Numer 4(17)/2020

SECURITY REVIEW

Numer 4(17)/2020

(październik – listopad – grudzień 2020)

Instytut Analizy Ryzyka Sp. z o. o.

ISSN 2543-6694

SECURITY REVIEW

NUMER 4(17)/2020

Szanowni Państwo,

Przed nami koniec 2020 roku - roku w którym cały Świat musiał zmagać się z pandemią COVID-19. To rok w którym wszelkie konferencje, organizowane były w systemie on-line. Nie przeszkodziło to jednak nam na zamieszczanie coraz to ciekawszych artykułów naukowych i recenzji. Coraz większa liczba czytelników, zarówno z Polski, jak i zagranicy sięga po lekturę „Security Review". Świadczą o tym między innymi statystyki internetowe oraz maile, które otrzymujemy od osób zainteresowanych publikacją na łamach naszego czasopisma.

Przedstawiam Państwu czwarty i ostatni w tym roku numer czasopisma „Security Review", w którym jako pierwszy przedstawiony został artykuł dotyczący problematyki dezinformacji jako zagrożenia dla bezpieczeństwa informacyjnego współczesnych społeczeństw. Polecam Państwa uwadze również drugi artykuł – „Informacyjne instrumenty przeciwdziałania i zwalczania terroryzmu". W numerze znajdziecie również sprawozdanie z II Międzynarodowej Konferencji Naukowej z cyklu „Prawa człowieka podstawą demokratycznego państwa prawnego" na temat: Informacyjny wymiar praw człowieka i obywatela. Mam nadzieję że zawarte artykuły staną się cenną literaturą dla Państwa.

Szanowni Państwo pozwólcie, że w związku ze zbliżającymi się Świętami Bożego Narodzenia oraz Nowym Rokiem w imieniu redakcji złożę Państwu najlepsze życzenia wszystkiego najlepszego i szczęśliwego nowego 2021 roku. Niech będzie on pełen miłych niespodzianek i wydarzeń. Zachęcam również do lektury naszego czasopisma i publikacji na jego łamach.

W imieniu Rady Naukowej
i Zespołu Redakcyjnego
gen. bryg. rez. dr hab. inż. Tomasz Bąk

W TYM NUMERZE:

Dezinformacja jako zagrożenie dla bezpieczeństwa informacyjnego współczesnych społeczeństw S. 3

Piotr Bączek

Informacyjne instrumenty przeciwdziałania i zwalczania terroryzmu S. 19

Waldemar Gołuchowski

Sprawozdanie z II Międzynarodowej Konferencji Naukowej z cyklu „Prawa człowieka podstawą demokratycznego państwa prawnego" na temat: Informacyjny wymiar praw człowieka i obywatela S. 29

DEZINFORMACJA JAKO ZAGROŻENIE DLA BEZPIECZEŃSTWA INFORMACYJNEGO WSPÓŁCZESNYCH SPOŁECZEŃSTW

Piotr Bączek

Akademia Finansów i Biznesu Vistula – Filia Akademia im. A. Gieysztora w Pułtusku

Abstract

Disinformation as a threat to the information security of contemporary societies

One of the methods of information warfare is disinformation. Its task is to mislead the opponent by giving him false information. The aim of the article is to present the phenomenon of disinformation as a threat to modern societies. The article discusses the following issues: threats to information security, classification of disinformation, disinformation operations in communist and democratic states, historical and contemporary examples of propaganda disinformation. In recent years, there has been an extensive use of electronic media to disseminate disinformation content, which poses a threat to societies.

Keywords: disinformation, information security, infosphere

Wstęp

Powstanie społeczeństwa informacyjnego sprawiło, że zagadnienia z zakresu bezpieczeństwa informacyjnego i zagrożeń informacyjnych stały się istotnymi problemami tak dla struktur państwowych, jak i poszczególnych osób. Znajduje to wyraz zarówno w działaniach praktycznych i tworzeniu kolejnych struktur, instytucji, regulacji prawnych dotyczących pozyskiwaniu i ochrony informacji, jak i w pracach teoretycznych z tego zakresu. Szczegółowym badaniom poddawane są zjawiska związane z cywilizacją informacyjną oraz nowymi wyzwaniami i zagrożeniami, które ona niesie. W ten nurt rozważań wpisują się zawarte w artykule rozważania. Ich celem jest scharakteryzowanie zjawiska dezinformacji jako metody walki informacyjnej państw, ale również jako zagrożenia dla współczesnych społeczeństw. Zaprezentowane analizy oparte zostały o krajową oraz zagraniczną literaturę przedmiotu, dokumenty międzynarodowych instytucji oraz inne źródła. Podstawą przeprowadzonych dociekań jest hipoteza mówiąca, że: dezinformacja jako szczególna forma walki informacyjnej oddziałuje na ośrodki władzy państwowej, służby specjalne, wojsko, ale istnieje także typ tajnej dezinformacji, który bezpośrednio wpływa na społeczeństwo.

Powyższa hipoteza zostanie zweryfikowana w oparciu o poszukiwanie odpowiedzi na następujące pytania problemowe:

- Na ile dezinformacja oddziałuje na struktury państwa i na jego obywateli?
- W jakim zakresie społeczeństwa w państwach demokratycznych są narażone na dezinformację?
- Jaka jest różnica pomiędzy dezinformacją realizowaną metodami operacyjnymi służb specjalnych a dezinformacją propagandową, czyli wykorzystującą mass media?

- Jak w epoce społeczeństwa informacyjnego zmieniły się uwarunkowania dezinformacji propagandowej?

Przedmiotem rozważań w artykule będą również kwestie dotyczące: bezpieczeństwa informacyjnego, zagrożeń informacyjnych, dezinformacji i jej typów, metod działań dezinformacyjnych realizowanych przez służby specjalne różnych państw, uwarunkowań politycznych i informacyjnych społeczeństw w różnych systemach politycznych.

Bezpieczeństwo informacyjne i zagrożenia informacyjne

W ostatnich dekadach w polskiej literaturze przedmiotu szereg badaczy łączy problematykę bezpieczeństwa informacyjnego z wolnościami obywatelskimi, prawami człowieka. Eugeniusz Nowak i Maciej Nowak wskazują, że bezpieczeństwo informacyjne umożliwia istnienie społeczeństwa informacyjnego. Według nich jest to „stan warunków wewnętrznych i zewnętrznych, który pozwala państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego" (Nowak i Nowak, 2011, s. 103). Z kolei Włodzimierz Fehler podkreśla aspekt wolnościowy bezpieczeństwa informacyjnego przy jednoczesnej ochronie wybranych informacji. W ocenie tego badacza jest to „stan w którym zapewniona jest swoboda dostępu i przepływu informacji połączona z racjonalnym i prawnym wyodrębnieniem takich kategorii, które podlegają ochronie ze względu na bezpieczeństwo podmiotów których dotyczą" (Fehler, 2012, s. 13-14). Społeczne ujęcie bezpieczeństwa informacyjnego zgodne z filozofią wyrażoną w Konstytucji RP, która stanowi, że każdemu gwarantuje się „wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji" (Konstytucja RP, 1997, art. 54). Skok technologiczny umożliwiający m.in. gromadzenie, przesyłanie i udostępnianie informacji w czasie rzeczywistym nie tylko sprzyja rozwojowi cywilizacyjnemu, ale również generuje nowe zagrożenia. Z kolei te dotychczasowe przybierają formy dostosowane do nowych realiów i przekształcają się niejednokrotnie w kolejne kategorie. Przywoływany już wcześniej Fehler za zagrożenia uznaje „stan w którym mamy do czynienia z aktualnie występującym lub w dużym stopniu prawdopodobnym zakłóceniem uznawanych za bezpieczne warunków funkcjonowania danego podmiotu" (Fehler, 2012, s. 20). Wyróżnia on następujące zagrożenia informacyjne:

- brak informacji,
- ograniczenia w dostępie do informacji,
- nadmiar informacji,
- manipulacje informacyjne,
- fałszerstwa informacyjne,
- napływ informacji nieczytelnej,
- utrata informacji chronionej,
- dystrybucja informacji pozyskanej nielegalnie,
- prezentowanie informacji zdezaktualizowanej" (Fehler, 2016, s. 36).

Przynajmniej dwa z wyżej wymienionych zagrożeń (tzn. manipulacje informacyjne i fałszerstwa informacyjne) można zakwalifikować do grupy działań dezinformacyjnych.

Istota i typologia dezinformacji

Badacze wskazują, że dezinformacja może oznaczać fałszywą informację, która jest świadomie i metodycznie zakłamywana, jak i planowy proces przekazywania nieprawdziwych treści przeciwnikowi. W tym drugim ujęciu działanie jest tajne i realizowane w zamiarze wywołania u odbiorcy nieprawdziwego obrazu rzeczywistości, oceny danej osoby, ukształtowania opinii o wydarzeniu, zjawisku zgodnej z interesem dezinformatora. Celem jest wpływanie na procesy decyzyjne władz innego państwa. Działania dezinformacyjne mogą być realizowane np. poprzez środki masowego przekazu albo drogą czynności operacyjnych służb specjalnych (Larecki, 2017, s. 211-212, Liedel i Serafin, 2011, s. 86-87). Dezinformacja w XX w., wraz z pojawieniem się wyspecjalizowanych struktur służb specjalnych, stała się jedną z ważniejszych metod stosowanych w walce z przeciwnikiem. Według klasycznej klasyfikacji wyróżniamy następujące typy dezinformacji:

- strategiczną,
- polityczną,
- dyplomatyczną,
- ekonomiczną,
- wojskową,
- techniczną (Golicyn, 2007, s. 53).

Klasyfikację tę zaproponował Anatolij Golicyn, były oficer KGB (ros. *Комитет государственной безопасности при Совете Министров СССР, КГБ СССР* – Komitet Bezpieczeństwa Państwowego przy Radzie Ministrów ZSRR), który w 1961 r. zbiegł na zachód. W jego ocenie służby specjalne ZSRR wyróżniały sześć kanałów rozpowszechniania dezinformacji:

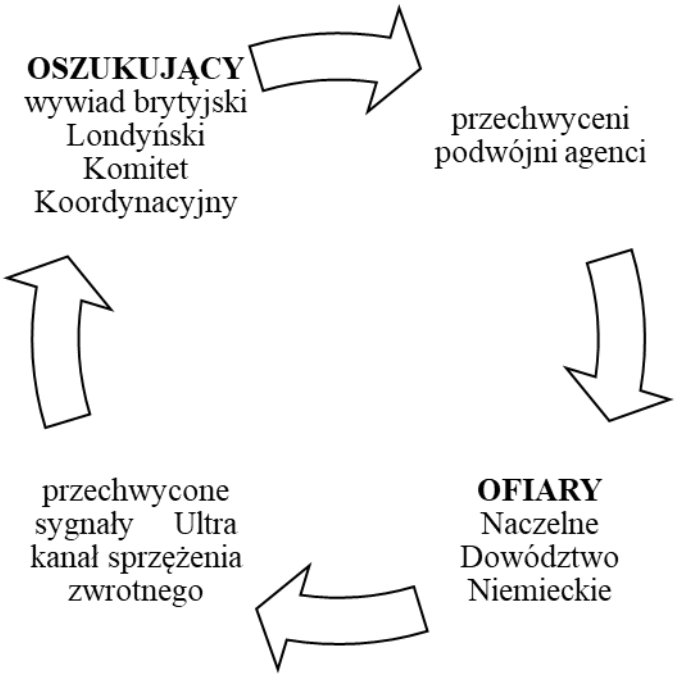
- deklaracje i przemówienia polityków i członków rządu,
- oficjalne dokumenty rządowe,
- gazety i inne materiały publikowane w danym państwie,
- zagraniczne publikacje inspirowane przez oficerów służb specjalnych pracujących z obcymi dziennikarzami i ekspertami,
- specjalne operacje wspierające,
- agenci wpływu i inni agenci oraz oficerowie w obcych krajach (Golicyn, 2007, s. 53).

W XX w. stosowano wszystkie wymienione typy dezinformacji, wykorzystując wskazane kanały jej rozpowszechniania. Czyniły tak państwa komunistyczne, ale również demokratyczne.

Dezinformacja w państwach komunistycznych i demokratycznych

Przykładem działań dezinformacyjnych prowadzonych przy pomocy agentury jest operacja służb specjalnych Rosji Radzieckiej z lat 1921-1927, znana pod nazwą „TRUST". Agenci policji politycznej GPU (ros. *Государственное Политическое Управление, ГПУ* – Państwowy Zarząd Polityczny) stworzyli fikcyjne ugrupowanie opozycyjne Monarchistyczna Organizacja Centralnej Rosji (MOCR). Zachodnie służby były skutecznie wprowadzane w błąd, uzyskiwały od przedstawicieli MOCR fałszywe informacje o opozycji i sytuacji w ZSRR (Świerczek, 2013, s. 271). W okresie II wojny światowej alianci wprowadzili w błąd Niemców, co do miejsca inwazji w Europie w 1944 r. Stworzono fikcyjną grupę armii amerykańskiej, która miała przeprowadzić desant. Brytyjska siatka podwójnych agentów przekazywała do Berlina meldunki, które potwierdzały tę mistyfikację. Złamany szyfr Enigmy umożliwił Anglikom sprawdzać reakcje Niemców. Dzięki temu alianci mogli modyfikować działania dezinformacyjne (Epstein, 1993,

s. 126-128; Minkina Gałek 2015, s. 61, 71, 81). W ten sposób Niemcy uznając fałszywe informacje za prawdziwe wpadli w tzw. „pętlę oszustwa" (zobacz Rysunek 1).



Rysunek 1. Pętla oszusta. Inwazja w dniu „D"

Źródło: Epstein, 1993, s. 128

Po zakończeniu II wojny działania dezinformacyjne i dezintegracyjne stały się dla służb specjalnych państw bloku wschodniego ważnymi metodami pracy. Za realizację operacji dezinformacyjnych odpowiedzialna była specjalna jednostka w strukturze I Zarządu Głównego KGB, czyli wywiadu zagranicznego. Początkowo był to Wydział „D" (ros. *деза* – dezinformacja), który następnie przekształcono w Służbę „A" (ros. *активка* – środki aktywne) (Darczewska, Żochowski, 2017, s. 17-18). Działania dezinformacyjne były prowadzone w bloku wschodnim m.in. przeciwko opozycji. Celem było zinfiltrowanie, zdezawuowanie i zniszczenie tych środowisk. Realizowano je do końca komunizmu, przykładowo, w 1988 r. funkcjonariusze SB zwalczając struktury NSZZ „Solidarność" w Nowej Hucie zalecali „prowadzić gry i kombinacje operacyjne oraz akcje dezinformujące i destrukcyjne w myśl oddzielnie opracowanych planów" (Zając, 2012, s. 26).

Istnieje również wiele przykładów prób wywierania wpływu przez zachodnie służby specjalne na opinię społeczną. We Francji Służba Dokumentacji Zagranicznej i Kontrwywiadu (fr. *Service de Documentation Exterieure et de Contre-espionnage* – SDECE) manipulowała jedną z agencji reportażu telewizyjnego i tajnie inwestowała w szkołę dziennikarstwa. SDECE posiadała wśród dziennikarzy współpracowników nie pobierających wynagrodzenia (fr. *honorable correspondant* – HC). Dzięki temu francuski wywiad mógł prowadzić działania wywiadowcze i dezinformacyjne (Faligot i in. 2019, s. 268, 356-357). Wiele wskazuje na to, że takie działania podjęto wobec byłego premiera Georges'a Pompidou. Sprawował on urząd szefa rządu do 10 lipca 1968 r., w następnym roku wystartował w wyborach. W tym czasie był już skonfliktowany z prezydentem Charlesem de Gaulle'em W październiku 1968 r.

w trakcie śledztwa w sprawie zabójstwa Stephana Markovica, ochroniarza znanego aktora Alaina Delona, SDECE uzyskała informacje kompromitujące Claude Pompidou, żonę byłego premiera. Rzekomo miała ona uczestniczyć w orgiach seksualnych. Wkrótce wśród dziennikarzy pojawiły się sfabrykowane pornograficzne zdjęcia z doklejoną głową żony byłego premiera. Wybrany w czerwcu 1969 r. na prezydenta G. Pompidou uważał, że za skandal odpowiedzialni są oficerowie SDECE (Ockrent i de Marenches,1992, s. 137-138; Faligot i in. 2019, s. 256-259; Kropp 1999, s. 611-612). Z kolei Dyrekcja Generalna Bezpieczeństwa Zewnętrznego (fr. *Direction Générale de la Sécurité Extérieure* - DGSE) zorganizowała w 1985 r. zamach na okręt organizacji „Greenpeace", który blokował przeprowadzenie prób broni atomowej na Pacyfiku. Zgodę na tę akcję wydały najwyższe władze Francji. W celu zmylenia dziennikarzy śledczych rozpowszechniano fałszywe informacje, m.in. o tym, że był to antyfrancuski spisek, który miał osłabić prezydenta Francoisa Mitteranda, zaś zamachowcami miały być osoby powiązane ze skrajną prawicą (Faligot i in. 2019, s. 338-339, 343-347).

Podsumowując ten fragment rozważań należy uznać, że dezinformację lub zbliżone metody wykorzystywały zarówno komunistyczne służby specjalne, jak i zachodnie. Jednak należy także wskazać na różnice w ich działaniach, które były spowodowane odmiennymi systemami politycznymi w obu blokach. W państwach zachodniej demokracji praktyki wykraczające poza ustalone normy, były wcześniej czy później ujawniane i krytykowane, poddane kontroli innych organów państwa oraz ocenie społecznej. W państwach komunistycznych władze i służby specjalne działały poza wszelką kontrolą. System polityczny determinował bowiem charakter infosfery, czyli środowiska informacyjnego funkcjonującego w danym państwie (zobacz Tabela 1). To z kolei pośrednio wpływało również na metody podejmowane przez służby specjalne. W państwach demokratycznych, w których wolność wypowiedzi jest prawnie zagwarantowana, działania służb specjalnych są ograniczane również z powodu potencjalnej krytyki społecznej i ze strony konkurentów politycznych. Jeszcze w okresie „zimnej wojny" dostrzegł to Vladimir Volkoff, który ocenił, że w zakresie dezinformacji państwa zachodnie „są pozbawione wszelkich możliwości ofensywnego działania" (Volkoff, 1991, s. 13). Dowodzą tego przytoczone przykłady działań francuskich służb specjalnych. Ich operacje dezinformacyjne były po jakimś czasie ujawniane i publicznie krytykowane. Tymczasem infosfera w systemach autokratycznych i totalitarnych jest podporządkowana wyłącznie władzy, wolność słowa jest ograniczona. Sprawia to, że służby specjalne w tych państwach znajdują się poza wszelką krytyką. Prowadzą operacje również przeciwko własnemu społeczeństwu. W swojej działalności nie są więc ograniczone opinią społeczną. Mogą więc bez przeszkód wykorzystywać rozmaite kontrowersyjne metody, np. aktywne działania dezinformacyjne w infosferze.

Kategorie	System demokratyczny	System autokratyczny/totalitarny
Wolność wypowiedzi	nieograniczona przy zachowaniu praw innych osób i podmiotów	cenzura prewencyjna, bariery administracyjne (np. limitowanie nakładów prasy, blokady Internetu, system koncesyjny)
Rynek mediów	otwarty	zamknięty i kontrolowany przez władze
Rynek opinii	pluralistyczny, możliwość poznania argumentów różnych grup interesu, prawo wyrażania opinii krytycznych	odgórnie scentralizowany, monolityczny, podporządkowany władzy, zablokowanie wymiany poglądów i krytyki władz
Rola władz państwowych	koordynująca, ograniczona do określenia ogólnych zasad funkcjonowania infosfery	nakazowo-kierownicza, nieograniczony wpływ na infosferę
Funkcja mediów	informująca, kontrolująca władze	propagandowa, jeden z instrumentów sprawowania władzy
Prawa odbiorcy informacji	możliwość weryfikacji informacji, wybór dowolnych kanałów informacyjnych, dostęp do opinii krytykujących władze	pozbawiony alternatywnych źródeł informacji, poddany presji propagandowej władz, sankcje za korzystanie z niezależnych źródeł informacji
Rola służb specjalnych	ingerencje prawnie ograniczone do wyjątkowych sytuacji, odstępstwa od tej reguły są krytykowane, penalizowane	kontrola mediów, działania represyjne, traktowanie mediów jako kanału wywierania wpływu i dezinformowania odbiorców

Tabela 1. Różnice funkcjonowania infosfery w systemach demokratycznym i autokratycznym/ totalitarnym

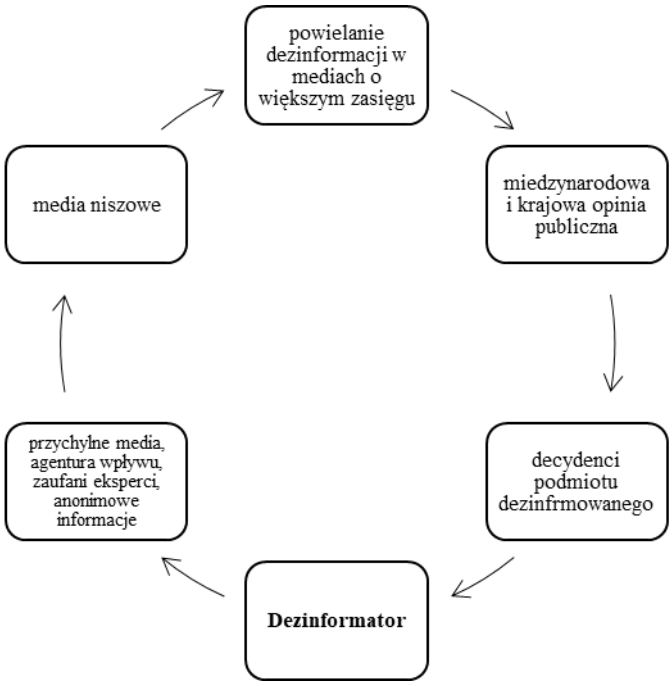
Źródło: opracowanie własne.

Dezinformacja propagandowa na przykładzie operacji „INFEKTION"

Agentura wpływu była wykorzystywana nie tylko do prowadzenia gier operacyjnych w celu dezinformowania obcych służb specjalnych, władz nieprzyjacielskiego państwa, ale również do oddziaływania na percepcję, decyzje i działania rządu oraz na postawy i nastroje społeczne zaatakowanego państwa. W przypadku działań ukierunkowanych na opinię publiczną efekty operacji dezinformacyjnych „nie są najczęściej widoczne od razu, ale stosowane systematycznie, przez dłuższy okres czasu, jako przemyślana i długofalowa polityka rządu mogą zaowocować efektem kumulacji, wpływając na opinię publiczną, zmianę nastawień i postaw" (Minkina, 2014, s. 235). Jedną z najgłośniejszych operacji KGB tego typu było rozpowszechnianie w latach 80. XX w. pogłosek o amerykańskim pochodzeniu choroby AIDS. Według tych plotek została ona sztucznie stworzona przez amerykańskich wojskowych. Pomimo tego, że od jej przeprowadzenia minęło ponad ćwierć wieku, warto ją przeanalizować jako przykład oddziaływania służb specjalnych na opinię publiczną. Operacja wykorzystywała tzw. „środki aktywne" i nosiła kryptonim „INFEKTION". Była rodzajem dezinformacji rozpowszechnianej poprzez „zagraniczne publikacje inspirowane przez oficerów służb specjalnych pracujących z obcymi dziennikarzami i ekspertami" (Golicyn, 2007, s. 53).

Teza o amerykańskim pochodzeniu choroby AIDS pojawiła się po raz pierwszy w indyjskiej gazecie „Patriot" w wydaniu z 17 lipca 1983 r. Redakcja wydrukowała anonimowy list zatytułowany „AIDS może zaatakować Indie. Tajemnicza choroba spowodowana przez amerykańskie eksperymenty". W anonimie stwierdzono, że AIDS jest wynikiem eksperymentów Pentagonu, który dąży do stworzenia nowej broni biologicznej. Autor, rzekomo amerykański naukowiec, napisał także, że Stany Zjednoczone będą chciały przenieść te badania do Pakistanu, co będzie zagrożeniem dla sąsiednich Indii. Rosjanie masowo rozsyłali sfabrykowane materiały na temat „amerykańskiego AIDS". W latach 80. XX w. w prasie ponad 40 krajów Trzeciego Świata opublikowano informacje, że wirus HIV miał zostać wyhodowany sztucznie w laboratoriach. W tych działaniach KGB uzyskało wsparcie od Głównego Zarządu Wywiadu (niem. *Hauptverwaltung Aufklärung, HVA*) Niemieckiej Republiki Demokratycznej. Niemcy, w ramach operacji „VORWÄRTS II", zainspirowali do badań nad AIDS zaufanego naukowca. Był nim dr Jacob Segal, który prawdopodobnie w okresie II wojny światowej związał się z radzieckim wywiadem. J. Segal oświadczył, że wirus został sztucznie zsyntetyzowany podczas eksperymentów genetycznych w amerykańskim laboratorium wojskowym w Fort Detrick. Broszurę z wynikami jego prac agenci KGB oraz HVA rozprowadzili przed ósmą konferencją państw zaangażowanych w Harare w Zimbabwe we wrześniu 1986 r. Anonimowe opracowanie HVA otrzymał również austriacki pisarz Johannes Mario Simmel. Jego książka na temat pochodzenia AIDS stała bestsellerem. Po jakimś czasie zachodnia prasa ujawniła działania KGB. Operacja „INFEKTION" zakończyła się jesienią 1987 r., kiedy urzędnicy USA przebywający w Moskwie zostali poinformowani, że fałszywe oskarżenia zostały zdementowane. Pomimo tej porażki KGB nie zaniechała prowadzenia dezinformacji przeciwko USA, m.in. rozpowszechniano pogłoski o rzekomym zabijaniu przez Amerykanów dzieci w celach uzyskania organów do transplantacji (Andrew, 1998, s. 542-543; Andrew i Gordijewski, 1999 s. 551-552; Andrew i Mitrochin, 2006, s. 374; Andrew i Mitrochin, 2009, s. 393-394; Boghardt, 2009, s. 4-13; Helma, 2018, s. 83-84). Operacja „INFEKTION" jest doskonałym studium przypadku prowadzenia tajnej dezinformacji poprzez tradycyjne media. Na jej podstawie można zrekonstruować ówczesny algorytm takich działań służb specjalnych, w tym przypadku z bloku komunistycznego. Działania operacyjne służb specjalnych służyły przede wszystkim do skompromitowania przeciwnika i pod-

ważenia zaufania do niego. Realizowano to poprzez rozpowszechnianie fałszywych informacji, nagłaśnianie opinii odpowiednio dobranych ekspertów oraz zmanipulowanie, zafałszowanie ewentualnie zdezawuowanie przekazu informacyjnego lub propagandowego przeciwnika. Fałszywe treści wprowadzono do infosfery poprzez anonimy, tajnych współpracowników, niszowe media. Przekaz dezinformacyjny został następnie wzmocniony poprzez media europejskie. Uwiarygadniali go przychylni eksperci, zwłaszcza z bloku komunistycznego. Operację „INFEKTION" zakończono w 1987 r., najprawdopodobniej z powodu sytuacji gospodarczej ZSRR i dążenia do ocieplenia stosunków z USA. Wprawdzie Kreml kontynuował działania dezinformacyjne, ale już w mniejszym zakresie. Pomimo to wytworzono atmosferę nieufności wobec władz USA (zobacz Rysunek 2). Celem operacji „INFEKTION" była dezinformacja propagandowa, czyli publiczne zdyskredytowanie przeciwnika, podważenie jego autorytetu. Zawierała ona elementy działań operacyjnych służb specjalnych, ale nie była typową dezinformacją operacyjną. Golicyn nie wyróżnił w swojej typologii dezinformacji propagandowej. Wskazał jedynie na media jako kanał rozpowszechniania fałszywych informacji (Golicyn, 2007, s. 53). Jednak ze względu na coraz częstsze, a w XXI w. wręcz powszechne, wykorzystanie mediów do takich działań należałoby wyodrębnić również taki rodzaj dezinformacji. Syntetycznie rzecz ujmując dezinformacja propagandowa charakteryzuje się tym, że chociaż zawiera przekaz propagandowy przeznaczony dla opinii publicznej, to jest realizowana w sposób tajny, w tym także metodami operacyjnymi. Ze względu na to, że jawny komponent propagandowy jest rozpowszechniany w sposób masowy, działania te powinny być określane terminem operacji, kampanii dezinformacyjno-propagandowych.



Rysunek 2. Pętla dezinformacji propagandowej na przykładzie operacji „INFEKTION"

Źródło: opracowanie własne

Pomimo istnienia różnic pomiędzy typami dezinformacji (zobacz Tabela 2) cel jest identyczny – zdominowanie przeciwnika i przejęcie nad nim władzy. Dezinformacja propagandowa sprawia, że to, co jest jedną z największych wartości demokracji i stanowi jej broń (tzn. wolność słowa), jest równocześnie słabością tego systemu. Państwom gwarantującym pluralizm opinii trudniej jest bronić się przed dezinformacją. Do infosfery państw demokratycznych mają dostęp podmioty, które zwalczają te państwa, promują wrogie ideologie, dążą do zdominowania społeczeństwa i negują system demokratyczny. Na to uwarunkowanie państw demokratycznych wskazał Volkoff., który stwierdził, że trudno im bronić się przed dezinformacją (Volkoff, 1991, s. 13).

Kategorie	**Dezinformacja operacyjna**	**Dezinformacyjna propagandowa**
Cel taktyczny działań	uzyskanie wpływu na decyzje władz państwa, służb specjalnych, decydentów	uzyskanie wpływu na opinię społeczną, zbudowanie w społeczeństwie interpretacji wydarzeń korzystnej dla przeciwnika
Instrumenty działań	przede wszystkim agentura: pod przykryciem, podwójna, wpływu	agentura wpływu w mediach i ośrodkach opiniotwórczych, przychylni eksperci, zainspirowani dziennikarze, opłaceni lobbyści, „pożyteczni idioci”
Metody działań	inspirowanie władz do podejmowania decyzji korzystnych dla przeciwnika	rozpowszechnianie fałszywych informacji, np. podważających zaufanie do władz, tworzących pozytywną atmosferę dla przeciwnika
Konsekwencje udanych działań	uzyskanie niejawnej kontroli nad władzami, decydentami, służbami specjalnymi	stworzenie w społeczeństwie wpływowej grupy lobbującej na rzecz decyzji korzystnych dla przeciwnika (np. ograniczenia modernizacji armii)
Cel strategiczny działań	zdominowanie percepcji społeczeństwa oraz podporządkowanie lub przejęcie ośrodków władzy państwa	

Tabela 2: Różnice pomiędzy dezinformacją operacyjną i dezinformacją propagandową

Źródło: opracowanie własne

Dezinformacja propagandowa w mediach elektronicznych

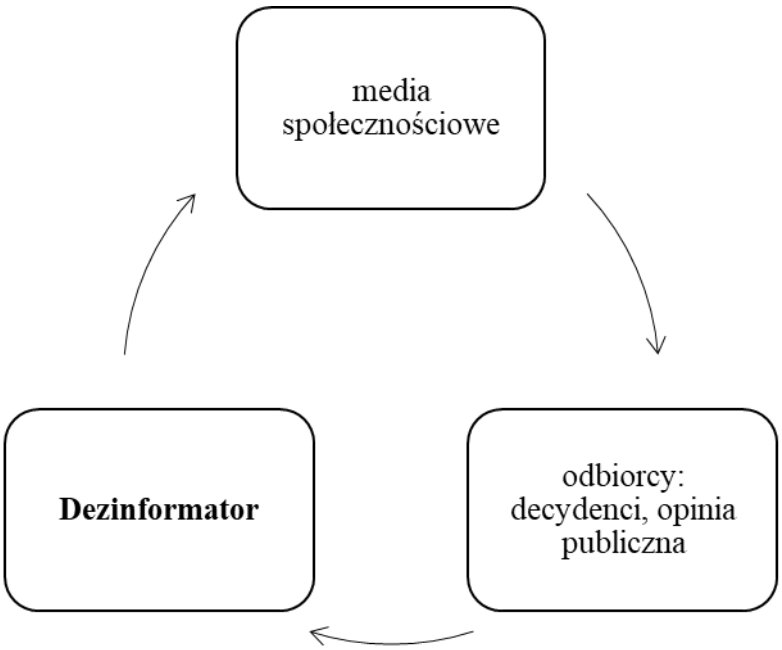
W erze mediów cyfrowych infosfera stała się w jeszcze większym stopniu środowiskiem bezpieczeństwa społeczeństwa i pojedynczego człowieka. Nieustannie jest on poddany „inwigilacji ze strony technologii informacyjnych, elit rządzących, użytkowników sieci i samych siebie" (Batorowska, 2018, s. 140). Stworzenie globalnej sieci komunikacyjnej, oprócz pozytywnych zmian (np. w zakresie dostępu do informacji), doprowadziło również do negatywnych konsekwencji (np. wzrost postaw indywidualistycznych, dezintegracja społeczności, rozpad więzi społecznych uznawanych dotychczas za trwałe). Podmioty stosujące dezinformację, w tym służby specjalne, uzyskały ogromne możliwości wywierania wpływu na społeczeństwa. Internet nie posiada takich ograniczeń jak radio, prasa, czy nawet telewizja (zobacz Tabela 3). Nieograniczone możliwości rozpowszechniania informacji, szybkość dotarcia do odbiorcy, niskie koszty przyczyniły się do tego, że Internet stał się środowiskiem, w którym prowadzone są działania wojenne. Celem ataku nie jest infrastruktura informatyczna, ale umysł człowieka. Dąży się do zmanipulowania odbiorców, wywarcia wpływu, zmiany ich percepcji oraz wywołania postaw pożądanych dla agresora (Wasiuta i Wasiuta, 2017, s. 72). Z tego powodu współczesne pole walki informacyjnej charakteryzuje się takimi działaniami jak dezinformacja, manipulacja, parainformowanie, zniekształcanie informacji. Umożliwiają one stworzyć fałszywy obraz danego obiektu oraz ukierunkować procesy decyzyjne i zarządcze w zgodzie z wolą agresora. (Batorowska, 2017, s, 181). Dzięki powszechnemu dostępowi do mediów społecznościowych stały się one ważnymi instrumentami prowadzenia takiej walki. Postęp technologiczny umożliwił rozpowszechnianie fałszywych treści przez smartfony. Stosowanie plotki, dezinformacji stało się bardzo proste, nigdy nie było do tego tak dogodnych warunków (Walewski, 2020, s. 12).

Uwarunkowania	Media tradycyjne	Media elektroniczne
Kanały rozpowszechniania dezinformacji	tytuły prasowe, rozgłośnie radiowe, stacje telewizyjne	media społecznościowe, twitter, facebook, komentarze na portalach
Zasięg dezinformacji	wąski i ograniczony do czytelników, słuchaczy, widzów	potencjalnie nieograniczony
Nakłady finansowe	wysokie, związane z utrzymaniem redakcji lub agentury wpływu; korumpowaniem środowisk opiniotwórczych	niskie, dotyczą wykorzystania istniejącej już infrastruktury cyfrowej
Autor dezinformacji (instrumenty dezinformacji)	konieczność posiadania w redakcji zaufanego redaktora, agenta wpływu lub możliwości zainspirowania redakcji do publikacji materiału dezinformacyjnego	praktyczna każda osoba mająca dostęp do sieci internetowej i korzystająca z niej
Powielanie dezinformacji	konieczność wskazania źródła cytowania, przytoczenie informacji	multiplikowanie bez ograniczeń, nawet bez zgody twórcy, pierwotnego autora treści
Szybkość rozpowszechniania	uzależniona od cyklu wydania tytułu prasowego, emisji programu	natychmiastowa, bieżąca, w czasie rzeczywistym
Możliwości kontroli treści w mediach	kontrola pierwotna wewnątrz redakcji: redaktor naczelny, wydawca, kolegium redakcyjne; wtórna sądowa; w państwach niedemokratycznych cenzura	brak systemu kontroli pierwotnej; tworzenie algorytmu selekcji treści i blokowania profili; uznaniowość kryteriów blokady; kontrola sądowa iluzoryczna
Odpowiedzialność za podanie fałszywej informacji	odpowiedzialność za zniesławienie na drodze sądowej	znikoma, uzależniona m.in. od ustalenia i wskazania autora zniesławiających treści w sieci

Tabela 3: Uwarunkowania dezinformacji propagandowej w mediach tradycyjnych (prasa, radio, telewizja) oraz w mediach elektronicznych (serwisy społecznościowe, komunikatory, portale informacyjne)

Źródło: opracowanie własne

O ile w przeszłości propaganda i związana z nią dezinformacja w tradycyjnych mediach była ważnym uzupełnieniem działań militarnych, to obecnie rola dezinformacji propagandowej niepomiernie wzrosła, stając się jednym z głównych instrumentów prowadzenia walki. Media społecznościowe gwarantują niskie nakłady finansowe, nieograniczony zasięg i szybkość rozprzestrzeniania dezinformacji oraz bardzo krótką tzw. „pętlę dezinformacji". Masowość mediów społecznościowych powoduje, że istnieje możliwość, choć nie jest to konieczne, wyeliminowania agentury wpływu w mediach. Podobnie etap uwiarygodniania przekazu dezinformacyjnego oraz korzystanie w tym celu z przychylnych ekspertów (zobacz Rysunek 3).



Rysunek 3. Skrócona pętla dezinformacji propagandowej. Masowe kampanie w mediach społecznościowych

Źródło: opracowanie własne

Państwa prowadzą takie działania w cyberprzestrzeni od ponad dekady. W 2008 r. podczas wojny gruzińsko-rosyjskiej obie strony konfliktu zamieszczały na stronach internetowych przeciwnika materiały mające go skompromitować (Lakomy, 2015, s. 102). Szczególnie aktywna pod tym względem jest Federacja Rosyjska. Na ten problem zwracały uwagę rządy państw UE i USA, instytucje międzynarodowe oraz prywatne think-tanki. W czerwcu 2017 r. Constanze Stelzenmüller z Brookings Institution oświadczyła przed komisją wywiadu Senatu USA, że celem rosyjskiej wojny informacyjnej jest osiągnięcie sukcesu w destabilizacji Europy. Innowacyjne zastosowanie środków technologicznych sprawiło, że działania te odznaczały się większą skutecznością niż wcześniejsze próby. Współczesna rosyjska teoria wojny informacyjnej jest zaktualizowaną wersją starszych metod pochodzących jeszcze z czasów komunizmu. Rosyjskie techniki walki informacyjnej są wyrafinowane i wielowymiarowe. (Cockrell, 2017). Na negatywny wpływ technologii informacyjnej i komunikacyjnej

na infosferę wskazano m.in. w raporcie Zgromadzenia Parlamentarnego NATO, który został opracowany pod kierunkiem Thomasa Joplinga. Rozwój mediów społecznościowych, pozwolił Moskwie zorganizować dezinformację i propagandę na wyższym poziomie. W dokumencie przytoczono wiele przykładów prokremlowskiej propagandy, np. bezpośrednie zagrożenie wojną domową w Szwecji, zrzucenie przez amerykański samolot bomby atomowej nad Litwą, wzrost liczby przypadków gwałtów w Szwecji o tysiąc procent (w rzeczywistości nastąpił o 1,4% od 2015 r.), tworzenie paniki w amerykańskim stanie Luizjana poprzez masowe tweetowanie na temat rzekomego wycieku chemicznego, opisywanie Ukrainy jako „państwa upadłego". (Committee on the Civil Dimension of Security NATO Parliamentary Assembly, 2018). Federacja Rosyjska była również oskarżana o wywieranie wpływu, m.in. za pomocą mediów społecznościowych, na referendum brexitowego w 2016 r. Celem propagandy Kremla było osłabienie międzynarodowej pozycji Wielkiej Brytanii oraz rozbicie wewnętrzne państwa i zdestabilizowanie sytuacji, polaryzacja mieszkańców oraz wprowadzenie zamieszania i dezinformacji w debacie publicznej (Ellehuus, 2020). Z kolei podczas wyborów prezydenckich we Francji w 2017 r. Rosja wsparła prawicową kandydatkę Marine Le Pen. Jej Front Narodowy otrzymał bezpośrednie wsparcie finansowe w formie pożyczek w wielomilionowych euro. W mediach społecznościowych wykorzystano rosyjskie boty, które rozpowszechniały treści promujące Le Pen i zwalczające jej przeciwnika Emanuela Macron (Cockrell, 2017). Rosja prowadziła również kampanię dezinformacyjną związaną z pandemią choroby COVID-19. Fałszywie informowano o przyczynach i charakterze choroby, sugerowano rozpad UE, rozpowszechniano treści mogące wywołać nieufność społeczeństw do władz państw. Aktywne były również konta na Twitterze zaliczane do tzw. „ruskich trolli" (Bączek, 2020, s. 8, 10; Jarynowski i in., 2020, s. 100). Rosja podjęła również kampanię dezinformacyjną, mającą przekonać, że m.in. zachodnie szczepionki są mało bezpieczne i najprawdopodobniej nie zadziałają (Broniatowski, 2020). Pomimo zmasowanych kampanii dezinformacyjnych, zachodnie demokracje nie wypracowały właściwej odpowiedzi na te zagrożenia. W kontekście niniejszych rozważań warto również przytoczyć opracowanie zespołu ekspertów UE, którzy przeanalizowali środki prawne i strategie polityczne państw członkowskich i Unii mające przeciwdziałać dezinformacji i propagandzie. Uznali oni, że ograniczenia prawne w zakresie treści „mogą spowodować większe szkody dla demokracji niż samo zjawisko dezinformacji" (Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego, marzec 2019). Z tego punktu widzenia przytoczona opinia Volkoffa z 1986 r., że zachodnie państwa mają wpisane w swój system nieumiejętność obrony przed dezinformacją (Volkoff, 1991, s. 13), nadal jest aktualna.

Podsumowanie

Reasumując przeprowadzone analizy, należy wskazać, że materiał badawczy pozwolił na pozytywne zweryfikowanie wstępnej hipotezy: dezinformacja jako szczególna forma walki informacyjnej oddziałuje na ośrodki władzy państwowej, służby specjalne, wojsko, ale istnieje także typ tajnej dezinformacji, który bezpośrednio wpływa na społeczeństwo. Typy dezinformacji podane przez Golicyna, czyli strategiczna, polityczna, wojskowa, techniczna, ekonomiczna, dyplomatyczna (Golicyn, 2007, s. 53), wpływają bezpośrednio na władze państwowe, służby specjalne, dyplomację, system gospodarczy państwa itp. Są to pierwotne cele operacji z tej kategorii dezinformacji. Społeczeństwo może również odczuć negatywne konsekwencje w sposób pośredni, np. po zmianie polityki władz, uwarunkowań zewnętrznych. Tak stało się w przypadku dezinformacji operacyjnej „TRUST". W przypadku dezinformacji propagandowej głównym celem jest opinia publiczna w danym państwie lub opinia międzynarodowa. Za wyodręb-

nieniem takiej kategorii dezinformacji przemawia również powszechne wykorzystanie mediów do takich działań. Dezinformacyjny przekaz propagandowy jest realizowany sposób tajny, w tym także metodami operacyjnymi, np. dzięki agenturze wpływu. Jawny komponent propagandowy jest rozpowszechniany w sposób masowy. Analiza konkretnych przedsięwzięć dezinformacyjnych umożliwiła również pozytywną weryfikację szczegółowych pytań problemowych. Ze względu na różnice, m.in. w celach taktycznych i metodach działań, należy rozróżnić dezinformację operacyjną służb specjalnych oraz dezinformacją propagandową, która wprost oddziałuje na opinię społeczną i w ten sposób pośrednio na decydentów. Dezinformacja propagandowa jest środkiem stosowanym w walce informacyjnej. Stworzenie cyberprzestrzeni oraz pojawienie się mediów społecznościowych zwiększyło możliwości takich działań. W ostatnich latach zaobserwowano intensywne wykorzystanie mediów elektronicznych do kampanii dezinformacyjnych. W epoce społeczeństwa informacyjnego zmieniły się uwarunkowania dezinformacji propagandowej (zobacz Tabela 3). Infosfera państw demokratycznych jest narażona na ciągłe ataki i nie jest skutecznie chroniona przed tymi zagrożeniami. Dlatego powinna być monitorowana przez instytucje bezpieczeństwa państwa, w tym wywiad i kontrwywiad, przy zachowaniu praw obywatelskich. Ciągły rozwój metod dezinformacyjnych powoduje, że należy przystąpić do tworzenia mechanizmów obronnych, zaś prawo obywatela do informacji powinno zostać uzupełnione o prawo do ochrony przed dezinformacją.

Bibliografia

1. Andrew, Ch. (1998). *Tylko dla oczu prezydenta. Od Washingtona do Busha – amerykańscy prezydenci i tajne służby.* Warszawa: Wydawnictwo Colori.
2. Andrew Ch., Gordijewski, O. (1999). *KGB.* Warszawa: Dom Wydawniczy Bellona.
3. Andrew, Ch., Mitrochin, W. (2006). *Archiwum Mitrochina II. KGB i świat.* Poznań: Dom Wydawniczy REBIS.
4. Andrew, Ch., Mitrochin, W. (2009). *Archiwum Mitrochina I. KGB w Europie i na Zachodzie*. Poznań: Dom Wydawniczy REBIS.
5. Batorowska, H. (2017). *Analityk w środowisku walki o dominację i przetrwanie*. (w:) Batorowska H. (red.). *Walka informacyjna: uwarunkowania, incydenty, wyzwania*. Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją.
6. Batorowska, H. (2018). *Indywidualne zarządzanie informacją zabezpieczeniem przed manipulacją w środowisku płynnej inwigilacji*. „Edukacja – Technika – Informatyka" nr 1 (23).
7. Bączek, P. (2020). *Kampanie dezinformacyjno-propagandowe jako rodzaj zagrożeń informacyjnych w sytuacjach kryzysowych na przykładzie pandemii choroby COVID-19*. „Security Review", nr 3 (16).
8. Boghardt, T. (2009). *Operation INFEKTION – Soviet Bloc Intelligence and Its AIDS Disinformation Campaign*, „Studies in Intelligence", vol. 53, nr. 4.
9. Broniatowski, M. (red.). (2020.11.24). *Koronawirus. W wyścigu po szczepionkę Rosja sięga po dezinformację*. https://www.onet.pl/informacje/onetwiadomosci/koronawirus-w-wyscigu-po-szczepionke-rosja-siega-po-dezinformacje/wvk31ce,79cfc278.
10. Cockrell, C.D. (2017). *Russian Actions and Methods against the United States and NATO*. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Russian-Actions-and-Methods/.

11. Committee on the Civil Dimension of Security (CDS) NATO Parliamentary Assembly (2018). *Countering Russia's Hybrid Threats: An Update. Special Report by Lord Jopling (United Kingdom) Special Rapporteur 166 CDS 18 E fin. Original: English*. https://www.nato-pa.int/view-file?filename=/sites/default/files/2018-12/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20-%20JOPLING_0.pdf.

12. Darczewska, J., Żochowski, P. (2017). *Środki aktywne. Rosyjski towar eksportowy.* Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia.

13. Ellehuus, R. (2020). *Mind the Gaps: Russian Information Manipulation in the United Kingdom*. https://www.csis.org/analysis/mind-gaps-russian-information-manipulation-united-kingdom.

14. Epstein, E.J. (1993). *Podstęp. Niewidzialna wojna między KGB a CIA*. Krosno: Oficyna Wydawnicza Scripta Manent.

15. Faligot, R., Guisnel, J., Kauffer, R. (2019). *Francuskie służby specjalne.* Warszawa: Oficyna Wydawnicza RYTM.

16. Fehler, W. (2012). *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne.* Warszawa: Arte.

17. Fehler, W. (2016). *O pojęciu bezpieczeństwa informacyjnego*. (w:) Kubiak M.. Topolewski S. *Bezpieczeństwo informacyjne w XXI wieku*. Siedlce-Warszawa: Pracownia Wydawnicza Wydziału Humanistycznego UPH w Siedlcach.

18. Golicyn, A. (2007). *Nowe kłamstwa w miejsce starych.* Warszawa: Biblioteka Służby Kontrwywiadu Wojskowego.

19. Helma, S. (2018). *Dezinformacja i wojna psychologiczna jako element polityki Związku Sowieckiego i Federacji Rosyjskiej*. „Zeszyty Naukowe Towarzystwa Doktorantów UJ. Nauki Społeczne", , nr 3 (22).

20. Jarynowski, A., Wójta-Kempa, M., Belik, V. (2020). Percepcja „koronawirusa" w polskim Internecie do czasu potwierdzenia pierwszego przypadku zakażenia SARS-CoV-2 w Polsce. Perception of "coronavirus" on the Polish Internet until arrival of SARS-CoV-2 in Poland. „Pielęgniarstwo i Zdrowie Publiczne", nr 10 (2) https://www.academia.edu/42148077/Percepcja_Koronawirusa_w_polskim_Interneciedo_potwierdzenia_pierwszego_przypadku_wirusa_w_Polsce.

21. Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego. (marzec 2019). *Dezinformacja i propaganda – wpływ na funkcjonowanie państwa prawa w UE i jej państwach członkowskich. Streszczenie*. https://ww.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019) 608864 (SUM01)_PL.pdf.

22. Kropp, P. (1999). *Sekrety wywiadu francuskiego.* Warszawa: Oficyna Wydawnicza RYTM, Dom Wydawniczy Bellona.

23. Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

24. Larecki, J.H. (2017). *Wielki leksykon służb specjalnych świata. Organizacje wywiadu, kontrwywiadu i policji politycznych, terminologia profesjonalna i żargon operacyjny*. Warszawa: Oficyna Wydawnicza RYTM.

25. Liedel, K., Serafin, T. (2011). *Otwarte źródła informacji w działalności wywiadowczej*. Warszawa: Difin.

26. Minkina, M. (2014). *Sztuka wywiadu w państwie współczesnym*. Warszawa: Wydawnictwo Bellona, Oficyna Wydawnicza Rytm.

27. Minkina, M., Gałek, B. (2015). *Kłamstwo i podstęp we współczesnym świecie*. Warszawa: Oficyna Wydawnicza RYTM.

28. Nowak, E., Nowak, M. (2011). *Zarys teorii bezpieczeństwa narodowego*. Warszawa: Difin.

29. Ockrent, Ch., de Marenches, A. (1992). *Sekrety szpiegów i książąt.* Warszawa: Editions SPOTKANIA.

30. Świerczek, M. (2013). *Władysław Michniewicz, Wielki bluff sowiecki*. „Przegląd Bezpieczeństwa Wewnętrznego", nr 9 (5).

31. Ustawa z 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm).

32. Volkoff, V. (1991). *Dezinformacja oręż wojny*. Warszawa: wydawnictwo Delikon.

33. Walewski, Ł. (2020). *Wł@dza w sieci. Jak nami rządzą social media*. Kraków: Wydawnictwo WAM.

34. Wasiuta, O., Wasiuta, S. (2017). *Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości*. (w:) Batorowska H. (red.). *Walka informacyjna: uwarunkowania, incydenty, wyzwania*. Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją.

35. Zając, E. (2012). *Tajna Komisja Robotnicza Hutników NSZZ „Solidarność" Huty im. Lenina (1982-1989)*. „Sowiniec Półrocznik Centrum Dokumentacji Czynu Niepodległościowego", nr 40.

INFORMACYJNE INSTRUMENTY PRZECIWDZIAŁANIA I ZWALCZANIA TERRORYZMU

Waldemar Gołuchowski

Abstract

Information instruments for counteracting and combating terrorism

The aim of the article is to present the role of information in combating terrorism. The first part of the article presents information instruments for counteracting terrorism, paying particular attention to the information and education policy and the need for an inter-institutional approach. Information instruments for combating terrorism are discussed in the second part. Particular attention was paid to the role of intelligence and counterintelligence as well as the Internet as the field in which the information fight against terrorism takes place. The article also highlights the role of the media in the discussed subject. In addition, it underlines the importance of information in countering terrorism at its root in its early stage and the need to create alternative and competitive patterns for the individuals / communities upon which terrorism is based.

Keywords: terrorism, information, information struggle, counter-terrorism policy, information warfare instruments

Wstęp

Informacja w dziejach człowieka zawsze odgrywała ważną rolę, bez względu na to, czy z tego zdawano sobie sprawę, czy nie. Jednak we współczesnym świecie nabierała ona szczególnej wartości, co więcej, jej znaczenie systematycznie wzrasta, co należy wiązać m.in. z rozwojem technologii, systemów informatycznych, pojawianiem się coraz to nowych narzędzi i powszechności dostępu do nich.

Wzrost roli i znaczenia informacji oraz technologii z nią związanych spowodował, że zmaterializowała się zrodzona w latach sześćdziesiątych XX w. idea społeczeństwa informacyjnego. Informacja i jej przekazywanie stanowią ważny element naszego życia codziennego. Jesteśmy coraz bardziej zależni od napływu różnych informacji, dostarczanych przez systemy informacyjne, które ulegają ciągłemu rozwojowi i ulepszaniu. W społeczeństwie informacyjnym informacja dominuje we wszystkich dziedzinach życia. Powoduje to, że współczesne społeczeństwo jest bardzo podatne na manipulowanie, dezinformację i inne formy ataków w tym obszarze, dokonywanych przez różne podmioty (państwa, organizacje i grupy interesów) dążące do osiągania zaplanowanych przez siebie celów.

W tak zarysowanym kontekście istnieje szereg mało rozpoznanych mechanizmów. Jeden z nich dotyczący miejsca i zakresu stosowania różnych form oddziaływania informacyjnego w procesie zapobiegania i zwalczania działalności grup terrorystycznych stanowi problem badawczy będący podstawą prowadzonych w dalszej części artykułu analiz.

Szeroką gamę możliwości tkwiących w społeczeństwie informacyjnym dostrzegają i wykorzystują także organizacje terrorystyczne. Terroryści szybko zrozumieli wartość systematycznego gromadzenia i analizy informacji w swojej działalności. Jednym z dowodów na to może być przechwycony przez służby wywiadowcze USA podręcznik treningowy Al-Kaidy, w którym podkreśla się wagę zbierania informacji o wrogu, terenie, infrastrukturze i sąsiadach, rozpowszechniania fałszywych informacji (plotek i oświadczeń, które nastawiają społeczeństwo przeciwko wrogowi); posługiwanie się fałszywymi dokumentami tożsamości; celowe, ale ostrożne korzystanie z nowoczesnych systemów informatycznych (czas trwania transmisji faksymile i bezprzewodowej nie powinien przekraczać pięciu minut w celu zapobiegania wskazaniu lokalizacji urządzenia) (Podręcznik treningowy Al Kaidy http://www.usdoj.gov/ag/ trainingmanual.html).

Znając te i inne poglądy terrorystów na rolę i znaczenie działalności informacyjnej, państwa i ich instytucje stosują coraz więcej nowych (ale także tradycyjnych) narzędzi informacyjnych służących do zapobiegania i zwalczania terroryzmu. Zasadniczym celem badawczym artykułu uczyniono ukazanie tego, jakie są to narzędzia i w jaki sposób są stosowane.

Informacyjne instrumenty przeciwdziałania terroryzmowi

Bardzo istotnym lub wręcz kluczowym elementem walki z terroryzmem jest działalność informacyjna i edukacyjna. Ważne w tym zakresie są działania profilaktyczne, komunikacja właściwych służb, organów i instytucji ze społeczeństwem w ramach polityki informacyjnej i edukacyjnej przeciwdziałającej terroryzmowi. Jej istotnym celem jest bieżące zapoznawanie społeczeństwa ze sposobami zachowania w przypadku wystąpienia określonych rodzajów incydentów terrorystycznych, poczynając od informowania odpowiednich służb o zaobserwowaniu podejrzanych zdarzeń i osób, aż po kwestie ogólnych zasad zachowania w konkretnych sytuacjach. Poprzez właściwie prowadzoną politykę w tej sferze, społeczeństwo może stać się ważnym ogniwem w zakresie rozpoznawania zagrożeń o charakterze terrorystycznym i ograniczania ich skutków.

W polityce informacyjnej istotne znaczenie ma również podnoszenie świadomości i kształtowanie pożądanych postaw ludzi w sytuacji wystąpienia kryzysów związanych z atakami terrorystów, a także wypracowanie mechanizmów współpracy oraz wymiany informacji między organami administracji publicznej a środkami masowego przekazu, uwzględniających sposób formułowania przekazu w przypadku wystąpienia bezpośredniego zagrożenia.
Także organizacje pozarządowe działające na rzecz edukacji w zakresie bezpieczeństwa i porządku publicznego mogą być wykorzystywane do działań profilaktyczno-edukacyjnych, a w przypadku wystąpienia sytuacji kryzysowej, dodatkowo angażowane również do działań w zakresie ochrony ludności.

Zauważyć w tym miejscu należy, że istnieje potrzeba międzyinstytucjonalnego podejścia do kwestii antyterrorystycznej polityki informacyjnej. Niezwykle istotną rolę ma do odegrania w tym względzie współpraca pomiędzy instytucjami i służbami państwowymi a środowiskiem dziennikarskim. W zakres tej współpracy wchodzić powinny m.in.: kwestia dziennikarskiej autocenzury (w przypadkach, w których publikacja danej informacji mogłaby stanowić zagrożenie dla bezpieczeństwa), szkolenia szefów redakcji/dziennikarzy (w zakresie zagrożeń związanych z ewentualnym wykorzystaniem przez terrorystów mediów oraz konieczność prowadzenia właściwej polityki informacyjnej), bieżąca współpraca służb i instytucji systemu antyterrorystycznego z mediami (w celu stworzenia atmosfery wzajemnego zrozumienia i zaufania). Istnieje potrzeba budowania płaszczyzny współpracy z mediami jeszcze przed wystąpieniem zda-

rzenia o charakterze terrorystycznym. Wskazane jest organizowanie szkoleń dla dziennikarzy z zakresu niwelowania propagandowego oddziaływania terrorystów, jak również podnoszenia świadomości społecznej na temat zagrożenia terrorystycznego. Kompleksowa, przeciwdziałająca terroryzmowi strategia informacyjna o charakterze komunikacyjno-edukacyjnym, prowadzona przy udziale oraz w kooperacji z mass mediami stanowi obecnie niezbędny składnik każdego nowoczesnego systemu przeciwdziałania terroryzmowi.

Zdaniem byłego doradcy amerykańskiego prezydenta Jimmy'ego Cartera – Zbigniewa Brzezińskiego, „ten kto zrobi pierwszy krok i puści informacje w świat może nadać całemu wydarzeniu swoją interpretację" (Gillert, 2007, s. 16). Uzyskanie takiej przewagi przez aparat państwowy w momencie zaistnienia sytuacji kryzysowej wydaje się być kluczowe. Pozwala to nadać danemu zdarzeniu pożądaną interpretację i postrzeganie. Państwa prowadzące na co dzień rzetelną oraz wyprzedzającą i przeciwdziałającą terroryzmowi politykę informacyjną, zyskują również wzrost zaufania zarówno ze strony własnych obywateli, jak i międzynarodowych partnerów. To z kolei wydatnie przedkłada się na zaangażowanie wspomnianych podmiotów w wielostronną współpracę, która jest nieodzownym składnikiem skutecznego zwalczania zjawiska terroryzmu.

Polityka informacyjna przeciwdziałająca zjawisku terroryzmu powinna zawierać dwa zasadnicze filary: prewencyjny i reaktywny. Obszar szeroko rozumianych działań prewencyjnych, to ten, w którym określone zostaną odpowiednie kanały informacyjne służące do komunikacji ze społeczeństwem na temat możliwych zagrożeń oraz właściwych postaw, jakie obywatele powinni wykazywać w przypadku zauważenia niepokojących sygnałów. Jest to bardzo istotny element polityki informacyjnej, w ramach którego zadaniem państwa jest dostarczenie opinii publicznej odpowiedniej ilości informacji (w tym o środkach i metodach ochrony bezpieczeństwa osobistego), przygotowującej społeczeństwo do właściwego postępowania w sytuacjach kryzysowych. W skład tego nurtu działań wchodzić powinno także budowanie odporności na przekazy informacyjne płynące od terrorystów (propagowanie ideologii, szerzenie dezinformacji, zastraszanie). W drugim filarze powinno się wypracować i umieścić stosowne informacyjne środki zaradcze, służące do ostrzegania opinii publicznej w sytuacjach realnego zagrożenia zamachem terrorystycznym oraz te, które będą używane podczas wystąpienia sytuacji kryzysowych, związanych z atakami terrorystycznymi.

W polityce informacyjnej służącej przeciwdziałaniu terroryzmowi równie ważną rolę odrywają wymienione już wcześniej media. Stanowią one wszechobecne narzędzie przekazu informacji na skalę masową. Posiadanie umiejętności komunikowania się i przekazywania informacji za pomocą tych mediów może stać się cennym elementem systemu przeciwdziałania terroryzmowi. Wpływowi środków masowego przekazu oprócz tak zwanych „zwykłych obywateli" podlegają bowiem także (i liczą się z tymi mediami) przedstawiciele władz, terroryści, ofiary ataków terrorystycznych i ich rodziny. Niebezpieczeństwo związane ze zbyt szybkim podawaniem przez media do publicznej wiadomości informacji wrażliwych tkwi w tym, że mogą być one wykorzystane przez terrorystów i/lub spowodować panikę wśród społeczeństwa, co może prowadzić do chaosu i innych zagrożeń. Do mediów należy zatem przekazywać wyłącznie sprawdzone i potwierdzone wiadomości, aktualizowane z odpowiednią częstotliwością, aby nie wprowadzać zamieszania. Dobra współpraca sektora służb kontrterrorystycznych z mediami w sytuacji zaistnienia zdarzenia terrorystycznego powinna się wyrażać między innymi w: wydawaniu oświadczeń dla prasy, regularnym zwoływaniu konferencji prasowych, organizowaniu wywiadów, zapewnieniu warunków pracy dla mediów, publikowaniu zdjęć i ilustracji związanych z zamachem, bieżącym przekazywaniu informacji, organizowaniu briefingów prasowych itp.

Bardzo ważnym instrumentem informacyjnego przeciwdziałania terroryzmowi jest Internet. Dla przykładu, w Republice Federalnej Niemiec w celu przeciwdziałania zagrożeniom terrorystycznym w Internecie powołane zostało Wspólne Centrum Internetowe. Jako internetowa placówka monitorująca, centrum to zajmuje się od 2007 r. terroryzmem międzynarodowym motywowanym religijnie. Dla zwiększenia możliwości w zakresie kontroli Internetu wykorzystuje ono specjalne oprogramowania mające na celu wykrywanie i przewidywanie przyszłych działań terrorystów. Dodatkowo niektóre kraje związkowe w RFN, dla zwiększenia możliwości przeciwdziałania terroryzmowi w Internecie, utworzyły tzw. on-line Wachen, czyli straż internetową (Hołyst, 2009 s. 10).

Istotnym zagadnieniem z zakresu informacyjnego przeciwdziałania terroryzmowi jest kwestia finansowania organizacji terrorystycznych. Dla przykładu, w Polsce mowa o tym jest zarówno w prawie krajowym jak i Unii Europejskiej. Najważniejszym dokumentem w tym zakresie jest ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2018 r., poz. 723, ze zm.). Wymienia się w niej organy i podmioty funkcjonujące w ramach tego systemu, a także definiuje ich obowiązki i uprawnienia. Najważniejszym elementem przeciwdziałania finansowaniu terroryzmu jest Generalny Inspektor Informacji Finansowej, który jest wspierany przez Departament Informacji Finansowej Ministerstwa Finansów. Zadaniem tego organu jest przeprowadzanie analiz, a następnie informowanie o swoich podejrzeniach co do potencjalnego finansowania terroryzmu.
W naszym kraju system przeciwdziałania finansowaniu terroryzmu tworzą:

- Generalny Inspektor Informacji Finansowej;
- instytucje obowiązane (tj. podmioty zarówno z sektora finansowego, jak i niefinansowego, które oferują usługi lub produkty mogące być wykorzystane wbrew ich przeznaczeniu do prania pieniędzy lub finansowania terroryzmu – lista kategorii instytucji obowiązanych znajduje się w art. 2 ust. 1 ustawy);
- jednostki współpracujące (organy administracji rządowej, organy jednostek samorządu terytorialnego oraz inne państwowe jednostki organizacyjne, a także Narodowy Bank Polski, Komisja Nadzoru Finansowego i Najwyższa Izba Kontroli).

Ustawa określa obowiązki wymienionych wyżej podmiotów szczególnie akcentując kwestie współpracy i wymiany informacji. Głównym zadaniem instytucji obowiązanych jest rozpoznanie i ocena ryzyka finansowania terroryzmu. W przypadku zaistnienia podejrzeń w tym zakresie zawiadamiają one Głównego Inspektora Informacji Finansowej (https://www.gov.pl/web/finanse/przeciwdzialanie-praniu-pieniedzy-i-finansowaniu-terroryzmu).

Reasumując ten fragment rozważań należałoby wskazać, że skuteczność polityki informacyjnej mającej zapobiegać terroryzmowi zależy od poziomu realizacji następujących zasadniczych celów:

- budzenie świadomości społecznej, poprzez regularne przekazywanie opinii publicznej informacji o planach oraz inicjatywach krajowych i zagranicznych, wprowadzanych dla zwiększenia bezpieczeństwa państwa na polu przeciwdziałania terroryzmowi;
- wprowadzenie czytelnego oraz powszechnie dostępnego dla ludności w mediach systemu wczesnego ostrzegania przed aktywnościami terrorystycznymi, w którym jeden z czterech określonych poziomów zagrożenia determinuje wprowadzenie danego scenariusza działania dla instytucji stanowiących narodowy system do walki z terroryzmem oraz postępowania ludności;
- nawiązanie antyterrorystycznej współpracy pomiędzy obywatelami oraz środowiskiem biznesu i instytucjami państwowymi odpowiedzialnymi za ich ochronę;

- przygotowanie społeczeństwa do właściwego reagowania, poprzez edukowanie jednostek oraz podmiotów zbiorowych w zakresie zasad bezpieczeństwa, w celu zapobiegania zagrożeniom terrorystycznym w ich wczesnym etapie przygotowania oraz na okoliczność zaistnienia sytuacji kryzysowych wywoływanych przez incydenty terrorystyczne.

Informacyjne instrumenty zwalczania terroryzmu

Podobnie jak w przeciwdziałaniu zjawisku terroryzmu, informacja odgrywa również bardzo ważną rolę w jego bezpośrednim zwalczaniu. Państwa w informacyjnym zwalczaniu terroryzmu wykorzystują różne instrumenty i narzędzia. Do głównych należą służby specjalne (w tym głównie wywiad i kontrwywiad oraz służby kontrterrorystyczne), które bazują na osobowych źródłach informacji, szerokiej gamie środków technicznych oraz otwartych źródłach informacji.

Uzyskiwanie informacji w oparciu o osobowe źródła informacji, zwane też jako HUMINT (ang. Human Intelligence, pol. rozpoznanie osobowe), to różnego rodzaje dane i informacje pozyskiwane od osób dysponującymi możliwościami docierania w sposób bezpośredni lub pośredni do interesujących nas informacji (w omawianej tematyce dotyczy to głównie danych osób zaangażowanych w działalność terrorystyczną, ale także planowanych operacji terrorystycznych, potencjalnych celów, struktur organizacji terrorystycznych, miejsc przechowywania broni i ładunków wybuchowych itp.). Głównych sposobem (ale nie jedynym) zdobywania tych informacji są bezpośrednie spotkania i rozmowy z osobowymi źródłami informacji. Należy pamiętać, że niesie to ze sobą duże zagrożenie dla obydwu stron, związane z potencjalną dekonspiracją. Tego typu spotkania wymagają zatem każdorazowo bardzo starannego przygotowania. Ważną kwestią jest również weryfikacja uzyskiwanych informacji od źródeł osobowych, aby określić wiarygodność danego źródła oraz uniknąć dezinformacji, czy też prowokacji strony przeciwnej, ale również zwykłej konfabulacji (z czym również można się spotkać).

W krajach ogarniętych konfliktami zbrojnymi (Irak, Afganistan, Kosowo czy Bośnia) bazuje się głównie na informacjach pozyskiwanych z osobowych źródeł informacji, dotyczy to zwłaszcza informacji z zakresu zagrożenia terrorystycznego. Jeżeli chodzi o kraje rozwinięte pod względem systemów informacyjnych to zdecydowana większość informacji pochodzi ze źródeł otwartych, tym niemniej najbardziej istotne i kluczowe informacje dotyczące zwłaszcza kwestii terrorystycznych w dalszym ciągu będą pochodziły ze źródeł osobowych (trudno się bowiem spodziewać, że znajdziemy informacje o planowanych zamachach terrorystycznych lub nazwiska terrorystów w prasie, Internecie, czy innych źródłach otwartych) (Stallings i Foley, 2003, s. 43).

Mając powyższe na uwadze wydaje się, że HUMINT jest najbardziej efektywnym sposobem zdobywania informacji w zakresie walki z terroryzmem.

Do bezosobowych źródeł informacji możemy zaliczyć szeroką gamę środków technicznych, a także otwarte źródła informacji często określane jako OSINT (ang. Open Source Intelligence). Spośród tych ostatnich szczególne miejsce zajmuje Internet. To właśnie Internet jest głównym polem, na którym toczy się walka informacyjna z terroryzmem. Poczucie anonimowości jaką daje sieć oraz brak możliwości jej pełnej kontroli powoduje, że terroryści rozlokowani w różnych zakątkach świata mogą tworzyć dobrze zorganizowane struktury. Pierwsze formy wykorzystywania Internetu przez terrorystów sprowadzały się do prostych form ko-

munikowania się oraz prezentowania poglądów. Z biegiem czasu i rozwojem możliwości tego narzędzia, terroryści zaczęli wykorzystywać Internet także w procesie przygotowywania ataków terrorystycznych.

Coraz większa aktywność terrorystów w Internecie oraz powszechność wykorzystywania przez nich tego instrumentu do swoich celów spowodowały, że państwa zaczęły tworzyć różnego rodzaju instytucje do zwalczania terroryzmu na tym polu. Dla przykładu w RFN stworzono Wspólne Centrum Internetowe (niem. Gemeinsame Internetzentrum – GIZ), w którym pracują funkcjonariusze z Federalnego Urzędu Kryminalnego, Urzędu Ochrony Konstytucji, Wywiadu Federalnego, Kontrwywiadu Wojskowego i Prokuratury Federalnej. Centrum to obserwuje cały zakres Internetu, ale samo nie prowadzi dochodzeń. Działają w nim policjanci i funkcjonariusze kontrwywiadu z ekspertami z zakresu językoznawstwa, orientalistami, technikami i prawnikami. Ta współpraca umożliwia analizę działań islamskich ekstremistów i terrorystów oraz szybsze ich rozpoznawanie. Wspomniane Wspólne Centrum Internetowe prowadzi i rozwija współpracę z odpowiednikami w innych państwach europejskich. Współpraca w Europie pozwala uniknąć podwójnej pracy. Kiedy np. terroryści rozpowszechniają deklaracje przez Internet, to nie miałoby sensu, by eksperci z wszystkich 27 krajów członkowskich Unii Europejskiej je wyszukiwali, tłumaczyli z arabskiego i oddzielnie analizowali. Dlatego rząd niemiecki zainicjował (w czasie swojej prezydencji w UE w 2007 r.) projekt check the web („kontroluj sieć") W maju 2007 r. przy Europolu, w Centrum Policyjnej Wymiany Informacji dla celów analizy przestępczości, powołano też portal informacyjny, przez który wszystkie państwa UE mogą dokonywać wymiany informacji. Zaplanowano również odbywanie regularnych spotkań ekspertów UE. Warto dodać, że tego typu działania są systematycznie doskonalone, bowiem terroryści w zakresie korzystania z Internetu starają się coraz bardziej profesjonalnie konspirować i obchodzić kontrolną sieć organów bezpieczeństwa (Hołyst, 2009, s. 7).

Aktywność w Internecie osób zaangażowanych w działalność terrorystyczną wymaga skutecznego przeciwstawienia się im. Tym bardziej, że terroryści znają możliwości jakie daje Internet, a także są szkoleni w zakresie korzystania ze sprzętu informatycznego oraz bezpiecznego korzystania z Internetu, aby uniknąć dekonspiracji. W tym celu często wykorzystują kawiarenki internetowe, czy też otwarte wejścia bezprzewodowej lokalnej sieci komputerowej. Dobrym sposobem zwalczania działalności terrorystycznej jest niezauważone przeszukanie online komputerów osób podejrzanych. Pozwala to na zdobycie takich informacji, których nie zdobyłoby się np. konfiskując komputer. W tym celu stosuje się różne oprogramowania. Dla zwiększenia skuteczności walki informacyjnej z terroryzmem naukowcy Dartmouth College stworzyli technologię, która umożliwi przedsiębiorstwom branży IT wykrywanie i usuwanie materiałów propagandowych terrorystów w sieci natychmiast po ich umieszczeniu. Nowy system polega na utworzeniu cyfrowej sygnatury dla filmów, zdjęć i plików audio. W zamyśle twórców ma to doprowadzić do stworzenia bazy danych takich oznaczonych plików. Metoda ta ma pomóc przedsiębiorstwom z branży IT weryfikować wgrywane na ich serwery treści, sprawdzając czy nie występuje podobieństwo z tymi, które znajdują się już w spisie rekordów. Jeśli zostanie ono wykryte, każde przedsiębiorstwo może ocenić, czy zostały złamane warunki umowy z użytkownikiem i zadecydować o reakcji. Dotychczas media społecznościowe usuwały treści ekstremistyczne głównie w ramach reagowania na powiadomienia ze strony użytkowników. Unikano jednak prowadzenia specjalnych, zakrojonych na szeroką skalę operacji przeciwko terrorystom. Inicjator nowego systemu i jednoczesny szef organizacji „Projekt przeciwdziałania ekstremizmowi" (Counter Extremism Project's) Mark Wallace uważa, że może on odegrać rewolucyjną rolę w przeciwdziałaniu propagandzie terrorystycznej w sieci. Program nazywany PhotoDNA analizuje pod tym kątem każde wgrywane zdjęcie na serwery Microsoftu, Facebooka i Google (Kozłowski, http://www.cyberdefence24.pl/401308,nowe-narzedzia-

do-walki-z-propaganda-terrorystow-w-sieci).

Internet zasadniczo wpłynął zarówno na struktury organizacyjne organizacji terrorystycznych jak i na ich sposób działania. Generalnie stał się on bardzo wygodnym narzędziem oraz dużym ułatwieniem w działalności terrorystycznej na różnych jej etapach. Wykorzystywany jest zarówno do propagowania swoich idei jak i rekrutacji kandydatów do swoich organizacji. Bardzo dobrym przykładem w ostatnim czasie jest bardzo skuteczna rekrutacja w różnych krajach europejskich (poprzez Internet) bojowników przez tzw. Państwo Islamskie. Ponadto, łatwy dostęp poprzez Internet do niezwykle bogatej i szerokiej bazy informacji znacząco ułatwia terrorystom ich działalność. W oparciu o Internet mogą oni typować potencjalne cele ataków oraz zdobywać szereg informacji na ich temat, które są pomocne w przygotowaniach do ataków jak i ich wykonywaniu.

Internet wykorzystywany jest również przez terrorystów do osiągania celów propagandowych a także w przypadku zamachów terrorystycznych do wywoływania strachu i paniki w atakowanym społeczeństwie, jak również wywieranie nacisków w sferze politycznej.
O skali aktywności terrorystów w Internecie może świadczyć ilośc stron internetowych wykorzystywanych przez różne organizacje terrorystyczne. Ich działania w Internecie są celowe i dobrze przemyślane. Swoje działania nakierowują na trzy grupy odbiorców: swoich zwolenników, międzynarodową opinię publiczną i wrogą opinię publiczną, Służby odpowiedzialne za monitorowanie działalności terrorystycznej w Internecie koncentrują się na wykrywaniu stron internetowych wykorzystywanych przez terrorystów, odczytu treści, ich tłumaczeniu oraz archiwizowaniu.

Sposób wykorzystania Internetu przez terrorystów zmienia się i ewoluuje wraz z pojawianiem się nowego oprogramowania oraz coraz to nowych aplikacji.

„Wzrost aktywności w Internecie grup terrorystycznych stanowi część ogólniejszego przesunięcia sposobów ich działania w kierunku, określanym przez Johna Arquilla i Davida Ronfeldta jako „wojna w sieci" (Netwar, Arquilla, Ronfeldt, 2003, s. 1-25). Pojęcie to oznacza nową formę rozgrywania konfliktów i przestępczości w płaszczyźnie społecznej, której uczestnicy działają w małych, rozproszonych grupach, bez centrum dowodzenia i koordynacji. Zdaniem byłego szefa CIA ds. zwalczania terroryzmu Vince'a Cannistraro komunikacja internetowa jest głównym systemem komunikacyjnym Al-Kaidy na całym świecie ponieważ jest bezpieczna, prosta i anonimowa. Właśnie dzięki zdecentralizowanej strukturze Al-Kaida okazała się zręczną, elastyczną, zdolną do dopasowywania się do różnych warunków organizacją. Jej kierownictwo jednak ostrzega członków, że ich strony mogą być obserwowane przez FBI i CIA (Arquilla, Ronfeldt, 2003, s. 1-25.)" Hołyst, 2009, s. 14.

Zakres dostępnych w Internecie informacji powoduje, że terroryści mogą je wykorzystywać w przygotowywaniu zamachów terrorystycznych. Dotyczy to obiektów o różnym znaczeniu i jak pokazują ostatnie przypadki nie muszą to być obiekty o znaczeniu strategicznym dla państwa. aczkolwiek ze względu głównie na wymiar propagandowy, te byłyby najbardziej interesującym celem dla terrorystów.

W świetle powyższego ważne jest odpowiednie wyważenie zakresu informacji podawanych do publicznej wiadomości i zamieszczanych w Internecie tak, aby nie ułatwiać zadania terrorystom, którzy mogliby wykorzystywać niektóre informacje, czy to na etapie przygotowań do zamachów terrorystycznych, czy też do innych własnych celów.

Bardzo ważnym polem walki informacyjnej z terroryzmem są media, które ze względu na oddziaływanie społeczne znajdują się w orbicie zainteresowań wszystkich stron. Spektakularność zamachów terrorystycznych sprawia, że stają się one jednym z ulubionych tematów w relacjach medialnych. Dziennikarze w sytuacjach zagrożenia terrorystycznego sprowadzają

rolę mediów do zadań informacyjnych. Pojawiają się więc niebezpieczeństwa związane ze sposobem relacjonowania wydarzeń, jak na przykład wywoływanie uprzedzeń wobec określonych grup, wzbudzanie poczucia zagrożenia, czy paniki. Powinny być zatem w ramach walki z terroryzmem ustalone jasne reguły przekazywania informacji przez administrację publiczną np. poprzez powołanie centrum kryzysowego lub przedstawiciela do spraw kontaktów z mediami w czasie sytuacji kryzysowej .

Jak już sygnalizowano wcześniej, terroryści dostrzegają znaczenie mediów i starają się je wykorzystywać do własnych celów. Wymiar propagandowy aktywności terrorystów, relacji z dokonywanych przez nich zamachów w światowych mediach ma na celu sparaliżowanie społeczeństwa, zastraszenie, sianie paniki i destabilizowanie państw. Przekaz medialny wywołuje o wiele większe skutki niż ten werbalny, pozbawiony drastycznych realistycznych obrazów skutków zamachu terrorystycznego. Dodać należy jeszcze, że wzniosłe hasła (np. wyzwoleńcze) przekazywane przez terrorystów za pomocą mediów mogą odwracać uwagę od prawdziwych efektów, czyli zabijania niewinnych ludzi. Spektakularność ataków terrorystycznych oraz efekty, jakie wywołują, mogą stanowić zachętę do naśladowania. (Liedel, 2010, s. 77). Konieczna i tu jest zatem współpraca z mediami, ponieważ to one najczęściej są pierwsze na miejscu zdarzenia. To one mogą pomóc i niejednokrotnie zapobiec niepotrzebnie szerzącej się fali paniki. Dzięki mediom sztaby kryzysowe prowadzące działania na miejscu ataku terrorystycznego mogą przekazać istotne informacje, dotyczące zachowania się w zaistniałej sytuacji, czy też miejsc schronienia lub punktów, w których zostanie udzielona pomoc. Większość państw na świecie współcześnie używa mediów do zwalczania terroryzmu. Do tego rodzaju działań potrzebni są odpowiednio przygotowani dziennikarze zajmujący się przygotowywaniem materiałów ukazujących terrorystów i skutków ich działań we właściwym dla tych groźnych przestępców świetle.

Zablokowanie relacjonowania informacji dotyczących akcji terrorystycznych nie jest możliwe w obecnych czasach. W dobie szybko rozwijających się technologii z dziedziny komunikacji oraz Internetu, nałożenie całkowitej cenzury jest bowiem niemożliwe. Ważne jest zatem, aby władze poszukiwały takich możliwości współpracy z mediami, które będą sprzyjały poprawie bezpieczeństwa i jednocześnie uniemożliwią wykorzystanie mediów przez terrorystów do upowszechniania ich ideologicznych poglądów (Bolechów, 2007, s. 29). Dokonując analizy, w jakich płaszczyznach ugrupowania terrorystyczne i rządy mogą wykorzystać media, należy w pierwszym rzędzie wskazać na propagandę. Terroryści do rozpowszechniania swoich ideologii używają mediów, zatem państwa mogą też je jawnie wykorzystywać, informując społeczeństwo o podejmowanych przedsięwzięciach w zakresie walki z terrorystami. Kolejna płaszczyzna to wywołanie strachu. Terroryści używają zastraszania jako najważniejszej i najskuteczniejszej metody oddziaływania na społeczeństwo. Aktywność mediów w tym przypadku powinna być zwrócona nie na relacje, przekazywane często na żywo przez terrorystów, a na to, w jaki sposób postępować w przypadku bezpośredniego zagrożenia życia.

Lekceważenie mediów w kontekście właściwego wykorzystania informacji w aspekcie zwalczania terroryzmu może przyczynić się do wykorzystania ich przez terrorystów (Liedel, 2010, s. 80). Wszystkie zasady dobrej i płynnej współpracy z mediami w przypadku zagrożenia terrorystycznego powinny opierać się na właściwym przekazywaniu informacji. Muszą być one rzetelne, wiarygodne, ale jednocześnie posiadać ogólny charakter ponieważ ujawnienie informacji chronionych operacyjnie i taktycznie może spowodować zagrożenie dla życia i zdrowia ludzi. To od przedstawicieli administracji publicznej zależy, jakie informacje przekażą, jakie będą ich źródła i jak zostaną one zinterpretowane przez media. Szczególnie ważne jest negowanie plotek, które mogą być bardzo szkodliwe oraz zapobieganie przejęcia kontroli nad przekazem do mediów przez ugrupowania terrorystyczne. Należy zaznaczyć, że wyżej opisane relacje

z mediami nie są czysto teoretyczne. Ta metoda współpracy jest stosowana przez państwa, które w szczególności zostały doświadczone atakami ze strony terrorystów (Bolechów, 2004, s. 31). Konkretnym przykładem opisania efektywnej współpracy z mediami jest raport sporządzony przez amerykańską Grupę Zadaniową ds. Zamieszek i Terroru (Bolechów, 2004, s. 31). Biorąc pod uwagę powyżej przedstawione rozważania należy przywołać jeden ważny punkt tego raportu. Na pierwszy plan wysuwa on konieczność wyznaczenia grupy dziennikarzy, którzy będą relacjonować w imieniu wszystkich mediów przebieg danego ataku terrorystycznego. Pomaga to nie tylko w monitorowaniu medialnego przekazu informacji, ale wpływa także na indywidualne postępowanie z przedstawicielami mediów. Kolejnymi zasadami wymienionymi w raporcie są: ograniczanie wywiadów z terrorystami, opóźnianie podawania szczegółów do mediów, które mogłyby zaognić sytuację. Nierozważny przekaz informacji do mediów może bowiem potencjalnie skłonić terrorystów do zabijania zakładników.

Odpowiednio wykorzystując media w ramach walki informacyjnej z terroryzmem można uderzyć w to, co dla terrorystów (w przypadku ataku terrorystycznego) jest najważniejsze, czyli w efekt propagandowy, niwelując go lub co najmniej znacząco zmniejszając.

Reasumując omawiane zagadnienie można stwierdzić, że główne uderzenie informacyjne w walce z terroryzmem powinno być skierowane w podstawy ideologiczne terroryzmu obierając za cel jego deprecjonowanie i dezawuowanie. Podejmowanie walki informacyjnej z terroryzmem już w początkowym stadium docierania terrorystów do nowych jego adeptów powinno powodować, że będzie on się jawił jako nieatrakcyjny i nieopłacalny zwłaszcza dla młodych ludzi (na których większość organizacji terrorystycznych bazuje). Należy zatem tworzyć i propagować alternatywne i atrakcyjniejsze wzorce dla tych osób. Ponadto, należy dążyć do tworzenia, zwłaszcza młodym osobom, atrakcyjniejszej z ich punktu widzenia i ciekawszej interpretacji Koranu – dotyczy to terroryzmu o korzeniach islamskich. Działania informacyjne powinny iść również w kierunku zmiany postrzegania cywilizacji zachodniej wśród społeczeństw reprezentujących inne kręgi kulturowe (szczególnie te muzułmańskie). Najogólniej rzecz ujmując chodzi o doprowadzenie do świadomości społeczności, na których bazują organizacje terrorystyczne, że cywilizacja zachodnia to nie tylko zepsucie i konsumpcjonizm, jak mogą usłyszeć w procesie indoktrynacji od swoich „autorytetów", czy podczas pobytu w meczetach od zradykalizowanych imamów, ale przede wszystkim cywilizacja postępu, nauki i rozwoju, bez którego nie mieliby dzisiaj telefonu komórkowego, Internetu, elektryczności, samochodu, czy też podstawowych leków i że to także cywilizacja, która posiada system wartości. Wymaga to nawiązania współpracy z autorytetami religijnymi i naukowcami zajmującymi się tą sferą w celu wypracowania wspólnej strategii i programów działania.

Podsumowanie

Syntetyzując przedstawioną analizę, należy stwierdzić, że odpowiednio przygotowywane informacje wraz z nowoczesnymi narzędziami służącymi do ich zastosowania, zarówno w przeciwdziałaniu terroryzmowi, jak i w bezpośrednim jego zwalczaniu, pozwolić mogą na znaczące zmniejszenie skali tego zjawiska, a w przypadku wystąpienia zdarzeń o charakterze terrorystycznym – zminimalizować ich skutki.

Skuteczna walka informacyjna z terroryzmem może na tyle ograniczyć zagrożenie terroryzmem, że operacje wojskowe (takie jak np. w Afganistanie), które koncentrują się tak naprawdę na zwalczeniu skutków, a nie przyczyn i co do których skuteczności (zwłaszcza jeśli weźmiemy pod uwagę stosunek kosztu do efektu) opinie są mocno podzielone, nie będą po-

trzebne. Stosując walkę informacyjną z terroryzmem powinno uderzać się przede wszystkim w jego przyczyny i uniemożliwiać lub co najmniej znacząco utrudniać jego rozwój.

Bibliografia

1. Arquilla, J., Ronfeldt, D. R. (2003). *Networks, Netwars and the Fight for the Future*.
2. Bolechów, B. (2004). *Terroryzm w świecie podwubiegunowym*. Toruń: Wydawnictwo Adam Marszałek.
3. Fehler, W. (2015). *Informacyjny wymiar zagrożeń dla bezpieczeństwa współczesnej Polski*. „Przegląd Strategiczny", nr 8.
4. Gillert, P. (8-9 grudnia 2007). *Koniec romantycznej ignorancji – wywiad ze Zbigniewem Brzezińskim*. Dodatek PlusMinus, „Rzeczpospolita".
5. Hołyst, B. (2009). *Internet jako miejsce zdarzenia*. „Prokuratura i Prawo", nr 4
6. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.htm.
7. *Human Intelligence Collector Operations*. (2006). Waszyngton: Departament of the Army.
8. *Intelligence in combatting terrorism*. (2002). Ft. Huachuca: U.S. Army Intelligence Center
9. Liedel, K. (2010). *Zarządzanie Informacją w Walce z Terroryzmu.* Warszawa: Wydawnictwo TRIO.
10. *Podręcznik treningowy Al Kaidy*. http://www.usdoj.gov/ag/ trainingmanual.html.
11. Stallings, R., Foley, M. (2003). *CI and HUMINT operations in support of operation enduring freedom*. „Military Intelligence Professional Bulletin". Ft. Huachuca: U.S. Army Intelligence Center.
12. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2018 r., poz. 723, ze zm.).
13. Verton, D. (2003). *Black Ice: The Invisible Threat of Cyberterrorism*. Nowy Jork: McGraw-Hill Osborne Media.
14. Weimann, G. (20-22 listopada 2007). *Terror im Internet. Der neue Schauplatz, die neuen Herausforderungen*. Materiały z „Herbsttagung des Bundeskriminalamtes".

Sprawozdanie z II Międzynarodowej Konferencji Naukowej z cyklu „Prawa człowieka podstawą demokratycznego państwa prawnego" na temat: Informacyjny wymiar praw człowieka i obywatela

W dniu 25 listopada 2020 roku, za pośrednictwem platformy komunikacyjnej Microsoft Teams, odbyła się II Międzynarodowa Konferencja Naukowa organizowana przez Instytut Nauk Społecznych Akademii Katolickiej w Warszawie oraz Instytut Nauk o Bezpieczeństwie Wydziału Nauk Społecznych Uniwersytetu Przyrodniczo – Humanistycznego w Siedlcach z cyklu „Prawa człowieka podstawą demokratycznego państwa prawnego" na temat: Informacyjny wymiar praw człowieka i obywatela. Mieliśmy okazję wysłuchać dziesięciu wystąpień prelegentów na tematy związane z prawami człowieka ze szczególnym uwzględnieniem płaszczyzny bezpieczeństwa informacyjnego.

Konferencja rozpoczęła się od powitania i wprowadzenia gości i prelegentów przez Przewodniczącego Komitetu Naukowego ks. dr. hab. Piotra Aszyka SJ, prof. AKW oraz Przewodniczącego Komitetu Organizacyjnego dr. hab. Włodzimierza Fehlera, prof. Uczelni.

Jako pierwszy wystąpił ks. dr Robert Wawer SJ, prezentując temat ***Wzrost znaczenia praw informacyjnych – współczesne dylematy***. Poruszył m.in. kwestie historii i genezy informacji od czasów prehistorycznych, aż do współczesnych. Referat stanowił dobry wstęp do poruszanej problematyki Konferencji.

Jako druga wystąpiła dr hab. Kinga Machowicz, prof. KUL. Temat ***Interakcje wolności wypowiedzi z innymi dobrami prawnie chronionymi*** pomógł w zrozumieniu istoty praw człowieka, ich wzajemnych interakcji, kolizji.

Mgr Piotr Bączek zaprezentował temat ***Dezinformacja jako zagrożenie dla bezpieczeństwa informacyjnego współczesnych społeczeństw***. Wyjaśnił m.in. pojęcia związane z dezinformacją, omówił przykłady działań dezinformacyjnych w oparciu o wiedzę historyczną, schematy działań dezinformacyjnych. Wspomniał mi.in o roli różnego rodzaju mediów w walce dezinformacyjnej oraz sposobach ochrony przed nią.

Kolejnym prelegentem był ks. dr Jarosław Charchuła SJ, który wygłosił referat nt. ***Godność ludzka jako wartość w społeczeństwie informacyjnym – próba opisu socjologicznego***. W swoim wystąpieniu zaznaczył rolę socjologii w kształtowaniu godności w kontekście kulturowym i społecznym. Zaznaczył także, że godność jest interpretowana na różne sposoby.

Dr hab. Włodzimierz Fehler, prof. Uczelni zaprezentował temat ***Tajemnica korespondencji jako składnik informacyjnego bezpieczeństwa jednostki***. Wyjaśnił podstawowe terminy związane z bezpieczeństwem i informacją, analizował m.in. zapisy Konstytucji RP dotyczące praw do tajemnicy korespondencji. Objaśniał także w jaki sposób może dojść do naruszenia tajemnicy korespondencji na gruncie polskiego prawodawstwa oraz jakie wynikają z tego skutki, zarówno prawne, jak i inne, np. finansowe, czy wizerunkowe.

Mgr Marzanna Mańkowska wystąpiła z tematem ***Rola rzecznika prasowego w realizacji prawa do informacji***. Wyjaśniła, jakie są zadania rzecznika prasowego, jakimi cechami powinien się charakteryzować, jakie powinien mieć predyspozycje. Omówiła też mankamenty pracy rzecznika prasowego i przeszkody, z którymi musi się nieustannie zmierzać.

Kolejnym prelegentem był mgr Andrzej Dziewulski, który przedstawił referat nt. ***Przestrzeganie informacyjnych aspektów ochrony praw człowieka i obywatela w działalności operacyjno-rozpoznawczej Policji***. Wyjaśnił, jakie są kontrowersje w zasadności stosowania kontroli informacji w Polsce oraz jakie są relacje pomiędzy prawami człowieka i obywatela

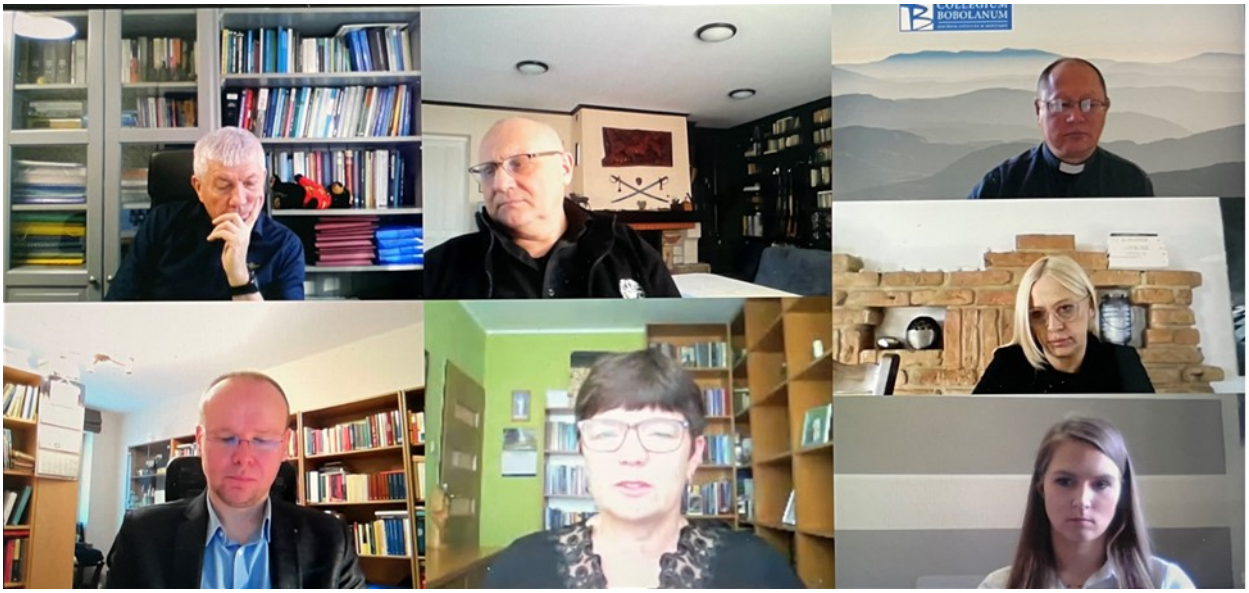
a działalnością operacyjną służb, takich jak Policja. Posłużył się też przykładami porównawczymi z innych państw Unii Europejskiej.

Mgr inż. Waldemar Gołuchowski wystąpił z tematem ***Informacyjne instrumenty przeciwdziałania i zwalczania terroryzmu***. W swoim referacie przekonywał, że odpowiednio przygotowywane informacje wraz z nowoczesnymi narzędziami służącymi do ich zastosowania, zarówno w przeciwdziałaniu terroryzmowi, jak i w bezpośrednim jego zwalczaniu, pozwolić mogą na znaczące zmniejszenie skali tego zjawiska. Stosując walkę informacyjną z terroryzmem powinno uderzać się przede wszystkim w jego przyczyny i uniemożliwiać lub co najmniej znacząco utrudniać jego rozwój.

Kolejną prelegentką była dr Bogumiła Pawlaczyk, która przedstawiła referat pt. ***Ograniczenia informacyjne w stanach nadzwyczajnych***. Referująca zauważyła, że możliwość dostępu do informacji dla obywatela w Polsce jest dość szeroki. Dużym dylematem jest określenie, czy lepsza jest większa swoboda obywateli odnośnie dostępu do informacji, czy bezpieczeństwo państwa, a w przypadku wprowadzenia jednego ze stanów nadzwyczajnych większą rolę odgrywa to bezpieczeństwo. Prelegentka objaśniła także na czym polega ograniczenie dostępu do informacji w trakcie obowiązywania poszczególnych stanów nadzwyczajnych.

Ostatnie wystąpienie pt. ***Prawo do informacji publicznej a bezpieczeństwo jednostki w miastach Smart City*** przypadło mgr inż. Kindze Augustyniak. Prelegentka omówiła zasady funkcjonowania miasta *Smart City*, czyli takiego, które w szerokim zakresie korzysta z dobrodziejstw technologii cyfrowej w jego funkcjonowaniu. Przedstawiła wady i zalety, cechy i funkcje rozwiązań technologicznych stosowanych w tego typu miastach. Podkreślała też istotę bezpieczeństwa obywateli, którzy zamieszkują miasta typu *Smart City*, odnośnie możliwości ich inwigilacji.

Po wystąpieniu wszystkich prelegentów nastąpiła krótka dyskusja pomiędzy uczestnikami na tematy związane z przedstawionymi prezentacjami. Po wymianie zdań i konkluzji, organizatorzy Konferencji, w tym Przewodniczący Komitetu Organizacyjnego, podziękowali wszystkim aktywnym uczestnikom i słuchaczom za udane jej przeprowadzenie w trybie zdalnym.



COLLEGIUM
BOBOLANUM

Czasopismo naukowe Security Review

Instytut Analizy Ryzyka
Sp. z o. o.
ul. Sucharskiego 2
35-225 Rzeszów

Redaktor Naczelny:
Anna Kardasz-Gefert
mail: annakardasz9@gmail.com

Redaktor Techniczny: Kamil Gefert

Sekretarz: Dorota Michalak

www.securityreview.pl