

OPERACJA KONTRTERRORYSTYCZNA – WYBRANE ELEMENTY BEZPIECZEŃSTWA INFORMACYJNEGO

Informacje odgrywają kluczową rolę w powodzeniu wszelkich działań, stanowiąc o ich sukcesie. Dlatego też zapewnienie odpowiedniego poziomu bezpieczeństwa informacyjnego operacji kontrterrorystycznej wydaje się być jej nieodzownym elementem. Mając jednak na uwadze jej specyfikę, działanie w sytuacji kryzysowej, wymagającej nieprzerwanego dostępu do informacji i współdziałania wielu różnych służb i instytucji, przyjęte procedury ochrony informacji muszą przede wszystkim wspierać proces decyzyjny dowodzenia.

Określenie problemu

Przeciwdziałanie zagrożeniom terrorystycznym i zwalczanie ich przejawów nazywane jest najczęściej działaniami antyterrorystycznymi. Nie jest to jednak podejście w pełni właściwe. W tym momencie należy zgodzić się z jednym z najwybitniejszych polskich badaczy tej problematyki – prof. Kubą Jałoszyńskim. Wskazuje on na fakt, że **ogół działań należy nazywać antyterroryzmem**, na który składają się **przedsięwzięcia defensywne**, mające na celu zmniejszenie podatności – **antyterrorystyczne**, oraz **ofensywne**, podjęte w celu prewencji, odstraszenia i odpowiedzi – **kontrterrorystyczne**.¹ Za takim podziałem przemawia także lektura światowej literatury przedmiotu. Pierwsze bezpośrednio kojarzone są z kwestiami bezpieczeństwa informacyjnego, gdyż ich głównym zadaniem jest uzyskiwanie, analizowanie, wykorzystanie i gromadzenie informacji. Ponadto realizowane są w głównej mierze przez służby specjalne o charakterze informacyjnym (wywiadowcze i kontrwywiadowcze). Drugie, oparte na działaniach bojowych w aspektach: ratunkowym (najczęściej w sytuacjach zakładniczych) i eliminacyjnym (zatrzymanie bądź likwidacja osób podejrzanych o działalność terrorystyczną), mają znacząco odmienny odbiór. Spowodowane może to być, m.in. także faktem, że realizowane są one przez siły specjalne pododdziałów

¹ Jałoszyński K.: *Współczesny wymiar antyterroryzmu*, Warszawa: Wydawnictwo TRIO – Collegium Civitas, 2008, s. 98.

(oddziałów) antyterrorystycznych, jako wiodących. Zgodnie z przyjętą wcześniej terminologią należy jej jednak określać mianem pododdziałów kontrterrorystycznych.²

Podobnie kształtuje się ujęcie problemów bezpieczeństwa informacyjnego w kontekście walki z terroryzmem w literaturze. Najczęściej podejmowanym problemem jest więc **znaczenie informacji dla skuteczności działań antyterrorystycznych** (defensywnych), a jeżeli dotyczy także działań ofensywnych to w większości na poziomie ich planowania. Zauważalny jest tym samym **brak analizy zagadnienia ochrony i zarządzania informacją w procesie dowodzenia operacją kontrterrorystyczną, szczególnie w aspekcie sytuacji kryzysowej**. Dlatego też tym artykułem chciałbym podjąć się chociażby zarysowania kilku jego podstawowych elementów.

Dowodzenie – aspekt informacyjny

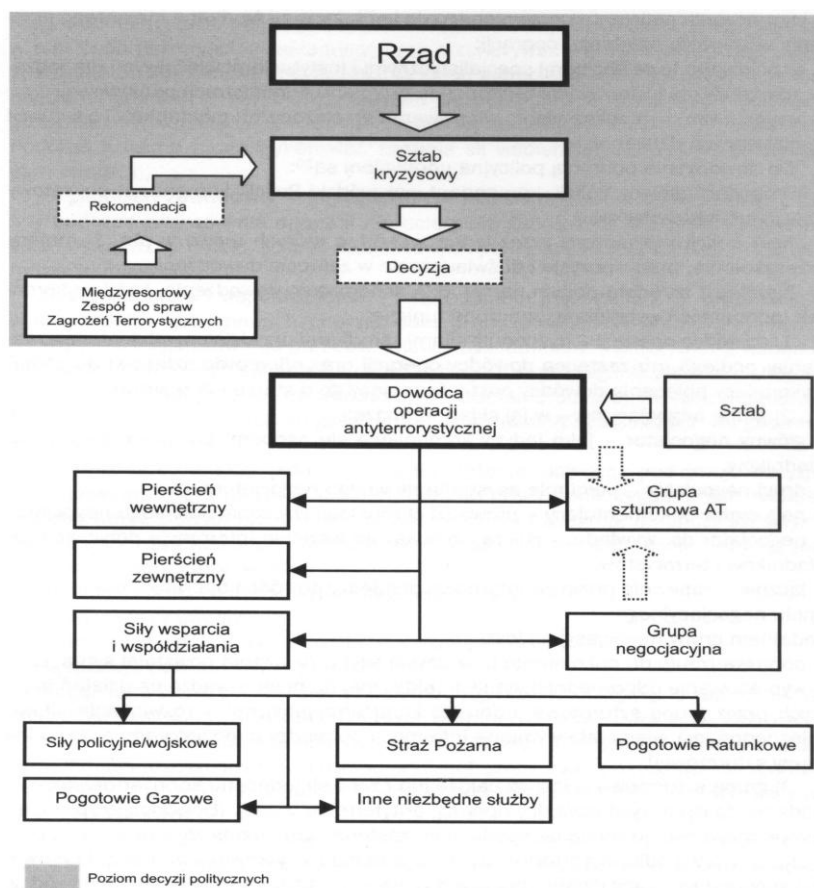
Dowodzenie jest to **specyficzna forma zarządzania**, odnosząca się do sformalizowanych i hierarchicznych struktur wojskowych czy policyjnych. Niemniej jednak opiera się na tych samych założeniach – **podejmowaniu decyzji w celu osiągnięcia wyznaczonego celu**, i w ten sam sposób **zależne jest od zmiennego otoczenia informacyjnego**.

Przez dowodzenie, w naszym przypadku operacją antyterrorystyczną, należy rozumieć **ukierunkowaną, celową działalność dowódcy, zapewniającą wysoką zdolność sił i środków do osiągnięcia celu tych działań oraz charakteryzującą się sprawnym, jednoosobowym podejmowaniem decyzji i ponoszeniem za nie odpowiedzialności, precyzyjnym rozdziałem i kontrolą przebiegu czynności**³.

W uproszczeniu można by powiedzieć, że **dowodzenie to sztuka osiągania celów za pomocą innych ludzi, której istota opiera się na komunikacji i kierowaniu przepływem informacji** (decyzji i rozkazów). Idealnie obrazuje ten proces decyzyjny schemat przedstawiony obok, wskazuje on bezpośrednio na znaczenie bezpiecznych kanałów informacyjnych dla jego skuteczności, stanowiąc tło dla dalszych rozważań.

² Tamże, s. 101.

³ Zarządzenie nr 213 KGP z dn. 28.02.2007r. w sprawie metod i form przygotowania i realizacji zadań Policji w przypadkach zagrożenia życia i zdrowia ludzi lub ich mienia albo bezpieczeństwa i porządku publicznego (Dz.Urz. KGP nr 5, poz. 49).



Rysunek 1. Proces decyzyjny w rozwiązywaniu sytuacji kryzysowej związanej z zamachem terrorystycznym.

Źródło: Jałoszyński K.: *op.cit.*, s. 255.

O znaczeniu informacyjnym procesu dowodzenia operacją, świadczy także jego zakres, który w szczególności obejmuje:

- **ocenę zagrożeń poprzez ustalenie jego rodzaju i przewidywanego rozwoju;**
- określeniu oraz koncentracji sił i środków niezbędnych do usunięcia zagrożenia;
- zorganizowaniu stacjonarnego lub ruchomego stanowiska dowodzenia;
- **zorganizowaniu łączności na potrzeby dowodzenia, współdziałania i alarmowania;**
- wyznaczeniu zadań dla odpowiedzialnych za realizację poszczególnych elementów akcji oraz koordynowaniu i kontrolowaniu przebiegu akcji;
- **wyznaczeniu uprawnionego do kontaktów ze środkami masowego przekazu w zakresie przebiegu akcji;**
- **współdziałaniu ze służbami specjalistycznymi i instytucjami właściwymi dla rodzaju zdarzenia oraz z właściwymi terytorialnie organami administracji publicznej;**

- **przygotowywaniu i przekazywaniu właściwemu przełożonemu meldunków o sytuacji i realizowanych działaniach.**⁴

Wszystkie te zadania w głównej mierze opierają się na **pozyskiwaniu, gromadzeniu, analizie i przekazywaniu (lub koordynowaniu obiegu) informacji.**

Atrybuty informacji w procesie decyzyjnym

Atrybuty informacji to jej **cechy jakościowe określające wartość dla osiągnięcia zamierzonego celu.** Znaczenie poszczególnych z nich zmienia się najczęściej wraz ze zmieniającym się otoczeniem procesu decyzyjnego (np. presja czasu, liczba i rozproszenie odbiorców).

W przypadku analizowanej sytuacji, za najważniejsze cechy bezpieczeństwa informacyjnego należy uznać:

- **Integralność** – właściwość oznaczająca, że informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób;
- **Rozliczalność** – właściwość pozwalająca na jednoznaczne przypisanie działań określonej podmiotowi;
- **Dostępność** – właściwość pozwalająca na możliwość uzyskania informacji niezbędnych dla podejmowania decyzji, niezależnie od tego, w jakim miejscu te informacje się znajdują;
- **Poufność** – to właściwość oznaczająca, że informacje nie zostaną udostępnione podmiotom nieupoważnionym.

Należy tu jednak stwierdzić, że **utrzymanie na wysokim poziomie wszystkich tych atrybutów w poruszanej sytuacji kryzysowej jest niemożliwe do osiągnięcia.** Największym wyzwaniem wydają się być zagwarantowanie niezbędnej (minimalnej) poufności.

Poufność operacji kontrterrorystycznej

Konieczność zapewnienia poufności informacjom przetwarzanym w trakcie realizacji operacji kontrterrorystycznej może wynikać z przepisów prawa, ale także, a może w szczególności, z potrzeb procesu decyzyjnego.

W pierwszym przypadku należy przede wszystkim określić z jakim rodzajem informacji możemy mieć do czynienia, wychodząc od dobra prawnie chronionego, które leży u celu operacji kontrterrorystycznej. W największym uproszczeniu jest to **interes państwa,**

⁴ Tamże.

zarówno w aspekcie **porządku publicznego, obronności, bezpieczeństwa**, jak również **stosunków międzynarodowych**, czy w niektórych przypadkach także **gospodarczy**. Oczywiście w bardzo wielu sytuacjach wynikający z zagrożenia dla jego bytu substancjalnego, jakim są **obywatele**. Na tej podstawie możemy bezpośrednio wywnioskować, że **informacje przetwarzane w związku z działaniami kontrterrorystycznymi należą do grupy informacji niejawnych**⁵. Mogą one stanowić zarówno tajemnicę państwową, jak również tajemnicę służbową, w zależności od ustalenia czy ich nieuprawnione ujawnienie może spowodować istotne zagrożenie, czy tylko narazić na szkodę wymienione interesy. W mojej ocenie, popartej analizą ostatnich wydarzeń, skłaniam się ku temu pierwszemu, wyższemu poziomowi ochrony. Niemniej jednak bez względu na wybrany rodzaj tajemnicy, **zapewnienie ustawowych środków ochrony informacji niejawnych w sytuacji dowodzenia operacją kontrterrorystyczną wydaje się być niemożliwe, lub znacząco utrudnione**. By nie wchodzić w szczegóły, wystarczy wskazać na podstawowe problemy, tj. **konieczność współdziałania (dostępu do informacji) wielu różnych służb i instytucji, bardzo wysoki priorytet (presja) czasu zdobywania i przetwarzania informacji, wykorzystywanie różnorodnych (dostępnych) kanałów transmisji (łączości)**, czy może najważniejszy jakim jest **świadome podejmowanie ryzyka i uwzględnianie niepewności**. Oczywiście nie może to oznaczać zupełnego ignorowania procedur ochrony informacji, w szczególności już tych będących składową decyzji o znaczeniu strategicznym dla wyniku realizowanej operacji. Stąd **poufność informacji należy w głównej mierze postrzegać przez pryzmat potrzeb samego procesu decyzyjnego**. Poparciem tego twierdzenia może być często spotykane podejście, że **decyzje operacyjne mają wartość, a więc należy im zapewnić poufność, tylko do momentu ich realizacji**.

W odniesieniu do przedstawionego schematu procesu decyzyjnego dowodzenia operacją kontrterrorystyczną na pierwszy plan wysuwają się dwa, wskazane już wyżej, elementy, które determinują poziom jej bezpieczeństwa informacyjnego, tj. dostępność informacji dla szerokiego grona odbiorców i środki ich transmisji (łączości).

W pierwszym przypadku ważnym problemem nie jest sama ilość odbiorców, ale raczej ich różnorodność. Dlatego też **należy jednoznacznie określić obszary działania, a tym samym rodzaj informacji niezbędnych do jego realizacji**. Pozwoli to na osiągnięcie zamierzonego poziomu poufności informacji strategicznych poprzez ograniczenie kręgu możliwych odbiorców, nie personalnie, ale z racji wykonywanych zadań. Jest to bezpośrednia realizacja nato'wskiej zasady wiedzy koniecznej – „**need to know**”.

Drugi – środki transmisji informacji, to nie tylko problem zapewnienia poufności, ale także ich szybkości i niezawodności. Na wstępie należy tu **odrzuć całkowicie możliwość przekazywania decyzji (rozkazów) w formie tradycyjnej (papierowej)**, jako nie spełniającej obu wskazanych postulatów. Następnie z tych samych powodów **zasadnym jest zrezygnować z wykorzystania tradycyjnych systemów łączności telefonicznej w sieci publicznej**. Także najpopularniejsze w działaniach służb policyjnych **radiotelefony**, choć dają

⁵ Ustawa z dn. 22.01.1999r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95 z późn. zm.).

właściwą szybkość komunikacji i względną niezawodność, to jednak **w kwestii poufności transmisji niestety nie wypadają najlepiej**. Oczywiście **niemożliwe jest całkowite ograniczenie łączności przy wykorzystaniu komunikatów głosowych**, z uwagi na specyfikę niektórych działań, jednak coraz częściej stosowanymi metodami transmisji informacji, których niezawodność, szybkość, a także możliwość szyfrowania została już wielokrotnie potwierdzona, są **teleinformatyczne komunikatory tekstowe**. Choć co do ich funkcjonalności także istnieją poważne zastrzeżenia. Bez względu jednak, który ze środków łączności wybierzemy jako podstawowy, musimy pamiętać o **dywersyfikacji kanałów informacyjnych**, najlepiej przy wykorzystaniu odmiennej technologii. Ponadto podobnie jak przy bezpieczeństwie osobowym, tak i w tym przypadku możliwe jest **stopniowanie użytkowanych systemów łączności w odniesieniu do znaczenia przekazywanych za ich pomocą komunikatów**.

Dezinformacja jako metoda ochrony informacji

Prowadzenie działań specjalnych, jak starałem się wcześniej przedstawić, może przysporzyć problemy w kwestii wykorzystania tradycyjnych metod zapewnienia odpowiedniego poziomu poufności przetwarzanych informacji, dlatego też coraz częściej stosowaną **techniką bezpieczeństwa informacyjnego jest dezinformacja**, lub **preparowanie informacji**. Wbrew pozorom, należy ona do najstarszych metod w dziejach ludzkości i polega na odpowiedniej zmianie prawdziwej informacji.

Celem takiego przekształcenia jest, w zależności od stosowanej metody:

- **ukrycie i zafałszowanie prawdziwej informacji;**
- **wprowadzenie w błąd przeciwnika;**
- **wywarcie zamierzonego wpływu na przeciwnika.⁶**

Możliwość realizacji dwóch ostatnich może być kluczowym elementem warunkującym powodzenie operacji, bez konieczności stosowania rozwiązań ostatecznych. W tym celu postulowane jest **właściwe „wykorzystanie” środków masowego przekazu, jako narzędzia dezinformacji**.

Tytułem zakończenia

Dowodzenie operacją kontrterrorystyczną niejednokrotnie wiązać się będzie z **podejmowaniem ryzyka określonych działań**. Decyzje, choć nie powinny, mogą być oparte na informacjach, których poziom bezpieczeństwa może być nieznany, na **subiektywnej ocenie sytuacji**, ze **świadomym uwzględnieniem niepewności i niebezpieczeństwa**. Wszystko to podyktowanej jest realizacją **celu głównego operacji – przywrócenia**

⁶ BĄCZEK P.: *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń: Wydawnictwo Adam Marszałek, 2006, s. 187-188.

akceptowalnego poziomu bezpieczeństwa. Niemniej jednak **nie można ignorować znaczenia bezpieczeństwa informacyjnego dla powodzenia całości działań,** zarówno od strony sprawności procesu decyzyjnego, jak również jego ochrony.

Oczywiście, jak łatwo można wywnioskować ze złożoności procesu decyzyjnego operacji kontrterrorystycznej, **zapewnienie bezpieczeństwa informacyjnego jest procesem skomplikowanym, wymagającym zastosowanie szerokiego spektrum środków technicznych i organizacyjnych dostosowanych do zmieniającego się dynamicznie otoczenia, jak również do znacznej różnorodności wykorzystywanych sił i środków.**