicznego nosi nazwę infrastruktury krytycznej (w skrócie IK). Warto zwrócić uwagę, że pojęcie „infrastruktura" nie musi się odnosić do obiektu fizycznego. Według ustawy o zarządzaniu kryzysowym, infrastrukturą krytyczną mogą być zarówno obiekty, w tym obiekty budowlane, urządzenia, instalacje, ale także usługi, o ile mają kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli albo służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Tak szeroki zakres potencjalnych obiektów IK i stosowanie przy ich opisie tak niejednoznacznych pojęć jak „poważny wpływ" czy „kluczowe znaczenie" powodują, że proces wyłaniania IK jest trudny i wielostopniowy. W myśl Narodowego Programu Ochrony Infrastruktury Krytycznej, wyłanianie obiektu IK odbywa się w trzech etapach. W pierwszym etapie ustala się, do którego systemu należy potencjalny obiekt IK i porównuje się jego cechy z kryteriami danego systemu (kryteria te są niejawne). W kroku drugim sprawdza się, czy dany obiekt pełni rolę, o której mowa w definicji IK. W trzecim kroku analizie podlegają potencjalne skutki dysfunkcji danego obiektu. O ile obiekt spełnia kryteria

etapu pierwszego i drugiego, a jednocześnie potencjalne skutki jego dysfunkcji są nieakceptowane, uznaje się ten obiekt za infrastrukturę krytyczną.

Równolegle funkcjonuje odmienne podejście do wyłaniania infrastruktury o istotnym znaczeniu dla funkcjonowania społeczeństwa. W myśl ustawy o krajowym systemie cyberbezpieczeństwa, wyłania się nie obiekty IK, lecz operatorów usług kluczowych. W tym rozumieniu usługa kluczowa to taka, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i jest wymieniona w wykazie usług kluczowych. Natomiast decyzję uznającą podmiot za operatora usługi kluczowej wydaje się o ile:

- podmiot świadczy usługę kluczową;
- świadczenie tej usługi zależy od systemów informacyjnych;
- incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.

Zasięg tej regulacji jest mocno ograniczony, gdyż odnosi się wyłącznie do usług ujętych w ustawie (bez możliwości dołączenia innych) i to tylko takich, które bazują na systemach informacyjnych. Ich zależność od innych czynników (np. od dostaw prądu) nie jest brana pod uwagę.

Opisany powyżej dualizm jest wynikiem funkcjonowania dwóch, niespójnych dyrektyw UE. Dyrektywa w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[1] nakazuje podejście obiektowe, podczas gdy dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[2] wprowadza podejście usługowe. Już sam fakt jednoczesnego funkcjonowania dwóch różnych podejść do wyłaniania IK wskazuje, że brak jest jednolitej metodyki w tej sprawie. Ponadto w obu przypadkach istnieje problem z jednoznacznym wskazaniem, które podmioty potencjalnie mogą spełniać kryteria zaliczające do IK lub usług kluczowych. Ustawa o zarządzaniu kryzysowym enigmatycznie wspomina, że wykaz obiektów sporządza dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z odpowiednimi ministrami odpowiedzialnymi za poszczególne systemy (ustawa o ZK art. 5b, ust. 7 pkt. 1). Natomiast ustawa o krajowym systemie cyberbezpieczeństwa w załączniku nr 1 wymienia 6 obszarów, w których funkcjonujące podmioty powinny być brane pod uwagę jako potencjalni operatorzy usług kluczowych. Oba podejścia nie są wprost powiązane ani z funkcjami państwa, ani z potrzebami obywateli. Dlatego z góry można założyć, że istnieją obiekty i usługi o istotnym czy wręcz krytycznym znaczeniu, które nie zostały uwidocznione ani w wykazie obiektów IK, ani w wykazie operatorów usług kluczowych. Oba podejścia mają jeszcze jedno ograniczenie. Wyłanianie operatora usługi kluczowej i obiektu IK odbywa się w odniesieniu do jego roli w rozumieniu państwa jako całości. Pomija się natomiast operatorów, których działalność ma krytyczne znaczenie dla społeczności lokalnych.

Rozwiązaniem powyższych dylematów może być oparcie procesu wyłaniania IK o podejście usługowe. W tym podejściu dla każdego z 11 systemów wymienionych w ustawie sporządza się katalog usług krytycznych z podziałem na usługi lokalne i krajowe. Przy czym usługi krytyczne to usługi, do których dostęp zapewnia administracja publiczna, a których zakłócenie mogłoby skutkować naruszeniem bezpieczeństwa publicznego. Zapewnienie dostępu do usługi nie musi oznaczać, że administracja samodzielnie ją dostarcza. Równie dobrze może ją kupować od podmiotów biznesowych (np. usługi zdrowotne) albo zapewniać dostęp poprzez regulację danego rynku (np. dostęp do telefonu 112). Zapewnienie dostępu do usług krytycznych można powiązać z potrzebami, które można podzielić na potrzeby indywidualne (np. ratownictwo), grupowe (np. transport publiczny) i narodowe (np. rejestry państwowe)[3].

Dla każdej z usług należy sporządzić kryteria pozwalające ocenić przy jakich warunkach usługa ma znaczenie krytyczne i czy jest to usługa krytyczna dla społeczności lokalnej czy dla całego państwa. Dopiero po tym etapie można wskazać operatora lub operatorów usługi krytycznej. Określenie „operatorów" zostało użyte celowo, gdyż często działalność kilku

[1] Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dz. Urz. UE L 345/75.

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE L 194/1.

[3] M. Bennett, V. Gupta, Dealing in Security understanding vital services and how they keep you safe, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

podmiotów jednocześnie pozwala na utrzymanie jednej usługi.

Przedstawiony schemat postępowania jedynie pozornie wydaje się prosty. We współczesnym świecie poszczególne systemy są wzajemnie zależne i bez wiedzy o tych zależnościach trudno wyrokować, jak zakłócenie u jednego operatora wpływa na działalność kolejnego. W efekcie, wystąpienie efektu domina jest coraz trudniejsze do przewidzenia. Generalnie przy opisie współzależności pomiędzy poszczególnymi rodzajami infrastruktury krytycznej i pomiędzy nią a administracją można wykorzystać następującą klasyfikację (Rinaldi i in. 2001):

- współzależność fizyczna – fizyczne połączenie wyjścia i wejścia, przykładowo usługa lub produkt dostarczane przez jedną infrastrukturę są niezbędne by inna infrastruktura mogła funkcjonować;
- współzależność cyfrowa – działalność infrastruktury jest uzależniona od informacji przesyłanych systemami transmisji danych;
- współzależność geograficzna – kilka obiektów lub rodzajów infrastruktury znajduje się w swoim bezpośrednim sąsiedztwie (w efekcie zagrożenie w jednym obiekcie może oddziaływać na pozostałe);
- współzależność logiczna – dwa lub więcej rodzajów infrastruktury wzajemnie na siebie oddziałuje bez żadnego powiązania fizycznego, cyfrowego czy geograficznego.

Oczywiście nie da się w jednym kroku wytypować operatorów bezpośrednio dostarczających usługi krytyczne i tych, którzy są niezbędni, ale w sposób pośredni. Dlatego zamiana sposobu wyłaniania IK z podejścia systemowo-obiektowego na podejście systemowo-usługowe będzie procesem wieloletnim, uzależnionym od rozpoznawania współzależności pomiędzy systemami. Jednak jego przeprowadzenie pozwoli poszerzyć pojęcie kompleksowej ochrony IK o kompleksową ochronę obiektów i systemów, od których dana IK jest uzależniona. W efekcie, optyka „chronimy ważne obiekty" zostanie poszerzona o optykę „budujemy społeczeństwo odporne na zakłócenia". I właśnie budowanie odporności powinno być głównym przesłaniem Narodowego Programu Ochrony Infrastruktury Krytycznej w nowym wydaniu.

Literatura:

1. Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. Dz. U. z 2018 r. poz. 1401 ze zm.)
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE L 194/1.
3. Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dz. Urz. UE L 345/75.
4. M. Bennett, V. Gupta, Dealing in Security understanding vital services and how they keep you safe, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf.
5. Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) przyjęty uchwałą nr 210/2015 Rady Ministrów z 2 listopada 2015 r., http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf (online 11.09.2017).
6. Rinaldi S.M., Peerenboom J.P., Kelly T.K. *Identifying, understanding, and analyzing critical infrastructure interdependencies*. IEEE Control Systems Magazine 2001:11-25.
7. Skomra W., 2018. Panowanie nad ryzykiem w ramach publicznego zarządzania kryzysowego, Warszawa Bel Studio.
8. Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Konflikty o charakterze hybrydowym – prawo jako narzędzie walki

Kamil Stobnicki
Rządowe Centrum Bezpieczeństwa

Walka z zagrożeniami hybrydowymi to szeroki problem, wymagający kompleksowego i wszechstronnego podejścia. Odnosi się właściwie do wszystkich dziedzin i obszarów życia społecznego. Zakres potencjalnych działań w samej cyberprzestrzeni, rozumianej jako nowy wymiar bezpieczeństwa międzynarodowego i nowa płaszczyzna walki, wydaje się praktycznie nieograniczony. Dodatkowo, wrogie działania prowadzone w jednym obszarze rzutują na funkcjonowanie innych. Np. seria cyberataków wymierzona w infrastrukturę krytyczną może kaskadowo doprowadzić do napięć politycznych, społecznych czy ekonomicznych w atakowanym hybrydowo państwie.

Zjawiska charakterystyczne dla konfliktu hybrydowego są nie tylko wyjątkowo trudne do sklasyfikowania, ale też mogą być w różny sposób interpretowane przez poszczególne państwa i organizacje bezpieczeństwa, co istotnie komplikuje ich zwalczanie. Działania hybrydowe, które w zasadzie są prowadzone w czasie pokoju, znacząco utrudniają więc reakcję podmiotów, przeciwko którym są skierowane. Czy wobec tak wielu niewiadomych w ogóle możliwa jest walka z zagrożeniami hybrydowymi w oparciu o prawo międzynarodowe, zwłaszcza humanitarne, skoro nie występuje w nim nawet definicja „hybrydowości"?

Zarówno wśród teoretyków, jak i praktyków prawa toczy się dyskusja, w jaki sposób sklasyfikować zdarzenia, które określa się ogólnie mianem „hybrydowych". Pojawiają się głosy, że współczesne prawo nie jest w stanie sprostać wyzwaniom wynikającym ze zjawiska, które gen. Walerij Gierasimow, szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, określił jako „wojna nowej generacji"[1]. Jedną ze wskazywanych przyczyn jest fakt, iż większość aktów prawnych dotyczących użycia siły i konfliktów zbrojnych powstawała wówczas, gdy pojęcie „wojna hybrydowa" nie zostało jeszcze szerzej przyjęte, a za najważniejszych aktorów konfliktów zbrojnych uważane były państwa[2].

Jednak są również przedstawiciele świata prawniczego, którzy widzą problem zupełnie gdzie indziej. Uważają oni, że chociaż we współczesnych konfliktach hybrydowych występują istotne, nowe elementy (jak np. działania w cyberprzestrzeni), prawo międzynarodowe zawiera mimo wszystko normy i reguły postępowania pozwalające na skuteczne odniesienie się do poszczególnych zjawisk, składających się na taki konflikt[3]. Większość z nich, w tym działania dywersyjne, sabotażowe, porwania, korupcja czy cyberprzestępczość, zostało opisanych w różnych aktach prawnych, w szczególności w międzynarodowym prawie humanitarnym[4]. Wprawdzie regulacje te nie są zebrane w jednym dokumencie, rezolucji czy deklaracji, nie powinno to jednak stanowić przeszkody w egzekwowaniu przestrzegania istniejących norm prawnych wobec podmiotów, odwołujących się do hybrydowej metody prowadzenia konfliktów[5].

[1] M. Wojnowski, Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, „Przegląd Bezpieczeństwa Wewnętrznego" 13/15.
William Hague, b. minister spraw zagranicznych Wielkiej Brytanii (w rządzie D. Camerona) uważa, że w obliczu takiej taktyki stosowanej przez Rosję, NATO potrzebuje nowych definicji pojęć: „atak" i „obrona", a także nowego artykułu do Traktatu uwzględniającego kolektywną odpowiedź w reakcji na atak hybrydowy, [w:] William Hague, NATO must confront Putin's stealth attacks with a new doctrine of war of its own, The Telegraph (Mar. 19, 2018).

[2] A. Kleczkowska, Wojna hybrydowa – uwagi z perspektywy prawa międzynarodowego publicznego, „Sprawy Międzynarodowe", PISM, nr 2/2015, str. 99.

[3] Większość elementów wymienianych jako modelowe przykłady „wojny hybrydowej" wykorzystywana była od wieków w międzynarodowych konfliktach np.: prowokacje w celu znalezienia pretekstu do agresji, działania dywersyjne i sabotażowe, presja ekonomiczna czy różne formy propagandy.

[4] Konwencje Genewskie (ostatnia z 12 sierpnia 1949 r.) oraz Protokoły dodatkowe I i II z 1977 r. do Konwencji Genewskich z 12 sierpnia 1949 r.

[5] Przykładem aktów prawa międzynarodowego odnoszących się do stosunkowo nowego obszaru cyberprzestrzeni może być Konwencja Rady Europy o cyberprzestępczości (ustawa z dnia 12.09. 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie w dniu 23.11. 2001 r.; Dz. U. 2014, poz. 1514) lub unijna dyrektywa NIS

Kwestią nastręczającą szczególnie wiele wątpliwości prawnych są działania podejmowane w cyberprzestrzeni, niezależnie od faktu, iż istnieją dokumenty międzynarodowe zawierające wyraźne odniesienia do tego obszaru. Pogląd, że prawo międzynarodowe ma tu swoje zastosowanie, został bowiem potwierdzony m.in. w dokumentach Zgromadzenia Narodowego Organizacji Narodów Zjednoczonych (UN GGE 2013 report A/68/98, pkt. 19, 20; UN GGE 2015 report, A/70/174[6]), czy w oświadczeniach takich organizacji jak NATO (w deklaracji końcowej ze Szczytu w Newport, pkt. 72; oraz kolejno podczas Szczytów w Warszawie, pkt. 70 i Brukseli, pkt. 20) i Unia Europejska (Wspólny Komunikat do Parlamentu Europejskiego i Rady, Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej, pkt. 4.1)[7]. Zostało to również zaakcentowane w tzw. Poradniku Tallińskim (Tallinn Manual on the International Law Applicable to Cyber Warfare), będącym analizą prawa międzynarodowego w odniesieniu do cyberprzestrzeni[8].

Niezależnie od tego, czy prawo pozwala na skuteczną walkę ze współczesnymi zagrożeniami, faktem jest używanie go przez aktorów państwowych i niepaństwowych jako środka realizacji swoich celów[9]. Koncepcja ta znana jest pod pojęciem „lawfare". Podobnie jak w przypadku zagrożeń hybrydowych, dla terminu lawfare nie przyjęto jednej, uniwersalnej definicja[10]. Przyjmuje się, że prawo używane jest jako substytut tradycyjnie pojmowanych metod i środków prowadzenia walki. Co ważne, jest to nie tyle używanie, co nadużywanie i manipulowanie instrumentarium prawnym. W tym kontekście prawo jest bronią, a więc narzędziem do osiągania celów przez adwersarza[11]. Taka interpretacja pojęcia lawfare zakłada, iż prawo traktowane jak broń staje się narzędziem służącym do realizacji interesów m.in. grup terrorystycznych, państw posługujących się środkami terrorystycznymi, a także państw wrogich systemom demokratycznym, które wykorzystują instytucje prawne w celu spowolnienia lub zablokowania państwom demokratycznym procesu decyzyjnego. Podmioty posługujące się tego typu metodami używają narracji prawnej, aby zaprezentować swoje działania jako mieszczące się w istniejących ramach prawnych, które jednocześnie nie przekraczają akceptowalnego progu legalności.

System prawny – nawet jeśli jest niedookreślony – stanowi nieodłączny element wojny hybrydowej, jako jeden z obszarów, w obrębie którego prowadzone są działania podprogowe[12]. Przybiera to praktyczny wymiar w przypadku np. działań podejmowanych w celu zamaskowania wyraźnego naruszenia danego traktatu, Karty Narodów Zjednoczonych czy konwencji ONZ, nawet jeśli działania te stanowią niezgodne z prawem użycie siły. Z prawnego punktu widzenia, kluczową kwestią w podejściu do zagrożeń hybrydowych jest zacieranie przez aktorów państwowych lub niepaństwowych wyraźnego, tradycyjnego rozgraniczenia między stanem pokoju a stanem wojny. I tak np. w kwestii Krymu w 2014 r. Federacja Rosyjska uzasadniła swoją interwencję na półwyspie jako działanie mające na celu ochronę praw rosyjskich obywateli, zapewnienie bezpieczeństwa rosyjskiej Flocie Czarnomorskiej i odpowiedź na prośby o pomoc wojskową skierowane

(w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, 2016/1148/UE, przyjęta 6 lipca 2016 r).

[6] Raporty opracowane przez grupę ekspertów rządowych ds. rozwoju w dziedzinie informatyki i telekomunikacji w kontekście bezpieczeństwa międzynarodowego (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security). Podkreślono m.in., że działalność państw i ich infrastruktury informacyjno-komunikacyjnej, zlokalizowanej na ich terytorium, podlega zarówno Karcie Narodów Zjednoczonych, jak i pozostałym przepisom prawa. Obecnie prawo międzynarodowe pozwala na legalne użycie siły w ramach samoobrony w odpowiedzi na poważny atak zbrojny i proporcjonalnie do poniesionej szkody.

[7] Dokument z dnia 13 września 2017 r., pkt. 4.1. […] *UE silnie propaguje stanowisko, w myśl którego prawo międzynarodowe, a w szczególności Karta Narodów Zjednoczonych, ma zastosowanie w odniesieniu do cyberprzestrzeni*. W tym samym punkcie pojawia się również nawiązanie do wyżej wymienionych dokumentów sporządzonych przez grupę ekspertów rządowych ONZ.

[8] *Poradnik został opracowany przez NATO Cooperative Cyber Defense Centre of Excellence. Dokument odnosi się m.in do kwestii stosowania prawa do operacji cybernetycznych w czasie pokoju oraz do działań, które nie przekraczają progu działań zbrojnych, ale są naruszeniem prawa międzynarodowego.*

[9] *A. Sari, Legal Resilience in an Era of Grey Zone. Conflicts and Hybrid Threats, 2019.*

[10] *Pojęcie użyte po raz pierwszy przez Major General Charlie Dunlap, C. Dunlap, Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts.*

[11] *The path to legal resilience, [w:] Exeter Conference on Legal Resilience, NATO ACO Office of Legal Affairs, s. 20, 2019.*

[12] Agresja podprogowa to działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

przez władze Autonomicznej Republiki Krymu[13] i przebywającego już wówczas w Rosji Wiktora Janukowycza[14]. Przeciwnik może więc wykorzystywać prawo instrumentalnie – do legitymizowania swoich działań oraz poszerzania ich swobody i zakresu, albo do delegitymizowania działań rywala i ograniczenia tym samym jego swobody[15]. To właśnie zrobiła Rosja podczas aneksji Krymu – podważała legalność ukraińskich działań, jednocześnie usprawiedliwiając swoje.

Temat instrumentalnego traktowania prawa jest dziś bardzo aktualny, szczególnie jeżeli spojrzymy na miejsca, gdzie toczą się konflikty. 5 maja 2019 roku armia izraelska (Israel Defense Forces, IDF) poinformowała o zniszczeniu atakiem lotniczym m.in. budynku, z którego Hamas przeprowadził cyberatak na nieokreślone cele na terenie Izraela. Z jednej strony atak ten został uznany za precedens, z drugiej jednak kwestionuje się jego legalność[16]. Militarna akcja odwetowa (obejmująca atak lotnictwa Izraela na około 260 celów należących do Hamasu i Islamskiego Dżihadu[17]), zdaniem wielu komentatorów, stanowiła przekroczenie nieprzekraczalnej do tej pory granicy[18]. W bezpośredniej odpowiedzi na operację prowadzoną w cyberprzestrzeni, został zainicjowany atak z użyciem broni kinetycznej. Przykład ten stanowi doskonałą ilustrację zasygnalizowanych wyżej wątpliwości prawnych. Obie strony – świadome braku jasnego i klarownego uregulowania w prawie kwestii cyberataków i potencjalnej odpowiedzi konwencjonalnej – realizują swoje cele, interpretując przepisy na swoją korzyść, to jest legitymizując swoje działania, jednocześnie delegitymizując poczynania przeciwnika.

Łatwość wykorzystywania aspektów prawnych do osiągania celów strategicznych sprawia, że do metody tej chętnie sięgają nie tylko państwa, lecz także podmioty niepaństwowe, świadome wysokiej wrażliwości zachodnich społeczeństw na prawa i wolności człowieka oraz prawa zagwarantowane w międzynarodowym prawie humanitarnym. Za przykład może tu posłużyć podręcznik w języku angielskim (Manchester Manual), znaleziony w domu członka Al-Kaidy podczas przeszukania w 2001 r., który zawierał instrukcje, jak należy wykorzystywać zachodnie przepisy prawa na korzyść zamachowców m.in. dla zakwestionowania legalności zatrzymania czy stosowanych metod przesłuchania[19].

Odpowiedzią na tego rodzaju wykorzystywanie podatności prawnej przeciwnika jest poprawa stopnia odporności prawnej (legal resilience), będąca z jednej strony zdolnością systemu prawnego do przetrwania i adaptacji w obliczu zagrożeń hybrydowych, z drugiej zaś stanowiąca część kompleksowego podejścia w przeciwdziałaniu zagrożeniom tego typu[20]. W pełni słuszne wydaje się stwierdzenie, iż tak, jak prawo wykorzystywane jest przez podmioty, które chcą podważyć czy zakwestionować obecny ład międzynarodowy, tak powinno stać się ono orężem w ręku tych, którzy tego ładu bronią. Prawo powinno stanowić integralną część kompleksowej odpowiedzi na zagrożenia o charakterze hybrydowym. Służyć temu może m. in. precyzyjne zdefiniowanie terminów takich jak: agresja podprogowa, próg wojny, działania prowadzone w cyberprzestrzeni czy presja militarna.

Za klasyczne przykłady uregulowań prawnych, mających zastosowanie w sytuacji przekroczenia przez przeciwnika tzw. czerwonej linii, uznawane są art. 5 Traktatu Północnoatlantyckiego, a także art. 42(7) Traktatu o Unii Europejskiej czy art. 222 Traktatu o funkcjonowaniu Unii Europejskiej. Przytoczone zapisy spełniają dwie podstawowe funkcje – wyrażają formalne zobowiązanie sygnatariuszy do wzajemnej pomocy, a zarazem są jasnym przesłaniem dla potencjalnego agresora, że wrogie działania spotkają się ze zbiorową reakcją.

[13] *O taką pomoc wystąpił samozwańczy Premier Siergiej Aksjonov, mianowany na tą pozycję z naruszeniem ukraińskiego prawa – kandydatury na stanowisko premiera Autonomicznej Republiki Krymu powinien przedstawiać prezydent Ukrainy.*

[14] *Wiktor Janukowycz stracił władzę na mocy decyzji parlamentu z 22 lutego 2014 roku. Rada Najwyższa Ukrainy uznała, że „samowolnie usunął się" od pełnienia funkcji szefa państwa.*

[15] *Aurel Sari, Dear Geneva: Let's talk hybrid warfare, https://www.gcsp.ch/global-insight/dear-geneva-lets-talk-hybrid-warfare.*

[16] R. Chesney, *Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility,* https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.

[17] *Setki rakiet spadło na Izrael. W odwecie zaatakowano cele w Strefie Gazy, Radio Zet, https://wiadomosci.radiozet.pl/Swiat/Izrael-odpowiedzial-na-atak-ze-Strefy-Gazy.-Wczesniej-200-rakiet-wystrzelil-Hamas.*

[18] Nie ma publicznej wiedzy, czy był to pierwszy przypadek użycia śmiercionośnej broni w odpowiedzi na operację w cyberprzestrzeni, ale był to pierwszy przypadek, kiedy strona odpowiadająca na cyberatak publicznie się do tego przyznała. Dotychczas oficjalnymi krokami odwetowymi były akcje również w cyberprzestrzeni.

[19] The path to legal resilience, op. cit s. 20.

[20] A. Sari, *Legal Resilience in an Era of Grey Zone. Conflicts and Hybrid Threats*, 2019, s. 19.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

W przypadku art. 5 i art. 42(7) obowiązek udzielenia pomocy jest uwarunkowany odpowiednio – zbrojną napaścią (armed attack) lub aktem zbrojnej agresji (armed aggression). Należy zaznaczyć przy tym, że próg ataku zbrojnego jest określany wyżej niż próg użycia siły, przeciwnik hybrydowy może zatem wykorzystać tę lukę, prowadząc swoje operacje na poziomie intensywności poniżej poziomu ataku zbrojnego[21].

Szczególnego znaczenia opisywane zjawisko lawfare nabiera w kontekście asymetrycznego charakteru współczesnych konfliktów. Jego istotą jest unikanie bezpośredniej konfrontacji na polu walki (omijanie obszarów, gdzie przeciwnik ma zdecydowaną przewagę) i posługiwanie się niekonwencjonalnymi metodami w postaci terroryzmu, wojny informatycznej, psychologicznej, ekonomicznej, informacyjnej, ale również samego prawa. Powszechność konfliktów asymetrycznych przyczyniła się w znacznej mierze do tego, że ludność cywilna staje się i celem, i ofiarą. Podmioty podejmujące takie działania w większym stopniu nadużywają prawa międzynarodowego, które tym samym nie jest w stanie zapewnić skutecznej ochrony ludności cywilnej. Częstym przykładem przywoływanym w tym kontekście jest wykorzystywanie osób cywilnych jako żywych tarcz (human shields) przez podmioty niepaństwowe, organizacje terrorystyczne i grupy zbrojne. Odbywa się to przy instrumentalnym wykorzystaniu międzynarodowego prawa humanitarnego, które zabrania użycia siły, jeżeli występują wątpliwości co do obecności osób cywilnych w zasięgu rażenia[22]. Organizacje terrorystyczne stosują tego rodzaju środki dla zabezpieczenia się przed ewentualnymi atakami, mając świadomość uwrażliwienia państw zachodu na przestrzeganie międzynarodowego prawa humanitarnego. Jednocześnie, w razie ataku, wykorzystują fakt ofiar wśród cywili do walki informacyjnej. W ostatnich latach, zarówno na forum ONZ jak i w poszczególnych krajach, podejmowane są wysiłki na rzecz rozwiązań prawnych ułatwiających ściganie stosowania takich metod.

Reasumując – koncepcja lawfare zakłada systematyczne wykorzystywanie zidentyfikowanych luk w regulacjach prawnych. Zacieranie granicy jawnego łamania prawa powoduje trudność w wykryciu tego procederu, a ponadto kreuje pewną dwuznaczność w jego interpretacji. Z tego względu zarówno państwa jak i organizacje międzynarodowe, w ramach swoich kompetencji, powinny na bieżąco udoskonalać ramy prawne adekwatnie do postępujących zagrożeń. Celem jest uniknięcie sytuacji, w której fakt przestrzegania przepisów prawa staje się dla podmiotów międzynarodowych słabością czy jedną z podatności na zagrożenia.

[21] Taktyka takich działań prowadzona jest m.in. przez Chiny oraz Rosję – wymuszające realizację swoich interesów poprzez użycie siły odpowiednio przez chińskie kutry rybackie czy jednostki paramilitarne na Morzu Południowochińskim względem łodzi i statków innych państw (toczących spory terytorialne na tym akwenie), a także rosyjski sprzęt wojskowy bez oznakowań państwowych w okręgu Donieckim i Ługańskim. Takimi operacjami poniżej progu zbrojnej agresji jest również zaopatrywanie w broń czy inna pomoc logistyczna siłom rebelianckim w państwie trzecim.

[22] M.in. wprowadzenie restrykcyjnych zasad użycia siły przez siły powietrzne NATO w 2007 roku w odniesieniu do misji w Afganistanie.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Służba kontrterrorystyczna w Policji

Mariusz Cichomski, Michał Horoszko
Ministerstwo Spraw Wewnętrznych i Administracji

Od 2016 roku na poziomie prawno-organizacyjnym dokonano kluczowych zmian dotyczących funkcjonowania polskiego systemu antyterrorystycznego. Wprowadzone zostały one przede wszystkim ustawą z 10 czerwca 2016 r. o działaniach antyterrorystycznych, która zmieniła również 31 innych ustaw regulujących tę problematykę. Nie można jednak zapomnieć o innych istotnych regulacjach w odniesieniu do zagrożeń terrorystycznych, które przyjęte zostały w tym okresie, w tym w szczególności ustawie z 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych, nowelizacji ustawy z 6 czerwca 1997 r. – Kodeks karny w zakresie wzmocnienia narzędzi prawych dotyczących przeciwdziałania finansowaniu terroryzmu oraz walki z tzw. cudzoziemskimi bojownikami czy ustawie z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Ustawa o działaniach antyterrorystycznych wprowadziła jasny podział zadań wykonywanych w poszczególnych fazach działań antyterrorystycznych. Zgodnie z jej przepisami, za zapobieganie zdarzeniom o charakterze terrorystycznym odpowiada Szef Agencji Bezpieczeństwa Wewnętrznego, natomiast za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym, reagowanie w przypadku wystąpienia takich zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia – minister właściwy do spraw wewnętrznych.

Regulacją tą wprowadzono również zmiany w ustawie z 6 kwietnia 1990 r. o Policji poprzez wskazanie wprost wśród zadań Policji prowadzenia działań kontrterrorystycznych[1]. Dostosowano również do rzeczywistych potrzeb przesłanki użycia oddziałów i pododdziałów Sił Zbrojnych RP do pomocy oddziałom i pododdziałom Policji[2].

Ustawa o działaniach antyterrorystycznych określiła ponadto szczegółowy mechanizm koordynacji działań na miejscu zdarzenia o charakterze terrorystycznym poprzez wyraźne wskazanie Policji jako służby odpowiedzialnej co do zasady za kierowanie działaniami antyterrorystycznymi na miejscu zdarzenia[3].

Ustawa o działaniach antyterrorystycznych wprowadziła również powszechnie obowiązujący i dostosowany do wymogów NATO czterostopniowy system stopni alarmowych na wypadek zagrożeń terrorystycznych oraz stopni alarmowych CRP w cyberprzestrzeni. Obowiązki wynikające z wprowadzenia stopni alarmowych zostały określone w rozporządzeniu Prezesa Rady Ministrów z 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP, które określa szczegółowy zakres przedsięwzięć wykonywanych w ramach kompetencji ustawowych przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego w poszczególnych stopniach alarmowych.

Z perspektywy Policji, wśród przedsięwzięć przewidzianych do realizacji po wprowadzeniu pierwszego stopnia alarmowego należy w szczególności zwrócić uwagę na obowiązek

[1] Art. 1 ust. 2 pkt 3a *ustawy z 6 kwietnia 1990 r. o Policji.*

[2] W art. 18 *ustawy o Policji* jednoznacznie wskazano w tym zakresie, że pomoc taka może być udzielona w zagrożeniu przestępstwem o charakterze terrorystycznym, mogącym skutkować niebezpieczeństwem dla życia lub zdrowia uczestników wydarzeń o charakterze kulturalnym, sportowym lub religijnym, w tym zgromadzeń lub imprez masowych, co ma szczególne znaczenie w kontekście organizowanych w Polsce imprez masowych oraz istotnych spotkań o charakterze międzynarodowym. Użycie Sił Zbrojnych RP nie musi ponadto wystąpić dopiero w sytuacji, kiedy siły i środki Policji okazały się niewystarczające, lecz już w przypadku, gdy ocena sytuacji wskazuje, że mogą okazać się niewystarczające. Analogiczne rozwiązanie wprowadzono w odniesieniu do możliwość użycia żołnierzy Żandarmerii Wojskowej przy udzieleniu pomocy Policji w razie zagrożenia bezpieczeństwa i porządku publicznego (art. 18a *ustawy o Policji*) – jeżeli siły Policji są niewystarczające lub mogą okazać się niewystarczające do wykonania ich zadań w zakresie ochrony bezpieczeństwa i porządku publicznego.

[3] W przypadku zdarzenia o charakterze terrorystycznym na obszarach lub w obiektach należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej rola kierującego działaniami przysługuje żołnierzowi Żandarmerii Wojskowej.

prowadzenia wzmożonej kontroli dużych skupisk ludności, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym, w tym imprez masowych i zgromadzeń publicznych. Natomiast w przypadku wprowadzenia drugiego stopnia alarmowego Komendant Główny Policji, Komendant Główny Straży Granicznej lub Komendant Główny Żandarmerii Wojskowej wprowadzają obowiązek noszenia broni długiej oraz kamizelek kuloodpornych przez umundurowanych funkcjonariuszy lub żołnierzy bezpośrednio realizujących zadania związane z zabezpieczeniem miejsc i obiektów, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym. Wśród przedsięwzięć przewidzianych do realizacji w tym stopniu alarmowym znalazły się również m.in.: wprowadzenie dodatkowych kontroli pojazdów, osób oraz budynków publicznych w rejonach zagrożonych, sprawdzenie ochrony ważnych obiektów publicznych, wzmocnienie ochrony środków komunikacji publicznej, czy wprowadzenie zakazu wstępu do przedszkoli, szkół i uczelni osobom postronnym.

Z systemem stopni alarmowych powiązany został system udzielania niezbędnego wsparcia ze strony Sił Zbrojnych RP w przypadku jeśli siły i środki służb bezpieczeństwa i porządku publicznego mogłyby okazać się niewystarczające do reagowania w przypadku zamachu.

Zgodnie z rozporządzeniem wydanym na podstawie art. 22 ust. 10 ustawy o działaniach antyterrorystycznych[4], oddziały Sił Zbrojnych Rzeczypospolitej Polskiej wydzielone do pomocy oddziałom Policji mogą być użyte w szczególności do: działań antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym, w tym działań kontrterrorystycznych; osłony lub izolacji określonych obiektów, dróg, wydzielonych ulic lub części miast; ochrony obiektów infrastruktury krytycznej; działań przywracających bezpieczeństwo i porządek publiczny. Rolę organu koordynującego działania pełni – w przypadku działań podejmowanych przez Policję oraz Siły Zbrojne RP na obszarze jednego województwa – właściwy miejscowo komendant wojewódzki Policji, zaś w przypadku działań podejmowanych na obszarze większym niż jedno województwo – Komendant Główny Policji.

W celu zapewnienia optymalnych warunków realizacji zadań wynikających z wiodącej roli Policji w zakresie działań kontrterrorystycznych, konieczne stało się określenie nowych mechanizmów dysponowania sił i środków jednostek kontrterrorystycznych na terytorium całego państwa oraz wprowadzenie jednolitej struktury dowodzenia. Niezbędne było także ujednolicenie taktyki działania oraz poziomu wyszkolenia tych jednostek. Dopełnienie zapoczątkowanych ustawą o działaniach antyterrorystycznych zmian w tym zakresie stanowi ustawa z 9 listopada 2018 r. o zmianie ustawy o Policji oraz niektórych innych ustaw. Została ona opracowana między innymi w oparciu o doświadczenia Policji uzyskane w ramach współpracy z państwami stowarzyszonymi w Grupie ATLAS, zrzeszającej europejskie jednostki kontrterrorystyczne. Tym samym stanowi odpowiedź na zmieniający się charakter zagrożeń o charakterze terrorystycznym w Europie, wymagający lepszej koordynacji działań Policji oraz jednolitego, wysokiego poziomu wyszkolenia jednostek kontrterrorystycznych.

Funkcjonujące przy komendach wojewódzkich Samodzielne Pododdziały Antyterrorystyczne Policji – a wcześniej także Sekcje Antyterrorystyczne – traktowane były przez lata jako jednostki służące wsparciu służby kryminalnej i śledczej, między innymi podczas zatrzymań szczególnie niebezpiecznych sprawców. Nie były zatem przygotowane do pełnego zaangażowania w realizację działań kontrterrorystycznych. Dotychczasowy system organizacyjny w praktyce zakładał więc, że działania kontrterrorystyczne realizowane będą przez Biuro Operacji Antyterrorystycznych Komendy Głównej Policji, które zlokalizowane jest w Warszawie. Rozwiązanie to nie było adekwatne w kontekście specyfiki współczesnych zagrożeń o charakterze terrorystycznym, które wymagają natychmiastowego reagowania. Zarówno działające centralnie BOA, jak i funkcjonujące na poziomie wojewódzkim jednostki kontrterrorystyczne powinny być zdolne jak najszybciej dotrzeć na miejsce zdarzenia i gwarantować spójność działania.

Realizując te założenia ustawa wyodrębnia w ramach Policji służbę kontrterrorystyczną. Zgodnie z nowym art. 5c ust. 1 ustawy o Policji, służba ta jest odpowiedzialna za prowadzenie działań

[4] Rozporządzenie Rady Ministrów z 21 lipca 2016 r. w sprawie *szczegółowych warunków i sposobu organizacji współdziałania oddziałów i pododdziałów Policji z oddziałami i pododdziałami Sił Zbrojnych w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego* (Dz. U. poz. 1087).

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

kontrterrorystycznych oraz wspieranie działań jednostek organizacyjnych Policji w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił i środków oraz specjalistycznej taktyki działania. Ma to na celu zarówno zwiększenie możliwości reagowania na zagrożenia o charakterze terrorystycznym, jak i usprawnienie działań innych jednostek Policji związane z realizacją szczególnie niebezpiecznych czynności.

Służba składa się z Centralnego Pododdziału Kontrterrorystycznego Policji „BOA" oraz samodzielnych pododdziałów kontrterrorystycznych Policji. BOA podlega bezpośrednio Komendantowi Głównemu Policji, a obsługę czynności wspomagających BOA w zakresie organizacyjnym, kadrowym, logistycznym i technicznym zapewnia Komenda Główna Policji.

Samodzielne pododdziały kontrterrorystyczne Policji podlegają natomiast bezpośrednio właściwym miejscowo komendantom wojewódzkim (lub Komendantowi Stołecznemu Policji) i umiejscowione są przy komendach wojewódzkich. Na co dzień mogą one więc być wykorzystywane do wsparcia działań Komend Wojewódzkich Policji. Rozwiązania przewidziane w ustawie zakładają przy tym usprawnienie procedur ich dysponowania i zwiększenie zdolności do realizacji działań kontrterrorystycznych. Mianowicie, w przypadku wystąpienia zdarzenia o charakterze terrorystycznym działania kontrterrorystyczne są przez te pododdziały realizowane przed innymi zadaniami[5]. Kluczowym elementem zapewniającym skuteczność działań kontrterrorystycznych jest bowiem szybkość reagowania i możliwość zapewnienia adekwatnych sił policyjnych.

W celu ujednolicenia systemu funkcjonowania oraz organizacji samodzielnych pododdziałów kontrterrorystycznych Policji, ustawa przypisała BOA kompetencje w zakresie koordynowania, przygotowania i realizacji działań kontrterrorystycznych w Policji, w tym kierowania do działań samodzielnych pododdziałów kontrterrorystycznych Policji[6]. Tym samym BOA będzie sprawować merytoryczny nadzór nad realizacją działań bojowych i szkoleniowych oraz wykorzystaniem sił i środków samodzielnych pododdziałów kontrterrorystycznych Policji.

Kluczowe jest także zapewnienie jednolitego standardu wyszkolenia w służbie kontrterrorystycznej, a także odpowiedniej struktury etatowej tych pododdziałów. Szczegółowe rozwiązania w tym zakresie określa na podstawie przepisów ustawy[7] Komendant Główny Policji.

Istotnym elementem proponowanych rozwiązań jest też zapewnienie odpowiednich kwalifikacji kadry dowódczej służby kontrterrorystycznej. W tym zakresie przyjęto rozwiązanie, zgodnie z którym dowódca BOA i jego zastępcy, a także dowódcy oraz zastępcy dowódców samodzielnych pododdziałów kontrterrorystycznych Policji powoływani są spośród oficerów służby kontrterrorystycznej. Dowodzenie działaniami kontrterrorystycznymi wymaga bowiem szczególnej wiedzy i doświadczenia. Mogą one zostać nabyte jedynie podczas pełnienia służby w pododdziale kontrterrorystycznym, z czym wiąże się realizacja czynności z wykorzystaniem specjalistycznej taktyki i w warunkach zagrożenia życia.

Podsumowując, wprowadzone rozwiązania przyznają BOA narzędzia pozwalające sprawować merytoryczny nadzór nad realizacją działań bojowych i szkoleniowych samodzielnych pododdziałów kontrterrorystycznych Policji oraz wykorzystaniem ich sił i środków do działań kontrterrorystycznych. Dzięki temu możliwe będzie zapewnienie jednolitego poziomu wyszkolenia i wyposażenia jednostek kontrterrorystycznych, a także zwiększenie sprawności reagowania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym.
Zasadnicze przepisy ustawy z 9 listopada 2018 r. o zmianie ustawy o Policji oraz niektórych innych ustaw obowiązują od 5 kwietnia 2019 r. Natomiast przepisy szczególne dotyczące warunków bezpieczeństwa i higieny służby weszły w życie 5 lipca 2019 r[8].

[5] Art. 5c ust. 12 *ustawy o Policji.*

[6] Art. 5c ust. 10 *ustawy o Policji*.
[7] Odpowiednio art. 7 ust. 1 pkt 12 i 11 *ustawy o Policji.*
[8] Art. 9 *ustawy z dnia 9 listopada 2018 r. o zmianie ustawy o Policji oraz niektórych innych ustaw.*

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

System zarządzania kryzysowego w Estonii

Republic of Estonia Government Office

Reforma systemów obrony i zarządzania kryzysowego została zainicjowana w 2011 r. przez estońskie Ministerstwo Spraw Wewnętrznych w wyniku zmian zachodzących w środowisku bezpieczeństwa. Ważną częścią tej reformy jest zdefiniowanie na nowo zagrożeń i scenariuszy oraz wprowadzenie wymogu regularnego organizowania ogólnokrajowych, międzysektorowych ćwiczeń zarządzania kryzysowego na poziomie polityczno-strategicznym.

Nowa ustawa o zarządzaniu kryzysowym, która weszła w życie 1 lipca 2017 r. stała się podstawą wprowadzenia szeroko zakrojonych zmian w dziedzinie zarządzania kryzysowego w Estonii. Innowacje koncepcyjne i wdrożenie rozwiązań prawnych spowodowały modyfikację dotychczasowych wytycznych i metodologii, a wiele zadań z dziedziny zarządzania kryzysowego zostało wskazanych po raz pierwszy.

Zgodnie z definicją ustawową, zarządzanie kryzysowe obejmuje zapobieganie kryzysom, przygotowanie się do nich, opracowanie planów kryzysowych oraz łagodzenie skutków kryzysów, a także zapewnienie nieprzerwanych dostaw usług kluczowych. W ustawodawstwie estońskim istnieją zasadniczo cztery rodzaje sytuacji kryzysowych. Sytuację kryzysową ogłasza się w przypadku wystąpienia klęski żywiołowej lub choroby zakaźnej. Stan wyjątkowy jest wprowadzany, gdy istnieje zagrożenie dla porządku konstytucyjnego. W przypadku, kiedy zagrożenie dla bezpieczeństwa Estonii wzrasta, ogłasza się podniesienie gotowości obronnej. Wreszcie w przypadku agresji zewnętrznej wprowadzany jest stan wojenny. Każdy z czterech rodzajów sytuacji kryzysowych ma swoją własną strukturę dowodzenia i zarządzania. Poniższe opracowanie dotyczy kryzysów i sytuacji kryzysowych o charakterze cywilnym.

Przez kryzys rozumie się zdarzenie lub serię zdarzeń, które zagrażają życiu bądź zdrowiu wielu ludzi, powodują duże szkody materialne, poważne szkody dla środowiska, a także zakłócenia usług kluczowych na dużą skalę. Aby przeciwdziałać kryzysom niezbędne jest podjęcie dodatkowych środków lub zastosowanie nietypowej organizacji zarządzania. Wystąpienie kryzysu w jakiejś konkretnej dziedzinie lub obszarze nie jest podawane do wiadomości, czy też ogłaszane przez właściwe władze. O tym, czy faktycznie mamy do czynienia z kryzysem, decyduje podmiot wskazany jako odpowiedzialny za prowadzenie działań w danym przypadku. Kryzysy są rozwiązywane na poziomie właściwych agencji (instytucji) lub przez dostawców usług kluczowych.

Rząd może ogłosić sytuację kryzysową w celu opanowania kryzysu w przypadku klęski żywiołowej, katastrofy lub rozprzestrzeniania się choroby zakaźnej na dużą skalę. Po ogłoszeniu sytuacji kryzysowej, rząd wyznacza jednego ministra do zarządzania tą sytuacją i określa koordynatora reagowania kryzysowego. Taka procedura na szczeblu rządowym sprawia, że osoby zarządzające sytuacją kryzysową i koordynujące reagowanie kryzysowe mają więcej uprawnień, m. in. mogą zobowiązać innych obywateli do wykonywania określonych prac czy wprowadzić ograniczenia w ruchu na niektórych obszarach. O terminie ogłoszenia i odwołania sytuacji kryzysowej decyduje rząd.

Zarządzanie kryzysowe w Estonii opiera się na czterech podstawowych zasadach. Pierwszą z nich jest zdecentralizowana zasada ciągłości. Zakłada ona, że organizacja odpowiedzialna na co dzień za dany obszar, odpowiada również za niezbędne przygotowania na wypadek zagrożenia oraz za zarządzanie zdarzeniami nadzwyczajnymi na tym obszarze. Kolejną zasadą jest zasada współpracy oznaczająca, że władze, przedsiębiorstwa lub agencje (instytucje) ponoszą niezależnie odpowiedzialność za zapewnienie możliwie najlepszej współpracy z odpowiednimi partnerami w zakresie działań związanych z zapobieganiem, osiągnięciem gotowości i zarządzaniem kryzysowym. Z kolei zasada pomocniczości mówi o tym, że pod względem organizacyjnym kryzysy należy rozwiązywać na możliwie jak najniższym poziomie. Ostatnią z czterech podstawowych zasad jest zasada podobieństwa – działanie organizacji w czasie kryzysu powinno być jak najbardziej zbliżone do jej normalnego (codziennego) funkcjonowania.

PRZYGOTOWANIE SIĘ NA WYPADEK KRYZYSÓW

W ramach przygotowania się na wypadek wystąpienia kryzysów sporządza się analizę ryzyka. W opracowaniu analizy ryzyka współpracują różne podmioty, co umożliwia dokonanie spójnej oceny głównych zagrożeń, jak również ich możliwych konsekwencji. Oceniana jest również zdolność do rozwiązywania sytuacji nadzwyczajnych. Analiza ryzyka jest przygotowywana co dwa lata. Jej elementem jest zestawienie środków ograniczających ryzyko. Odnosi się to do działań poszczególnych ministerstw w zakresie zapobiegania kryzysom oraz łagodzenia ich ewentualnych skutków.

REAGOWANIE NA KRYZYS

W celu przeciwdziałania poważnym wypadkom i kryzysom, tworzy się plany reagowania kryzysowego. Plany te określają strukturę zarządzania kryzysowego, zadania zaangażowanych podmiotów lub osób, zarządzanie wymianą informacji, a także zasady i sposób realizacji powiadamiania ludności o zagrożeniach. Plany te opisują również organizację współpracy międzynarodowej. Plany reagowania kryzysowego są zatwierdzane decyzją rządu estońskiego. Ocena i ewentualna aktualizacja planów reagowania kryzysowego przeprowadzana jest raz w roku. Poniższa tabela zawiera przegląd scenariuszy kryzysowych, dla których opracowano plany reagowania kryzysowego.

Tabela 1. Scenariusze kryzysowe

Kryzysy spowodowane zjawiskami naturalnymi	• kryzysy spowodowane przez burze; • powodzie na gęsto zaludnionych obszarach; • wielkoobszarowe pożary lasów.
Kryzysy na lądzie	• pożar na dużą skalę lub wybuch w budynku przemysłowym; • katastrofa pociągu skutkująca dużą liczbą ofiar lub znaczącymi szkodami dla środowiska naturalnego; • zdarzenie w ruchu drogowym z dużą liczbą ofiar; • wypadek drogowy skutkujący znaczącymi szkodami dla środowiska naturalnego.
Kryzysy na morzu	• wypadek morski z wieloma ofiarami; • wypadek z wieloma ofiarami spowodowany tworzeniem się lub topnieniem lodu.
Kryzysy w środowisku naturalnym	• zanieczyszczenia morskie na dużą skalę; • zanieczyszczenie spowodowane materiałami radioaktywnymi lub nuklearnymi; • zanieczyszczenie wód śródlądowych lub wód podziemnych.
Kryzysy dotyczące bezpieczeństwa i porządku publicznego	• masowe zamieszki; • zdarzenie z zakładnikami; • atak z zaskoczenia.

Źródło: *Ustawa o zarządzaniu kryzysowym, 2017 r.*

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

USŁUGI KLUCZOWE

Usługi kluczowe to takie, których przerwanie zagrażałoby życiu lub zdrowiu ludzi, sparaliżowałoby funkcjonowanie państwa lub zmniejszyłoby poziom bezpieczeństwa publicznego. Dostawcy takich usług zobowiązani są do zapobiegania zakłóceniom lub, w razie konieczności, zapewnienia szybkiego przywrócenie usług.

Instytucje państwowe i przedsiębiorstwa mają określone zadania związane z zapewnieniem funkcjonowania usług, na przykład przygotowanie analizy ryzyka w odniesieniu do usług i opracowania konkretnych planów. W Estonii za kluczowe uważa się 14 usług. Wymienione są one w § 36 Ustawy o zarządzaniu kryzysowym.

Tabela 2. Kluczowe usługi i odpowiedzialne instytucje

Ministerstwo Gospodarki i Łączności	• dostawy energii elektrycznej; • dostawy gazu ziemnego; • dostawy paliw płynnych; • zapewnienie funkcjonalności przejezdności dróg krajowych; • funkcjonowanie usług telefonicznych; • funkcjonowanie telefonii komórkowej; • usługa transmisji danych; • identyfikacja cyfrowa i podpis cyfrowy.
Ministerstwo Spraw Społecznych	• system ratownictwa medycznego
Bank Estonii	• usługi płatnicze; • przepływ gotówki.
Samorządy	• zapewnienie przejezdności dróg lokalnych; • funkcjonowanie lokalnego systemu grzewczego; • funkcjonowanie systemu wodno-kanalizacyjnego.

Źródło: Ustawa o zarządzaniu kryzysowym, 2017 r.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l