Andrzej ŻEBROWSKI

WALKA INFORMACYJNA WSPARCIEM TERRORYZMU ISLAMSKIEGO (wybrane aspekty)

Wstęp

Walka informacyjna zawsze była ważnym elementem ludzkiego działania, a szczególnie była widoczna w trwających konfliktach zbrojnych i pozazbrojnych. Jej skala i dynamika była (jest) zróżnicowana i zależy od wielu wzajemnie powiązanych elementów, które wdrażane w praktyczne działanie pozwalają na osiągnięcie założonych celów. Postęp w łączności i informatyce został zaadoptowany przez uczestników walki informacyjnej, których głównym celem jest uzyskanie przewagi informacyjnej nad przeciwnikiem i zakłócenie jego percepcji. Aktywnymi uczestnikami walki informacyjnej są m.in. organizacje terrorystyczne. W artykule uwzględnione zostały problemy dotyczące walki informacyjnej, która wspiera działania podejmowane przez organizacje terrorystyczne, oraz towarzyszące tej działalności zagrożenia dla bezpieczeństwa państwa.

Charakterystyka walki informacyjnej

Środowisko bezpieczeństwa międzynarodowego u progu XXI wieku, to pasmo kooperacji negatywnej i pozytywnej, z dominacją tej pierwszej. Trudno jednak prowadzić rozważania na temat zachodzących procesów w sferze bezpieczeństwa bez uwzględnienia następstw rozpadu dwubiegunowego podziału świata, globalizacji, przemian cywilizacyjnych, dynamiki i skali rozwoju przestępczości zorganizowanej o charakterze ponadnarodowym, terroryzmu międzynarodowego, wyścigu zbrojeń, czy dominacji Stanów Zjednoczonych w kształtowaniu międzynarodowej przestrzeni bezpieczeństwa. Tym złożonym i asymetrycznym zmianom towarzyszy wszechobecna walka informacyjna, która pozwala zainteresowanym państwom, grupom państw, czy organizacjom pozapaństwowym (np. terrorystycznym) na realizację swoich partykularnych celów strategicznych.

Wskazane wydarzenia wpisują się w obecną rzeczywistość, która jest przede wszystkim asymetryczna, zakłócająca równowagę w sferze bezpieczeństwa narodowego i międzynarodowego (w porównaniu z bipolarnym podziałem świata), różnorodna, zmienna i nieprzewidywalna. Można nawet postawić tezę, że jest chaotyczna i turbulentna.. W zachodzące zmiany wpisuje się walka informacyjna, która odgrywa coraz większą rolę w osobowej i technicznej przestrzeni bezpieczeństwa podmiotów państwowych i pozapaństwowych. Z jednej strony służy procesowi budowania bezpieczeństwa jednostki (narodu, państwa, podmiotów

pozapaństwowych), a z drugiej jest źródłem poważnych zagrożeń, których skala, dynamika i jakość zaskakuje praktycznie wszystkich. Jest skuteczna w procesie eskalacji napięć, jakie występują wzdłuż linii błędów i interesów (np. manipulowanie świadomością i psychiką społeczeństwa w skali globalnej – przyp. autora)[1].

Charakter i postać zagrożeń bezpieczeństwa w XXI wieku wynika przede wszystkim z wyzwań związanych z zachodzącymi ogólnoświatowymi procesami (mega trendami), jak: postępująca dyfuzja cywilizacyjno - kulturowa i towarzyszące jej globalizacja zjawisk i procesów społecznych, nabierających dynamikę ponadnarodowej struktury świata, kształtowanie się nowego ładu polityczno – gospodarczo – militarnego, gwałtowny postęp naukowo – techniczny, osiąganie przez cywilizację granic biosfery, przechodzenie od mechanistycznej do systemowej wizji świata oraz megatrend integracji lub zbieżności technicznej[2].

Mając na uwadze powyższe uogólnienia warto wskazać te zjawiska postrzegane w kategoriach szczególnych zagrożeń dla bezpieczeństwa narodowego i międzynarodowego, np.:[3]

- terroryzm sterowany przez państwa i organizacje narodowe (niepaństwowe),
- terroryzm religijny (w szczególności islamski), jako instrument praktyki politycznej,
- nowy terroryzm: cyberterroryzm, terroryzm ekologiczny, superterroryzm,
- zjawisko podatności państw, organizacji niepaństwowych, banków, instytucji międzynarodowych na możliwość destrukcyjnego informatycznego, elektronicznego, cybernetycznego oddziaływania,
- ruchy polityczne odwołujące się do agresywnego nacjonalizmu, rasizmu, ksenofobii i innych form nietolerancji,
- masowe migracje na tle ekonomicznym oraz zjawisko uchodźctwa politycznego,
- cyberprzestrzeń jako obszar konfliktu.

Strach przed każdym zagrożeniem jest niewątpliwie zróżnicowany, jednak strach związany z terroryzmem, jego nieprzewidywalnością, co do czasu i miejsca ataku, stosowanych form i metod, a przede wszystkim użytych środków, jest obecny w naszej codziennej rzeczywistości.

Państwa będące uczestnikami stosunków międzynarodowych angażują się w prowadzenie walki informacyjnej, która zawsze towarzyszy procesowi decyzyjnemu. W przypadku dominacji państw narodowych na jej prowadzenie monopol posiadały państwa. Przemiany systemowe zapoczątkowane na przełomie XX i XXI wieku na świecie związane m.in. z upadkiem bipolarnego podziału świata i zintensyfikowanymi procesami towarzyszącymi globalizacji (np. w sferach politycznej, społecznej, gospodarczej, wojskowej), to również zintensyfikowana działalność wielu podmiotów pozapaństwowych, która ma m.in. charakter

[1] M. S. Witecka, *Zagrożenia asymetryczne a technologie informacyjne*, „Zeszyt Problemowy Towarzystwo Wiedzy Obronnej" 2011, nr 4, s. 11.
[2] A. Dawidczyk, Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku, Warszawa 2001, s. 38.
[3] Ibidem.

przestępczy (np. organizacji terrorystycznych), a ich skala i umiędzynarodowienie stanowi poważny problem dla procesu zapewnienia bezpieczeństwa..

Walka informacyjna, to kooperacja negatywna wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej[4]. W innym ujęciu walka informacyjna, to przygotowanie, do użycia lub użyciem fizycznej lub cyfrowej broni dla dezorganizacji lub niszczenia informacji lub systemów informacyjnych w celu degradowania lub przerwania wykonywania funkcji, które zależą od informacji lub systemów informacyjnych[5]. Sugeruje się także definicję wojny informacyjnej na tyle obszerną, że mieszczą się w niej przestępstwa finansowe, działania wywiadowcze, oraz zagrożenia ze strony terrorystów i państw[6]. Z kolei dyrektywa Departamentu Obrony Stanów Zjednoczonych z grudnia 1996 roku, wojnę informacyjną określa jako operacje informacyjne prowadzone podczas kryzysu lub konfliktu w celu osiągnięcia lub poparcia konkretnych przeciwników lub przeciwnika[7]. Operacje informacyjne są to działania podjęte w celu wywarcia wpływu na informacje i systemy informacyjne przeciwnika przy jednoczesnej obronie własnych informacji i systemów informacyjnych[8]. Natomiast specjaliści rosyjscy, walkę informacyjną postrzegają jako kompleks przedsięwzięć obejmujących wsparcie, przeciwdziałanie i obronę informacyjną, prowadzonych według jednolitej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem w dziedzinie informacyjnej podczas przygotowania operacji wojskowej oraz prowadzenia działań bojowych[9].

Walka informacyjna ma wpływ na procesy kształtujące bezpieczeństwo międzynarodowe i poszczególnych państw. Należy mieć jednak świadomość tego, że jej znaczącymi uczestnikami są podmioty pozapaństwowe, których działalność niejednokrotnie narusza bezpieczeństwo społeczności międzynarodowej, np. terroryzm. Obejmuje szerokie spektrum oddziaływania na otoczenie wewnętrzne i zewnętrzne praktycznie wszystkich państw, a także podmiotów pozapaństwowych. Jest obecna w życiu człowieka, grup społecznych, narodów, państw, organizacji międzynarodowych i innych podmiotów pozapaństwowych (np. organizacji przestępczych, terrorystycznych, firm oferujących usługi o charakterze militarnym).

Organizacje przestępcze i terrorystyczne to potęgi bezpaństwowe, różnego rodzaju kartele narkotykowe z Ameryki Południowej i Azji (przestępczość

---

[4] L. Ciborowski, *Walka informacyjna*, Warszawa 1996, s. 187.

[5] R. J., Knecht, *Thoughts about Information Warfare*, [w:] A. D Campen, D. H. Deart, R. T. Goodden, Cyberwar: *Securty, Strategy, and Conflict in the Information Age*, AFCEA International Press, Fairfax 1996.

[6] Zaczerpnięte z: Alger John I., *Introduction to Information Warfare*, [w:] Winn Schwartau: *Information Warfare: Chaos on the Electronic Superhighway*, 1 st ed. (New York, Thunder Mouth Press, 1994), s. 12.

[7] Dorothy E., Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 11.

[8] Departament of Defense Directive S-3600.1, Information Operations, December 9, 1996, [za:] Dorothy E., Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 11.

[9] J. L., *Rosyjska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" nr 1, 1999, s. 80.

rosyjskojęzyczna – przyp. autora), ugrupowania terrorystyczne Hamas i Al. Kaida, nowej generacji odpryski mafii i Cosa Nostra, a także efemeryczni hakerzy komunikujący się ze sobą i współpracujący za pośrednictwem Internetu[10].

Walka informacyjna, to działania których celem jest zdobycie lub wykorzystanie zasobów informacyjnych m.in. przez organizacje terrorystyczne, co oznacza:

- uzyskanie przewagi nad potencjalnym przeciwnikiem w dziedzinie rozpoznania,
- zapewnienie przez organizacje terrorystyczne możliwości *oślepienia*, poz*bawienia słuchu* przeciwnika i jego *demoralizowanie*, naruszenie krytycznej infrastruktury państwa (w tym krytycznej infrastruktury teleinformatycznej),
- zapewnienie przez organizacje terrorystyczne łączności, przesyłanie sygnałów powiadamiania i alarmowania, przesyłanie instrukcji, wskazywanie obiektów ataków, stawianie zadań członkom organizacji w czasie rzeczywistym; szerzenie określonych idei, pozyskiwanie nowych członków i zwolenników; przesyłanie środków finansowych,
- zneutralizowanie przewagi przeciwnika w dziedzinie łączności i informatyki,
- zerwanie procesów informatycznych, obezwładnianie lub zniszczenie systemów informacyjnych i zasobów przeciwnika,
- uniemożliwianie przeciwnikowi korzystanie ze wsparcia informacyjnego; problematyka ta obejmuje blokadę zdobywania, przetwarzania i wymiany informacji oraz prowadzanie dezinformacji.

Realizacja powyższych celów i dążenie do uzyskania dominacji informacyjnej przez organizacje terrorystyczne wymaga stosowania ofensywnych, jak i defensywnych form walki informacyjnej.

Na walkę informacyjną składają się działania, których celem jest ochrona, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacji albo też zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem[11].

Zakres postrzegania walki informacyjnej jest bardzo zróżnicowany. Jedni ograniczają się do stosowania szerokiego spektrum środków promieniujących fale elektromagnetyczne w celu uzyskania przewagi konwencjonalnej, z kolei inni uważają, że walka informacyjna to użycie informacji do osiągnięcia celów przez państwo, czy inny podmiot, w tym i organizacje terrorystyczne. Jest to duże uproszczenie ponieważ tym podstawowym podmiotem – uczestnikiem walki informacyjnej jest człowiek z uwagi na posiadaną wiedzę, umiejętności i dostęp do informacji interesujących uczestników kooperacji negatywnej (a niekiedy i pozytywnej).

Wykorzystywanie informacji w każdym środowisku, w tym i technicznej przestrzeni informacyjnej, wspierane przez środki łączności i informatyki dla realizacji przyjętych celów strategicznych przez podmioty państwowe i

[10] Yourdon E., *Wojna na bity*, Warszawa 2004, s. 146.
[11] W. Schwartau, *Information Warfare*, 2nd ed., Thunder' s Mouth Press, 1996, s. 12, [za:] Dorothy E., Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 11.

pozapaństwowe stanowi nową postać wojny, wspieranej przez walkę informacyjną na każdym etapie jej prowadzenia.

Terminem walka informacyjna określa się szeroki zakres działań zarówno podmiotów państwowych, jak i pozapaństwowych (w tym i organizacji terrorystycznych). Ich aktywność obejmuje m.in.: włamania do komputerów, co może prowadzić do wywołania awarii samolotów, w komunikacji kolejowej, lądowej, morskiej, rzecznej, miejskiej; przerwy w dostawie energii elektrycznej, gazu, wody pitnej; naruszenia reżimów bezpieczeństwa w elektrowniach jądrowych, liniach przesyłowych gazu i ropy, zaporach na rzekach; naruszenia procesów produkcji żywności (zatrucie), lekarstw (modyfikacja składu) i ich dystrybucji; zakłócenie procesów e-medycyna (diagnoza, operacje); manipulowanie operacjami finansowymi (atak na giełdę, banki); zakłócenie procesu alarmowania i powiadamiania (w tym służb ratowniczych). Ponadto: szpiegostwo; sabotaż; wywiad; kontrwywiad; podsłuch i oszustwa telekomunikacyjne; manipulowanie percepcją i wojna elektroniczna; broń elektromagnetyczna; fizyczne niszczenie urządzeń komunikacyjnych; kradzież tożsamości i tajemnic (w tym prawnie chronionych); fałszowanie dokumentów; fałszowanie poczty elektronicznej; zbieranie informacji na temat przedstawicieli: polityki, przywódców partii politycznych, rządzących, wojskowych, sędziów, prokuratorów, funkcjonariuszy służb specjalnych, funkcjonariuszy służb policyjnych, urzędników administracji, przywódców duchowych i dowódców organizacji przestępczych; struktur i zasad działania: organów ścigania i wymiaru sprawiedliwości, służb specjalnych, służb policyjnych, organizacji przestępczych, organizacji terrorystycznych itd.

Wyróżnia się dwa rodzaje działań ukierunkowanych na zasoby informacyjne znajdujące się w osobowej przestrzeni informacyjnej i technicznej przestrzeni informacyjnej, w ramach wojny informacyjnej – działania ofensywne i działania defensywne. Działania defensywne są najczęściej prowadzone bez zgody (wiedzy) strony atakowanej. Ich celem jest zwiększenie wartości określonych zasobów informacyjnych przez stronę atakującą, przy jednoczesnym zmniejszeniu ich wartości dla strony defensywnej[12]. Działania defensywne opierają się na zapewnieniu bezpieczeństwa zasobów informacyjnych przed celowymi działaniami, których potencjalnym skutkiem jest utrata ich wartości[13].

Walką informacyjną zainteresowane są także organizacje terrorystyczne, które mogą m.in. demonstrować przemoc lub groźbę jej użycia z zamiarem zastraszenia lub przymuszenia społeczeństw lub rządów[14].

W ramach wojny informacyjnej dokonuje się niekiedy rozróżnienia na *netwar*, *cyberwar i softwar.*

12 Dorothy E., Denning, *Wojna informacyjna ... op. cit.*, s. 13.
13 Ibidem.
14 Ibidem, s. 77.

Tabela 1. Rozróżnienia w ramach wojny informacyjnej

Pole walki	Szczegóły
Networ	polem walki netwar jest świadomość grupowa społeczeństwa, celem ataku – ludzki umysł, a metodami walki – modyfikowanie i manipulowanie świadomością społeczeństwa. Jednym z rezultatów kształtowania się społeczeństwa informacyjnego jest swoista pułapka w postaci zwiększenia podatności cyfrowego, zglobalizowanego społeczeństwa na panikę, lęk i strach, intensyfikowanie i podsycanie przez multimedia. Netwojna odnosi się do konfliktu i przestępstw, które nie są jeszcze wojna, a atakującymi są aktorzy niepaństwowi (terroryści, kryminaliści, fundamentaliści, radykałowie, rewolucjoniści itp.), którzy bazują na sieciowych formach organizacji, komunikacji i strategii,
Cyberwar	jest to dążenie do zniszczenia lub przerwania funkcjonowania systemów informacji i komunikacji przeciwnika. Celem ataku jest informacja oraz zdolność adwersarza do obserwowania i orientowania się w środowisku pola bitwy,
Softwar	to nowoczesne formy walki psychologicznej, propagandy, informacji i dezinformacji. Jest to typ wojny posługującej się tworzeniem faktów, skłonnością społeczeństwa do taniej sensacji w poszukiwaniu rzekomych ukrytych motywacji, teorią spiskową oraz współczesnymi technikami rzeczywistości wirtualnej. Softwar może w ten sposób spowodować nie tylko upadek morale przeciwnika, ale również podkopać jego system wartości i wpłynąć na jego postępowanie, aby zmienić je na korzyść naszych (np. terrorystów) interesów i zamierzeń.

Źródło: M. S. Witecka, *Zagrożenia asymetryczne a technologie informacyjne*, „Zeszyt Problemowy Towarzystwo Wiedzy Obronnej" 2011, nr 4, s. 5 – 66.

„Technika informacyjna stanowi pole bitwy, na którym w nadchodzących latach wystąpi wiele konfliktów. Niektóre z nich będą związane z techniką informacyjną w sposób oczywisty i bezpośredni: *cyberwojna* jako słowo – wytrych obejmuje różne formy działalności hakerów, wirusy, fizyczne ataki na ośrodki komputerowe lub szkieletową strukturę Internetu i tak dalej. W niektórych przypadkach przedmiotem ataku mogą być nie same komputery, lecz zdolność systemów komputerowych do obsługiwania ważnych obiektów dla bezpieczeństwa państwa. […] Ważne jest również, abyśmy zdawali sobie sprawę z tego, że technika informacyjna jest pośrednio związana niemal z każdym aspektem wrogości, z jakim możemy mieć do czynienia w nadchodzących latach – łącznie z wrogą konkurencją."[15]

Organizacje terrorystyczne, które adoptują postęp w komunikacji i informatyce zaczynają powoli, ale systematycznie oddziaływać na poziom bezpieczeństwa poszczególnych państw i środowiska międzynarodowego, gdzie walka informacyjna zaczyna dominować nie tylko w życiu pojedynczego człowieka, ale narodów, państw, organizacji międzynarodowych. Tym samym jesteśmy świadkami rewolucyjnych procesów, gdzie zmiany we współczesnym świecie niosą ze sobą poważne wątpliwości, co do ich skali, dynamiki i kierunków, ponieważ

[15] Yourdon E., *Wojna ... op. cit.*, s. 23.

stanowią źródło wielu problemów o zasięgu globalnym. Jednym z nich jest terroryzm, który z uwagi na globalny zasięg, działania punktowe, a przed wszystkim negatywne skutki (liczne ofiary, straty materialne), strach i nieprzewidywalność stanowi poważne zagrożenie dla bezpieczeństwa społeczności międzynarodowej.

Walka informacyjna prowadzona przez organizacje terrorystyczne, to również „operacje psychologiczne, które są przeznaczone do przekazywania informacji i sugestii przywódcom państw, społeczeństwu, grupie społecznej, narodom, aby wpływać na ich emocje, motywy, rozumowanie i zachowanie na korzyść własnych celów (np. przywódców organizacji przestępczych – przyp. autora). Działania psychologiczne, według przyjętej koncepcji stanowią atak psychologiczny,"[16] Skutki działań psychologicznych są potęgowane możliwościami technicznymi jakimi dysponują organizacje terrorystyczne w zakresie komunikacji (np. powszechny dostęp do technologii teleinformatycznych, Internet, telefonia mobilna, media elektroniczne i tradycyjne) w zakresie komunikacji. Możliwości te wiążą się z precyzją i różnorodnością oraz dużą ilością informacji przekazywanej dla wywarcia wpływu na wyselekcjonowanych odbiorców w celu zmiany ich percepcji i sterowania procesami decyzyjnymi (np. pozyskiwanie sponsorów finansujących działalność terrorystyczną, czy żołnierzy dla organizacji terrorystycznych – przyp. autora)[17]. Przykłady tych informacji to obietnice, szerzenie ideologii, groźby ataku, groźby odwetu na działania podejmowane przez władze państwowe, warunki poddania się, wsparcie grup społecznych, wsparcie narodu, wsparcie grup oporu.

Organizacje terrorystyczne mogą wykorzystywać wspomniany powszechny dostęp do technik teleinformatycznych i komunikacji do przekazywania: określonych informacji, instrukcji, rozkazów, wskazywania obiektów ataku, sygnałów powiadamiania i alarmowania, rozpowszechniania ideologii, co wpływa na działalność poszczególnych grup, mogą także wpływać na społeczeństwa, pozyskiwać nowych członków i zwolenników itp.

W walce informacyjnej organizacje terrorystyczne stosują dwie podstawowe metody prowadzenia działań psychologicznych:

bezpośrednia, stanowi pomocniczy sposób oddziaływania na małe grupy i pojedyncze osoby, która polega na bezpośrednim kontakcie nadawcy i odbiorcy (np. indoktrynowanie przyszłych zamachowców – samobójców),

pośrednia, stanowi podstawowy sposób oddziaływania na obiekty zainteresowania (własne i przeciwnika). Realizowana jest za pomocą materiałów drukowanych, audycji telewizyjnych, radiowych, Internetu, za pomocą których nadawca przenosi określoną informację (sugestię, apel) na odbiorcę nie będącego z nim w bezpośrednim kontakcie.

Przedsięwzięciom tego charakteru sprzyja postępujący rozwój społeczeństwa informacyjnego i stopniowa utrata przez państwa monopolu na przemoc, kontrolę społeczeństwa, stosowania kryptografii.

Korzyści strony atakującej mogą być różne: korzyści finansowe w przypadku kradzieży i sprzedaży zasobów informacyjnych lub wprowadzenie zmian w

[16] Szpyra R., *Militarne operacje informacyjne*, Warszawa 2003, s. 130.
[17] Ibidem, s. 130.

dokumentach bankowych; transakcje finansowe na *podziemnym rynku*, z *czarnym* i *szarym* rynkiem włącznie; sabotaż, który obejmuje fizyczne, elektroniczne i programowe ataki, które powodują degradację, uszkodzenie lub zniszczenie zasobów informacyjnych; kradzież, to dostawanie się na teren strony będącej obiektem ataku, do budynków oraz do systemów komputerowych, co pozwala na zdobycie dokumentów drukowanych i elektronicznych; cenzura jest formą manipulowania percepcją, tzn. bez naruszania źródeł informacji uniemożliwia się dostęp do nich; manipulowanie, przenikanie i fabrykowanie[18].

Warto odnieść się do przyczyn zainteresowania walką informacyjną, które upatruje się w rozwoju informatyki i środków łączności. Jest to jednak wąskie jej postrzeganie, ponieważ była i jest ona uprawiana w trakcie bezpośrednich i pośrednich kontaktów miedzy ludzkich. Propaganda, manipulacja, dezinformacja, maskowanie, szpiegostwo, fałszowanie dokumentów, fałszowanie pieniędzy, cenzura, wojny, manewr, podstęp, obserwacja, działania psychologiczne, przesłuchania jeńców i dezerterów, intrygi, pomówienia zawsze towarzyszą ludzkiemu działaniu, co jest wykorzystywane w trakcie prowadzenia walki informacyjnej m.in. przez organizacje terrorystyczne.

Tabela 2. Przyczyny zainteresowania się walką informacyjną w drugiej połowie XX wieku

Przyczyny
1. przebieg i skutki wojny antyirackiej w rejonie Zatoki Perskiej, która została określona przez Amerykanów jako pierwsza w historii wojskowości wojna informacyjna. Według części ekspertów była to ostatnia wojna starego typu. Walka informacyjna, stanowiąca istotne uzupełnienie tradycyjnych metod walki, w formie uderzeń ogniowych na systemy informacyjne Iraku (stacje radiolokacyjne, stanowiska dowodzenia, węzły systemów telekomunikacyjnych itp.) przyniosła zwielokrotnienie skutków uderzeń ogniowych na wojska irackie, i różnorodnych baz danych i masowy charakter wykorzystania komputerów osobistych,
2. upowszechnienie systemów łączności elektronicznej,
3. istnienie licznych i różnorodnych baz danych i masowy charakter wykorzystywania komputerów osobistych,
4. masowe wykorzystywanie techniki komputerowej w siłach zbrojnych, środowisku cywilnym, a także przez organizacje przestępcze, terrorystyczne,
5. rosnące uzależnienie środków ogniowych jakimi dysponują siły zbrojne państw od systemów łączności, rozpoznania i techniki komputerowej oraz perspektywa tworzenia systemów rozpoznawczo – uderzeniowych szczebla operacyjnego,
6. nieprzewidywalne i przypadkowe dotychczas wyniki operowania informacją mogą obecnie przyjąć formę działań zinstytucjonalizowanych i przewidywalnych, ale bardzo ograniczonym zakresie,

[18] Dorothy E., Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 32 - 39.

7. powstanie światowej sieci informatycznej, obejmującej komputerowe sieci lokalne LAN i regionalne WAN, w tym sieci systemów bankowych, wielkich i małych firm, zasilanie w energię elektryczną, kierowanie ruchem lotniczym (obserwacji przestrzeni powietrznej), centralnej administracji rządowej oraz instytucji wojskowych, przemysłu i zaplecza badawczego,
8. rosnące uzależnienie sił zbrojnych, służb policyjnych, służb specjalnych, służb ratowniczych od cywilnej infrastruktury łączności naziemnej i satelitarnej oraz od komercyjnej techniki informatycznej,
9. wysoką i rosnącą liczbę przypadków prób penetracji sieci komputerowych przez osoby, instytucje nie uprawnione.

Źródło: Opracowano na podstawie: J. L., *Amerykańska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" nr 4, 1998; zob. też J. L., *Rosyjska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" nr 1, 1999.

Prowadzona walka informacyjna przez organizacje terrorystyczne jest rzeczywistym i poważnym zagrożeniem dla bezpieczeństwa poszczególnych państw, są to:[19]

a) zagrożenia oparte na prostej technice (powszechny dostęp do teleinformatyki),
b) samobójcy,
c) rozwój potęg bezpaństwowych (organizacje terrorystyczne, zorganizowane grupy przestępcze o charakterze trans granicznym),
d) szybkie zmiany.

Te cztery wzajemnie powiązane elementy przy umiejętnym powiązaniu i wykorzystaniu przez organizacje terrorystyczne stanowią poważne zagrożenie dla bezpieczeństwa państwa.

Należy mieć świadomość tego, że organizacje tego charakteru nie będą tylko wykorzystywać np. Internetu do wpływania na opinię publiczną. Ich rzeczywiste zainteresowania są bardziej szerokie, których skutki pozwalają na osiągnięcie własnych celów strategicznych nie zawsze zgodnych z interesem państwa. Takim przykładem jest krytyczna infrastruktura państwa, organizacji międzynarodowych.

Zagrożeniem dla krytycznej infrastruktury teleinformatycznej ze strony organizacji przestępczych, terrorystycznych to każde zdarzenie, które może zapoczątkować wyrządzenie niematerialnych lub nawet materialnych szkód[20].

[19] E. Yourdon, *Wojny ... op. cit.*, s. 144.

[20] M. Ludwiszewski, *Monitoring stanu bezpieczeństwa teleinformatycznego państwa*, [w:] *Bezpieczeństwo teleinformatyczne państwa* (red.) M. Madej, M. Terlikowski, Warszawa 2009, s. 128.

Tabela 3. Przykładowy scenariusz zagrożeń na poziomie państwa

Typ działań destrukcyjnych	Skutek bezpośredni	Skutek dalszy	Przeciwdziałanie
Atak elektromagnety-czny			
Wyzwolenie impulsów elektromagnetycznych w rejonach węzłów sieci. Uruchomienie urządzeń zakłócających pracę nadajników łączności bezprzewodowej.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznych – zakłócanie pracy lub paraliż tych sieci. Zniszczenie stacji nadawczych telefonii komórkowej zakłócenia w pracy sieci. Zakłócenie pracy stacji nadawczej telefonii bezprzewodowej.	Utrata informacji administracyjnych. Zakłócenie pracy lub paraliż systemu administrowania miastem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń. Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny. Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Atak ogniowy			
Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci. Przerywanie linii magistralnych sieci.	Zniszczenie central telefonicznych i serwerowni-paraliż pracy sieci. Zakłócenie pracy lub paraliż systemu administrowania miastem.	Utrata informacji administracyjnych. Zakłócenie pracy lub paraliż systemu administrowania państwem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń. Fizyczne uodpornienie sieci na atak ogniowy. Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Działania psychologiczne			
Inżynieria społeczna-pozyskiwanie personelu urzędów do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów administrowania państwem, ujawnienie niejawnej informacji. Sabotaż	Zewnętrzny atak informatyczny na sieci. Zagrożenie bezpieczeństwa informacyjnego państwa. Kradzież niejawnych informacji (np.	Wykrywanie i ocena zagrożeń. Podnoszenie świadomości stanów osobowych. Doskonalenie procedur kontroli dostępu do informacji.

	wewnętrzny ze strony pozyskanego personelu. Defraudacje finansowe dokonywane przez pracowników administracji.	danych osobowych czy finansowych). Pogorszenie bezpieczeństwa finansowego. Zakłócenia w administrowaniu państwem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	
Dezinformacja			
Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz i kierownictw organizacji systemu administrowania państwem. Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu. Rozpowszechnianie fałszywych informacji o zamiarach władz państwa. Podawanie fałszywych informacji o pracy na rzecz interesów obcych państw i organizacji przez przedstawicieli władz.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywołania paniki, pogorszenie jakości funkcjonowania państwa. Próby zachwiania stabilnością finansową i płynnością finansową. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Szybka reakcja władz na fałszywe informacje. Sprawne docieranie do ludności i personelu firm z obiektywną informacją. Zachowywanie prawdy w informowaniu. Wykrywanie i piętnowanie dezinformatorów.

Źródło: T. Jemioło, P. Sienkiewicz (red.), *Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa. Teoria walki informacyjnej*, Warszawa 2004.

„W powyższej tabeli przedstawione zostały scenariusze działań destrukcyjnych, które mogłyby być prowadzone przez podmioty pozapaństwowe, również nieustrukturyzowane, a mieściłyby się w szeroko pojmowanej walce informacyjnej, prowadzonej przeciwko państwu, być może także z inspiracji innego kraju (w tym

sponsorującym lub uprawniającym terroryzm- przyp. autora). Poszczególnym przykładom zagrożeń podporządkowano ich bezpośrednie skutki, potencjalne pośrednie rezultaty oraz metody przeciwdziałania."[21]

Mając powyższe na uwadze można stwierdzić, że walka informacyjna może:

a) stanowić element każdego działania organizacji terrorystycznych,
b) mieć zasięg ograniczony co do państwa, kontynentu,
c) mieć zasięg nieograniczony, tzn. może być prowadzona w dowolnym miejscu i czasie,
d) może mieć zasięg globalny, czego skutkiem może być dezorganizacja globalnej sieci informacyjnej,
e) dla organizacji terrorystycznych może przynieść korzyści o charakterze strategicznym.

Terroryści uczestnikami walki informacyjnej

Państwa i regiony są zróżnicowane pod względem rozwoju społeczno – gospodarczym i naukowo – technicznym, gdzie widoczne są zapóźnienia w rozwoju cywilizacyjnym. Ponadto wielokulturowość, ścieranie się różnych idei, nasilające się zjawiska nacjonalizmu, szowinizmu i fundamentalizmu religijnego oraz terroryzmu organizacji anarchistycznych, religijnych i mafijnych, to zjawiska konfliktogenne o zróżnicowanym natężeniu, co do państwa (regionu). Jeśli nałoży się to na zróżnicowanie w rozwoju przemysłowo – gospodarczego i poziomu życia, wówczas wyraźnie zarysowuje się rozbieżność aspiracji i dążeń, które wcześniej czy później mogą doprowadzić do walki z zastosowaniem przemocy[22]. Niektóre państwa z uwagi na obowiązujące rozwiązania prawno – organizacyjne, przestrzeganie praw człowieka, potencjał przede wszystkim ekonomiczny są atrakcyjne dla ludności innych regionów. Na przykład Stanu Zjednoczone, czy Europa Zachodnia posiadają atuty, które z jednej strony przyciągają swoją zamożnością i są kierunkiem masowego przemieszczania się ludności z państw biednych, gdzie trwają konflikty zbrojne, którym towarzyszą ludobójstwa, czystki etniczne, czy religijne. Ponadto głód, choroby, brak perspektyw na normalne życie.

W ten złożony scenariusz wpisują się m.in. organizacje terrorystyczne, których formy i metody, oraz stosowane środki, a także brak przewidywalności co do miejsca i czasu ataku, czynią je szczególnie niebezpiecznymi. Cele ataków terrorystycznych, metody i wykorzystywane środki ulegają ewolucji w czasie i przestrzeni. Ataki terrorystyczne należy postrzegać w kategorii działań niekonwencjonalnych, co dla obiektów ataku (najczęściej niewinna ludność) i podmiotów zwalczających tego rodzaju działalność stanowi poważne zagrożenie. Ta nieprzewidywalność w zachowaniu terrorystów jest wyznacznikiem bezpieczeństwa międzynarodowego na przełomie XX i XXI wieku.

---

[21] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] *Bezpieczeństwo teleinformatyczne państwa* (red.) M. Madej, M. Terlikowski, Warszawa 2009, s. 92.

[22] S. Dworecki S., *Od konfliktu do wojny*, Warszawa 1996, s. 24.

Zachodzące procesy na świecie i w Europie wspierane były i są przez wszechobecną walkę informacyjną, która z uwagi na swoją naturę wynikającą z niejawności (w uzasadnionych przypadkach jest prowadzona jawnie) i destrukcyjnego wpływu na systemy i sieci informacyjne, a przede wszystkim na naszą percepcję jest szczególnie niebezpieczna.

Działalność organizacji terrorystycznych ma ścisły związek z walką informacyjną, która jest prowadzona w skali globalnej. Ta zależność ma istotny wpływ na realizację celów strategicznych, operacyjnych i taktycznych.

Terroryzm jest użyciem przemocy lub groźby jej użycia z zamiarem zastraszenia lub przymuszenia społeczeństwa lub rządów. Stroną wywierającą terror mogą być jednostki lub grupy (rządy – przyp. autora), które działają często z pobudek ideologicznych lub politycznych (a nawet ekonomicznych – przyp. autora)[23].

Podstawowe cechy terroryzmu, jako zjawiska asymetrycznego:[24]

- uczestnikami tego rodzaju działalności są zarówno podmioty państwowe, jak i pozapaństwowe,
- charakter totalny,
- transnarodowy oznacza, że zagrożenie może powstać na terytorium jednego państwa, a wystąpić na terytorium innego,
- aterytorialny, tzn. brak konkretnego obszaru występowania,
- niekonwencjonalny z uwagi na stosowane metody i wykorzystywane środki,
- quasi – militarny charakter.

Rozpad bipolarnego podziału świata, to także zmiana motywacji terrorystów, gdzie podłoże ideologiczne zostało zdominowane m.in. przez zjawiska o charakterze: religijnym, fundamentalistycznym, separatystycznym, nacjonalistycznym, a nawet rasistowskim.

Należy zaznaczyć, ze terroryzm i walka informacyjna mają kilka cech wspólnych, są zjawiskiem złożonym, otwartym na różnorodną interpretację, mają charakter globalny, ofensywny i agresywny, a także cel jakim jest zysk, np. polityczny, gospodarczy, militarny.

Można przyjąć, że terrorysta wybiera bitwy, które będą wystarczająco duże, żeby się liczyć i wystarczająco małe, żeby mógł być pewny zwycięstwa[25].

„Walka informacyjna pełni rolę wspierającą ten rodzaj działalności i to bardzo skutecznie. To nie tylko komunikacja związana z przekazem głoszonej ideologii, ale także pozyskiwaniem zwolenników, przekazywanie poleceń, szeroko rozumiane zabezpieczenie logistyczne (w tym finansowe, w dokumenty, broń, materiały wybuchowe, broń biologiczna, broń chemiczna), kontakty z mediami, bezpośrednia relacja zamachu terrorystycznego (jego negatywnych skutków).Walka informacyjna to również powszechny strach przed kolejnym atakiem

[23] Dorothy E., Denning, *Wojna informacyjna ... op. cit.*, s. 77.

24 M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państwa obszaru transatlantyckiego*, „PISM", Warszawa 2007, s. 55 i n.

25 K. Bojarski, *Międzynarodowy terroryzm a turystyka*, [w:] *Współczesne dylematy bezpieczeństwa – nowe wyzwania* (red.) J. Pięta, B. Purski, Warszawa 2011, s. 252.

terrorystycznym, a więc permanentne zagrożenie ludności tym negatywnym zjawiskiem."[26]

Mając na uwadze globalną ekspansję tego negatywnego zjawiska można wskazać kilka elementów, które przyczyniają się do jego eskalacji, np. brak jednolitej definicji terroryzmu uznanej przez społeczność międzynarodową; brak spójności prawa międzynarodowego i krajowego, co przekłada się na swobodny przepływ; ludzi, kapitału, informacji, wiedzy, idei; brak skutecznej współpracy i współdziałania. Takim przykładem jest m.in. układ z Schengen znoszący kontrolę n granicach wewnętrznych państw członkowskich Unii Europejskiej, a także wspieranie terroryzmu przez państwa. Na uwadze należy mieć przede wszystkim przepływ ludzi i idei, a także środków finansowych wspierających tego rodzaju działalność, którzy kierując się zróżnicowanymi motywami przemieszczają się w poszukiwaniu swojego miejsca w nowym środowisku nie zawsze o intencjach zgodnych z prawem państwa pobytu[27].

Powyższe uwarunkowania są źródłem szerokiego spektrum zagrożeń dla bezpieczeństwa wewnętrznego i zewnętrznego państw, gdzie terroryzm z uwagi na swój niszczycielski charakter posiada naturalne warunki do podejmowania ofensywnych działań związanych nie tylko z głoszeniem idei, ale i stosowanej fizycznej destrukcji towarzyszącej każdemu zamachowi terrorystycznemu.

„Terroryści korzystają z procesów globalizacyjnych pobudzanych postępem technologicznym. Technika pozwala im działać z ogromną siłą rażenia, sprzyja też budowie i utrzymaniu organizacji na skalę globalną oraz globalnych sieci wsparcia."[28]

Przywódcy organizacji terrorystycznych mają świadomość tego, że poruszają się w złożonym i niejednorodnym środowisku międzynarodowym, które zdominowane jest przez cyberprzestrzeń i wszechobecną informację, która ma coraz większe znaczenie w prowadzanych operacjach za pośrednictwem globalnej sieci informacyjnej. W tej kooperacji negatywnej terroryści są aktywnymi jej uczestnikami uznając, że terminowe i dokładne informacje pozwalają na swobodne poruszanie na kierunkach zainteresowania określonym obiektem, gdzie atakowane obiekty postrzegają w kategoriach strategicznych.

Warto mieć na uwadze to, że obecne organizacje terrorystyczne nie mają tradycyjnych struktur hierarchicznych, natomiast dominują struktury sieciowe z zdecentralizowanym kierowaniem, co oznacza, że podmioty zwalczające tego rodzaju działalność mają trudności w prowadzeniu ich rozpoznania m.in. za pośrednictwem osobowych źródeł informacji. Coraz częściej w działalności terrorystycznej występują elementy powiązane z zarządzaniem organizacją sieciową, psychologiczne, techniczne, technologiczne, gdzie postęp naukowo – techniczny i technologiczny jest przystosowywany do zabezpieczenia i przeprowadzenia zamachu terrorystycznego.

---

26 A. Żebrowski, *Walka informacyjna na służbie terrorystów*, cz. 1, e – terroryzm 2014, nr 2, s. 4.
27 Ibidem, s. 4.
28 J. D. Kiras, *Terroryzm i globalizacja*, [w:] *Globalizacja polityki światowej. Wprowadzenie Dos stosunków międzynarodowych*, (red.) J. Baylis, S. Smith, Kraków 2008, s. 594.

Organizacje terrorystyczne w swojej działalności stosują następujące formy walki informacyjnej:

- ❖ atak informacyjny, czyli zdobywanie informacji o obiekcie zainteresowania (w tym przyszłych obiektach ataku),
- ❖ zakłócanie informacyjne, które pozwala na manipulowanie percepcją, gdzie prowadzone są operacje psychologiczne, propaganda, dezinformacja,
- ❖ obrona informacyjna własnych zasobów osobowych i informacyjnych, struktur przed penetracją podmiotów zwalczających działalność terrorystyczną.

Atak informacyjny stanowi podstawę do budowania bazy danych o obiektach znajdujących się w operacyjnym zainteresowaniu organizacji terrorystycznych. Jednym z zadań jest pozyskiwanie nie tylko zwolenników, ale nowych członków dla organizacji, którzy po odpowiedniej selekcji i przygotowaniu (np. systematyczne, natarczywe wpajanie jakichś idei, doktryn) będą zdolni do wykonania każdego zadania (w tym zamachu samobójczego poświęcając własne życie w imię uznawanych idei).

Atak informacyjny organizacji terrorystycznych to nie tyko zdobywanie informacji o obiektach zainteresowania, czy przedsięwzięciach organów ścigania, uniemożliwienie im wykorzystanie posiadanych informacji, ale także przedsięwzięcia związane z:

1. maskowaniem własnych planów (np. logistycznych, operacyjnych związanych z przygotowaniem ataku na określony obiekt),
2. dezinformacją planowanych i prowadzonych działań,
3. wprowadzaniem w błąd,
4. zaskoczeniem,
5. przeciwdziałaniem identyfikacji członków organizacji terrorystycznych, osób finansujących tego rodzaju działalność.

Oznacza to, że członkowie organizacji terrorystycznych stosując zróżnicowane techniki mogą niszczyć lub uniemożliwiać organom ścigania zdobywanie danych o przywódcach, strukturach, planach, obiektach ataku, źródeł pochodzenia środków finansowych, źródeł i magazynów broni i materiałów wybuchowych, miejsc szkolenia itp. Ponadto mogą zmieniać strukturę nośników danych i sygnałów, co przekłada się na zwiększenie stanu nieuporządkowanej wiedzy o własnych przedsięwzięciach, a tym samym zwiększają entropię informacyjną. Jest to złożony i zróżnicowany proces tak w zakresie obszarów oddziaływania, jak i metod postępowania[29].

Należy podkreślić, że zdeterminowany zamachowiec jest bardzo niebezpieczny, a proces jego przygotowania pod względem typowania, opracowania i indoktrynacji, przy uwzględnieniu indywidualnych cech psychologicznych, gdzie obecne jest tzw. pranie mózgu przynosi zakładane efekty z punktu widzenia przywódców ideologicznych[30].

Elementy walki informacyjnej są wykorzystywane w procesie przygotowania członków organizacji terrorystycznych do przeprowadzenia zamachu na

[29] J. Janczak, *Zakłócanie informacyjne*, Warszawa 2001, s. 15.
[30] A. Żebrowski, *Walka informacyjna na służbie terrorystów*, cz. 1, e – terroryzm 2014, nr 2, s. 7.

wytypowany obiekt, gdzie obok przedsięwzięć zaliczanych do wojny psychologicznej (tzw. pranie mózgu), to również praca operacyjna właściwa dla służb specjalnych. Obok działań ofensywnych, wyspecjalizowane komórki organizacyjne realizują przedsięwzięcia o charakterze defensywnym, które maja na celu nie tylko obronę informacyjną przed atakiem podmiotów zajmujących się zwalczaniem terroryzmu, ale i zakłócanie ich percepcji.

Organizacje terrorystyczne należy traktować jako wyrafinowanych graczy, dla których zasoby konieczne do przeprowadzenia ataku mają określoną wartość. Jest ona funkcją sześciu czynników: poglądów i zobowiązań danego gracza (terrorystów), możliwości tego gracza, dostępność danego zasobu dla danego gracza, dostępność dengo zasobu dla innych graczy (np. podmiotów zwalczających działalność terrorystyczną), integralność zasobu i czasu:[31]

- ❖ poglądy i zobowiązania terrorystów. Aby zasób przedstawiał jakąś wartość, musi się on przyczynić do działań i procesów, które mają znaczenie dla określonej organizacji terrorystycznej, możliwości organizacji terrorystycznych, to wiedza i umiejętności członków tej organizacji a także i narzędzia, którymi się posługują. Zasoby informacyjne mają wartość dla tej kategorii graczy tylko wówczas gdy mają oni możliwości ich wykorzystania w procesie przygotowania i przeprowadzenia ataku terrorystycznego na określony obiekt,
- ❖ dostępność danego zasobu dla organizacji terrorystycznej. Jest to miara możliwości wykorzystania tego zasobu w sposób dla nich właściwy, tzn. czy organizacja terrorystyczna może zasoby: obejrzeć, przetwarzać, zmieniać, kopiować, rozprowadzać lub sprzedawać. Prowadzone operacje to: zdobywanie tajemnic w ramach prowadzonej działalności szpiegowskiej, piractwo informacyjne, przenikanie, fałszowanie przez nakładanie, kradzież tożsamości, kradzież fizyczna, manipulowanie percepcją,
- ❖ dostępność zasobów dla innych podmiotów. W aspekcie walki informacyjnej wartość operacyjna jest zazwyczaj odwrotnie proporcjonalna do dostępności danego zasobu dla innych jej uczestników. Wartość zasobów wynika z posługiwania się nimi jako narzędziem pozwalającym organizacjom terrorystycznym dotarcie do przestrzeni informacyjnej obiektów zainteresowania i do umysłów członków, sprzymierzeńców, istniejącej bazy werbunkowej, wyselekcjonowanych środowisk (osób) poddawanych indoktrynacji,
- ❖ integralność, tzn. czy zasoby znajdujące się w zainteresowaniu organizacji terrorystycznych są dokładne, kompletne, prawdziwe i wiarygodne. Np. integralność plików komputerowych służb zwalczających terroryzm międzynarodowy, do których włamali się terroryści można określić na podstawie tego, jak te pliki korespondują z faktami i innymi informacjami znajdującymi się w posiadaniu terrorystów. Jeżeli terroryści manipulowali którymś z plików, to w następstwie tego ich integralność ulega zmniejszeniu i dla wspomnianych służb nie przedstawiają żadnej wartości operacyjnej,

[31] Dorothy E., Denning, *Wojna informacyjna ... op. cit.*, s. 26-27.

❖ czas, to podstawowy czynnik skutecznego działania. W odniesieniu do zasobów informacyjnych należy mieć świadomość tego, że informacje się starzeją, przez to stają się nieaktualne.

Każdy atak terrorystyczny, to innowacyjne podejście do kolejnego zamachu, to proces polegający na przekształcaniu istniejących idei w nowe, przystosowaniu posiadanych możliwości (sił i środków) do nowych warunków, wykorzystywanie przez terrorystów swoich najsilniejszych stron, co jest skutkiem ich negatywnych zachowań. Innowacyjność ma utrudniać nam codzienne życie, przez komplikowanie otoczenia swojej działalności. „Ukierunkowana jest na bliżej nieokreślonego przeciwnika, gdzie najczęściej ofiarami staje się przypadkowa ludność. Jednak celem terrorystów są także określone, np. państwa, organizacje, politycy, grupy społeczne (np. narodowościowe, religijne), grupy zawodowe, obiekty (np. bazy wojskowe, budynki administracji państwowej, szpitale, szkoły, instalacje, lotniska, statki powietrzne i morskie). Organizacje terrorystyczne koncentrują swoją uwagę również na innowacjach technicznych i technologicznych, co sprawia, że są nieprzewidywalni jeżeli chodzi o wykorzystywane środki w kolejnym ataku (możliwości są nieograniczone).”[32]

Walka informacyjna to potężna broń nie tylko w rękach terrorystów, ale i wielu podmiotów państwowych i ich wyspecjalizowanych agend. Dla terrorystów ważnym narzędziem prowadzenia walki informacyjnej są „media (tradycyjne i elektroniczne), które wciągane są w ich służbę, aby skanalizować i kształtować opinię publiczną przede wszystkim w duchu głoszonych idei. Przekaz telewizyjny z odpowiednim komentarzem i bezpośrednia transmisja z miejsca zamachu (tragedii), zaangażowanie służb ratowniczych , a przede wszystkim ilość ofiar to cel terrorystów, gdzie media doskonale wpisują się w prowadzoną walkę informacyjną przez terrorystów. Jednocześnie pokazanie opinii międzynarodowej, że ich determinacja pozwala na dokonanie ataku praktycznie na każdy obiekt, co uwiarygodnia ich bezwzględność i pokazuje nieograniczone możliwości z wykorzystaniem dowolnych środków.”[33]

Należy mieć świadomość tego, że relacje środków masowego przekazu, to rzeczywisty obraz zamachów terrorystycznych wprost do domów, gdzie masowy odbiorca śledzi przebieg wydarzeń. Relacje dziennikarzy porównywalne są do *tlenu utrzymującego terroryzm przy życie,* ale terroryści szybko odkryli, że zainteresowanie widzów i samych dziennikarzy trzeba stale podsycać, nie ograniczając się do powtarzania podobnych akcji, lecz sięgając po nowe, spektakularne działania[34].

Prowadzona przez organizacje terrorystyczne walka informacyjna, pozwala na operowanie przesłaniami złożonymi z kilku niezależnych od siebie elementów:[35]

1. odbudowy dawnej świadomości islamu drogą jego wybiórczej interpretacji historycznej,

[32] A. Żebrowski, *Walka informacyjna na służbie terrorystów*, cz. 2, e – terroryzm 2014, nr 4, s. 7.
[33] Ibidem, s. 9.
[34] J. D. Kiras, *Terroryzm i globalizacja* … op. cit., s. 598.
[35] A. Żebrowski, *Walka informacyjna na służbie terrorystów*, cz. 2, e – terroryzm 2014, nr 4, s. 9.

2. obrony prześladowanych muzułmanów i walka do ostatecznego zwycięstwa z religijnymi wrogami islamu,
3. wezwanie do najwyższej pobożności i czci religijnej,
4. spiskowa teoria globalnej ekonomii, wyjaśniająca przyczyny nędzy i cierpienia na świecie,
5. sprzeciw wobec świeckiego materializmu.

Okazuje się, że przesłania te atrakcyjne dla pojedynczych ludzi i grup społecznych w miejscach bardzo odległych, gdzie pokazuje się cierpienie i nędzę w różnych zakątkach świata w połączeniu ze sprawczą siecią takie sytuacji – państwami Zachodu, które m.in. narzucają wzorce kulturowe do naśladowania, jako bezwzględnie obowiązujące[36].

Wiele narodów, grup etnicznych, religijnych, czy państw jest zdeterminowanych zachodzącymi procesami w różnych obszarach, które kształtują ich bezpieczeństwo wewnętrzne i pozycję w środowisku międzynarodowym. Ich asymetryczne otoczenie, gdzie nierówności polityczna, społeczna, ekonomiczna a także ograniczony dostęp do nowoczesnych technik i technologii skutkują konfliktami do użycia przemocy włącznie. Trwająca kooperacja negatywna, to także rozwój działalności organizacji terrorystycznych o zróżnicowanym podłożu. Działalność ta wspierana jest przez walkę informacyjną, która w konfrontacji z podmiotami zwalczającymi organizacje terrorystyczne odnosi sukcesy. Sukces i poparcie pozwala na prowadzenie ofensywnych działań, które trudno zwalczać przy braku politycznej woli społeczności międzynarodowej.

Zakończenie

Prowadzenie walki informacyjnej przez organizacje terrorystyczne ma na celu uzyskanie przewagi informacyjnej nad przeciwnikiem i zakłócenie jego percepcji. Ponadto realizacja głoszony idei przez terrorystów jest ukierunkowana na konfrontację. Skutki to śmierć niewinnych ludzi, starty materialne i ciągły strach przed kolejnym zamachem. Obecny terroryzm jest nieprzewidywalny co do miejsca i czasu, a także stosowanych metod i wykorzystywanych środków do fizycznej destrukcji. Jej prowadzenie ułatwia niewątpliwie stopniowa utrata przez państwa monopolu na kontrolę społeczeństwa. Kolejnym niezmiernie ważnym czynnikiem, to rewolucja w komunikacji i informatyce. Ponadto powszechny dostęp do techniki teleinformatycznej i uzależnienie od jej sprawności funkcjonowanie krytycznej infrastruktury państw, organizacji międzynarodowych - jest źródłem jakościowo nowych zagrożeń. Skutki ataku informacyjnego (wspieranego przez zakłócanie informacyjne) organizacji terrorystycznych na zasoby informacyjne np. organów ścigania, to dezorganizacja ich procesu wykrywczego wspomnianych podmiotów pozapaństwowych.

[36] Ibidem, s. 9.

Bibliografia

K. Bojarski, *Międzynarodowy terroryzm a turystyka*, [w:] *Współczesne dylematy bezpieczeństwa – nowe wyzwania* (red.) J. Pięta, B. Purski, Warszawa 2011,

Ciborowski L., *Walka informacyjna*, Warszawa 1996,

Dawidczyk A., *Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku*, Warszawa 2001,

Departament of Defense Directive S-3600.1, Information Operations, December 9, 1996, [za:] Denning Dorothy E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002,

Denning Dorothy E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002,

Dworecki S., *Od konfliktu do wojny*, Warszawa 1996,

Janczak J., *Zakłócanie informacyjne*, Warszawa 2001,

J. L., *Rosyjska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" nr 1, 1999,

J. L., *Amerykańska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" nr 4, 1998,

Jemioło T., Sienkiewicz P (red.), *Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa. Teoria walki informacyjnej*, Warszawa 2004,

Kiras J. D., *Terroryzm i globalizacja*, [w:] *Globalizacja polityki światowej. Wprowadzenie Dos stosunków międzynarodowych*, (red.) Baylis J., Smith S., Kraków 2008,

Knecht R. J., *Thoughts about Information Warfare*, [w:] Campen A. D., Deart D. H., Goodden R. T., Cyberwar: *Securty, Strategy, and Conflict in the Information Age*, AFCEA International Press, Fairfax 1996,

Ludwiszewski M., *Monitoring stanu bezpieczeństwa teleinformatycznego państwa*, [w:] *Bezpieczeństwo teleinformatyczne państwa* (red.) Madej M., Terlikowski M., Warszawa 2009,

Madej M., *Zagrożenia asymetryczne bezpieczeństwa państwa obszaru transatlantyckiego,* „PISM", Warszawa 2007,

Schwartau W., *Information Warfare*, 2nd ed., Thunder' s Mouth Press, 1996, s. 12, [za:] Denning Dorothy E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002,

Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] *Bezpieczeństwo teleinformatyczne państwa* (red.) Madej M., Terlikowski M., Warszawa 2009,

Szpyra R., *Militarne operacje informacyjne*, Warszawa 2003,

Witecka M. S., *Zagrożenia asymetryczne a technologie informacyjne*, „Zeszyt Problemowy Towarzystwo Wiedzy Obronnej" 2011, nr 4,

Yourdon E., *Wojny na bity*, Warszawa2004,

Żebrowski A., *Walka informacyjna na służbie terrorystów*, cz. 1, e – terroryzm 2014, nr 2,

Żebrowski A., *Walka informacyjna na służbie terrorystów*, cz. 2, e – terroryzm 2014, nr 4.