CZASOPISMO STUDENCKIEGO KOŁA NAUKOWEGO BEZPIECZEŃSTWA WEWNĘTRZNEGO

5/2018

SECURO

CYBERBEZPIECZEŃSTWO W XXI WIEKU

Aleksandra Gasztold, Jakub Sabała (red.)

STUDENCKIE KOŁO NAUKOWE BEZPIECZEŃSTWA WEWNĘTRZNEGO

CZASOPISMO
STUDENCKIEGO KOŁA NAUKOWEGO
BEZPIECZEŃSTWA WEWNĘTRZNEGO

SECURO

Nr 5

Cyberbezpieczeństwo w XXI wieku

pod redakcją
Aleksandry Gasztold i Jakuba Sabały

Warszawa 2018

Redaktor naukowy tomu:
dr Aleksandra Gasztold
mgr Jakub Sabała

Recenzenci:
dr Krzysztof Liedel
dr Witold Ostant

Redaktor techniczny:
Lucyna Całka

Projekt okładki:
Agnieszka Miłaszewicz

Publikacja dofinansowana przez Wydział Nauk Politycznych
i Studiów Międzynarodowych Uniwersytetu Warszawskiego

Wydział Nauk Politycznych
i Studiów Międzynarodowych
Uniwersytet Warszawski

ISSN: 2353-6330

Nakład: 40

Wersja on-line: www.sknbwuw.cba.pl

Opracowanie komputerowe, druk i oprawa:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel./fax 22 635 03 01, 22 635 17 85
e-mail: elipsa@elipsa.pl, www.elipsa.pl

SPIS TREŚCI

RECENZJE

WYDARZENIA

Cybersecurity in 21.st Century

eds. Aleksandra Gasztold and Jakub Sabała

CONTENTS

VARIA

REVIEW

EVENTS

WPROWADZENIE

Ze względu na postępującą informatyzację społeczeństwa oraz wyrafinowane środki i metody przestępców w wirtualnym świecie, tematyka ta zasługuje na szczególne wyróżnienie. Dlatego motywem przewodnim piątego tomu *Securo* jest problematyka bezpieczeństwa i ochrony cyberprzestrzeni. Cyberzagrożenia przestały być wymysłem literatury fantastyczno-naukowej, stając się realną groźbą[1]. Cyberprzestępcy wykorzystują Internet głównie wymuszając na przedsiębiorcach płacenie okupu za odzyskanie wykradzionych danych lub ponowne uruchomienie systemu (cyberszantaż). Gwałtownie rośnie liczba ataków, w szczególności z użyciem złośliwego oprogramowania typu ransomware[2]. Działalność przestępcza w cyberprzestrzeni nie ogranicza się wyłącznie do pozyskania gratyfikacji finansowych, mając charakter stricte kryminalny, ale coraz częściej ma wymiar polityczny (cyberszpiegostwo, cyberterroryzm, wojna cybernetyczna). Cyberbezpieczeństwo i ochrona cyberprzestrzeni stają się obowiązkiem zarówno państw, jak i podmiotów prywatnych oraz każdego użytkownika Internetu. Troska i dbałość o bezpieczne korzystanie z nowych technologii jest jednym z największych wyzwań XXI wieku.

W roku 2014 Zarząd Koła wspólnie z pracownikami Katedry Nauk o Bezpieczeństwie zaprezentował inicjatywę stworzenia czasopisma naukowego poświęconego sprawom bezpieczeństwa. Tom pierwszy, który ukazał się jeszcze w tym samym roku, poświęcony był zagadnieniom bezpieczeństwa imprez masowych. Drugi numer zaprezentowaliśmy w połowie 2015 roku. Podejmował on problematykę bezpieczeństwa społeczności lokalnych. W 2016 roku, ze względu na intensyfikację zagrożenia terrorystycznego w Europie, powstał tom dotyczący współczesnego terroryzmu. Rok później opublikowano *Securo* poświęcone tragedii na stadionie Hillsborough w dniu 15 kwietnia 1989 r. Wszystkie dotychczasowe publikacje można znaleźć w otwartym dostępnie m.in. na stronie internetowej SKNBW (sknbwuw.cba.pl). Spotkały się one z dużym zainteresowaniem Czytelników, w tym studentów, zarówno „Bezpieczeństwa wewnętrznego", jak i „Bezpieczeństwa narodowego" na innych uczelniach oraz na kierunkach politologii, stosunków międzynarodowych oraz prawa. W tym roku, ze względu na duże zainteresowanie wśród studentów problematyką cyberbezpieczeństwa podjęliśmy decyzję o skoncentrowaniu się na zagadnieniach związanych z użytkowaniem Internetu. Przedkładany numer *Securo* jest efektem aktywności naukowej studentów i doktorantów Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego (WNPiSM UW). Rezultaty swoich prac badawczych

[1] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 12.

[2] Internet Security Threat Report ISTR 2017, Vol. 22, Symantec: April 2017, s. 56–62.

w niniejszym tomie prezentują absolwenci kierunku bezpieczeństwo wewnętrzne, członkowie oraz sympatycy Studenckiego Koła Naukowego Bezpieczeństwa Wewnętrznego (SKNBW), które istnieje od 2008 roku w Instytucie Nauk Politycznych UW.

Numer otwiera artykuł współredaktora tomu JAKUBA SABAŁY *Cyberprzestrzeń jako teatr działań wywiadu*, w którym autor podjął próbę ukazania Internetu jako narzędzia do pozyskiwania i wytwarzania informacji o znaczeniu strategicznym dla bezpieczeństwa państwa. Wyeksponował on również metody charakterystyczne dla cyberwywiadu. Kolejnym artykułem jest *Internet Rzeczy-wistych zagrożeń* MATEUSZA DECYKA, w którym autor zwrócił uwagę na postępującą informatyzację i problem ochrony danych przechowywanych w Internecie. Technologie ingerują w coraz szersze aspekty życia człowieka, także gromadząc spersonalizowane informacje, o których ochronie użytkownicy często zapominają. RAFAŁ SKÓRA w tekście *Ransomware – jako zagrożenie dla cyberbezpieczeństwa. Analiza przypadku ataku WannaCry* przedstawił działanie złośliwego oprogramowania ransomware. Zdaniem autora jest to najszybciej ewoluująca i najbardziej niebezpieczna metoda stosowana przez cyberprzestępców. Kolejnym artykułem jest *Charakterystyka współczesnej cyberprzestępczości zorganizowanej* PAULINY ŁOJEWSKIEJ. Autorka analizuje charakter zorganizowanych grup cyberprzestępczych oraz taktykę wykorzystywania technologii IT do nielegalnej działalności w cyberprzestrzeni. Dodatkowo zaprezentowane zostały sposoby przeciwdziałania tego typu zagrożeniom. DANIEL M. ZAWADKA w tekście *Współczesna przestępczość związana z pieniądzem elektronicznym. Rola organów ścigania* zaprezentował działania przestępcze wymierzone w legalnych posiadaczy kart płatniczych. Następnie ALEKSANDRA NOWICKA w artykule *Medialny fenomen bezpieczeństwa* wskazała na problem złożonej relacji między środkami masowego przekazu a bezpieczeństwem w Polsce. Poddała charakterystyce proces mnożenia informacji, szczególnie o wydźwięku negatywnym i kompromitującym instytucje bezpieczeństwa, które ponadto eksponują konkretne zagrożenia. Autorka kwestionuje stwierdzenie, że środki masowego przekazu we właściwy sposób dostarczają informacji o stanie bezpieczeństwa.

W części *Varia* zamieszczono artykuły TAMAR LORTKIPHANIDZE *Koreańska Republika Ludowo-Demokratyczna – mocarstwo atomowe?*, MICHAŁA PIOTRA BROMIŃSKIEGO *Zjawisko migracji a terroryzm – bezpieczeństwo UE w drugiej dekadzie XXI w.* oraz MICHAŁA SZOTKA *Oblicza terroryzmu islamskiego w Europie i próby przeciwdziałania.* Do numeru dołączono również artykuł recenzyjny książki Farhada Khosrokhavara *Radicalization: Why Some People Choose the Path of Violence* (2017) przygotowany przez ALEKSANDRĘ GOŁAŚ oraz dwa raporty. Pierwszy z konferencji *Defence Summit 2017 Polska Strategia Obronności. Rola Strategicznego Przeglądu Obronnego – Planowanie obronne – wyzwania w ramach NATO* sporządzony przez KLAUDIĘ BOGACKĄ oraz drugi autorstwa DANIELA KASPERKIEWICZA z zajęć praktycznych *RUN – HIDE – FIGHT: jak przeżyć zamach? Powstrzymaj Terrorystę!*, które miały miejsce na Uniwersytecie Warszawskim.

Doświadczenia kilkuletniej pracy ze studentami „Bezpieczeństwa wewnętrznego" na Uniwersytecie Warszawskim są bardzo pozytywne, o czym świadczy między innymi zaangażowanie w pracę nad piątym numerem *Securo*. Studenci aktywnie i z dużym zapałem organizują liczne dyskusje, debaty, wizyty studyjne i seminaria oraz biorą udział w konferencjach kół naukowych. Między innymi praca z nimi w roku akademickim 2016/2017 była

głównym impulsem do przygotowania niniejszego tomu. Dziękuję wszystkim Autorom, z których część ukończyła już studia magisterskie, za ciekawe i potrzebne teksty oraz dobrą współpracę.

Składam serdeczne podziękowania za nieustające wsparcie Prodziekanowi ds. finansowych i rozwoju WNPiSM UW doktorowi Danielowi Przastkowi umożliwiające realizację przedsięwzięć SKNBW. Szczególne podziękowania za pomoc w przygotowaniu niniejszego tomu należą się doktorowi Piotrowi Potejce, magistrowi Jakubowi Sabale i Klaudii Bogackiej.

Mam nadzieję, że zaprezentowane artykuły staną się przyczynkiem do dyskusji nad problematyką współczesnych zagrożeń generowanych przez cyber-świat oraz przestrogą dla użytkowników Internetu. Zagadnienia poruszone w niniejszym numerze wymagają dalszych wszechstronnych i pogłębionych analiz. Zamieszczone w tomie teksty posłużyć mogą jako literatura uzupełniająca do dyskusji publicznej oraz prowadzonych w ramach kierunków „Bezpieczeństwo wewnętrzne" i „Bezpieczeństwo narodowe" przedmiotów – „Ochrona cyberprzestrzeni", „Bezpieczeństwo w sieci", „Bezpieczeństwo cybernetyczne" oraz „Zwalczanie przestępczości w cyberprzestrzeni".

Życzę interesującej lektury

dr Aleksandra GASZTOLD
Redaktor Naczelna

JAKUB SABAŁA*

CYBERPRZESTRZEŃ JAKO TEATR DZIAŁAŃ WYWIADU

Abstrakt

Cyberprzestrzeń stanowi już nieodłączną część współczesnego życia. Przetwarzanie oraz przechowywanie informacji w sieciach teleinformatycznych stało się już standardem, ponieważ wiele systemów opiera swoje działanie na technologiach informacyjnych. Niezliczone ilości tych informacji są cennym źródłem dla służb wywiadowczych, dlatego wywiad w cyberprzestrzeni stanowi współcześnie nowe, sukcesywnie rozwijane pole aktywności służb. Artykuł ma za zadanie przybliżyć znaczenie tego sektora wywiadu, jakie niesie za sobą szanse i możliwości oraz postawić hipotezy, które mogą być elementem dyskursu akademickiego w tym temacie.

Słowa kluczowe: Cyberprzestrzeń, Internet, wywiad, cyberszpiegostwo, CYBINT.

Wstęp

Internet oraz szerzej – cyberprzestrzeń to już immanentna część współczesnego życia. Osoby prywatne, jak i instytucje, przedsiębiorstwa coraz częściej korzystają z technologii informacyjnych, zarówno w zakresie marketingu, jaki i komunikacji. To sprawia, iż coraz więcej aktywności społeczeństwa, a co za tym idzie informacji zostaje umieszczanych w cyberprzestrzeni. Historia świata dowiodła, że służby wywiadowcze podążają za potężnymi informacji.

Problematyka wywiadu w cyberprzestrzeni jest bardzo szeroka i jest sukcesywnie rozwijana na gruncie akademickiego dyskursu. Celem artykułu jest ukazanie podstawowych zagadnień związanych z podejmowanym tematem oraz uwypuklenie krytycznych jego elementów, co powinno być preludium do dalszych rozważań na gruncie nauki i sektora bezpieczeństwa. Ponadto autor pragnie w niniejszym artykule ukazać wywiad w cyber-

* Jakub Sabała – absolwent studiów licencjackich i magisterskich na kierunku bezpieczeństwo wewnętrzne w Instytucie Nauk Politycznych UW. Doktorant Nauk o Bezpieczeństwie na Wydziale Nauk Politycznych i Studiów Międzynarodowych UW. Zawodowo związany z pozyskiwaniem informacji w sektorze finansowym.

przestrzeni nie jako zagrożenie, lecz jako możliwość i szansę na lepsze zapewnianie bezpieczeństwa.

Pragnąc zrealizować cel należy postawić kilka pytań badawczych, na które autor postara się odpowiedzieć w niniejszym artykule. Jakie znaczenie ma współcześnie cyberszpiegostwo i jakie znaczenie będzie miało w przyszłości?; Jakie są zalety i wady zastosowania wywiadu w cyberprzestrzeni we współczesnym świecie?; Co wpływa na sukcesy i porażki cyberszpiegów?; Jakie są perspektywy rozwoju wywiadu w cyberprzestrzeni?

Wywiad w cyberprzestrzeni, cyberszpiegostwo stanowić będą coraz szersze pole działania dla agencji wywiadowczych na całym świecie i wraz z rozwojem technologii informacyjnych zaangażowanie w tej dyscyplinie pozyskiwania informacji będzie rosło. Teza ta nie może dziwić, gdyż każdego roku zastosowania informatyki w różnych sektorach polityki, gospodarki, czy życia codziennego rośnie. Wraz z tym wzrostem ilość danych dostępnych w cyberprzestrzeni zwiększa się, przez co stanowić będzie proporcjonalnie istotniejsze źródło informacji dla wywiadu. Cyberszpiegostwo niesie za sobą wiele możliwości i szans, których nie niosła za sobą żadna inna dyscyplina wywiadowcza.

Celem uporządkowania rozważań należy wyjaśnić termin cyberprzestrzeni. Pojęcie cyberprzestrzeni użył po raz pierwszy w 1982 roku William Gibson na kartach swojej powieści „Burning Chrome”[1]. Na gruncie rozwoju cyberprzestrzeni powstało kilka definicji. Jedną z nich, która jest wystarczająco kompleksowa dla tematyki, jest definicja zawarta w raporcie „Zagraniczni szpiedzy wykradają gospodarcze tajemnice USA w cyberprzestrzeni” Biura Dyrektora Krajowego Kontrwywiadu USA, która określa cyberprzestrzeń jako powiązaną ze sobą sieć infrastrukturalną technologii informatycznych, obejmujące Internet, sieci telekomunikacyjne, systemy komputerowe oraz systemy kierujące procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego[2].

Z początkiem lat 90. XX wieku pojęcie cyberprzestrzeni weszło do powszechnego użytku. Technologie informacyjne w tamtym okresie były już na takim poziomie rozwoju, że Nicholas Negroponte stwierdził, iż atom przestał być podstawowym składnikiem elementarnym, a zastąpiła go cyfra binarna[3]. Świadczyć o tym może fakt, że obecnie poziom prowadzenia działań wojennych – szczególnie z zakresie wojny informacyjnej – nie jest już domeną lądu, morza czy powietrza, lecz również świata cyfrowego w sieciach teleinformatycznych. Różnicami jakie wiążą się z tym środowiskiem działań jest to, iż środowisko to zostało w sposób całkowity stworzone przez człowieka, a efektem walk prowadzonych w nim może być całkowita zmiana specyfiki, cech i topografii terenu działań[4]. Ponadto, sama geografia, geopolityka czy geolokalizacja traci na znaczeniu. Wojna informacyjna

---

1 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego”, 9/13, 2013, s. 226.

2 *Foreign Spies Stealing US Economic Secrets in Cyberspace*, [w:] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf [dostęp: 2.12.2017].

3 S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki, organizacji, państwa*, Warszawa 2016, s. 212.

4 Wpływ aktorów na środowisko walki w cyberprzestrzeni jest tak silny, iż eksperci porównując to z walką lądową w sposób konwencjonalny wskazują za przykład pojawiającą się lub znikającą górę. Zastosowanie najpotężniejszej współcześnie broni tj. bomby atomowej wg ekspertów nie niesie za sobą takich zmian w środowisku, jakie mogą nieść wpływy oponentów w środowisku cyfrowym.

w cyberprzestrzeni nie posiada jasno wytyczonych granic państwowych oraz sama odległość między państwami traci na znaczeniu. RAND Corporation w 1995 r. zbadała, na zlecenie Departamentu Obrony Stanów Zjednoczonych, możliwości jakie będzie niosła za sobą wojna informacyjna w cyberprzestrzeni. W raporcie końcowym stwierdzono, iż technologia informacyjna pozwoli zatrzeć odległości, które miały znaczenie w walce konwencjonalnej, a tym samym cele ataku w Stanach Zjednoczonych staną się tak samo narażone na ingerencję, jak cele lokalne[5].

Znaczenie wywiadu w cyberprzestrzeni

Od samego początku istnienia cyberprzestrzeni i kolejne lata jej rozwoju zastanawiano się nad istotą tego zjawiska. Oczywiście, w zależności od sektora, w jakim ta cyberprzestrzeń jest wykorzystywana, może przynosić różne profity i ułatwienia. Dla wywiadu i cyberszpiegostwa można wytypować kilka podstawowych korzyści. Po pierwsze, sprawcy szpiegostwa cyfrowego są znacznie trudniej wykrywalni niż ci konwencjonalni. Szpiedzy mogą wykradać informacje na odległość przy jednoczesnym ukrywaniu swojej tożsamości, lokalizacji. Po drugie, sprawcami kradzieży informacji w cyberprzestrzeni mogą być zarówno pojedyncze osoby, korporacje, państwa o znacznie mniejszym potencjale ekonomicznym i technologicznym niż światowe mocarstwa. Po trzecie, cyberprzestrzeń powoduje, że trudniej jest ustalić motywy działania sprawców kradzieży informacji. W konwencjonalnej działalności wywiadowczej pozyskanie jakiegoś dokumentu czy informacji wiązało się z ujawnieniem obszaru zainteresowania służby wywiadowczej, natomiast w cyberszpiegostwie możliwe jest pobieranie ogromnych ilości informacji, które mogą być ze sobą niepowiązane, dlatego łatwiej jest ukryć prawdziwy cel kradzieży. Po czwarte, wywiad w cyberprzestrzeni redukuje zagrożenie dla sprawców i agentów wewnątrz organizacji, poprzez brak fizycznego spotkania agenta z funkcjonariuszem prowadzącym, co stanowczo zmniejsza ryzyko wykrycia. Po piąte, cyberszpiegostwo jest działalnością szybszą i tańszą w stosunku do podstawowych dyscyplin pozyskiwania informacji. Cyberprzestrzeń oferuje możliwość natychmiastowego transferu ogromnych ilości informacji[6].

Znaczenie pozyskiwania informacji w cyberprzestrzeni zauważył amerykański teoretyk badacz wywiadu Robert M. Clark, który w swoim opracowaniu *Intelligence Collection* wyróżnił pośród głównych dyscyplin wywiadowczych[7] subdyscyplinę CYBINT – Cyber Intelligence.

Wywiad w cyberprzestrzeni czy też cyberszpiegostwo są działaniami wymierzonymi w pozyskiwanie informacji, które są przetwarzane w systemach teleinformatycznych,

---

5 S. Wojciechowska-Filipek, Z. Ciekanowski, dz. cyt., s. 212–213.

6 M. Ciecierski, R. Nogacki, *Bezpieczeństwo współczesnej firmy. Wywiad, szpiegostwo, ochrona tajemnic*, Warszawa 2016, s. 204.

7 Pięć głównych dyscyplin wywiadowczych funkcjonujących w teorii wywiadu i kontrwywiadu to HUMINT (wywiad osobowy); OSINT (wywiad jawnoźródłowy); IMINT (wywiad obrazowy); SIGINT (wywiad ze źródeł elektromagnetycznych) oraz MASINT (wywiad pomiarowo-badawczy).

i nie zawsze można je kategoryzować w ramach klasycznych dyscyplin wywiadowczych. CYBINT jest subdyscypliną, w której możemy odnaleźć elementy takich dyscyplin jak OSINT, HUMINT, SIGINT[8], które to elementy odpowiadają pozyskiwaniu informacji z cyberprzestrzeni.

Wywiad w cyberprzestrzeni bez wątpienia ma zastosowanie, kiedy mówimy o wywiadzie jawnoźródłowym – OSINT. Internet jest obecnie najpowszechniejszym źródłem informacji jawnych, a przy tym łatwo dostępnym szczególnie w świecie zachodnim. Wielu ludzi współcześnie pozyskuje informacje z Internetu, już nie tylko za pomocą komputera, lecz również innych urządzeń mobilnych tj. tablet czy smartphone, który znajduje się już niemalże w każdej kieszeni. Powszechność dostępu do Internetu sprawia, że poza tym, iż chętnie pozyskiwane są informacje z tego źródła, to również społeczeństwo pozostawia o sobie informacje w np. mediach społecznościowych. Same informacje pozostawione przez nas to nie jedyne źródło informacji, gdyż współcześnie w ramach wywiadu jawnoźródłowego w cyberprzestrzeni znaczenie mają metadane, czyli np. gdzie publikujemy informację, na jakim urządzeniu, co znajduje się w naszej historii wyszukiwania etc. To pozwala korporacjom takim jak np. Google do profilowania naszej osoby na potrzeby reklam, ale jest również znaczącym źródłem informacji dla wywiadu, szczególnie kiedy jesteśmy osobami publicznymi.

Na przestrzeni lat wystąpiło kilka przykładów upublicznienia informacji w Internecie, które miały znaczenie dla systemu bezpieczeństwa. Po pierwsze, publikowanie w sieci zdjęć żołnierzy w bazach wojskowych, dzięki czemu możliwe jest oglądanie wyposażenia, usytuowanie obiektów chronionych. Ten typ działania umożliwił atak na bazę Polskiego Kontyngentu Wojskowego w Afganistanie lub w 2007 roku w Republice Iraku atak moździerzowy, czego skutkiem były straty w sprzęcie. Po drugie, ujawnienie wizerunków osób pracujących w instytucjach bezpieczeństwa, posiadających niejednokrotnie ogromną władzę i dostęp do ściśle tajnych informacji i będących podatnymi na werbunek zagranicznego wywiadu. Po trzecie, dziennikarskie doniesienia o podróżach, miejscu pobytu lub zamieszkania najważniejszych osób w państwie, mogące narażać je na różne ataki. Po czwarte, konta w portalach społecznościowych funkcjonariuszy służb i żołnierzy, które regularnie monitorowane przez zagraniczny wywiad mogą dostarczać informacji potrzebnych do profilowania kandydata do werbunku. Po piąte, serwisy gromadzące przyjaciół ze szkół, w tym także o profilach wojskowo-policyjnych i publikowane wspólne zdjęcia wraz z informacjami szczegółowymi mogą narażać funkcjonariuszy pracujących pod przykryciem na dekonspirację[9].

Ilość informacji produkowanych w Internecie znacznie przekracza możliwości ich dokładnej penetracji. Do tego celu wykorzystywane są specjalistyczne wyszukiwarki

[8] R.M. Clark, *Intelligence collection*, Washington 2014, s. 121.

[9] M. Frączek, *Wybrane problemy zastosowania nowoczesnych technologii do gromadzenia danych w zakresie bezpieczeństwa*, [w:] *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa. Historia i współczesność*, M. Górka (red.), Toruń 2016, s. 61–62.

horyzontalne i wertykalne[10] oraz programy automatyzujące wyszukiwanie w jawnych źródłach[11].

OSINT to przede wszystkim informacje publicznie dostępne, ale też te, które nie są w żaden sposób chronione. OSINT to jedynie część informacji, które znajdują się w świecie cyfrowym, a są w kręgu zainteresowania wywiadu.

Tak jak już było wspomniane wcześniej, cyberprzestrzeń to coś więcej niż tylko Internet. To również sieci lokalne, intranety, systemy teleinformatyczne instytucji, systemy obsługujące infrastrukturę, w tym infrastrukturę krytyczną, etc. Te systemy w odróżnieniu do informacji jawnoźródłowych są chronione w mniejszy lub większy sposób. Systemy bezpieczeństwa IT muszą odpierać każdy rodzaj ataku na jakie będą narażone, natomiast atakujący haker musi odnaleźć jeden słaby punkt, który pomoże mu dostać się do systemu. Jak stwierdził były haker Dustin Dykes „System bezpieczeństwa musi wygrywać cały czas. Haker musi wygrać tylko raz”[12].

Na sukces hakerów i cyberszpiegów wpływa wiele czynników. Są to przede wszystkim trzy, które mają największe znaczenie w walce w cyberprzestrzeni. Po pierwsze, sposób myślenia specjalistów bezpieczeństwa IT, po drugie, złożoność systemów bezpieczeństwa lub systemów informatycznych sensu largo oraz po trzecie, najsłabsze ogniwo każdego systemu bezpieczeństwa, czyli ludzki błąd[13].

Sposób myślenia specjalistów bezpieczeństwa IT, administratorów systemów i sieci powoduje, że nie są w stanie postawić się w roli hakera, osoby atakującej system. Specjaliści bezpieczeństwa IT chcą wierzyć, że ich system jest najbezpieczniejszy i nie posiada żadnych wad ani słabości. Programy bezpieczeństwa systemów i sami operatorzy skupiają się przede wszystkim na słabościach całego systemu, a nie zagrożeniach płynących z zewnątrz. Słabości systemu są w znacznej mierze dużo łatwiejsze w ocenie niż potencjalne zagrożenie zewnętrzne. Myślenie wewnętrzne zamiast wyjść poza granice systemu powoduje, że skupiają się nie na tym, co haker lub osoba atakująca próbuje osiągnąć. Osoby odpowiedzialne za bezpieczeństwo systemu nie wykonują oceny zagrożenia prawidłowo z punktu widzenia atakującego i nie poświęcają dostatecznie dużo sił i środków pozostawiając system podatnym na ingerencję zewnętrzną.

Złożoność systemów również ma wpływ na jego słabość w zabezpieczeniach. Duże i skomplikowane sieci komputerowe, oprogramowanie posiadają znacznie więcej niedociągnięć, a co za tym idzie słabości, które są chętnie wykorzystywane przez atakujących hakerów. Co więcej, rozwój technologii i możliwości obu stron konfliktu, każdego dnia wyłania kolejne słabości w częściach systemu, które do tej pory były uważane za bezpieczne. Ciągłe zmiany w sprzęcie informatycznym, aktualizacje oprogramowania, sieci i połączenia bezprzewodowe wystawiają każdego dnia system na nowe zagrożenia. Każda

---

10 Wyszukiwarki horyzontalne tj. Google, Bing, DuckDuckGo wyszukują w powierzchownym Internecie wszystkich stron powiązanych z wyszukiwaną frazą; Wyszukiwarki wertykalne są ograniczone do konkretnej dziedziny tj. medycyna, prawo, inżynieria i wyszukują powiązań z frazą w ramach swojej dziedziny zarówno w Internecie powierzchownym jak i deepweb.

11 Przykładami tego typu programów mogą być np. Lockheed Martin Wisdom lub Maltego.

12 R.M. Clark, dz. cyt., s. 121.

13 Tamże, s. 122.

modyfikacja w systemie tworzy pole do potencjalnej słabości, która może zostać wykorzystana przez hakerów[14].

Błąd ludzki pozostaje nadal domeną wielu zagrożeń, na które narażony jest system bezpieczeństwa czy to konwencjonalny czy cyfrowy, a samo pozyskiwanie informacji w swojej naturze często z niego korzysta. W przypadku cyberprzestrzeni błędy popełniają przede wszystkim operatorzy i osoby odpowiedzialne za bezpieczeństwo systemu. W tych granicach najczęstszymi błędami napotykanymi przez hakerów są złe konfiguracje systemu, połączenia urządzeń z siecią lub niefrasobliwość przy korzystaniu z systemu.

W ramach pozyskiwania informacji z cyberprzestrzeni możemy rozgraniczyć dwa zasadnicze typy: pozyskiwanie informacji z sieci teleinformatycznych lub pośrednie i bezpośrednie wykorzystanie pojedynczych komputerów czy intranetów[15].

Ingerencja w sieci komputerowe i systemy teleinformatyczne opiera się na wielowarstwowych i zróżnicowanych metodach działania. Współczesny rozwój możliwości technologicznych spowodował również rozrost możliwości hakerskich, który z pewnością znajduje zastosowanie w działaniach wywiadu w cyberprzestrzeni. E. Lichocki wyróżnił takie metody ingerencji jak:

- malware, czyli oprogramowanie złośliwe – wirusy, robaki – programy rozprzestrzeniające się w zainfekowanym systemie informatycznym, zmieniając sposób jego funkcjonowania, naruszając możliwości procesora i dysku twardego, uniemożliwiając korzystanie z danych;
- bomby logiczne – programy aktywujące nowe funkcje elementów logicznych komputera, które w efekcie końcowym prowadzą do zniszczenia systemu i oprogramowania;
- konie trojańskie – oprogramowanie, które podłączone do innego programy dostając się do systemu komputerowego umożliwia podejmowanie działań bez wiedzy użytkownika zainfekowanego komputera;
- próbkowanie – uzyskiwanie dostępu do komputera poprzez analizę jego charakterystyki;
- uwierzytelnianie – podszywanie się pod osobę uprawnioną do dostępu;
- ominięcie – omijanie zabezpieczeń systemu;
- czytanie – nieuprawniony dostęp do informacji w systemie;
- kopiowanie – nieuprawnione kopiowanie informacji z systemu;
- kradzież – przejęcie informacji i plików z systemu bez pozostawienia kopii;
- modyfikacja – zmiana zawartości lub charakterystyki informacji i danych zawartych w systemie;
- usunięcie – zniszczenie informacji zawartych w systemie lub całego systemu informatycznego;
- złośliwe podzespoły – umieszczanie w komputerach części, które umożliwiają nieuprawniony dostęp do systemu lub wadliwa konstrukcja systemu;
- tylne drzwi (backdoor) – tworzenie przez twórców oprogramowania wejścia do systemu poza wiedzą użytkownika;
- maskarada – podszywanie się pod użytkownika przez jednego za atakujących system;

[14] Tamże.

[15] Tamże, s. 123.

- przechwycenie transmisji – uzyskanie dostępu do treści przesyłanych pomiędzy komputerami;
- podsłuchiwanie – śledzenie ruchu sieciowego;
- receptory van Ecka – podglądanie przez atakującego replik obrazów przesyłanych z monitora użytkownika;
- DDoS (distributed denial of service, rozproszona odmowa usługi);
- e-mail bombing – przesyłanie do skrzynki ofiary ataku wielkiej ilości danych, co powoduje przepełnienie i nieprawidłowości w działaniu;
- promieniowanie elektromagnetyczne, które swoim działaniem niszczy urządzenia elektroniczne oraz zawarte na nich dane[16];
- Keystroke loggers (Keyloggery) – oprogramowanie lub sprzęt przechwytujące frazy wpisywanie za pomocą klawiatury, dzięki czemu możliwe jest uzyskanie loginów i haseł dostępu do systemu.

Proces pozyskiwania informacji wywiadowczej z cyberprzestrzeni ma wiele zalet, ale jest nie mniej złożony od innych dyscyplin. Cały proces wymaga przede wszystkim personelu, osób obdarzonych wiedzą, umiejętnościami informatycznymi i talentem, które będą się chciały podjąć takich działań na rzecz wywiadu. Proces cyberwywiadu czy cyberszpiegostwa możemy podzielić na pięć zasadniczych etapów – selekcji celu, analizy celu, wykrywania słabości i wrażliwości systemu, eksploracji, czyli właściwego działania oraz wyczyszczenie śladów działalności i pozostawienie „furtki" do przyszłych działań[17].

Selekcja celu ataku jest pierwszą fazą przygotowywania cyberszpiegostwa. Informacje na temat potencjalnych celów są gromadzone z różnych źródeł, publicznych rekordów, społecznych i profesjonalnych sieci internetowych, konferencji branżowych, etc. Wszystkie informacje gromadzone mają na celu jak najlepsze profilowanie jednostki atakowanej, a przy tym mają za zadanie uwypuklenie pierwszych wrażliwych stron, dzięki czemu możliwy jest wybór celu najbardziej podatnego na ingerencję.

Analiza celu i jego mapowanie jest fazą rozpoznania wybranego już obiektu ataku, mającą na celu bezinwazyjne sondowanie go, potwierdzenie obecności urządzeń w systemie i mapowanie połączeń w tym systemie. Analiza ma na celu najlepsze zrozumienie systemu od najmniejszych fragmentów po system jako całość. W uproszczeniu faza ta ma za zadanie stworzenie szczegółowego modelu atakowanego obiektu, bez ryzyka bycia wykrytym przez specjalistów ds. cyberbezpieczeństwa.

Skanowanie obiektu pod kątem potencjalnych wrażliwych punktów to kolejna faza, która nawiązuje kontakt z systemem atakowanym i jego elementami składowymi. Skanowanie słabości może odbywać się zarówno za pomocą i bez Internetu, i wykorzystuje cały wachlarz narzędzi, które zostały wymienione wyżej w artykule. W tym etapie również możliwa jest ludzka ingerencja w system, który nie jest bezpośrednio dostępny z ogólnie dostępnej cyberprzestrzeni.

---

16 T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, za: E. Lichocki, Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego SZ RP, rozprawa doktorska, Wydział Bezpieczeństwa Narodowego Akademii Obrony Narodowej, Warszawa 2009, s. 62–63.

17 R.M. Clark, dz. cyt., s. 126.

Faza określana jako eksploracja systemu to już właściwy moment hackingu i uzyskiwania nieautoryzowanego dostępu do systemu teleinformatycznego. Atakujący uzyskuje dostęp, instaluje potrzebne oprogramowanie, pozyskuje potrzebne informacje i dane.

Ostatnim etapem w omawianym procesie jest zacieranie śladów ingerencji, aby osoby odpowiedzialne za zabezpieczenia nie zorientowały się, że doszło do infiltracji systemu oraz na potrzeby przyszłych eksploracji instalowane są backdoory, czyli „furtki" umożliwiające atakującemu łatwiejsze dostanie się do systemu, bez potrzeby ponownego łamania zabezpieczeń lub instalacja oprogramowania, które w sposób ciągły będzie przesyłało potrzebne informacje z systemu atakowanego do systemu atakującego.

Cyberszpiegostwo na świecie

Cyberszpiegostwo i wywiad w cyberprzestrzeni to działania wywiadowcze, które są stosowane od niedawna, lecz mają za sobą już dość bogatą historię, biorąc pod uwagę doniesienia prasowe lub wycieki tajnych informacji np. przez Wikileaks.

Sprawą, która wywarła ogromne piętno w masowej świadomości społeczeństwa zachodniego, w kontekście funkcjonowaniu wywiadu w cyberprzestrzeni była sprawa programu PRISM wykorzystywanego przez Agencję Bezpieczeństwa Narodowego Stanów Zjednoczonych. Sprawę tę w 2010 roku ujawnił opinii publicznej Edward Snowden, który później został oskarżony o szpiegostwo i uciekł do Federacji Rosyjskiej. Ujawnione przez Snowdena informacje wskazywały, iż w ramach programu PRISM amerykanie podsłuchiwali i infiltrowali swoich sojuszników (m.in. Niemcy, Wielka Brytania, Japonia i Polska) oraz sieci komputerowe należące do organizacji międzynarodowych tj. ONZ, NATO oraz Unii Europejskiej.

Inwigilacja osób publicznych nie stanowi jednego celu dla służb wywiadowczych. Coraz częściej służby wykorzystują cyberprzestrzeń do gromadzenia informacji o obywatelach, tworząc ich profile. Przykładem są również Stany Zjednoczone, które wykorzystują narzędzie nazwane RIOT, którego zadaniem jest gromadzenie i katalogowanie profili użytkowników Internetu i informacji zamieszczanych przez nich np. w serwisach społecznościowych[18].

Cyberszpiegostwo w sieci jest działalnością częstokroć dobrze zorganizowaną i zaplanowaną, a odkrycie takiej działalności wymaga niewiele mniej czasu niż w przypadku konwencjonalnego szpiegostwa. Jednym z najgłośniejszych incydentów wykradania informacji z cyberprzestrzeni było działalnie chińskiej jednostki wywiadowczej odpowiedzialnej za ataki komputerowe, która ukierunkowana była na amerykańskie instytucje rządowe. Hakerzy zdobyli dostęp do amerykańskich sieci energetycznych oraz ważnych systemów uzbrojenia tj. myśliwce F/A-18 i F-35, śmigłowce Black Hawk, samolot V-22 Osprey, czy system Patriot PAC-3[19].

---

[18] D. Dziwisz, *Cyberbezpieczeństwo – nowy priorytet strategii obrony Stanów Zjednoczonych?*, „Sprawy Międzynarodowe" 2011, nr 3, s. 103–122.

[19] M. Grzelak, *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" 2013/2, s. 112.

Chińska Republika Ludowa zaczęła wyrabiać sobie nawet już markę pod kątem cyberszpiegostwa, szczególnie w zakresie nowoczesnych zaawansowanych technologii. Anegdotą już jest, iż w Chinach został wypuszczony na rynek podrobiony iPhone 7, zanim jeszcze firma Apple dokonała jego oficjalnej premiery i prezentacji. Chińskie służby wywiadowcze i korporacje często usiłują wykorzystać chińskich obywateli i osoby mające rodzinę poza granicami do pozyskiwania informacji. Specjaliści od cyberbezpieczeństwa częstokroć zgłaszają incydenty wymierzone w sieci komputerowe opatrzone adresami IP pochodzących właśnie z Chin. W 2011 roku Firma McAfee ustaliła, iż incydent nazwany Nocnym Smokiem nastąpił z chińskiego adresu IP, a pozyskiwane informacje dotyczyły energetyki. Od listopada 2009 roku pracownicy atakowanych firm byli nękani inżynierią społeczną i próbami phishingu. W 2010 roku niezidentyfikowani sprawcy włamali się do Ministerstwa Finansów Republiki Francuskiej i przekierowali dane dotyczące francuskiej prezydencji w G20 na chińskie strony internetowe, przez co oskarżenia pod adresem Chin stały się uzasadnione[20].

Wywiad w cyberprzestrzeni wykorzystuje osiągnięcia technologii informacyjnych prywatnych firm. Przykładem tego mogą być powtarzające się już od kilku lat oskarżenia pod adresem firmy Kaspersky Labs, która jest podejrzewana o to, że oprogramowanie antywirusowe spod jej marki szpieguje swoich użytkowników (zarówno osoby prywatne, jak i instytucje, przedsiębiorstwa) na rzecz Kremla. Można zauważyć, iż oskarżenia te przybierają w ostatnich dniach na sile. Brytyjskie Centrum ds. Cyberbezpieczeństwa wydało ostatnio ostrzeżenie przed używaniem tego oprogramowania przez instytucje państwowe[21]. To właśnie Federacja Rosyjska jest drugim po Chinach państwem oskarżanym o stosowanie cyberszpiegostwa. Wraz z zastosowaniem wywiadu osobowego i innych dyscyplin wywiadowczych Rosja próbuje wyrównać dysproporcje gospodarcze i technologiczne względem Stanów Zjednoczonych, żyjąc w przekonaniu, iż globalna gospodarka kieruje się właśnie interesami USA kosztem Rosji. Federacja Rosyjska dzięki włamaniom do sieci teleinformatycznych i przechwytywaniu e-maili oszczędza miliardy dolarów na badaniach i rozwoju technologicznym w energetyce, technologiach informacyjnych czy sektorze bezpieczeństwa. Wielka Brytania utrzymuje, iż Rosja stale penetruje cyberprzestrzeń jej systemu finansowego[22].

Rewolucja zastosowania cyberprzestrzeni w działalności wywiadowczej rozwija się w sferze międzypaństwowej, ale nie ominęła również sektora prywatnego, gdzie szpiegostwo przemysłowe przeniosło się również do cyfrowego świata. Cyberprzestrzeń z powodu unikalnych właściwości jakimi się charakteryzuje jest szczególnie narażona na akty cyberszpiegostwa, a co więcej, nie stanowi już monopolu działania dla służb państwowych.

Nie bez znaczenie jest również kradzież informacji przez osoby/grupy niepowiązane z państwem, które włamują się do zabezpieczonych systemów przetwarzających tajne dane, a następnie sprzedają wykradzione informacje czy dokumenty w darkwebie, co również nie powinno ujść uwadze służb wywiadowczych. W tym kontekście należy wspomnieć

20 M. Ciecierski, R. Nogacki, dz. cyt., s. 206–207.

21 G. Corera, *Kaspersky Labs: Warning over Russian anti-virus software*, BBC [w:] http://www.bbc.com/news/uk-42202191 [dostęp: 2.12.2017].

22 M. Ciecierski, R. Nogacki, dz. cyt., s. 207–208.

o działającej od lat grupie Anonymous, czyli grupie hakerów włamujących się i przeprowadzających ataki wobec różnych instytucji, czy przedsiębiorstw. Uznawani są bardziej za wojowników o przekonania, aniżeli realną grupę interesu.

Podsumowanie

Rozważając problematykę wywiadu w cyberprzestrzeni należy zwrócić uwagę na fakt, iż jesteśmy świadkami stałego „zakorzenienia" się tej dyscypliny w światowej działalności wywiadowczej. Powszechny trend informatyzacji jest już obecnie nie do zatrzymania, dlatego zjawisko cyberszpiegostwa będzie sukcesywnie wzrastać, proporcjonalnie do informacji przetwarzanych w systemach informatycznych. Cyberprzestrzeń na stałe zadomowiła się w społeczeństwie i staje się nieodłączną częścią walki informacyjnej pomiędzy państwami, ale również pomiędzy podmiotami niepaństwowymi.

Cyberszpiegostwo czy cyberwywiad jest bez wątpienia działalnością, która niesie ze sobą ogromne możliwości i zalety. Po pierwsze, relatywnie niskie koszty w porównaniu z innymi dyscyplinami. Po drugie, oszczędność czasu na prowadzeniu skomplikowanej gry wywiadowczej. Czas potrzebny jedynie na znalezienie luki w systemie. Po trzecie, bezpieczeństwo cyberszpiegów, który nie muszą się fizycznie znajdować przy urządzeniu, z którego wykradane są dane, a mogą być po drugiej stronie globu, poza jurysdykcją państwa atakowanego. Po czwarte, wykradane informacje mogą zawierać nie tylko dokumenty oficjalne, ale również korespondencję decydentów politycznych, co z kolei może pomóc w rozpoznaniu zamierzeń polityków, a nie tylko oficjalnych wersji zawartych w dokumentach. Po piąte, cyberszpiegostwo może zapewniać anonimowość sprawców. Zastosowanie technologii anonimizującej może skutecznie uniemożliwić wykrycie prawdziwych atakujących, a tym samym możliwe jest uniknięcie odpowiedzialności i skandalu międzynarodowego. Po szóste, cyberszpiegostwo umożliwia wykradanie jednocześnie wielkich zbiorów informacji, co jest jednocześnie oszczędnością działań, ale również umożliwia ukrycie realnego celu i motywu ataku.

Bez wątpienia cyberprzestrzeń, cyberszpiegostwo, cyberterroryzm i inne działania człowieka w świecie cyfrowym stanowią ogromne wyzwanie dla systemów bezpieczeństwa. Niemniej jednak należy pamiętać, iż działa to w obie strony i oponenci również korzystają z systemów teleinformatycznych do przetwarzania własnych informacji. Na cyberprzestrzeń należy patrzeć nie tylko z punktu widzenia potencjalnych zagrożeń, ale również szans i możliwości, jakie ze sobą niesie wykorzystanie cyberprzestrzeni w działalności wywiadowczej zarówno w sferze państwowej, jak i komercyjnej. Można śmiało powiedzieć, iż cyberprzestrzeń na stałe zagościła w świecie współczesnym obok lądu, morza i powietrza, jako arena walki człowieka z drugim człowiekiem.

Tytuł w języku angielskim:
CYBERSPACE AS A THEATER OF INTELLIGENCE ACTIVITIES

Bibliografia

Publikacje zwarte

Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Warszawa 2016.

Ciecierski M., Nogacki R., *Bezpieczeństwo współczesnej firmy. Wywiad, szpiegostwo, ochrona tajemnic*, Warszawa 2016.

Clark R.M., *Intelligence Collection*, Washington 2014.

Górka M. (red.) *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa. Historia i współczesność*, Toruń 2016.

Mądrzejowski W., *Przestępczość zorganizowana. System zwalczania*, Warszawa 2017.

Mądrzejowski W., Śnieżko S., Majewski P., *Zwalczanie przestępczości. Wybrane metody i narzędzia*, Warszawa 2017.

Siemiątkowski Z., Zięba A. (red.), *Służby specjalne we współczesnym państwie*, Warszawa 2016.

Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki, organizacji, państwa*, Warszawa 2016.

Artykuły

Dziwisz D., *Cyberbezpieczeństwo – nowy priorytet strategii obrony Stanów Zjednoczonych?*, „Sprawy Międzynarodowe" 2011, nr 3.

Grzelak M., *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" 2013/2.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", 9/13, 2013.

Źródła internetowe

Corera G., *Kaspersky Labs: Warning over Russian anti-virus software*, BBC [w:] http://www.bbc.com/news/uk-42202191 [dostęp: 2.12.2017].

Foreign Spies Stealing US Economic Secrets in Cyberspace, [w:] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf [dostęp: 2.12.2017].

MATEUSZ DECYK*

INTERNET RZECZY-WISTYCH ZAGROŻEŃ

Abstrakt

Internet Rzeczy to technologia zwiększającą komfort użytkownika, niezależnie od sfery życia, w której się pojawia. Zjawiskiem powszechnym jest podłączanie urządzeń codziennego użytku do sieci, co sprawia że bezpieczeństwo w cyberprzestrzeni zaczyna mieć rosnący wpływ na szeroko pojęte bezpieczeństwo w świecie realnym. Urządzenia te nie są odpowiednio zabezpieczone, a przeciętny użytkownik sam nie jest w stanie zadbać o swoje bezpieczeństwo. To stwarza szeroką gamę możliwości dla przestępców, ale też wiele nowych zagrożeń nie tylko dla jednostki, ale również innych podmiotów.

Słowa kluczowe: Internet Rzeczy, cyberprzestrzeń, ochrona informacji, bezpieczeństwo, cyberbezpieczeństwo, hacking.

Wprowadzenie

Dynamiczny rozwój nowych technologii pozwala na zwiększenie dotychczasowego potencjału państw, społeczeństw, a także jednostek. Aparat państwowy staje się bardziej skuteczny i szybszy w wykonywaniu swoich obowiązków względem obywateli, społeczeństwa są lepiej zintegrowane i skomunikowane. Obywatele zyskują szeroką gamę nowych możliwości, a ich życie staje się wygodniejsze. Postępująca cyfryzacja zmusza świat nauki do nieustannego rozszerzania definicji bezpieczeństwa, wprowadzając do życia człowieka nie tylko szereg udogodnień, ale także nowe, nieznane dotąd zagrożenia. Znaczącym wpływem na bezpieczeństwo jednostki odznacza się środowisko „Internetu Rzeczy", technologii niezwykle trudnej do wąskiego zdefiniowania, wnikającej w niemal każdy aspekt życia człowieka. Często użytkownik nie jest nawet świadom korzystania z konkretnych udogodnień. „Internet Rzeczy" wspiera procesy związane z komunikacją międzyludzką, przemysłem, handlem, opieką zdrowotną, czy transportem, a koszty jego wykorzystania wykraczają daleko poza konieczność zakupu urządzeń, czy oprogramowania. Wprowadza-

* Mateusz Decyk – student stosunków międzynarodowych ze specjalizacją bezpieczeństwo i studia strategiczne na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Kontakt e-mail: decykopen@gmail.com

jąc do cyberprzestrzeni ogromne ilości informacji oraz przenosząc odpowiedzialność za czynności i procesy na maszyny, użytkownik żyje wygodniej, jednocześnie narażając się na nowe zagrożenia. Do stworzenia skutecznych zabezpieczeń potrzebny jest czas, a także praktyka. Jak w każdym przypadku, budowanie infrastruktury bezpieczeństwa polega na pościgu za światem przestępczym i jego metodami działania, a Internet oraz technologie pokrewne zaopatrują przestępców w nowe możliwości działania, obnażając podatności i wrażliwość społeczeństwa informacyjnego[1]. To pokrewne technologie informacyjne posiadają największy potencjał kryminogenny oraz nieprzewidywalne kierunki rozwoju wskutek kolaboracji z technologią sztucznej inteligencji. Coraz więcej przedmiotów podłączonych jest do sieci, przetwarzając dane o nieświadomych tego użytkownikach. W nadchodzących latach liczba urządzeń codziennego użytku przetwarzających dane i łączących się z Internetem będzie wzrastać, w ramach obniżających się kosztów samej technologii[2]. Cyberbezpieczeństwo nie figuruje na szczycie listy priorytetów producentów sprzętu, jednak nawet zwiększenie wydatków na ten cel nie gwarantuje skuteczności podjętych działań. Temat „Internetu Rzeczy" staje się coraz bardziej popularny wśród ekspertów, a reforma prawa ochrony danych osobowych[3] oraz kroki podejmowane przez Komisję Europejską wskazują kierunek nadchodzącej rewolucji w zakresie cyberbezpieczeństwa.

Czym jest „Internet Rzeczy"?

Termin „Internet of Things" przypisuje się osobie Kevina Ashtona, brytyjskiego badacza MIT[4], który w 1999 roku stwierdził: „gdyby wszystkie przedmioty w codziennym życiu były wyposażone w identyfikatory i łączność bezprzewodową, mogłyby porozumiewać się ze sobą i być zarządzane za pomocą komputera[5]". W latach dziewięćdziesiątych wizja była niemożliwa to zrealizowania, jednak rozwój łączności bezprzewodowej sprawił, że słowa naukowca stały się fundamentem prób definiowania tego zjawiska. To zadanie wypełnił m.in. Międzynarodowy Związek Telekomunikacji[6], który określa „Internet Rzeczy" jako „globalną infrastrukturę dla społeczeństwa informacyjnego, umożliwiającą działanie zaawansowanym usługom poprzez łączenie fizycznych i wirtualnych rzeczy w oparciu

1 *European Police Chiefs Convention: The future of organised crime chellenges and recommended*, uropol, źródło:https://www.europol.europa.eu/publications-documents/european-police-chiefs-convention-future-of-organised-crime-challenges-and-recommended [dostęp: 02.2017 r.], s. 2.

2 *Twitter, Snapchat, Internet Rzeczy. Dane konsumenta na wyciągnięcie ręki*, źródło: http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1017004,twitter-snapchat-iot-czyli-dane-konsumenta-na-wyciagniecie-reki-20-00.html [dostęp: 02.2017 r.].

3 The General Data Protection Regulation została zatwierdzona 24 maja 2016 roku i wejdzie w życie 25 maja 2018 roku, źródło: http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679 &from=en [dostęp: 09.2017 r.].

4 Massachusetts Institute of Technology, amerykańska prywatna politechnika założona w 1861 roku.

5 M. Goodman, *Zbrodnie przyszłości: jak cyberprzestępcy, korporacje i państwa mogą użyć technologii przeciwko Tobie*, Gliwice 2016, s. 250.

6 International Telecommunication Union – najstarsza na świecie organizacja międzynarodowa powstała pierwotnie jako Międzynarodowy Związek Telegraficzny 17 maja 1865 roku w Paryżu.

o istniejące i rozwijane zdolne do współpracy technologie informacyjne i komunikacyjnej[7]". Rzecz rozumiana jest jako „obiekt fizycznego lub wirtualnego świata, który jest zdolny do bycia zidentyfikowanym i zintegrowanym w sieci komunikacyjnej[8]". Popularnym stało się określenie „ekosystemu", który umożliwia pełną synchronizację działań podejmowanych przez urządzenia, bez udziału człowieka[9]. Technologia ta zakłada wyposażanie wszystkich urządzeń codziennego użytku w zaawansowaną elektronikę w celu zwiększenia ich funkcjonalności[10]. Infrastruktura „Internetu Rzeczy" dzieli się na czujniki i mikrokontrolery. Ich rozmiar oraz zapotrzebowanie na energię ulegają zmniejszeniu. Tym samym w danym systemie będzie można zastosować więcej takich urządzeń, potęgując tym samym pobór danych i potencjał „ekosystemu". Wydajniejsze sieci bezprzewodowe pozwolą „rzeczom" na lepszą komunikację nie tylko w sieci Internet, ale także między sobą. Do telefonów, czy tabletów podłączonych do Internetu dołączać będą mieszkania, pojazdy, elementy infrastruktury miejskiej oraz urządzenia medyczne[11].

Nie samo zwiększanie funkcjonalności przedmiotów, a proces przetwarzania przez nie danych tworzy potencjalne zagrożenia dla człowieka. Często to użytkownik wprowadza do sieci dane na swój temat, ale w ramach rosnącego zaawansowania technologii, to urządzenia zbierają dane o nim, niezależnie od jego woli. W ten sposób „Internet Rzeczy" łączy się bezpośrednio z koncepcją „Big Data", reprezentującą innowacyjne sposoby analizy, wizualizacji oraz pozyskiwania ogromnej ilości informacji w czasie rzeczywistym[12]. Dane zbierane przez urządzenia wysyłane są na ogół do tzw. „chmury obliczeniowej"[13]. „Ekosystem" obejmujący fizyczne przedmioty zbierające dane oraz mechanizm gromadzący je w jednym miejscu, do wypełnienia koncepcji Ashtona, wymaga dodatkowo procesu odpowiedniej analizy danych i podejmowania autonomicznych działań niezależnych od woli człowieka. Do tego służy technologia sztucznej inteligencji. W kontekście „Internetu Rzeczy" należy odejść od klasycznego rozumowania tego pojęcia, w którym propagowano wizję stworzenia robota, o inteligencji przewyższającej ludzką[14]. Właściwsze jest

---

7 W. Rorot, *Rzeczy Internetu Rzeczy*, źródło: http://2016.dariah.pl/wpcontent/uploads/sites/3/2016/04/Wiktor.Rorot_.pdf [dostęp: 02.2017 r.].

8 *ITU-T Y.4000/Y.2060 (06/2012) – Overview of the Internet of things*, ITU, 15.06.2015, źródło:http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 [dostęp: 02.2017], s. 1 (tłum. własne).

9 P. Kolenda (red.), Raport – *Internet Rzeczy w Polsce*, IAB Polska, źródło: http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf [dostęp: 02.2017 r.].

10 K. Świrski, *Internet Rzeczy(Internet of Things), czyli trend, który zmieni nasz sposób kupowania i używania*, źródło: http://konradswirski.blog.tt.com.pl/internet-rzeczy-internet-of-things-czyli-trend-ktory-zmieni-nasz-sposob-kupowania-i-uzywania/ [dostęp: 04.2017 r.].

11 M. Goodman, *Zbrodnie*..., dz. cyt., s. 360.

12 *IOCTA – Internet Organised Crime Threat Assessment*, Europol, źródło: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 [dostęp: 04.2017 r.].

13 Według Głównego Urzędu Statystycznego usługi chmury obliczeniowej to możliwość korzystania ze skalowalnych usług ICT przy zastosowaniu Internetu. Usługi świadczone w chmurze obliczeniowej mogą obejmować dostęp do oprogramowania, korzystanie z określonej mocy obliczeniowej, przechowywanie danych, *Chmura obliczeniowa*, źródło: http://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/3086,pojecie.html [dostęp: 04.2017 r.].

14 B. Hołyst, *Bezpieczeństwo gatunku ludzkiego*, t. 4, Warszawa 2016, s. 135–139.

postrzeganie sztucznej inteligencji jako zbioru systemów informatycznych, które przy użyciu odpowiednich algorytmów są w stanie wykonywać czynności, do których normalnie potrzebna jest ludzka inteligencja, takich jak podejmowanie decyzji, czy rozpoznawanie. To pozwala na stworzenie procesów autonomicznych, uniezależnionych od człowieka, za pomocą narzędzi oferowanych przez infrastrukturę „Internetu Rzeczy"[15]. Technologia ta jest mocno niedoceniana, jednak wszechobecna, zainteresowane są nią wszystkie sektory przemysłu (w tym zbrojeniowy), usług, a także podmioty państwowe. Bez niej nie mogłyby funkcjonować współczesne systemy nawigacji, portale społecznościowe, czy wyszukiwarki internetowe. Rozwój sztucznej inteligencji wywołuje ogromne kontrowersje w środowisku naukowców, ale też producentów powiązanych usług i produktów, zdominowanego przez entuzjastów reklamujących same zalety swoich produktów[16]. Na czele sceptyków przesadnego uniezależniania procesów od ludzkiej woli stoi E. Musk, który stał się propagatorem stwierdzenia: „sztuczna inteligencja i rywalizacja na polu jej rozwoju na szczeblu narodowym może być czynnikiem, który wywoła trzecią wojnę światową". Musk stanął na czele grupy 116 ekspertów, którzy wystosowali list otwarty do ONZ[17], apelując o podjęcie działań mających zatrzymać rozwój broni autonomicznej, która ma być przyczynkiem do „trzeciej rewolucji pola walki" po wprowadzeniu prochu strzelniczego i broni nuklearnej w przeszłości. Główną obawą sygnatariuszy listy jest możliwość wymknięcia się maszyn spod ludzkiej kontroli[18].

Z powyższych twierdzeń można wysnuć wniosek, że zwyczajne przedmioty stają się *de facto* urządzeniami o podobnej charakterystyce co komputery. Poparciem dla takiego rozumowania wydaje się próba legalnego zdefiniowania pojęcia „komputer" podjęta w Stanach Zjednoczonych – „wszelkie obiekty przeznaczone do przechowywania danych lub komunikacji bezpośrednio związane lub współdziałające z takimi urządzeniami"[19]. Stopniowo kolejne przedmioty codziennego użytku uzyskują możliwość podłączenia do sieci. Dla uporządkowania, warto przywołać klasyfikację systemowych zastosowań Internetu Rzeczy utworzoną przez M. Kołodzieja:

1) inteligentne domy, budynki, posesje;
2) inteligentne miasta;
3) monitoring pojazdów;
4) inteligentne sieci medyczne;
5) inteligentne przedsiębiorstwa i przemysł;
6) inteligentne systemy energetyczne i pomiarowe;

---

15 Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, *Innowacyjna gospodarka, analiza na zlecenie Ministerstwa Cyfryzacji*, źródło: https://mc.gov.pl/files/innowacyjna_cyfryzacja_0.pdf [dostęp: 03.2017 r.], s. 34–35.

16 G. Hall, *Zuckerberg blasts Musk warnings against artificial intelligence as 'pretty irresponsible'*, źródło: https://www.bizjournals.com/sanjose/news/2017/07/24/elon-musk-artificial-intelligence-risk-zuckerberg.html [dostęp: 09.2017 r.].

17 Organizacja Narodów Zjednoczonych.

18 S. Gibbs, *Elon Musk leads 116 experts calling for outright ban of killer robots*, źródło: https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war [dostęp: 09.2017.].

19 M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 10.

7) systemy monitorowania środowiska[20].

Ten sam autor wśród przykładowych zastosowań „Internetu Rzeczy" wymienia między innymi inteligentny budzik, który dostosuje porę alarmu w zależności od natężenia ruchu na drodze do pracy, sportowe obuwie zastępujące powszechnie używane już opaski sportowe wykonujące pomiary poszczególnych parametrów takich jak tętno, pojemnik na leki przypominający choremu o konieczności zażycia lekarstwa, czy też systemy w infrastrukturze miejskiej ułatwiające kierowcom znalezienie miejsca parkingowego.

Według raportu „Digital in 2017" udział urządzeń mobilnych na rynku elektroniki stale rośnie. Polska znajduje się w czołówce państw, pod względem korzystania z Internetu za pomocą urządzeń mobilnych. Około 57% ruchu internetowego w Polsce w 2016 roku przypadało w udziale smartfonom i tabletom. Skala wzrostu znaczenia tych urządzeń widoczna jest w statystykach światowego udziału urządzeń mobilnych w ruchu internetowym. W 2009 roku udział ten wynosił poniżej 0,7%. W roku 2016 było to już około 50% globalnego ruchu internetowego. Po raz pierwszy urządzenia mobilne wyprzedziły tradycyjne komputery w udziale w globalnym ruchu internetowym. Ten wzrost pokazuje pewien trend, który będzie się utrzymywał, a największy na to wpływ mają państwa rozwijające się, co zdają się potwierdzać światowi liderzy w zestawieniu – Nigeria, Indie, RPA i Indonezja, z udziałem urządzeń mobilnych w sieci około 80%[21]. Według Komisji Nadzoru Finansowego w 2015 roku 43% użytkowników smartfonów w Polsce korzystała z usługi bankowości mobilnej[22]. O rosnącej skali zjawiska opróżniania kont bankowych użytkowników smartfonów za pomocą złośliwego oprogramowania media informowały wraz ze wzrostem skalą tego zjawiska. Już kilka lat temu zauważono, że nie są to przypadkowe ataki, a przestępczy biznes, ukierunkowany na możliwie jak największą efektywność. Koncentracja hakerów[23] na urządzeniach mobilnych nie może dziwić, gdyż zabezpieczenia w nich stosowane są jeszcze mniej skuteczne niż te w komputerach personalnych, czy laptopach[24]. Od wielu lat firma KasperskyLab w swoich raportach umieszcza szczegółowe dane dotyczące ataków i standardowych zagrożeń czyhających w sieci na urządzenia mobilne. Do największych należy zaliczyć:

1) niekontrolowane wycieki danych powodowane przez aplikację;

---

20 M. Kołodziej, *Internet Rzeczy, nowe spojrzenie na ochronę prywatności*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna 2015*, Szczytno 2015, s. 14–19.

21 S. Kemp, *Digital 2017: Global Overview*, źródło: https://wearesocial.com/special-reports/digital-in-2017-global-overview [dostęp: 09.2017 r.].

22 *KNF wydała rekomendację dot. bezpieczeństwa transakcji płatniczych w internecie*, bankier.pl, z dn. 17.11.2015, źródło: http://www.bankier.pl/wiadomosc/KNF-wydala-rekomendacje-dot-bezpieczenstwa-transakcji-platniczych-w-internecie-3442312.html [dostęp: 02.2017 r.].

23 Według Administratora Bezpieczeństwa Informacji UW T. Śmigielskiego, obecnie nie istnieje potrzeba szczególnego tytułowania złośliwych sprawców w cyberprzestrzeni. Istnieje terminologiczny podział na hackerów (hakerów) i crackerów ze względu na typy i charakter działań tych jednostek, jednak dla osoby potencjalnie zaatakowanej nie ma to znaczenia, a sformułowanie „hacker" weszło już do powszechnego użycia, T. Śmigielski, *Hacker i cracker*, źródło: https://portal.uw.edu.pl/web/ado/hacker-i-cracker [dostęp: 04.2017 r.].

24 M. Sparkes, *Hackers focus on stealing money from mobile banking*, źródło: http://www.telegraph.co.uk/technology/internet-security/10662106/Hackers-focus-on-stealing-money-from-mobile-banking.html [dostęp: 02.2017 r.].

2) korzystanie z darmowych, niezweryfikowanych sieci Wi-Fi;
3) „spoofing"oraz „phishing"[25] (szeroka gama metod wyłudzania danych);
4) złośliwe oprogramowanie gromadzące informacje – „ransomware", „malware", „spyware";
5) ataki na aplikacje modyfikujące ich kod, a w efekcie działanie.

W 2016 roku w ponad 30% państw członkowskich Unii Europejskiej organa ścigania wszczęły postępowania w sprawach nadużyć dotyczących przetwarzania danych w chmurze, a w blisko 50% z nich informowało o potrzebie gromadzenia dowodów z tego źródła. „Internet Rzeczy" stanie się w przyszłości nieodłącznym elementem „infrastruktury krytycznej", która będzie narażona na zagrożenia płynące z cyberprzestrzeni mogące skutkować fizycznym lub psychicznym uszczerbkiem na zdrowiu[26]. Zagrożenie dostrzega Europol, obecnie na celowniku cyberprzestępców znajdują się głównie dane osobowe i informacje biznesowe[27]. Techniki te nie są nowym wynalazkiem, jest to po prostu adaptacja metod wymyślonych już na początku istnienia sieci Internet, przy wykorzystaniu pełni możliwości jaką daje „Internet Rzeczy". Większość cyberprzestępców nieustannie skupia się na kradzieży danych, bo to one stanowią wartość samą w sobie, bądź są swego rodzaju „wytrychem" do dalszej przestępczej i szkodliwej działalności. Już w 2012 roku dane okrzyknięto „nową ropą naftową", a slogan ten jest szeroko powtarzany w środowiskach naukowych i publicystycznych[28].

Dla „Internetu Rzeczy" największym zagrożeniem wydaje się być „hacking", którego definicja sensu *stricto* została ujęta w kodeksie karnym, jako uzyskanie nieautoryzowanego dostępu do informacji. Nie oddaje to pełni zagrożeń, jakie „hacking" tworzy dla przedmiotów podłączonych do sieci. F. Radoniewicz rozszerza samo pojęcie na art. 267–269b Kodeksu Karnego. Jest to zjawisko, które może być rozumiane na wiele sposobów, a jego definicja będzie musiała obejmować coraz szersze spektrum czynności w toku postępu technologicznego. Prawo od dawna nie nadąża za rozwojem cyberprzestrzeni, a dystans ten będzie się pogłębiał. Problemem jest nie tylko definiowanie pojęć, ale również atrybucja czynów przestępczych i transgraniczny charakter działań[29]. Uściślając pojęcie, „hacking" można określić jako uzyskanie dostępu do systemu teleinformatycznego, zakłócenie jego

---

25 Definicje firmy Avast: „Spoofing" ma miejsce, gdy hacker podszywa się pod inne urządzenie lub innego użytkownika w sieci, aby wykraść dane, zainstalować złośliwe oprogramowanie lub ominąć mechanizmy kontroli dostępu, źródło: https://www.avast.com/pl-pl/c-spoofing [dostęp: 04.2017 r.], „Phishing" to przebiegła metoda, której używa cyberprzestępca, aby nakłonić użytkownika do ujawnienia informacji osobistych, takich jak hasła lub numery kart kredytowych, ubezpieczeń i kont bankowych. Robią to poprzez wysyłanie fałszywych e-maili lub przekierowywanie na fałszywe strony internetowe, *Phishing*, źródło: https://www.avast.com/pl-pl/c-phishing [dostęp: 04.2017 r.].

26 Europol, IOCTA…, *cyt. wyd*., s. 54.

27 *SOCTA 2017 – Serious and Organized Crime Threat Assesments*, Europol, źródło: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [dostęp: 04.2017 r.], s. 24.

28 P. Rotella, *Is Data The New Oil?*, źródło: https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#41d038e57db3 [dostęp: 09.2017 r.].

29 A. Brachman, *Internet przedmiotów – raport*, Obserwatorium ICT, wrzesień 2013 r.

pracy oraz modyfikację lub usunięcie danych w nim zawartych[30]. Większość ekspertów do spraw cyberbezpieczeństwa jest zgodna, że ścisłe definiowanie każdego cyberzagrożenia jest niezwykle trudne, a będzie ono zawsze zależało od atrybucji i celu napastnika, którym może być uzyskanie dostępu, oszustwo, kradzież, bądź zniszczenie danych[31]. Wykorzystywane przez hakerów narzędzia różnią się, są przedmiotem specjalistycznej debaty, w której osoba nie będąca informatykiem łatwo może się pogubić. Dlatego na potrzeby zwykłego użytkownika National Cyber Security Centre (komórka GCHQ[32]) utworzyła klasyfikację cyberataków (na potrzeby przedsiębiorstw, jednak dotyczą one również użytkownika indywidualnego):

1) atak nieukierunkowany – napastnik obiera za cel jak największą liczbę urządzeń, usług i użytkowników. Najważniejsza jest liczba ofiar, a nie ich tożsamość. Do ich przeprowadzenia używane są techniki takie jak:
   a) „phishing" – uzyskiwanie wrażliwych danych poprzez wysłanie wiadomości e-mail i użycie narzędzi inżynierii społecznej,
   b) „waterholing" – tworzenie fałszywej strony internetowej, bądź przejmowanie tej prawdziwej w celu wykorzystania odwiedzających użytkowników,
   c) „ransomware" – rozpowszechnianie złośliwego oprogramowania szyfrującego urządzenia (np. dyski twarde),
   d) „scanning" – wyrywkowe ataki na przypadkowe urządzenia podłączone do Internetu;
2) atak ukierunkowany – w tym przypadku napastnik atakuje określonego użytkownika urządzenia, bądź usługi. Atak tego rodzaju może być złożoną operacją trwającą miesiące i na ogół jest procesem o specyfikacji dostosowanej do ofiary, dlatego może wyrządzić znacznie większe szkody. Takie ataki należy podzielić na:
   a) „spear-phishing" – dystrybucja wiadomości e-mail, zawierających załącznik ze złośliwym oprogramowaniem, bądź link powodujący automatyczne pobieranie i instalacje takiego programu,
   b) „botnet" – przejęcie kontroli nad urządzeniem, w celu przeprowadzenia ataku DDoS na innym urządzeniu,
   c) przerywanie łańcucha dostaw – bezpośrednie atakowanie urządzeń, bądź oprogramowania zapewniającego usługi[33].

Do powyższej klasyfikacji warto dodać tezę K. Mitnick'a, który jako najsłabsze ogniwo w każdym systemie bezpieczeństwa informatycznego określa człowieka. Inżynieria społeczna wykorzystuje perswazję i wpływ do oszukania jednostki. Dobry inżynier społeczny jest w stanie wykorzystać ludzi do uzyskania potrzebnej mu informacji, nawet bez użycia

---

30 F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, Instytut Wymiaru Sprawiedliwości, Warszawa 2012, źródło: https://www.iws.org.pl/pliki/files/IWS_Radoniewicz_Odp%20za%20przest%20hackingu.pdf [dostęp: 02.2017 r.], s. 1–3.

31 B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, źródło: http://docplayer.pl/14827446-Artykuly-cyberprzestepczosc-ochrona-informacji-i-kryptologia-brunon-holyst-jacek-pomykala-streszczenie.html#show_full_text [dostęp: 04.2017 r.], s. 6.

32 Government Communications Headquarters (pol. Centrala Łączności Rządowej) – służba specjalna Wielkiej Brytanii zbierająca informacje pochodzące z wywiadu radioelektronicznego.

33 National Cyber Security Centre, źródło: https://www.ncsc.gov.uk/articles/how-cyber-attacks-work [dostęp: 09.2017 r.]

technologii[34]. Jeszcze do niedawna wydawało się, że tego typu zagrożenia dotyczą tylko komputerów personalnych, ale właśnie ze względu na internetową ekspansję „rzeczy" już dziś wiele urządzeń z podłączeniem do sieci można zainfekować za pomocą najbardziej prymitywnych działań, takich jak wysłanie wiadomości MMS na smartfon[35]. Jak wskazuje raport Europolu dotyczący zorganizowanej przestępczość internetowej, gama złośliwego oprogramowania stosowanego przez cyberprzestępców nieustannie rozszerza się, a sztywne definiowanie zagrożeń traci na znaczeniu. Wpływ miał na to postęp w telefonii komórkowej, zamieniający aparaty w *de facto* mobilne komputery. Oprócz złośliwego oprogramowania cyberprzestępcy wykorzystują system płatności anonimowych oraz rozwój tzw. „kryptowalut"[36] do działań korupcyjnych, fałszerstw, czy prania brudnych pieniędzy. Internet oraz sieci ukryte stały się rynkiem handlu nielegalnymi dobrami oraz przestępczymi usługami. Kryminaliści wykorzystują zakodowane kanały komunikacji w taki sposób, by pozostać nieuchwytnymi dla organów ścigania[37].

Wprowadzanie autonomicznych procesów w ramach „Internetu Rzeczy" zwiększa liczbę zsynchronizowanych urządzeń, czujników, czipów i mikrokontrolerów, które często nie są nawet objęte ochroną oprogramowania antywirusowego[38]. Skuteczność programów to kolejny problem wymagający pogłębionej refleksji. Dowodem na ich słabość stał się antywirus „Flame", który wstrząsnął sektorem informatycznym i obnażył prawdziwą skalę zaniedbań producentów i ich bezbronność w obliczu zagrożeń. Mimo pogłębionej dyskusji w środowisku, nie znaleziono do tej pory złotego środka[39]. Problemem jest nie tylko sama świadomość, ale również możliwość wykrycia ataku, która jest czasem mocno ograniczona, podobnie jak szansa na wykrycie sprawcy[40].

Współczesne systemy zabezpieczeń M. Goodman określił mianem „cyfrowej linii Maginota", ze względu na mnogość połączonych ze sobą urządzeń, danych wprowa-

---

34 K. Riccio, *Kevin Mitnick: 'People, Not Technology, Weakest Security Link'*, źródło: https://www.afcom.com/Public/Resource_Center/Articles/Kevin_Mitnick_People_Not_Technology_Weakest_Security_Link.aspx [dostęp: 09.2017 r.].

35 *Największa w historii luka w Androidzie. Twój telefon rozbroi zwykły MMS*, źródło: http://tvn24bis.pl/tech,80/luka-w-androidzie-na-atak-hakerow-narazonych-jest-950-mln-smartfonow,563931.html [dostęp: 02.2017 r.].

36 Wg Rafała Prabuckiego – „Pomimo tego, że w działaniu przypominają one pieniądz elektroniczny to w kontekście prawa nie są one ani pieniądzem, ani też walutą, na co wskazywałaby ich potoczna nazwa. Mimo to zyskały one rzeszę sympatyków, którzy monetom kryptograficznym nadali wartość i wyprowadzili tą ideę poza ramy cyberprzestrzeni, czyniąc pierwszą z nich – bitcoina – obiecującym eksperymentem w ujęciu płatności on-line za dobra, usługi i treści cyfrowe", R. Prabucki, *Kryptologia, a prawo – wybrane zagadnienia: idea kryptowaluty i jej wpływu na ewolucję oszustw w internecie*, [w:] M. Zieliński (red.), *Przegląd Nauk Stosowanych*, Nr 10, źródło: http://pns.po.opole.pl/pns/PNS_10.pdf#page=106 [dostęp: 04.2017 r.], s. 106.

37 *IOCTA…*, *cyt. wyd.*, s. 10–11.

38 *Top 7 Mobile Security Threats: Smart Phones, Tablets & Mobile Internet Devices – What the Future Has in Store*, źródło: https://usa.kaspersky.com/internet-security-center/threats/mobile-device-security-threats#.WJ7UxlU1_IU [dostęp: 02.2017 r.].

39 T. Simonite, *The Antivirus Era is Over*, źródło: https://www.technologyreview.com/s/428166/the-antivirus-era-is-over/ [dostęp: 02.2017 r.].

40 L. Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, źródło: https://www.scientificamerican.com/article/tracking-cyber-hackers/ [dostęp: 09.2017 r.].

dzanych do sieci i brak skutecznych środków bezpieczeństwa[41]. Flagowym przykładem wykorzystania podatności układu „naczyń połączonych" jest historia amerykańskiego dziennikarza M. Honana z 2012 roku. Głównym celem cyberprzestępców, którzy zaatakowali Honana było jego konto na Twitterze, jednak w międzyczasie uzyskali oni dostęp do kilku kont ofiary oraz wrażliwych danych osobowych. W pierwszej kolejności hakerzy uzyskali podstawowe dane osobowe dziennikarza. Te informacje dosyć łatwo można było znaleźć w Internecie, a dane te posłużyły przestępcom do zmanipulowania pracownika centrali telefonicznej firmy Amazon, obsługującej sklep internetowy, w taki sposób, by ten wyjawił cztery ostatnie cyfry karty kredytowej Honana. Te dane w połączeniu z adresem zamieszkania ofiary i odpowiednimi zabiegami inżynierii społecznej zastosowanymi wobec pracowników działu obsługi klienta pozwoliły na uzyskanie dostępu do konta AppleID, do którego przypisany był adres konta Google, połączonego z kontem Twitter. Włamanie się na te konta, przy zebranych już informacjach nie stanowiło problemu. W trakcie całej operacji cyberprzestępcy uzyskali dane o obecnej lokalizacji dziennikarza, usunęli zawartość dysków wszystkich urządzeń firmy Apple, które znajdowały się w pobliżu. Honan utracił dostęp do kilku kont, a jego reputacja została nadszarpnięta, bowiem hakerzy wykorzystali konto Twitter to publikacji obraźliwych komentarzy i wiadomości. Warto zwrócić uwagę, że napastnicy posiadali już tak ogromną liczbę danych, że wyrządzone przez nich szkody mogły być znacznie większe, w przypadku włamania się na konto bankowe Honana. Okazało się, że połączenie odpowiednich narzędzi inżynierii społecznej z podstawową wiedzą na temat informatyki, pozwala na wyrządzenie ogromnych szkód użytkownikowi sieci Internet i urządzeń „Internetu Rzeczy". Obnażone zostały słabości systemów bezpieczeństwa największych światowych korporacji, obsługujących miliony klientów na całym świecie i gromadzących dane na ich temat. W tym przypadku został wykorzystany nie tylko mechanizm synchronizacji kont internetowych, ale również urządzeń, ponieważ uzyskując dostęp do jednego urządzenia Apple, „włamywacz" zlokalizował pozostałe zsynchronizowane urządzenia tej firmy w pobliżu, przez co również one stały się obiektem ataku[42]. Brak spójności i integralności między poszczególnymi zabezpieczeniami, różne standardy bezpieczeństwa poszczególnych dostawców usług są przyczynkiem dodatkowych zagrożeń dla użytkowników[43]. „Internet Rzeczy" to przestrzeń, w której przetwarzane są informacje zawierające dane osobowe, ale również informacje dotyczące ich aktywności i działań. Celowa ingerencja, bądź wpłynięcie na działanie jednego z elementów sytemu, może bardzo źle wpłynąć na pozostałe, powodując reakcję łańcuchową, a w efekcie spowodować dysfunkcję całego systemu. Urządzenia zbierają i przetwarzają dane o coraz większym stopniu wrażliwości, zwiększając dolegliwość konsekwencji ich nieodpowiedniego zabezpieczenia[44].Urządzenia mobilne stają się nieodłączną częścią ludzkiej codzienności. Jednak nie tylko dorośli stają się beneficjentem coraz szerszego dostępu do zaawansowanej technologii. Również osoby niepełnoletnie korzystają z urządzeń podłączonych do sieci i mogą

41 M. Goodman, *Zbrodnie…*, dz. cyt., s. 15.

42 M. Honan, *How Apple and Amazon security flaws let to my epichacking*, źródło: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ [dostęp: 02.2017 r.].

43 M. Goodman, *Zbrodnie…*, dz. cyt., s. 15.

44 M. Kołodziej, *Internet…*, [w:] J. Kosiński (red.), dz. cyt., 2015, s. 20–21.

stać się ofiarą cyberprzestępców. Dane dotyczące dzieci po raz pierwszy padły łupem hakerów w 2015 roku, kiedy to jedna z firm produkujących zabawki podłączone do sieci została okradziona z danych około sześciu milionów osób nieletnich[45]. Było to wydarzenie bezprecedensowe, w trakcie postępowania wykryto rażące nieprawidłowości w zakresie polityki ochrony danych osobowych, a rodzice zostali wezwani do zbojkotowania produkowanych przez nią zabawek[46]. Obecnie większą obawę wzbudzają zabawki z technologią „Internetu Rzeczy". Jednym z takich przypadków jest sprawa „Hello Barbie" – lalki umożliwiającej dziecku rozmowę z zabawką wyposażoną w mikrofony oraz funkcję rozpoznawania głosu. Nie budziłoby to wielkich kontrowersji, gdyby nie fakt, że zabawki posiadają połączenie z siecią, która umożliwia jej zsynchronizowanie ze smartfonem, a treść rozmów dziecka i zabawki zostaje przetrzymywana w „chmurze" producenta. Nie jest jasne do czego te dane są wykorzystywane[47]. Norwescy eksperci przeprowadzili eksperyment, po którym określili „Hello Barbie" jako najbardziej podatną na cyberataki w związku z podłączeniem zabawki do sieci, które sprawia, że niemal każdy może dokonać próby jej zaatakowania[48]. Podobne obawy pojawiają się w społeczeństwie niemieckim. Federalna Agencja ds. Sieci (Bundesnetzagentur) określiła inną zabawkę tego typu – „My FriendCayla" jako „nielegalne narzędzie szpiegowskie", wymuszając na producencie wyłączenie funkcji sieciowych zabawki, która mogła zostać uznana za „narzędzie inwigilacyjne" w świetle niemieckiego Kodeksu Karnego[49]. Wyniki przeprowadzonego przez niemieckich dziennikarzy eksperymentu pokazały, że za pomocą łączności Bluetooth można uzyskać nieuprawniony dostęp do lalki i rozmawiać z dzieckiem. Lalka nie została zabezpieczona hasłem[50].

Praktyka pokazuje również, że urządzenia podłączone do sieci mogą stać się narzędziem znacznie poważniejszych nadużyć wobec nieletnich. Zagadnienie stało się poważne wraz z wybuchem afery w USA, kiedy to dyrekcja jednej ze szkół, udostępniając szkolne laptopy do użytku domowego swoim uczniom, jednocześnie zainstalowała w nim oprogramowanie szpiegowskie w celu obserwacji ich zachowań[51]. Wykorzystanie urządzeń rejestrujących w komputerach, czy smartfonach staje się powszechne w gronie cyberprzestępców. Rynek „elektronicznych niani" zyskuje na coraz większej popularności, a problemy z zabezpieczeniami zastosowanymi w tych urządzeniach pojawiły się w 2008 roku, gdy

---

45 *Millions of children's data hacked after 'biggest ever cyber attack' on toy firm*, Telegraph, 25.12.2015, źródło: http://www.telegraph.co.uk/news/uknews/law-and-order/12051439/Millions-of-childrens-data-hacked-after-biggest-ever-cyber-attack-on-toy-firm.html [dostęp: 02.2017 r.].

46 L. Kelion, *Parents Arged to boycott VTech toy safter hack*, źródło: http://www.bbc.com/news/technology-35532644 [dostęp: 02.2017 r.].

47 A. Walkowiak, *Szpieg pod choinkę?*, źródło: https://panoptykon.org/wiadomosc/szpieg-pod-choinke [dostęp: 02.2017 r.].

48 A. Johnsen, *Investigation of privacy and security issues with smart toys*, źródło: https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf [dostęp: 02.2017 r.].

49 P. Olterman, *German parents told to destroy doll that can spy on children*, źródło: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children [dostęp: 02.2017 r.].

50 C. Leistenschneider, *Die Abhöranlage im Kinderzimmer*, źródło: http://www.saarbruecker-zeitung.de/sz-spezial/internet/art371089,6380949 [dostęp: 02.2017 r.].

51 D. Kravets, *School District Allegedly Snapped Thousands of Student Webcam Spy Pics*, źródło: https://www.wired.com/2010/04/webcamscanda/ [dostęp: 02.2017 r.].

pewien mieszkaniec Stanów Zjednoczonych odkrył, że jego sąsiad posiadający takie samo urządzenie, tego samego producenta, jest w stanie podsłuchiwać i podglądać, co dzieje się w jego domu[52]. Poważniejszy przypadek miał miejsce w stanie Texas (USA) kilka lat później. Nieznany sprawca przejął kontrolę nad „elektroniczną nianią", służącą do opieki nad dwuletnim dzieckiem użytkowników. „Włamywacz" oprócz możliwości rejestrowania tego co dzieje się w pokoju dziecka, uzyskał dostęp do mikrofonu, mówił do dziecka po imieniu, dodatkowo napastując je nieprzyzwoitymi wyrażeniami[53]. Podobny przypadek miał miejsce w Ohio (USA), kiedy to kobieta odkryła, że z używanej przez nią „elektronicznej niani" wydobywa się męski głos, używający „obscenicznych" słów skierowanych do dziecka[54]. Tego typu urządzenia nie tylko posiadają podłączenie do Internetu, ale również często są zsynchronizowane z tabletami, bądź smartfonami użytkowników, przez które „nianie" są często obsługiwane. Z raportu senackiej Komisji Handlu, Nauki i Transportu (USA), wynika, że producenci zabawek rzadko dbają o bezpieczeństwo informacji dotyczących dzieci, zbierając jednocześnie ich podstawowe dane osobowe, zdjęcia, treść wiadomości pisemnych oraz głosowych, czy dane dotyczące lokalizacji. Analizie zostały poddane przypadki masowych wycieków danych z takich firm jak VTech, czy Fisher-Price[55]. Jak podkreśla Federalna Komisja Handlu (USA) wykradzione dane dzieci mogą być narzędziem w wyłudzeniach świadczeń socjalnych, otwieraniu kont bankowych, uzyskiwaniu pożyczek lub najmowaniu mieszkania[56].

Rozwijająca się automatyzacja nie pominęła budynków. Angielski termin „Smart Home" („Inteligentne Domy") to inaczej obiekty, które wysyłają dane do sieci, a jednocześnie potrafią je odbierać i przetwarzać. To „ekosystem", w którym przedmioty, sensory, czy urządzenia mogą się ze sobą komunikować, wymieniając dane za pośrednictwem łączności bezprzewodowej. Zebrane dane są przesyłane do chmury, gdzie następuje proces ich przetwarzania. Używając interfejsu (np. smartfon lub tablet), użytkownik może zdalnie korzystać z usług „Smart Home"[57]. Wszystkie urządzenia w takim systemie (podobnie jak komputer) posiadają indywidualny adres sieciowy, a oprócz możliwości obsługi przez interfejs, system posiada zdolność do autonomicznego wykonywania różnych operacji[58].

---

52 K. Zetter, *Man Sues Over Leaky Baby Monitor*, źródło: https://www.wired.com/2009/11/baby-monitor/ [dostęp: 02.2017 r.].

53 D. Gross, *Foul-mouthed hacker hijacks baby's monitor*, źródło: http://edition.cnn.com/2013/08/14/tech/web/hacked-baby-monitor/ [dostęp: 02.2017 r.].

54 *Hacker hijacks baby monitor*, FOX19, źródło: http://www.fox19.com/story/25310628/hacked-baby-monitor [dostęp: 02.2017 r.].

55 B. Nelson, *Children's Connected Toys: Data Security and Privacy Concerns*, źródło: https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf [dostęp: 09.2017 r.].

56 *7 Child Identity Theft*, Federal Trade Commission, źródło: https://www.consumer.ftc.gov/articles/0040-child-identity-theft [dostęp: 02.2017 r.].

57 B. Risteska Stojkoska, K. Trivodaliev, *A review of Internet of Things for Smart Home Challenges and solutions,* źródło: https://www.researchgate.net/publication/308975029_A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions [dostęp: 02.2017 r.], s. 5–6.

58 A. Ożadowicz, *Internet Rzeczy w systemach automatyki budynkowej*, źródło: https://www.researchgate.net/publication/269628658_Internet_Rzeczy_w_systemach_automatyki_budynkowej [dostęp: 02.2017 r.], s. 2–3.

Do najpopularniejszych rozwiązań w „Smart Home" należą systemy HVAC (ogrzewania, wentylacji i klimatyzacji), kontroli oświetlenia, systemy bezpieczeństwa i kontroli dostępu, systemy alarmowe, systemy przeciwpożarowe oraz systemy audiowizualne[59]. Urządzenia produkowane są z myślą o minimalizacji kosztów i poboru energii. Na tym skupiają się producenci, kosztem kwestii bezpieczeństwa. Biorąc pod uwagę ilość połączeń oraz zsynchronizowanych urządzeń „Internetu Rzeczy" w systemach automatyki domowej, łatwo wyobrazić sobie skalę szkód jaką mogą wywołać cyberprzestępcy mając dostęp do ogromnej ilości danych wrażliwych domowników i mnogość potencjalnych punktów dostępowych. W jednym z raportów firma Kaspersky podkreśla rosnący udział cyberataków na urządzenia „Internetu Rzeczy" poprzez router, za pośrednictwem którego urządzenia łączą się z siecią[60].

Mimo początkowej fazy rozwoju systemów automatyki domowej, nie brakuje przykładów na ich podatności w zakresie bezpieczeństwa. W 2013 roku dziennikarz K. Hill, podczas pracy nad artykułem, wpisała w wyszukiwarkę internetową frazę „Smart Home". Bez szczególnych umiejętności w zakresie informatyki ta czynność doprowadziła ją na stronę internetową firmy Insteon oferującej instalacje automatyki domowej, gdzie uzyskała dostęp do systemów kilku klientów firmy. Z poziomu strony internetowej Hill mogła kontrolować urządzenia (manipulować temperaturą w domu, a nawet otworzyć bramę garażową) w domach rodzin korzystających z usług Insteon oraz uzyskała dostęp do informacji na temat domowników. Afera, którą wywołała ta sytuacja, doprowadziła do odkrycia kolejnych nieprawidłowości w stosowanych przez firmę systemach[61]. Ofiarą przestępców może zostać niemal każde urządzenie w „Inteligentnym Domu", nie wykluczając z tego grona tostera podłączonego do sieci. Nie oznacza to, że haker za wszelką cenę chce przejąć kontrolę nad urządzeniem wykorzystywanym do przygotowywania posiłków, po prostu zaprogramowane przez niego złośliwe oprogramowanie automatycznie wyszukuje niezabezpieczone porty w całej sieci[62]. Być może toster nie jest kluczem pozwalającym przestępcy na fizyczne włamanie się do domu, ale synchronizacja wszystkich „rzeczy" może doprowadzić cyberprzestępcę do innych urządzeń, przetwarzających wrażliwe dane, bądź będących elementami systemu bezpieczeństwa[63]. Ataki na sprzęt AGD nie są jednak tak powszechne, jak te na sprzęt audiowizualny. Niepokojące stają się doniesienia o wrażliwości na cyberataki urządzeń takich jak „Apple Siri", „Google Home", czy „Amazon Echo". Są to zyskujący na popularności „asystenci" dowodzenia „Inteligentnych Domów", sterowane za pomocą komend głosowych. Możliwe jest zainfekowanie wirusem tych urzą-

---

59 N. Ul Mushtaq, *Smart Home*, źródło: http://cctvinstitute.co.uk/smart-home/ [dostęp: 02.2017 r.].

60 A. DeNisco, *Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the rise*, źródło: http://www.techrepublic.com/article/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/ [dostęp: 09.2017 r.].

61 K. Hill, *When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet*, źródło: http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#49e204f546a5 [dostęp: 02.2017 r.].

62 A. McGill, *The Inevitability of Being Hacked*, źródło: https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/ [dostęp: 02.2017 r.].

63 A. Greenberg, *Flaws in Samsung's 'Smart' Home Let Hackers Unlock Doors and Set Off Fire Alarms*, źródło: https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/ [dostęp: 02.2017 r.].

dzeń w tradycyjny sposób, jednak chińscy i amerykańscy eksperci twierdzą, że za pomocą odtwarzania dźwięku o wysokiej częstotliwości (niesłyszalnych dla ludzkiego ucha) są w stanie przejąć kontrolę nad „asystentami”[64]. Mało prawdopodobne by taka praktyka stała się powszechna, jednak takie przykłady pokazują, że wystarczająco zmotywowany napastnik może uzyskać nieuprawniony dostęp do urządzenia, bądź danych w sposób niemożliwy do przewidzenia. Wiele urządzeń w „Smart Home” wykorzystuje łącze Bluetooth. We wrześniu 2017 roku firma Armis odkryła nowe narzędzie w rękach hakerów zagrażające urządzeniom mobilnym, komputerom oraz urządzeniom „Internetu Rzeczy”. Eksperci Armis określili jako najbardziej zagrożone wszystkie rodzaje telefonów, tabletów oraz urządzenia „ubierane”. Zagrożone są również urządzenia w systemach automatyki domowej oraz „elementy infrastruktury krytycznej”, takie jak samochody i urządzenia medyczne. Łączna liczba urządzeń potencjalnie podatnych na atak została obliczona na ponad 8 miliardów. Wiele z nich zostanie uodpornionych na atak poprzez aktualizację oprogramowania, lecz będą to głównie smartfony i komputery[65]. Nową podatność nazwano „BlueBorne”, nie jest to rodzaj złośliwego oprogramowania, a „wektor ataku”, który hakerzy wykorzystują dzięki wrażliwości urządzeń z włączoną łącznością Bluetooth. Uzyskując dostęp do jednego urządzenia, można z łatwością „włamać się” do kolejnego urządzenia z włączonym Bluetooth, nawet jeśli oba urządzenia nie zostały ze sobą wcześniej zsynchronizowane[66]. Wielu użytkowników smartfonów posiada aktywną łączność Bluetooth przez cały czas użytkowania urządzenia. Można sobie łatwo wyobrazić sytuację, w której właściciel restauracji postanowił skorzystać w swoim lokalu ze sprzętu grającego z technologią Bluetooth (takie urządzenia zyskują na popularności, podobnie jak bezprzewodowe zestawy słuchawkowe). Gdyby hakerowi udało się uzyskać dostęp do wspomnianego głośnika, mógłby on za jego pośrednictwem „włamać się” do smartfonów dużej części klientów restauracji. Podobnie, mógłby przejąć kontrolę nad wszystkimi tabletami, komputerami i innymi urządzeniami z tym standardem łączności, które znalazły się w zasięgu głośnika. Identyczny scenariusz mógłby mieć miejsce w każdym domu i to niekoniecznie tym „inteligentnym”. Już dzisiaj w wielu gospodarstwach domowych znajduje się kilkanaście urządzeń Bluetooth, a część z nich korzysta również z łączności internetowej[67].

Zagrożenia dla prywatności płyną nie tylko ze świata przestępczego, ale również od producentów. Przykładem jest autonomiczny odkurzacz firmy Roomba, którego producenci chwalą się, że urządzenie zbiera informacje na temat swojego otoczenia w trakcie pracy

64 *‘Dolphin’ attacks fool Amazon, Google voice assistants*, BBC, źródło: http://www.bbc.com/news/technology-41188557 [dostęp: 09.2017 r.].

65 B. Seri, G. Vishnepolsky, *The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks*, źródło: http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf [dostęp: 09.2017 r.].

66 *The Attack Vector “BlueBorne” Exposes Almost Every Connected Device*, źródło: https://www.armis.com/blueborne/ [dostęp: 09.2017 r.].

67 M. Nowak, *Nasze lenistwo jeszcze odbije się czkawką. Blue Borne to spełnienie najczarniejszej wizji dla smart domów*, źródło: http://www.spidersweb.pl/2017/09/blueborn-bluetooth-bezpieczenstwo.html [dostęp: 09.2017 r.].

„mapując" przy okazji mieszkanie użytkownika, a zebrane dane, mają być sprzedawane producentom systemów automatyki domowej[68].

Podsumowanie

Jeden artykuł nie jest formatem wystarczającym do ukazania pełnej skali zagrożeń jakie prezentuje sobą „Internet Rzeczy" i związane z nim technologie. Ingerencja w życie człowieka urządzeń podłączonych do sieci będzie coraz większa, wraz z postępem technologicznym, rozwojem technologii „ubieranych", zautomatyzowanych i autonomicznych środków transportu, urządzeń medycznych podłączonych do sieci, czy rozwoju „Smart Cities". Na przestrzeni lat zdaje się podupadać mit o skuteczności oprogramowania antywirusowego, producenci przeznaczają nieznaczne środki finansowe na wzmocnienie cyberbezpieczeństwa, a przestępcy znaleźli w Internecie bezpieczną przystań, chroniącą od atrybucji potencjalnych działań. Gromadzone dane będą wykorzystywane nie tylko przez przestępców, ale również przez międzynarodowe korporacje oraz podmioty państwowe. Zakres oraz sposoby ich użycia będą ograniczone jedynie wyobraźnią i możliwościami technicznymi dysponenta danych. Tworzy to wiele potencjalnych niebezpieczeństw, których skutki trudno jest przewidzieć. Wyzwania w zakresie cyberbezpieczeństwa stoją nie tylko przed indywidualnymi użytkownikami, ale również przed korporacjami, służbami bezpieczeństwa, prawodawcami. „Internet Rzeczy" staje się integralną częścią życia, której zabezpieczenie jest kwestią nieodzowną do zapewnienia bezpieczeństwa jednostki, społeczeństw i państwa. Niezwykle ważna jest współpraca i spójność podejmowanych działań, bowiem każda niezgodność i brak synchronizacji, będzie tworzyć luki w systemie bezpieczeństwa. Ich stopniowym wypełnianiem powinni zająć się eksperci, jednak odpowiedzialność spoczywa również na użytkownikach. Dlatego na koniec warto przytoczyć cytat K. Mitnick'a: „Odkryłem, że łatwiej jest manipulować ludźmi niż technologią"[69].

Tytuł w języku angielskim:
INTERNET OF REAL THREATS

Bibliografia

Publikacje zwarte i artykuły naukowe

Brachman A., *Internet przedmiotów – raport*, Obserwatorium ICT, wrzesień 2013 r.

Goodman M., *Zbrodnie przyszłości: jak cyberprzestępcy, korporacje i państwa mogą użyć technologii przeciwko Tobie*, Gliwice 2016.

[68] R. Jones, *Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder*, źródło: http://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829 [dostęp: 09.2017 r.].

[69] *Kevin Mitnick Quotes*, źródło:https://www.brainyquote.com/quotes/quotes/k/kevinmitni613263.html [dostęp: 09.2017 r.].

Hołyst B., *Bezpieczeństwo gatunku ludzkiego*, t. 4, Warszawa 2016.

Kołodziej M., *Internet Rzeczy, nowe spojrzenie na ochronę prywatności*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna 2015*, Szczytno 2015.

Siwicki M., *Cyberprzestępczość*, Warszawa 2013.

Źródła internetowe

7 Child Identity Theft, Federal Trade Commission, źródło: https://www.consumer.ftc.gov/articles/0040-child-identity-theft [dostęp: 09.2017 r.].

Allen G.C., źródło: http://edition.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-allen/index.html [dostęp: 09.2017 r.].

BBC, *'Dolphin' attacks fool Amazon, Google voice assistants*, źródło: http://www.bbc.com/news/technology-41188557.

Chmura obliczeniowa, http://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/3086,pojecie.html.

DeNisco A., *Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the rise*, źródło: http://www.techrepublic.com/article/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/ [dostęp: 09.2017 r.].

Europol, *IOCTA – Internet Organised Crime Threat Assessment*, źródło: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 [dostęp: 09.2017 r.].

Europol, *SOCTA 2017 – Serious and Organized Crime Threat Assesments*, źródło: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [dostęp: 09.2017 r.].

European Police Chiefs Convention: The future of organised crime chellenges and recommended, Europol, źródło: https://www.europol.europa.eu/publications-documents/european-police-chiefs-convention-future-of-organised-crime-challenges-and-recommended [dostęp: 09.2017 r.].

Gibbs S., *Elon Musk leads 116 experts calling for outright ban of killer robots*, źródło: https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war.

Greenberg A., *Flaws in Samsung's 'Smart' Home Let Hackers Unlock Doors and Set Off Fire Alarms*, źródło: https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/.

Greenemeier L., *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, źródło: https://www.scientificamerican.com/article/tracking-cyber-hackers/.

Gross D., *Foul-mouthed hacker hijacks baby's monitor*, http://edition.cnn.com/2013/08/14/tech/web/hacked-baby-monitor.

Hacker hijacks baby monitor, FOX19, źródło: http://www.fox19.com/story/25310628/hacked-baby-monitor.

Hall G., *Zuckerberg blasts Musk warnings against artificial intelligence as 'pretty irresponsible'*, źródło: https://www.bizjournals.com/sanjose/news/2017/07/24/elon-musk-artificial-intelligence-risk-zuckerberg.html [dostęp: 09.2017 r.].

Hołyst B., Pomykała J., *Cyberprzestępczość, ochrona informacji i kryptologia*, źródło: http://docplayer.pl/14827446-Artykuly-cyberprzestepczosc-ochrona-informacji-i-kryptologia-brunon-holyst-jacek-pomykala-streszczenie.html#show_full_text.

Honan M., *How Apple and Amazon security flaws let to my epic hacking*, źródło: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.

Hill K., *When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet*, źródło: http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#49e204f546a5.

ITU-T Y.4000/Y.2060 (06/2012) – Overview of the Internet of things, ITU, 15.06.2015, źródło: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

Johnsen A., *Investigation of privacy and security issues with smart toys*, źródło: https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf.

Jones R., *Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder*, źródło: http://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829.

Kelion L., *Parents urged to boycott VTech toys after hack*, źródło: http://www.bbc.com/news/technology-35532644.

Kemp S., *Digital 2017: Global Overview*, źródło: https://wearesocial.com/special-reports/digital-in-2017-global-overview.

Kevin Mitnick Quotes, źródło: https://www.brainyquote.com/quotes/quotes/k/kevinmitni613263.html [dostęp: 09.2017 r.].

KNF wydała rekomendację dot. bezpieczeństwa transakcji płatniczych w internecie, bankier.pl, 17.11.2015, źródło: http://www.bankier.pl/wiadomosc/KNF-wydala-rekomendacje-dot-bezpieczenstwa-transakcji-platniczych-w-internecie-3442312.html.

Kolenda P. (red.), Raport – *Internet Rzeczy w Polsce*, IAB Polska, źródło: http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf.

Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, *Innowacyjna gospodarka, analiza na zlecenie Ministerstwa Cyfryzacji*, źródło: https://mc.gov.pl/files/innowacyjna_cyfryzacja_0.pdf [dostęp: 09.2017 r.].

Kravets D., *School District Allegedly Snapped Thousands of Student Webcam Spy Pics*, źródło: https://www.wired.com/2010/04/webcamscanda/ [dostęp: 09.2017 r.].

Leistenschneider C., *Die Abhöranlage im Kinderzimmer*, źródło: http://www.saarbruecker-zeitung.de/sz-spezial/internet/art371089,6380949 [dostęp: 09.2017 r.].

McGill A., *The Inevitability of Being Hacked*, źródło: https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/ [dostęp: 09.2017 r.].

Millions of children's data hacked after ‚biggest ever cyber attack' on toy firm, Telegraph, 25.12.2015, źródło: http://www.telegraph.co.uk/news/uknews/law-and-order/12051439/Millions-of-childrens-data-hacked-after-biggest-ever-cyber-attack-on-toy-firm.html [dostęp: 09.2017 r.].

Największa w historii luka w Androidzie. Twój telefon rozbroi zwykły MMS, źródło: http://tvn24bis.pl/tech,80/luka-w-androidzie-na-atak-hakerow-narazonych-jest-950-mln-smartfonow,563931.html [dostęp: 09.2017 r.].

National Cyber Security Centre, źródło: https://www.ncsc.gov.uk/articles/how-cyber-attacks-work.

Nelson B., *Children's Connected Toys: Data Security and Privacy Concerns*, źródło: https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf [dostęp: 09.2017 r.].

Nowak M., *Nasze lenistwo jeszcze odbije się czkawką. BlueBorne to spełnienie najczarniejszej wizji dla smart domów*, źródło: http://www.spidersweb.pl/2017/09/blueborn-bluetooth-bezpieczenstwo.html [dostęp: 09.2017 r.].

Olterman P., *German parents told to destroy doll that can spy on children*, źródło: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children [dostęp: 09.2017 r.].

Ożadowicz A., *Internet Rzeczy w systemach automatyki budynkowej*, źródło: https://www.researchgate.net/publication/269628658_Internet_Rzeczy_w_systemach_automatyki_budynkowej [dostęp: 09.2017 r.].

Prabucki R., *Kryptologia, a prawo – wybranezagadnienia: idea kryptowaluty i jej wpływu na ewolucję oszustw w internecie*, [w:] M. Zieliński (red.), *Przegląd Nauk Stosowanych*, Nr 10, źródło: http://pns.po.opole.pl/pns/PNS_10.pdf#page=106 [dostęp: 09.2017 r.].

Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, Instytut Wymiaru Sprawiedliwości, Warszawa 2012, źródło: https://www.iws.org.pl/pliki/files/IWS_Radoniewicz_Odp%20za%20przest%20hackingu.pdf [dostęp: 09.2017 r.].

Riccio K., *Kevin Mitnick: 'People, Not Technology, Weakest Security Link'*, źródło: https://www.afcom.com/Public/Resource_Center/Articles/Kevin_Mitnick_People_Not_Technology_Weakest_Security_Link.aspx. [dostęp: 09.2017 r.].

Risteska Stojkoska B., Trivodaliev K., *A review of Internet of Things for Smart Home Challenges and solutions*, źródło: https://www.researchgate.net/publication/308975029A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions [dostęp: 09.2017 r.].

Rorot W., *Rzeczy Internetu Rzeczy*, źródło: http://2016.dariah.pl/wpcontent/uploads/sites/3/2016/04/Wiktor.Rorot_.pdf [dostęp: 09.2017 r.].

Rotella P., *Is Data The New Oil?*, źródło: https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#41d038e57db3 [dostęp: 09.2017 r.].

Seri B., Vishnepolsky G., *The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks*, źródło: http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf.

Simonite T., *The Antivirus Era is Over*, źródło: https://www.technologyrview.com/s/428166/the-antivirus-era-is-over/ [dostęp: 09.2017 r.].

Śmigielski T., *Hacker i cracker*, źródło: https://portal.uw.edu.pl/web/ado/hacker-i-cracker [dostęp: 09.2017 r.].

Swirski K., *Internet Rzeczy (Internet of Things), czyli trend, który zmieni nasz sposób kupowania i używania*, źródło: http://konradswirski.blog.tt.com.pl/internet-rzeczy-internet-of-things-czyli-trend-ktory-zmieni-nasz-sposob-kupowania-i-uzywania/ [dostęp: 09.2017 r.].

The Attack Vector "BlueBorne" Exposes Almost Every Connected Device, źródło: https://www.armis.com/blueborne/ [dostęp: 09.2017 r.].

The General Data Protection Regulation została zatwierdzona 24 maja 2016 roku i wejdzie w życie 25 maja 2018 roku, źródło: http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679&from=en [dostęp: 09.2017 r.].

Top 7 Mobile Security Threats: Smart Phones, Tablets & Mobile Internet Devices – What the Future Has in Store, źródło: https://usa.kaspersky.com/internet-security-center/threats/mobile-device-security-threats#.WJ7UxlU1_IU [dostęp: 09.2017 r.].

Twitter, Snapchat, Internet Rzeczy. Dane konsumenta na wyciągnięcie ręki, źródło: http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1017004,twitter-snapchat-iot-czyli-dane-konsumenta-na-wyciagniecie-reki-20-00.html [dostęp: 09.2017 r.].

Ul Mushtaq N., *Smart Home*, źródło: http://cctvinstitute.co.uk/smart-home/ [dostęp: 09.2017 r.].

Walkowiak A., *Szpieg pod choinkę?*, źródło: https://panoptykon.org/wiadomosc/szpieg-pod-choinke [dostęp: 09.2017 r.].

Zetter K., *Man Sues Over Leaky Baby Monitor*, źródło: https://www.wired.com/2009/11/baby-monitor [dostęp: 09.2017 r.].

RAFAŁ SKÓRA*

RANSOMWARE – JAKO ZAGROŻENIE DLA CYBERBEZPIECZEŃSTWA. ANALIZA PRZYPADKU ATAKU WANNACRY

Abstrakt

Artykuł ma za cel zdefiniowanie czym jest ransomware oraz jak wyglądała ewolucja tego rodzaju złośliwego oprogramowania. Kolejną kwestią poruszoną w niniejszym opracowaniu jest znalezienie odpowiedzi na pytanie – dlaczego cyberprzestępcy wybierają ransomware – jako metodę ataku? Czy należy spodziewać się wzrostu ataków tego typu w przyszłości? Analiza przypadku ataku WannaCry pozwoli ustalić: dlaczego tak szybko doszło do rozpropagowania robaka na całym świecie? Jak dużo ofiar zostało zainfekowanych? Jakie podmioty zostały ofiarami? Główną hipotezą pracy jest twierdzenie, że ransomware jest jednym z głównych cyberzagrożeń dla współczesnego państwa i przedsiębiorstwa.

Słowa kluczowe: cyberbezpieczeństwo, ransomware, WannaCry, zagrożenia cyberbezpieczeństwa, bezpieczeństwo informacji.

Informacja dla dzisiejszego państwa i biznesu staje się zasobem strategicznym, a jej właściwa ochrona i wykorzystanie mają przemożny wpływ na uzyskanie przewagi i powodzenia współczesnych narodów i przedsiębiorstw. Wraz z rozwojem technologii informacyjnych oraz Internetu systematycznie rośnie ilość przetwarzanych danych i informacji. Informacja jest podstawowym zasobem współczesnego świata, zasobem społeczeństwa informacyjnego, a w tego rodzaju społeczeństwie aktywność wszystkich podmiotów (państw, instytucji, organizacji, przedsiębiorstw) wiąże się nierozłącznie z szybkim i bezpiecznym przetwarzaniem ogromnych ilości informacji. Ich znaczenie wynika z faktu, iż autentyczna i dostępna w pożądanym czasie informacja może stanowić kluczowy czynnik sukcesu, zaś jej brak może być przyczyną klęski i niepowodzenia. Zagrożeń dla aktywów informacyjnych jest niezliczona ilość, nie sposób przygotować się do każdego z nich, nie tylko dlatego, że trudno je wszystkie zidentyfikować, ale dlatego, że będzie to

* mgr Rafał Skóra – absolwent Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego, kierunek: Bezpieczeństwo wewnętrzne (2017). Kontakt e-mail: rafal.sakora@gmail.com

pochłaniało ogromne nakłady finansowe. Wobec tego ważne jest aby analizować środowisko oraz zabezpieczać te obszary które są najistotniejsze dla funkcjonowania państwa bądź firmy oraz w których istnieje najwyższe prawdopodobieństwo penetracji i wycieku informacji[1]. Jednym z dzisiejszych szybko ewoluujących zagrożeń dla państw i przedsiebiorstw w obszarze cyberbezpieczeństwa jest z ang. *Ransomware*. Wielu ekspertów, a także firm w Polsce[2] i na świecie[3] w swoich artykułach czy też raportach – zajmujących się bezpieczeństwem informacji – uznało 2016 rok jako rok ransmware'u. W branży cyberbezpieczeństwa jest on dziś jednym z głównych zagrożeń dla infrastruktury IT państw i przedsiębiorstw. Ransomware nie jest już tylko znany specjalistom zajmującym się podatnościami i zagrożeniami w cyberprzestrzeni, ale także przeszedł do mainstreamu i jest powszechnie znany z powodu dużej ilości doniesień prasowych w ogólnonarodowych mediach (w szczególności przez ostatnie ataki *ransomware* WannaCry[4] i Petya[5] w 2017 r.).

Warto zacząć od tego, czym tak naprawdę jest *ransomware*. Słowo *ransomware* wywodzi się z połączenia dwóch angielskich słów *ransom* oraz *software*. W wolnym tłumaczeniu z ang. *ransom* oznacza okup, zaś *software* oprogramowanie. Złączenie tych dwóch słów dało – Ransomware. Zatem najprostsze tłumaczenie tego słowa to „złośliwe oprogramowanie wymuszające okup czy też oprogramowanie szantażujące". Ransomware zalicza się do klasy złośliwego oprogramowania przeznaczonego specjalnie dla uzyskania zysku finansowego[6]. W przeciwieństwie do wirusów używanych podczas ataków typu z ang. *hacking* – kradzież danych – ransomwarenie nie jest przeznaczony do uzyskiwania dostępu do komputera lub systemu informatycznego aby pozyskać dane, ale w celu zablokowania części lub całości funkcjonalności systemu operacyjnego użytkownika albo zaszyfrowanie części lub całości danych znajdujących się na urządzeniu ofiary. Komputer lub urządzenie zainfekowane ransomwarem zmusza użytkownika do zapłacenia haraczu w zamian za przywrócenie kontroli nad systemem operacyjnym i dostępem do danych. Ransomware zakłóca działanie systemu komputerowego, czyniąc go niezdatnym do użytku. Sprawcy następnie wysyłają właścicielowi żądanie okupu, oczekując pieniędzy w zamian za cofnięcie dokonanych zmian czyli przywrócenie kontroli nad systemem czy uzyskanie dostępu do zaszyfrowanych danych. *Ransomware* można zatem podzielić na dwie grupy[7]:

---

1 P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30.

2 W. Pawłowicz, *Ransomware to największe zagrożenie dla bezpieczeństwa IT*, źródło: https://www.computerworld.pl/news/Ransomware-to-najwieksze-zagrozenie-dla-bezpieczenstwa-IT,404822.html [dostęp: 20.09.2017].

3 McAfeeLabs, *Threats Report: December 2016*, https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-dec-2016.pdf [dostęp: 20.09.2017].

4 R. Tomański, *Twórcy WannaCry mogli pochodzić z południowych Chin*, źródło: http://www.pap.pl/aktualnosci/news,952948,tworcy-wannacry-mogli-pochodzic-z-poludniowych-chin.html [dostęp: 20.09.2017].

5 J. Snoch, *Kolejny globalny atak ransomware. Petya zaatakował także Polskę!*, źródło: http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2017/26/kolejny-globalny-atak-ransomware-petya-zaatakowal-takze-polske.aspx [dostęp: 20.09.2017].

6 A. Liska, T. Gallo, *Ransomware. Defending Against Digital Extortion*, O'Reilly Media, USA 2016, s. 3.

7 B. Botezatu, *Czym jest ransomware?*, źródło: https://bitdefender.pl/czym-jest-ransomware-przewodnik-zapoznawczy-czesc-i [dostęp: 20.09.2017].

- blokujące część lub całość funkcji systemu. Niektóre wirusy ransomware blokują użytkownikowi dostęp do urządzenia, programów, zmniejszają moc obliczeniową urządzenia przez co staje się one często bezużyteczne;
- szyfrujące cześć lub całość danych. Tego typu ransomware szyfruje dyski i ich zawartość co uniemożliwia użytkownikowi otwieranie plików lub uruchamianie aplikacji.

Sposobów w jaki cyberprzestępcy infekują komputery złośliwym oprogramowaniem wymuszającym okup jest wiele, jednak najczęściej dochodzi do tego z wykorzystaniem[8]:

- spamu i socjotechniki. Ataki socjotechniczne są jedną z metod działania cyberprzestępców, polegają one na wywarciu wpływu lub manipulacji użytkownika danego systemu[9]. Obecnie zaobserwować można rosnącą liczbę incydentów wykorzystujących socjotechnikę, aby pozyskać informacje od osób wewnątrz danej organizacji, lub zainfekować ją złośliwym oprogramowaniem. Dobrze spreparowana wiadomość e-mail podszywająca się pod zaufany podmiot trafiająca na nieświadomego pracownika zapewnia wysokie prawdopodobieństwo skuteczności ataku;
- ataków typu z ang. *Drive by download*. Atak ten polega na tym, że do kodu strony internetowej wstrzykiwany jest złośliwy skrypt zawierający odnośnik do witryny zawierającej szkodliwe oprogramowanie. Po wejściu na zmodyfikowaną w ten sposób stronę następuje niewidoczne dla użytkownika przekierowanie do szkodliwego adresu, uruchomienie kodu zwanego *exploitem*[10], a następnie pobranie i instalacja niebezpiecznego oprogramowania na komputerze ofiary. Ataki *Drive-by download* są bardzo popularne przede wszystkim ze względu na prostotę działania i dużą skuteczność[11];
- stron internetowych. Nieświadomi użytkownicy Internetu wchodzą na strony internetowe których celem jest infekowanie komputerów czy też pobierają pliki z niezaufanych źródeł.

Zagrożenie jakim jest ransomware nie jest niczym nowym w bezpieczeństwie IT, pierwszym atakiem którego celem było zaszyfrowanie plików, a za ich odszyfrowanie żądano zapłaty okupu był atak tzw. *AIDS* znany również jako *PC-Cyborg* w 1989 r. Znaczny rozwój tego typu zagrożeń zaczął się w roku 2005 i 2006. Wraz z rozwojem kryptografii i Internetu, rozprzestrzenianie się wszelkiego rodzaju złośliwego oprogramowania stało się znacznie łatwiejsze dla cyberprzestępców, a kolejne lata umożliwiły hakerom opracowanie znacznie bardziej skutecznych metod szyfrowania niż te stosowane w ataku *PC-Cyborg*[12]. Jednak prawdziwa ewolucja i ekspansja złośliwego oprogramowania typu ransomware miała miejsce po 2013 r. a przyczyną tego są głównie trzy czynniki:

- sukces ataku *Cryptolocker* z 2013 r. który zaszyfrował dane zaskakująco dużej liczbie użytkowników i wymusił na nich okup o łącznej wartości 12 mln złotych[13]. Ransomware stał się metodą szybkiego i wysokiego zarobku;

---

8 A. Liska, T. Gallo, dz. cyt., s. 7.

9 T. Chandler, P. Wilson, *Social Engineering: The Art of Human Hacking*, Onepress, Warszawa 2013, s. 31.

10 Exploit – program mający na celu wykorzystanie błędów w oprogramowaniu.

11 N. Narine, *Ataki drive by download*, źródło: http://securelist.pl/threats/5891,ataki_drive_by_download_siec_w_oblezeniu.html [dostęp: 20.09.2017].

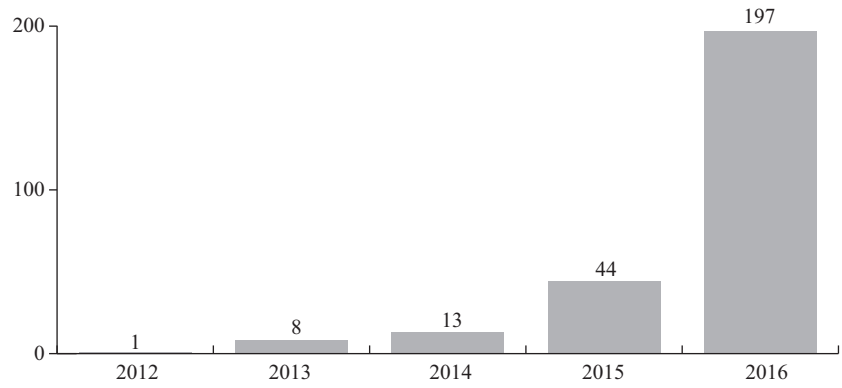
12 A. Liska, T. Gallo, *Ransomware*..., s. 5.

13 Symantec, *Ransomware and Businesses 2016*, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf [dostęp: 20.09.2017].

- rozwój kryptowalut. To nie przypadek, że ransomware upowszechnił się, kiedy w 2009 r. Bitcoin został wprowadzony jako kryptowaluta. Bitcoin pozwala cyberprzestępcom otrzymać zapłatę z zaszyfrowane pliki i pozostać anonimowym, ponieważ jest niemal niemożliwy do wyśledzenia przez organy ścigania, gdyż korzysta z sieci *peer-to-peer*[14];
- wzrastający zysk z tego typu ataków. Według badań IBM dochód cyberprzestępców w 2016 r. z tytułu oprogramowania szyfrującego wyniósł niemal 1 bilion dolarów[15]. Średni okup waha się w przedziale od 300 do 500 dolarów w BTC. Dla dużych przedsiębiorstw jest to stosunkowo niewiele w porównaniu z potencjalnymi stratami wynikającymi z utraty dostępności danych, dlatego też około 60% przedsiębiorstw płaci cyberprzestępcom okup w zamian za odzyskanie danych.

Cyberprzestępcy coraz częściej wybierają oprogramowanie szyfrujące jako metodę ataku, główną przyczyną jest zysk dużo większy niż w przypadku innego rodzaju cyberprzestępstw np. kradzieży danych osobowych klientów banku.

Wykres 1. Liczba nowych rodzin *ransomware*



Źródło: F-Secure, *State of cybersecurity 2017*, https://business.f-secure.com/the-state-of-cyber-security-2017 [dostęp: 20.09.2017].

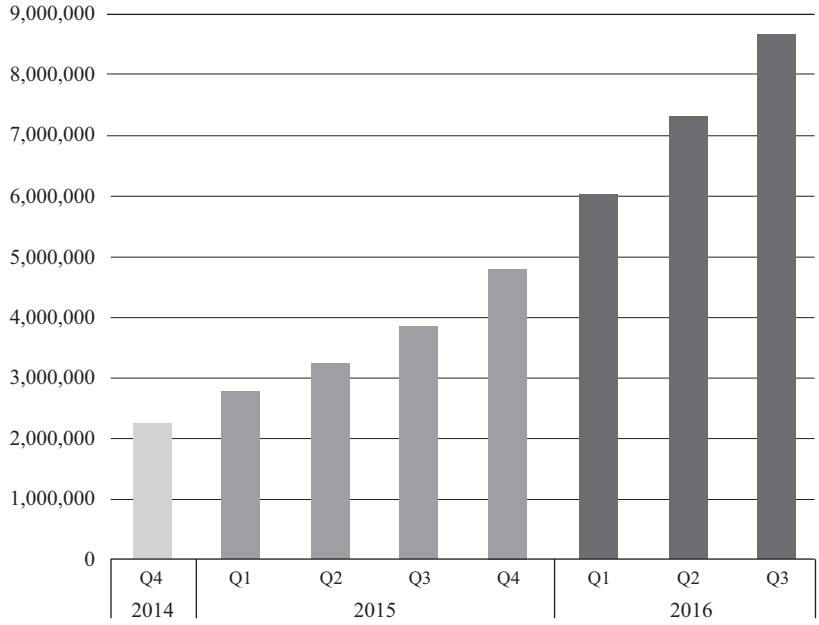
Wysokie prawdopodobieństwo pozostania anonimowym i uniknięcia wymiaru sprawiedliwości dzięki płatnościom dokonywanym w krypotowalutach oraz wysoki odsetek osób płacących okup przestępcom (relatywnie niska cena okupu wobec prawdopodobnych strat podmiotów zainfekowanych) jest przyczyną gwałtownego wzrostu nowych *rodzin ransomware* oraz liczby zainfekowanych użytkowników na przestrzeni 2013–2017 r. Na powyższym wykresie pochodzącym z raportu F-Secure widać szybki rozwój nowych wariantów ransomware'u, ich liczba podwoiła się w 2014 i 2015 roku, a w 2016 roku wzrosła niemal pięciokrotnie.

[14] M. Muszyński, *Hakerzy kochają bitcoiny. Bez wzajemności*, https://www.forbes.pl/finanse/bitcoin-podstawa-atakow-ransomware-hakerzy-go-uwielbiaja/g284n23 [dostęp: 20.09.2017].

[15] K. Torpey, *2016 Big Year for Ransomware – 70% Pays in This $1 BillionIndustry*, https://news.bitcoin.com/2016-big-year-for-ransomware-70-pays-in-this-1-billion-industry/ [dostęp: 20.09.2017].

Wzrasta nie tylko liczba wariantów złośliwego oprogramowania, ale także jego ilość w cyberprzestrzeni, wg Firmy McAfee w przeciągu dwóch lat ogólna liczba ransomware'u na świecie powiększyła się z 2 mln do aż 9 mln.

Wykres 2. Ogólna liczba *ransomware*na świecie



Źródło: McAfeeLabs, *Threats Report: December 2016*, https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-dec-2016.pdf [dostęp: 20.09.2017].

Firma Google w jednym z raportów dotyczącym bezpieczeństwa Internetu z 2017 r. ostrzega, że tego typu ataki stały się *bardzo opłacalne i należy spodziewać się, że będzie do nich dochodzić w przyszłości*[16].

Pokłosiem sprzyjających warunków tego rodzaju złośliwego oprogramowania był atak z 12 maja 2017 r. Poniższy ekran pojawił się zastraszająco dużej liczbie użytkowników na niemal całym świecie w ciągu zaledwie kilku dni:

[16] PAP, *Google ostrzega przed dynamicznym rozwojem ransomware*, http://www.rp.pl/Telekomunikacja-i-IT-/170729310-Google-ostrzega-przed-dynamicznym-rozwojem-ransomware.html [dostęp: 20.09.2017].

Zdjęcie 1. Okienko informacyjne – ransmoware WannaCry

Źródło: https://zaufanatrzeciastrona.pl/post/jak-najprawdopodobniej-doszlo-do-globalnej-infekcji-ransomare-wannacry/ [dostęp: 20.09.2017].

Ransomware – WannaCry – swoim zasięgiem objął ponad 150 krajów infekując przy tym ponad 250 tys. użytkowników w ciągu tylko 2 dni. Zainfekowane komputery otrzymały nową tapetę oraz okno z informacją o ataku. Co ciekawe ransomware komunikował się z zainfekowanymi osobami w 28 różnych językach. Cyberprzestępcy najprawdopodobniej wiedzieli o tym, że znaleźli podatność, która pozwoli im osiągnąć międzynarodową skalę ataku. W okienku powyżej ofiara zostaje poinformowana o tym, że jej pliki zostały zaszyfrowane, a żeby odzyskać te dane musi zapłacić 300 dolarów (w bitcoinach). Jeżeli tego nie zrobi w przeciągu 3 dni, kwota haraczu wzrasta do 600 dolarów. Jeśli przestępcy nie otrzymają okupu w ciągu 7 dni, ofiara straci na zawsze możliwość odzyskania swoich danych (choć w przedstawionym komunikacie jest pewna sprzeczność, gdyż przestępcy zastrzegają, że jeśli ktoś jest tak *biedny*, że nie będzie w stanie zapłacić, to po 6 miesiącach przewidują uruchomienie możliwości darmowego odzyskania danych). Ofiarami ataku WannaCry zostały podmioty prywatne i publiczne; do najważniejszych z nich należą: National Health Service (służba zdrowia w Wielkiej Brytani)[17], Nissan i Renault, Telefonica[18], FedEx, VTB (Rosyjski bank), RZD (Rosyjskie koleje), Shaheen Airlines (Pakistańskie linie lotnicze) i wiele innych. Zainfekowane zostały nawet podmioty wchodzące w skład infrastruktury krytycznej państw, jak wspomniane wyżej NHS czy spółki energetyczne. Nissan i Renault wydały oficjalne oświadczenia o tym, że zostały zarażone WannaCry, a z powodu ataku

17 K. Rawlinson, *NHS leftreeling by cyber-attack: We areliterallyunable to do any x-rays*, https://www.theguardian.com/society/2017/may/13/nhs-cyber-attack-patients-ransomware [dostęp: 20.09.2017].

18 F. Palazuelos, *How the WannaCryransomwareattackaffectedbusinesses in Spain*, https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [dostęp: 20.09.2017].

linie produkcyjne stanęły, co spowodowało duże straty finansowe[19]. W przypadku National Health Service pacjenci czekający na ważną operację nie mogli skorzystać z rezonansu oraz rentgenów ponieważ urządzenia te są sterowane poprzez komputer z Windowsem XP podatnym na tego typu atak, które zostały zaszyfrowane. Jeden z pracowników brytyjskiej służby zdrowia w wywiadzie powiedział, że *część pacjentów prawdopodobnie umrze ze względu na to, że infrastruktura szpitalna nie działa poprawnie*[20]. Atak mógł być także fatalny w skutkach dla podróżujących rosyjskimi pociągami, gdyż centrum zarządzania infrastrukturą kolejową również zostało zainfekowane, a w przypadku przejęcia kontroli przez cyberprzestępców nad systemem zarzadzania ruchem lub wyłączeniem części funkcjonalnych tego systemu mogło dojść do wypadku.

Sposób działania WannaCry był następujący: kiedy ransom (*dropper exe*) zostanie osadzony na komputerze próbuje odwołać się do domeny (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) jeśli żądanie to powiedzie się, gdy taka domena istnieje – robak ten przestaje działać. Połączenie z tą domeną działa bowiem jak swoisty wyłącznik (tzw. killswitch). Kiedy analitycy badający kod źródłowy tego wirusa zauważyli, że w pierwszej kolejności próbuje on odwołać się do wspomnianej domeny od razu wykupili tą domenę, tym samym zaprzestając dalszego rozpropagowywania (Marcus Hutchins z KryptosLogic postanowił zarejestrować domenę na siebie, co zatrzymało infekowanie kolejnych komputerów). Jednak w momencie, kiedy nie było dostępu do domeny, ścieżka działania była następująca: robak skanuje sieć lokalną w poszukiwaniu komputerów, które mają wystawione usługi związane z protokołem SMB w wersji 1 i 2 są to porty 445 i 139. Następnie infekuje je poprzez dziurawy SMB i szyfruje pliki. WannaCry szyfruje pliki (179 rozszerzeń), dodając rozszerzenie WNCRY i wyświetla komunikat z żądaniem okupu. Przestępcy w komunikacie okupu na przemian pokazywali ofiarom tylko 3 adresy portfeli Bitcoin:

1. https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
2. https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
3. https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Jeden portfel zebrał 19 BTC, zaś wszystkie trzy portfele razem 52 BTC[21], a więc wpływy stanowiły łącznie około 140 tys. dolarów, co w przeliczeniu na polskie złote wynosi średnio pół miliona. Większość mediów opisywała ten atak jako *największy w historii*, jako *atak bez precedensu* jednak w rzeczywistości nie jest to do końca prawdą. W przeszłości miały miejsce podobne ataki, jednym z nich był Conficer, atak przez inną podatność, który swoim zasięgiem objął 15 mln ofiar czy wspomniany wcześniej Cryptolocker, który rozpoczął się w 2013 roku i zgromadził z okupu aż 12 mln złotych. Kampania WannaCry mimo ogromnego zasięgu nie odniosła sukcesu komercyjnego – zdecydowało się zapłacić ponad 200 osób, a całkowita suma wpłat wynosi około 140 tysięcy dolarów.

---

19 L. Frost, *Renault-Nissan isresuming production after a global Cyberattack caused stoppagesat 5 plants*, http://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5?IR=T [dostęp: 20.09.2017].

20 R. Daws, *State of the NHS' security makes you WannaCry*, https://www.telecomstechnews.com/news/2017/may/15/nhs-security-makes-you-wannacry/ [dostęp: 20.09.2017].

21 Stan na 24 lipca 2017 r.

Wobec tak szybko postępującego rozwoju złośliwego oprogramowania szyfrującego nasuwa się pytanie – jak się bronić przed ransomwarem? Przede wszystkim należy używać wspieranego aktualizacjami systemu operacyjnego, główną przyczyną tak szybkiego rozprzestrzenienia się robaka WannaCry była podatność starego systemu operacyjnego (Windowsa XP), komputery z oprogramowaniem nowszym nie zostały zainfekowane. Cyberprzestępcy nie próżnują i w miejsce jednego zablokowanego złośliwego oprogramowania tworzą kilka kolejnych wariantów. Chcąc się przed nimi zabezpieczyć, należy zawsze korzystać z aktualnego systemu operacyjnego oraz aktualizować urządzenia i oprogramowanie. Ponadto należy regularnie tworzyć kopie zapasowe, a najlepiej opracować plan kopii zapasowych i odzyskiwania. Przygotowane kopie powinno się przechowywać na osobnym, niepodłączonym do sieci urządzeniu oraz testować przywracanie systemu i plików ze zrobionych kopii zapasowych. Jeśli mimo stosowania powyższych rekomendacji użytkownik zostanie zainfekowany oprogramowaniem szyfrującym może skorzystać z inicjatywy *No More Ransom*, która została uruchomiona 25 lipca 2016 r. przez holenderską policję, Europol, Intel Security oraz Kaspersky Lab, zapoczątkowując nowy poziom współpracy między organami ścigania, a sektorem prywatnym w zakresie zwalczania oprogramowania ransomware. Celem projektu *No More Ransom* jest zapewnienie przydatnego zasobu dla ofiar oprogramowania ransomware. Użytkownicy mogą znaleźć tam informacje odnośnie tego, co to jest oprogramowanie ransomware, jak działa i co ważniejsze, jak się przed nim ochronić. W ciągu pierwszych dwóch miesięcy funkcjonowania portalu ponad 2500 osobom udało się odszyfrować swoje dane bez płacenia okupu przestępcom. Kolejnym celem inicjatywy jest uściślenie i rozwój współpracy między organami ścigania, a podmiotami sektora prywatnego w celu zwalczania tego zagrożenia[22].

Tytuł w języku angielskim:
RANSOMWARE – ONE OF THE BIGGEST THREATS IN CYBER SECURITY: CASE STUDY WANNACRY ATTACK

Bibliografia

Książki:

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006.

Chandler T., Wilson P., *Social Engineering: The Art of Human Hacking*, Warszawa 2013.

Liska A., Gallo T., *Ransomware. Defending Against Digital Extortion*, USA 2016.

Raporty:

McAfee Labs, *Threats Report: December 2016*.

Symantec, *Ransomware and Businesses 2016*.

[22] Inicjatywa No More Ransom, https://www.nomoreransom.org/crypto-sheriff.php?lang=en [dostęp: 20.09.2017].

Źródła internetowe:

Botezatu B., *Czym jest ransomware?*, źródło: https://bitdefender.pl/czym-jest-ransomware-przewodnik-zapoznawczy-czesc-i [dostęp: 20.09.2017].

Daws R., *State of the NHS' security makes you WannaCry*, https://www.telecomstechnews.com/news/2017/may/15/nhs-security-makes-you-wannacry/ [dostęp: 20.09.2017].

Frost L., *Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plant*s, http://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5?IR=T [dostęp: 20.09.2017].

Inicjatywa *No More Ransom*, https://www.nomoreransom.org/crypto-sheriff.php?lang=en [dostęp: 20.09.2017].

Muszyński M., *Hakerzy kochają bitcoiny. Bez wzajemności*, https://www.forbes.pl/finanse/bitcoin-podstawa-atakow-ransomware-hakerzy-go-uwielbiaja/g284n23 [dostęp: 20.09.2017].

Narine N., *Ataki drive by download*, źródło: http://securelist.pl/threats/5891,ataki_drive_by_download_siec_w_oblezeniu.html [dostęp: 20.09.2017].

Palazuelos F., *How the WannaCry ransomware attack affected businesses in Spain*, https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [dostęp: 20.09.2017].

PAP, *Google ostrzega przed dynamicznym rozwojem ransomware*, http://www.rp.pl/Telekomunikacja-i-IT/170729310-Google-ostrzega-przed-dynamicznym-rozwojem-ransomware.html [dostęp: 20.09.2017].

Pawłowicz W., *Ransomware to największe zagrożenie dla bezpieczeństwa IT*, źródło: https://www.computerworld.pl/news/Ransomware-to-najwieksze-zagrozenie-dla-bezpieczenstwa-IT,404822.html [dostęp: 20.09.2017].

Rawlinson K., *NHS left reeling by cyber-attack: We are literally unable to do any x-rays*, https://www.theguardian.com/society/2017/may/13/nhs-cyber-attack-patients-ransomware [dostęp: 20.09.2017].

Snoch J., *Kolejny globalny atak ransomware. Petya zaatakował także Polskę!*, źródło: http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2017/26/kolejny-globalny-atak-ransomware-petya-zaatakowal-takze-polske.aspx [dostęp: 20.09.2017].

Tomański R., *Twórcy WannaCry mogli pochodzić z południowych Chin*, źródło: http://www.pap.pl/aktualnosci/news,952948,tworcy-wannacry-mogli-pochodzic-z-poludniowych-chin.html [dostęp: 20.09.2017].

Torpey K., *2016 Big Year for Ransomware – 70% Pays in This $1 Billion Industry*, https://news.bitcoin.com/2016-big-year-for-ransomware-70-pays-in-this-1-billion-industry/ [dostęp: 20.09.2017].

PAULINA ŁOJEWSKA*

CHARAKTERYSTYKA WSPÓŁCZESNEJ CYBERPRZESTĘPCZOŚCI ZORGANIZOWANEJ

Abstrakt

Nieustanny rozwój i postępująca rewolucja technologiczna wpływa na wszystkie sfery życia współczesnego człowieka. Możliwość wykorzystania nowoczesnych technologii w celu czerpania zysków z prowadzenia działalności przestępczej została dostrzeżona przez międzynarodowe zorganizowane grupy przestępcze. Poniższa analiza traktuje o charakterze zorganizowanych grup cyberprzestępczych oraz wykorzystywaniu technologii IT do nielegalnej działalności w cyberprzestrzeni. Ukazuje także powody dla których ściganie i zapobieganie tym przestępstwom jest wyzwaniem dla społeczności międzynarodowej.

Słowa kluczowe: cyberprzestępczość, zorganizowana grupa przestępcza, technologia.

Internet stał się nieodzowną częścią życia, prowadzenia biznesu. Posiada on dużo zalet wynikających z korzystania z niego, jednakże pełen jest również wielu zagrożeń. Korzyści mogące płynąć z popełniania przestępstw w intrenecie oraz zyski z tego płynące zostały dostrzeżone przez zorganizowane grupy przestępcze[1]. Rewolucja informacyjna, której jesteśmy świadkami to niezwykle dynamiczny proces. Od momentu gdy wprowadzono pierwszy komputer osobisty oraz uruchomiono pierwszą sieć komputerową – ARPAnet do chwili obecnej postęp informatyczny objął już wszystkie dzieciny życia współczesnego człowieka. Szacuje się, że dziennie użytkownicy sieci Internet wysyłają 144 mld e-maili, zaś na samych tylko urządzeniach mobilnych przetwarza się około 1.3 EB danych[2].

Wzrost przestępczości zorganizowanej w cyberprzestrzeni wiąże się z brakiem ujednoliconych uregulowań w prawie międzynarodowym. Wynikają z tego rozbieżności oraz niespójności, które ułatwiają sprawcom unikanie odpowiedzialności za przestępstwa popeł-

* Paulina Łojewska – absolwentka studiów licencjackich i magisterskich na kierunku bezpieczeństwo wewnętrzne INP UW. Aktualnie funkcjonariusz Komendy Miejskiej Policji we Włocławku. Kontakt e-mail: pjlojewska@gmail.com

1 A. Boszko, *Finanse przestępczości zorganizowanej*, Toruń 2014, s. 147.

2 P. Ciszek, *Cyberprzestępczość (z)organizowana*, [w:] W. Zubrzycki (red.), *Przez przestępczość zorganizowaną do terroryzmu*, Szczytno 2015, s. 49.

niane w sieci z wykorzystaniem urządzeń multimedialnych[3]. Zagrożenie zorganizowaną cyberprzestępczością jest problemem na tyle istotnym, że Federalne Biuro Śledcze umieściło ją wysoko na liście priorytetów działania zaraz po terroryzmie i działalności antyamerykańskiej. Ukazuje to skalę problemu oraz wskazuje, że ten rodzaj popełnianych przestępstw charakteryzuje się dużą dynamiką rozwoju oraz znacznym potencjałem możliwości osiągania zysków[4]. Konwencja Rady Europy określa cztery formy cyberprzestępczości, której dopuszczają się sprawcy:

- przestępstwa związane z pornografią z udziałem małoletnich (oferowanie oraz udostępnianie materiałów, przesyłanie, wytwarzanie w celu udostępniania, posiadanie na nośnikach danych bądź w systemie informatycznym, pozyskiwanie dla siebie lub innej osoby);
- przestępstwa z wykorzystaniem komputera (oszustwa i fałszerstwa komputerowe – modyfikowanie, usuwanie danych bądź ingerowanie w systemy komputerowe);
- przestępstwa dotyczące poufności, dostępności i integralności danych, systemów komputerowych (zakłócanie pracy systemu komputerowego, ingerencje w całość bądź część danych, ich przechwytywanie w trakcie transmisji, umyślne usuwanie bądź niszczenie danych);
- przestępstwa przeciwko własności intelektualnej (rozpowszechnianie utworów, wykonań artystycznych bez zgody twórcy)[5].

Zorganizowana cyberprzestępczość posiada charakter elastyczny, dostosowuje się do zmian oraz rozwoju technologicznego. Dzięki globalnemu ukierunkowaniu sieci Internet ułatwione jest stworzenie grupy przestępczej o zasięgu międzynarodowym[6]. Fakt, iż trudno jest ujednolicić definicyjnie ramy zjawiska przestępczości zorganizowanej ukazuje, że aktualnie dochodzi do dynamicznych oraz gwałtownych zmian nie tylko w kontekście przemian społeczno-gospodarczych, ale także technologicznych, do których adaptują się również grupy przestępcze[7]. Członkowie zorganizowanych grup przestępczych, analogicznie do gospodarki, nieustannie ewoluują oraz dostosowują się do panującej sytuacji, a także w dużym stopniu korzystają ze zdobyczy współsennej techniki. Do swoich potrzeb przestępcy adaptują narzędzia dostępne w sieci komputerowej[8]. W związku z rozwojem technologicznym oraz postępującą globalizacją grupy przestępcze dostosowują zakres swojej działalności oraz formę strukturalną do otoczenia, w jakim muszą funkcjonować. Prowadzi to do powstania różnorodności form działalności przestępczej oraz czasowego działania sprawców[9].

Przestępstwa w cyberprzestrzeni są domeną głównie grup przestępczych o zasięgu międzynarodowym. Dla ochrony przed atakiem hackerskim, kradzieżą danych, zainfe-

---

3 D. Krawczyk, *Internet zagrożeniem dla bezpieczeństwa wewnętrznego*, „Horyzonty Bezpieczeństwa" 2016, nr 2 (1) 2, s. 43.

4 W. Mądrzejowski, *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015, s. 108.

5 Tamże, s. 108–109.

6 Tamże, s. 109.

7 W. Krukowski, *Pojęcie organizacji przestępczej i przestępczości zorganizowanej*, „Prokuratura i Prawo" 2006, nr 1, s. 26.

8 P. Ciszek, dz. cyt., s. 51.

9 W. Krukowski, dz. cyt., s. 26.

kowaniem szkodliwym oprogramowaniem nie wystarczą typowe systemy zabezpieczające. Sprawcy przestępstw, którzy są członkami grup przestępczych, to grupa przestępców wyspecjalizowanych. Ich działalność skupia się na osiągnięciu maksymalnego zysku, a ich działania nie posiadają ideologicznego charakteru[10]. Wśród zmian w zorganizowanych grupach przestępczych można również zaobserwować łączenie potencjału posiadanego przez grupę z wiedzą oferowaną przez specjalistów od informatyki, nowoczesnych technologii[11]. Zorganizowane grupy przestępcze korzystają z dostępu do oprogramowania oraz usług funkcjonujących w chmurze. Programy oraz oprogramowania z jakich korzystają, poziomem skomplikowania dorównują tym, które używane są przez międzynarodowe korporacje oraz wysoko rozwinięte firmy[12].

Cyberprzestępcy nie stwarzają nowych rodzajów czynów zabronionych. Nowoczesne technologie dostarczają nowych rozwiązań i sposobów do popełniana przestępstw dobrze znanych organom ścigania. Nowoczesna technika wykreowała jedynie nowy rodzaj obszaru, przestrzeni w której popełnianie mogą być przestępstwa[13]. Członkowie zorganizowanych grup mogą za pośrednictwem sieci dokonywać przestępstw z obszaru handlu narkotykami, przestępstw ekonomicznych. Wykorzystanie komputera oraz dostępu do sieci nie musi być równoznaczne z popełnianiem przestępczości cybernetycznej np. oszustw internetowych[14]. Grupy przestępcze prowadzą działalność o różnorodnym charakterze: działania nielegalne, półlegalne – w tzw. „szarej strefie", zgodną z prawem, legalną działalność gospodarczą. Różnokierunkowość działalności pozwala ukryć czyny nielegalne, przeprowadzić „pranie brudnych pieniędzy" pochodzących z działalności przestępczej, ułatwia także zdobywanie kontaktów z osobami z innych państw[15].

Grupę przestępczą tworzą jej członkowie, którzy przyczyniają się do realizacji zamierzonych celów oraz zapewniają zyski z prowadzonej działalności. Działalność prowadzona przez zorganizowane organizacje przestępcze przypomina przedsiębiorstwo[16]. Cechami grupy przestępczej są:

- posiadanie wewnętrznej struktury, podziału ról, zbioru zasad, hierarchii w strukturze organizacji oraz wewnętrzna dyscyplina wśród członków grupy;
- celowe działanie;
- działanie o charakterze rozmyślnym, modyfikowanie poczynań aby jak najszybciej doszło do osiągnięcia celu;
- osiąganie celów końcowych poprzez wykorzystanie różnego rodzaju środków;
- posiadanie osób koordynujących działania członków grupy, zarządzających;
- współdziałanie w realizacji określonego celu;
- dążenie do zwiększenia efektywności w realizacji określonego celu;
- trwałość grupy;

10 A. Boszko, dz. cyt., s. 157.

11 J. Kosiński, *Paradygmaty cyberterroryzmu*, Warszawa 2015, s. 260.

12 P. Ciszek, dz. cyt., s. 51.

13 W. Mądrzejowski, dz. cyt., s. 109.

14 Tamże, s. 109.

15 W. Krukowski, dz. cyt., s. 26–27.

16 Tamże, s. 31.

- wykonywanie działań przestępczych zarówno w sposób bezpośredni w celu osiągniecia korzyści finansowych oraz w sposób pośredni w celu zdobycia wpływów;
- używanie różnych form przemocy w celu zrealizowania celu;
- korzystanie podczas realizacji celu z usług specjalistów, wysokiej klasy konsultantów;
- prowadzenie działalności o charakterze międzynarodowym, mobilność w działaniu, wykorzystywanie różnic w prawie poszczególnych państw[17].

W zorganizowanych grupach przestępczych nie tylko działania mają charakter zorganizowany, jest to także cecha samych sprawców. Zaplanowane działanie ma na celu zgromadzenie dużych zysków w przemyślany sposób, w podejmowanych przedsięwzięciach nie ma przypadkowego, impulsywnego działania[18].

Pierwsze cyberprzestępstwa obejmowały ataki skierowane na komputery bądź sieci komputerowe oraz dane, które się w nich znajdowały. W późniejszym etapie przestępstwa te polegały na ataku na integralność systemów teleinformatycznych. Aktualnie dochodzi do cyberprzestępstw trzeciej generacji, charakteryzują się one używaniem specjalistycznego oprogramowania do popełniania przestępstw. Ewolucja działań przestępczych doprowadziła do tego, że czyny zabronione nie są popełniane bezpośrednio przez sprawców, lecz za pomocą oprogramowania stworzonego w danym celu[19]. Podział aktualnie popełnianych cyberprzestępstw przyjęty przez międzynarodową Organizację Policji Interpol:

- oszustwa dokonane przy pomocy komputera;
- przestępstwa popełniane w sieci;
- dokonywanie sabotażu oprogramowania i sprzętu;
- naruszenie dostępu do zasobów, nieupoważnione wejście do systemu informatycznego[20].

Początki przestępczej działalności w cyberprzestrzeni to czas, gdy dominującą grupą były osoby indywidualne. Aktualnie za większością przestępstw, które są dokonywane stoją zespoły sprawców, które przybierają nowatorską do tej pory formę. Zespół, grupa składa się z osób, które kontaktują się ze sobą w niespotykany do tej pory sposób. Sprawcy prowadzą wymianę informacji poprzez korzystanie z komunikatorów gier online. Grupy, które komunikują się w wyżej przedstawiony sposób charakteryzują się małą liczebnością, skupiają jednak osoby posiadające określoną wiedzę oraz umiejętności, a ich sposób współpracy przypomina funkcjonowanie przedsiębiorstwa[21]. W zespole panuje odpowiedzialność za poszczególne elementy działalności oraz realizowanie określonych zadań. W przypadku gdy grupa przestępcza posiada wystarczające środki, staje się samowystarczalna w zakresie zapewnienia sobie wszystkich usług niezbędnych do popełnienia przestępstwa. Nie musi ona zlecać poszczególnych zadań osobom indywidualnym, które do grupy nie należą. Dzięki posiadaniu odpowiednich środków grupa może stać się na tyle hermetyczna i samodzielna, by znacznie zmniejszyć prawdopodobieństwo rozpracowania, identyfikacji przez służby oraz organy ścigania[22]. Grupy przestępcze przy planowaniu przedsięwzięcia przestępczego

17 Tamże, s. 36–37.

18 Tamże, s. 38.

19 M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 244.

20 Tamże, s. 249.

21 P. Ciszek, dz. cyt., s. 55.

22 Tamże, s. 55.

współpracują ze sobą, lecz ta współpraca przybiera nową formę. Nad zaplanowaniem oraz realizacją zadania czuwa zespół złożony z osób, które są ekspertami z dziedziny informatyki, używają one pseudonimów podczas kontaktowania się ze sobą, używają sieci Tor, która zapewnia anonimowość w czasie korzystania z zasobów Internetu bądź komunikatorów gier internetowych. Zorganizowane grupy przestępcze, które w swoich szeregach posiadają ekspertów z dziedziny informatyki, świadczą także usługi w tzw. „podziemiu internetowym", wyróżnia się cztery rodzaje usług internetowych świadczonych przez grupy przestępcze:

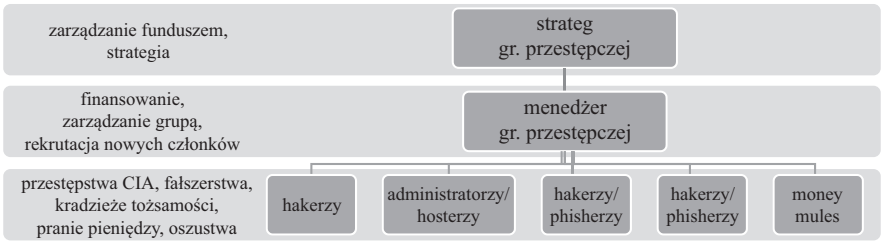
1. Stwarzanie narzędzi służących do popełniania przestępstw internetowych („crimeware as a service") – w tę kategorie usług wpisuje się tworzenie oprogramowania, które wychwytuje luki oraz błędy programów, które następnie sprawcy wykorzystują do popełniania konkretnych przestępstw. Jest to także tworzenie oprogramowania, które ma funkcję pomocniczą podczas ataku, popełniania przestępstwa oraz narzędzi, które mają ukryć obecność złośliwego oprogramowania, konstruowanie sprzętu służącego do pozyskiwania danych np. skimmery kart płatniczych a także urządzeń ułatwiających włamania np. podsłuchy.
2. Zlecanie wykonania cyberprzestępstwa („hucking as a service") – czyli zlecenie wykonania konkretnego przestępstwa innym osobom, należy pamiętać, że w tym przypadku zleceniodawca usług nie musi posiadać wiedzy specjalistycznej dotyczącej ataku, koszt takiej usługi przewyższa koszt nabycia poszczególnych programów oraz narzędzi służących do popełnienia czynu zabronionego. Ten rodzaj usług oferowanych przez cyberprzestępców obejmuje także dostarczanie informacji służących do kradzieży tożsamości, dane dotyczące logowania.
3. Badania („research as a service") – jest to oferowanie podatności oprogramowania, nim na rynku pojawi się poprawka, ulepszony program który naprawił tę podatność. W przeciwieństwie do pozostałych rodzajów usług świadczonych przez grupy przestępcze badania nie muszą pochodzić ze źródeł nielegalnych.
4. Infrastruktura cyberprzestępstw („cybercrime infrastructure as a service") – opracowanie narzędzi służących do popełnienia przestępstwa i ich wykorzystanie np. wynajęcie sieci komputerów w celu przeprowadzenia ataku. Jest to zapewnienie sobie narzędzi niezbędnych do popełnienia przestępstwa, w poczet tych działań wchodzi wymiana narzędzi bądź ich odpowiednia konfiguracja poprzez posiadanie odpowiedniej platformy do tego służącej[23].

Zorganizowane grupy cyberprzestępcze stwarzają pomiędzy członkami powiązania o charakterze funkcjonalnym, następuje także rozdział zadań w sieci przestępczej. Grupa przestępcza musi posiadać osobę, która pełni role stratega, to ona wyznacza podejmowane działania aktualne oraz przyszłe, zarządza też finansami. Tak jak w przypadku współczesnych korporacji oraz przedsiębiorstw, w strukturze grupy przestępczej wykształciła się rola menedżera, który zajmuje się zarządzaniem bezpośrednim, to on kontaktuje się osobami, które wykonują zlecone przez niego zadania, polecenia. Określenie zadań scedowanych na poszczególnych wykonawców jest zależne od ich obszaru działania. Wyraźnie określona hierarchia każdemu z członków grupy jasno przydziela jego rolę w procederze przestęp-

[23] Tamże, s. 52–53.

czym. Na najniższym szczeblu znajdują tzw. „mules" – „muły", które odpowiedzialne są za całość przygotowań. Na średnim szczeblu hierarchii znajdują się osoby świadczące usługi takie jak pranie pieniędzy, wynajem botnetów. Najwyższy szczebel grupy stanowią osoby, które są specjalistami, wysokokwalifikowanymi ekspertami dziedzinowymi, administratorami, doskonalą narzędzia przestępcze. Członkowie grupy, którzy należą do najwyższego poziomu czerpią największe zyski z działalności przestępczej[24].

Rysunek 1. Poziomy oraz funkcje pełnione przez członków grupy cyberprzestępczej



Źródło: J. Kosiński, *Paradygmaty cyberterroryzmu*, Warszawa 2015.

Popełnianie przestępstw w sieci Internet, bądź za pomocą komputera zostało określone mianem cyberprzestępstwa. Termin ten jest szeroko definiowany jako działanie w sferze IT podmiotów niepaństwowych o charakterze nielegalnym, gdzie celem jest zdobycie zysku. Nie zawsze jest to jedyny cel sprawcy, ale zawsze jest to główny czynnik jego działania[25]. Pierwsze przestępstwa, których dopuszczano się w cyberprzestrzeni były popełniane przez hakerów, którzy kierowali się w swoich działaniach chęcią pokazania swoich umiejętności lub pomocą przyjacielską dla innych hakerów. Włamania na strony internetowe bądź kradzieże danych usprawiedliwiali niekiedy większym dobrem np. chęcią by jak najwięcej osób poznało prawdę o danym wydarzeniu[26]. Wraz z rozwojem technologii oraz możliwości popełniania przestępstw w sieci doszło do przekształcenia się pojedynczego sprawcy w grupę, która dostrzegła korzyści płynące z popełniania przestępstw w sieci. W 2012 roku oszacowano, że zyski cyberprzestępczości wynosiły 1 bilion dolarów[27]. Aktualnie około 80% przestępstw popełnianych w intrenecie jest popełnianych przez zorganizowane gangi, grupy przestępcze. Cechami przestępczości w przestrzeni cybernetycznej są:

- międzynarodowy zasięg;
- niskie koszty działalności przestępczej, duże korzyści;
- nieświadomość ofiary oraz rzadko składane doniesienie z wyłączeniem przypadków w których doszło do dużych strat;
- łatwość w obsłudze technologii informatycznej;
- krótki czas potrzebny do popełnienia przestępstwa[28].

24 J. Kosiński, dz. cyt., s. 262–263.

25 D. Krawczyk, dz. cyt., s. 44.

26 P. Ciszek, dz. cyt., s. 50.

27 Tamże, s. 50.

28 Tamże, s. 50.

Wyżej przytoczone cechy przestępstw w cyberprzestrzeni były powodami dla których zainteresowanie tą formą działalności przestępczej zbudziło zainteresowanie zorganizowanych grup przestępczych. Należy jednak zauważyć, że działalność zorganizowanych grup w cyberprzestrzeni nie zawsze spełnia wszystkie przesłanki potrzebne do sklasyfikowania jej jako przestępczość zorganizowaną z uwagi na fakt, iż brak jest w nich jednego wyraźnego przywódcy oraz z uwagi na to, że w realizacji swoich celów nie zawsze sięgają po przymus fizyczny[29]. Cyberprzestępczość zorganizowana to dziedzina działalności nielegalnej zdominowana przez grupy przestępcze o charakterze transnarodowym, nie jest to jednak reguła gdyż działalność tego typu prowadzić mogą również grupy o mniejszym zorganizowaniu, które nie posiadają tak rozległego zaplecza finansowego oraz naukowego, których zasięg działalności ogranicza się do terytorium jednego państwa[30]. Dzięki rozwiniętej komunikacji oraz różnorodności kanałów do niej służących kontakt z osobami na innej części globu nie jest problemem, także w kontekście planowania działań przez grupę przestępczą. Posługując się stosownym oprogramowaniem oraz dostępem do sieci, sprawca jest zdolny do popełnienia przestępstwa na terenie jednego państwa będąc jednocześnie na terenie innego. Z uwagi na różnorodność przestępstw popełnianych w cyberprzestrzeni powstają grupy przestępcze, które odchodzą od multiprzestępczości, specjalizując się w tej konkretnej dziedzinie[31]. Grupy te skupiają osoby, które posiadają identycznie motywy działania oraz niezbędne umiejętności i wiedzę by popełniać przestępstwa w cyberprzestrzeni. Przestępczość komputerowa to działalność przynosząca duże dochody. Jej dochodowość znacznie przewyższa zyski narkotykowych karteli. W roku 2011 straty poniesione w wyniku działania cyberprzestępców zostały w Stanach Zjednoczonych określone na 12 mld USD. Równocześnie ze wzrostem przestępczości w cyberprzestrzeni, FBI odnotowało znaczny spadek tradycyjnych form przestępczości o charakterze fizycznym[32]. Poprzez wykorzystanie technologii oraz narzędzi komunikacji w sferze biznesowej, a także gospodarczej dochodzi do ułatwień w procesie popełniania przestępstw z katalogu zainteresowań zorganizowanych grup przestępczych popełnianych dotychczas poza cyberprzestrzenią. Dzięki wykorzystaniu komunikatorów internetowych, e-maili, telefonii internetowej w przepływie informacji wzrasta anonimowość członków grupy przestępczej oraz maleje prawdopodobieństwo wykrycia rozmów[33]. Przestępstwa komputerowe to głównie przestępstwa o tradycyjnym charakterze, do których używa się komputera. Dzięki zastosowaniu najnowszej dostępnej technologii ich popełnianie jest znacznie ułatwione. Do tej kategorii zalicza się także wyłudzenia kwot pieniędzy poprzez przesyłanie na telefon płatnych wiadomości sms[34]. Do korzystania z dostępnych narzędzi dochodzi w zależności od rodzaju planowanego ataku. Jakość narzędzi, jakie posiadają sprawcy przestępstw pozwala na niewidoczną penetrację sieci komputerowej z możliwością braku wykrycia przestępstwa przez

29 Tamże, s. 50.

30 D. Krawczyk, dz. cyt., s. 44.

31 Z. Płoszyński, *Przestępczość internetowa*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2012, nr 3, s. 42.

32 P. Ciszek, dz. cyt., s. 48.

33 J. Kosiński, dz. cyt., s. 261.

34 Tamże, s. 59.

miesiące lub nawet lata. W swojej działalności przestępczej zorganizowane grupy niejednokrotnie korzystają z tzw. botnetów, czyli grup komputerów zainfekowanych szkodliwym oprogramowaniem. Sam handel botnetami jest działalnością wysokodochodową[35]. Sposoby popełniania przestępstw w cyberprzestrzeni można podzielić na 3 rodzaje:

- posłużenie się dostępną technologią IT w celu usprawnienia przepływu informacji pomiędzy członkami grupy, bardziej zaawansowanego zorganizowania grupy;
- użycie technologii IT bezpośrednio w celu realizacji procederu przestępczego;
- wykorzystanie posiadanej technologii IT w kontekście ofensywnym jako działanie wymierzone przeciwko użytkownikom cyberprzestrzeni[36].

Na ataki cyberprzestępców narażone są głównie systemy, w których dochodzi do przesyłania informacji, ich wymiany, głównie oprogramowania zarówno użytkowników indywidualnych jak i organizacji, przedsiębiorstw a także aplikacje[37]. Wzrost zorganizowanej przestępczości w cyberprzestrzeni spowodował, że wyodrębniono nowy rodzaj zagrożeń – *Advanced Presistent Threats*. Jest to atak na wybrany cel np. bank, który charakteryzuje się swoistym skoncentrowaniem oraz wielowymiarowością. Podczas ataku dochodzi do prób sforsowania zabezpieczeń, wyszukiwania luk w oprogramowaniu a także wykorzystania wszelkich czynności mających miejsce w systemie organizacji np. wejście na portal społecznościowy przez pracownika. Ten rodzaj ataku został sklasyfikowany jako osobna kategoria zagrożeń przestępstw komputerowych, z uwagi na fakt wykorzystania podczas ataku każdego urządzenia, które posiada dostęp do infrastruktury organizacji, przy czym tym urządzeniem nie musi być komputer. Poprzez uzyskanie dostępu do urządzeń multimedialnych używanych przez pracobiorców można dokonać przesłania pracownikowi wiadomość email, która będzie zainfekowana, w takim stopniu poddaną spreparowaniu, że jej zawirusowanie nie zostanie rozpoznawane przez system bezpieczeństwa oprogramowania ochronnego. Tak przesłany wirus nie musi się uaktywnić od razu po otworzeniu wiadomości. Może przebywać w systemie będąc w trybie uśpienia i dopiero w sprzyjającym momencie rozpocząć infiltrację i atak na system. Wirus ten może także w odpowiednim momencie przygotować dane a następnie dokonać ich wysłania za pomocą transmisji szyfrowanej z wcześniej zidentyfikowanym serwerem. Po ukończonym zadania dochodzi do samozniszczenia wirusa, co doprowadza do tego, że użytkownik pozostaje w niewiedzy o wykonanej operacji oraz w przeświadczeniu bezpieczeństwa danych i systemu na którym pracuje[38]. Inwestowanie w środki ochrony komputera podczas korzystania z sieci stwarzają fałszywe poczucie bezpieczeństwa nie tylko wśród użytkowników indywidualnych, ale również w organizacjach komercyjnych. Mimo daleko idących przedsięwzięć mających na celu zabezpieczenie przed atakiem, nie są one w stanie uchronić systemu przed cyberprzestępcami. Dzieje się tak dlatego, że pojawiają się coraz to nowe formy ataków, przy których sprawcy korzystają z wyspecjalizowanych narzędzi bardziej zaawansowanych niż przyjęte formy ochrony[39]. Jako przykład w wykorzystywaniu przez przestępczość zorganizowaną

35 P. Ciszek, dz. cyt., s. 52.

36 D. Krawczyk, dz. cyt., s. 44.

37 Z. Płoszyński, dz. cyt., s. 38.

38 P. Ciszek, dz. cyt., s. 54.

39 Tamże, s. 53.

nowoczesnych technologii można podać funkcjonowanie tzw. botnetów. Warto zaznaczyć, że nie są one wykorzystywane jedynie jako rozwiązanie o charakterze informatycznych, lecz również należą do biznesowej platformy sprawców przestępstw[40]. Grupy przestępcze używające botnetów w swoim działaniu nie posiadają wszystkich cech charakteryzujących zorganizowaną przestępczość, działają poza przyjętymi do tej pory schematami. Rodzi to trudności w ich identyfikacji oraz w procesie zwalczania oraz ścigania. W ich strukturach często brakuje wyraźnego lidera, nie sięgają po przymus fizyczny. Należy jednak zaznaczyć, że spełniają 4 podstawowe kryteria identyfikacji zorganizowanej przestępczości tj.:

- współpraca więcej niż 2 osób;
- stosowanie form dyscypliny/ kontroli;
- wyznaczenie zadań do realizacji dla każdej z osób;
- współdziałanie osób w grupie przez czas nie określony bądź określony (kryterium to służby ukazaniu stabilności oraz trwałości grupy)[41].

Zarówno w sferze gospodarczo-biznesowej, jak i sferze użytkowników indywidualnych poprzez korzystanie z sieci można dotrzeć ze swoim komunikatem w dowolnie wybrany przez nas rejon świata. Międzynarodowe firny większość spraw związanych ze swoją działalnością realizują za pośrednictwem komunikowania się w sieci. Aby ułatwić transakcje internetowe stworzono wirtualną walutę tj. bitcoin, która nie posiada swojej materialnej wersji. Bitcoin nie jest jako waluta przypisany do żadnego państwa, nie jest również zależny od polityki jakiegokolwiek banku. Obrót wirtualną walutą opiera się na technologiach informatycznych, gdzie w sieci dochodzi do transakcji pomiędzy poszczególnymi użytkownikami[42]. Każdy z użytkowników programu może liczyć na anonimowość, gdyż zawartość jego wirtualnego portfela nie jest przypisana do konkretnej osoby. Transakcje pomiędzy użytkownikami oparte są na zasadzie węzłów „Peer-to-Peer". Waluta wirtualna jest w zainteresowaniu zorganizowanych grup przestępczych z uwagi na zalety wynikające z przeprowadzania nim transakcji[43]. Zainteresowanie prowadzeniem transakcji poprzez używanie bitcoina jest spowodowane maksimum anonimowości, która zapewniana jest podczas wykonywanej transakcji. Przepływ pieniądza realizowany za pośrednictwem programu, nie jest w żaden sposób kontrolowany, śledzony bądź archiwizowany, a dane które należy wpisać w potwierdzeniu przelewu są ograniczone do absolutnego minimum. Także szybkość wykonywanych transakcji jest niewątpliwą zaletą tego programu. Niemożliwym także staje się ustalenie stron uczestniczących w transakcji, gdy w krótkim czasie dochodzi do wielu operacji. Dużym atutem wirtualnej waluty jest swoboda dostępu do niej z dowolnego miejsca oraz bezpieczeństwo posiadanego wirtualnego portfela[44].

W kręgu zorganizowanych grup przestępczych pozostają także spamy. Są to niepożądane wiadomości głównie o charakterze marketingowym, które przesyłane są na skrzynkę email lub na telefony komórkowe. Z uwagi na fakt, że Internet jest miejscem, gdzie marketing się nieustannie rozwija, niemożliwym jest obecnie nie mieć choćby najmniejszego

40 J. Kosiński, dz. cyt., s. 261.

41 Tamże, s. 261.

42 A. Boszko, dz. cyt., s. 148.

43 Tamże, s. 148.

44 Tamże, s. 148–149.

kontaktu ze spamem. Spamy rozsyłane przez grupy przestępcze dotyczą zakupu leków, podrabianej markowej odzieży, bądź elektroniki. Do wysyłania tych wiadomości są wykorzystywane komputery umiejscowione głównie na terenie Azji. Dziennie komputery te są w stanie wysłać około 10 milionów spamów co przynosi miesięczny dochód wahający się w granicach 4000000 USD[45].

Nie tylko spamy są formą internetowej działalności zorganizowanych grup przestępczych. Zagrożenie związane jest z wirusami, trojanami, a także programami: spywere, adwere. Przesyłanie zainfekowanych plików, bądź oferowanie zainfekowanego programu ma na celu kradzież posiadanych przez użytkownika danych. Dane te dotyczą wszelkich operacji, które są wykonywane przez użytkownika w sieci, począwszy od haseł logowania i kodów kończąc na danych logowania do rachunku bankowego. Posiadając powyższe dane z łatwością można się podszyć pod daną osobę w sieci. Z uwagi na fakt, iż wiele z transakcji realizowanych jest poprzez internetowe przelewy prawdopodobieństwo użycia skradzionych danych związanych z rachunkiem bankowym staje się realne. Programy typu spywere są także umieszczane w różnego rodzaju gadżetach komputerowych np. grach komputerowych oraz dyskach zewnętrznych. Programy typu spywere są często używanym narzędziem służącym do wyłudzania danych. Natomiast programy typu adwere zazwyczaj ukryte są w ogłoszeniach o charakterze marketingowym, gdzie otworzenie przesłanej wiadomości powoduje automatyczne zakończenie pracy komputera. Po przechwyceniu danych oraz dokonaniu transakcji z użyciem skradzionych danych logowania, kradzieży tożsamości w ostatecznej fazie dochodzi do lokowania środków finansowych na bezpiecznych kontach bankowych sprawców przestępstwa[46].

Najczęstszym rodzajem cyberprzestępstw są te popełniane przy pomocy internetowych, elektronicznych metod płatniczych tzw. phishing. Przestępstwo to polega na uzyskaniu danych dotyczących logowania się na internetowe kontro bankowe tj. loginów, haseł, które umożliwiają wykonywanie transakcji internetowych. Przestępstwo to może być wykonywane przez międzynarodową grupę przestępczą i mieć charakter globalny a skradzione dane wrażliwe mogą dotyczyć użytkowników bankowości elektronicznej w różnych częściach globu[47]. Przestępczość związana z elektronicznymi sposobami płatności może być popełniana także na zasadzie skimmingu, czyli fałszowania kart płatniczych poprzez ich przerabianie, kopiowanie, podrabianie. Dane dotyczące kart płatniczych pozyskiwane są poprzez zakładanie w bankomatach urządzeń mających na celu zeskanowanie danych z pasków magnetycznych karty[48]. Do pozyskania danych w przestępstwie phishingu dochodzi także poprzez podszywanie się pod strony banków, które funkcjonują oficjalnie. Osoba, która myśli, że znajduje się na stronie swojego banku, w sposób nieświadomy podaje przestępcom swoje dane potrzebne do zalogowania się na swoje konto – login i hasło, kody dostępu[49]. Próby wyłudzenia danych wrażliwych konta internetowego polegają na:

45 Tamże, s. 151.

46 Tamże, s. 151.

47 W. Mądrzejowski, dz. cyt., s. 109.

48 Tamże, s. 110.

49 A. Boszko, dz. cyt., s. 152.

- wysyłaniu fałszywych wiadomości email posiadających odnośnik do nieprawdziwej strony banku, serwisu płatności on-line;
- rozsyłania oprogramowania komputerowego który jest zainfekowany poprzez np. konie trojańskie, programy spywere;
- zmiany w pliku hosts, który odpowiada za interpretowanie adresów IP i domen;
- zmiany w adresie IP, przekierowywanie użytkownika na inny serwer, na którym znajduje się podstawiona fałszywa strona np. banku;
- przesyłanie fałszywych wiadomości email, które mają udawać wiadomości dotyczące bezpieczeństwa podczas operacji elektronicznych w banku, emaile te posiadają w swojej treści prośbę o przesłanie kodów, pinów w celu wykonania weryfikacji[50].

Phishing to nie tylko kradzież danych potrzebnych do zalogowania się na konto bankowe, to również kradzież tożsamości użytkownika. Poprzez działania przestępcze sprawca pozyskuje dane osób, by wykorzystać je w dalszym procederze przestępczym. Do przestępstwa dochodzi dzięki wykorzystaniu odpowiednich środków technicznych oraz technologii informatycznej. W przypadku phishingu kradzież tożsamości może zostać poprzedzona oszustwem internetowym[51]. W Internecie funkcjonuje wiele forów internetowych, na których możliwe jest dokonanie zakupu szkodliwego oprogramowania, bądź danych niezbędnych do autoryzacji internetowych rachunków bankowych, cena dostępu zależy od lokalizacji konta oraz wysokości środków na nim dostępnych[52]. Także kradzież praw autorskich jest domeną zorganizowanych grup przestępczych, które czerpią zyski z nielegalnego upowszechniania w sieci utworów pozyskanych bez zgody ich twórców. Dodatkowo sprawcy dokonują ściągnięcia utworów z Internetu i przenoszą je na urządzenia przenośne, które trafiają do nielegalnej sprzedaży[53].

Z wirtualną działalnością zorganizowanych grup przestępczych związane są również gry hazardowe online. Firmy, które prowadzą tego rodzaju działalność zarejestrowane są w krajach, w których nie trzeba odprowadzać podatku np. Kajmany, Cypr. Z uwagi na fakt, iż gra odbywa się za pośrednictwem Internetu bądź drogą telefoniczną, trudno jest oszacować, jaka dokładnie jest skala zjawiska. Wysokość dochodów osiąganych przez grupy przestępcze trudniące się hazardem online są znane dopiero gdy dochodzi do zatrzymania sprawców procederu, gdy zapadają wyroki, a wysokie grzywny są natychmiastowo regulowane przez sprawców przestępstw. Świadczy to o tym, iż dochody uzyskane tytułem hazardu muszą być znacznie wyższe[54].

Cyberprzestępczość jest obecnie zjawiskiem dynamicznym, nieustannie ewoluującym. Przekształcenia oraz zmiany jakie mają miejsce wiążą się z dostępem do najnowszych technologii. Zorganizowane grupy przestępcze trudniące się procederem działają na zasadach syndykatu z międzynarodowym zasięgiem. Dla tych grup nie istnieją ograniczenia finansowe oraz legislacyjne z uwagi na fakt, iż do popełniania przestępstw używają one narzędzi

---

50 K. Ciulkin-Sarnocińska, *Phishing- specyficzna forma pozyskiwania danych newralgicznych*, [w:] E. Guzik-Makaruk, E. Pływaczewski, *Współczesne oblicza bezpieczeństwa*, Białystok 2015, s. 114.

51 Tamże, s. 116.

52 P. Ciszek, dz. cyt., s. 48.

53 A. Boszko, dz. cyt., s. 152.

54 Tamże, s. 155.

i rozwiązań technologicznych opartych na legalnej działalności. Uzależnienie współczesnego świata od technologii oraz postępująca informatyzacja wszystkich sektorów gospodarki, sfer życia czyni cyberprzestępczość problemem istotnym w kontekście międzynarodowym. Przekształcenia grup przestępczych jakie nastąpiły spowodowały utrudnienia w zidentyfikowaniu sprawców przestępstw z uwagi sposób komunikacji pomiędzy członkami grupy oraz wyspecjalizowanych narzędzi służących do popełniania procederu przestępczego. Walka z tym procederem jest wyzwaniem dla państw oraz organizacji międzynarodowych z uwagi na fakt, iż niektóre z państw nie są w posiadaniu narzędzi, które ułatwiłby reagowanie na cyberprzestępczość, nie mają stosownych uregulowań prawnych oraz nie posiadają odpowiednich rozwiązań technicznych. Niezbędne jest wypracowanie międzynarodowego porozumienia, gdyż żaden kraj nie jest sam bezpieczny w sieci globalnej[55].

Tytuł w języku angielskim:
CHARACTERISTICS OF CONTEMPORARY ORGANIZED CRIME

Bibliografia

Publikacje zwarte

Boszko A., *Finanse przestępczości zorganizowanej*, Toruń 2014.

Guzik-Makaruk E., Pływaczewski E. (red.), *Współczesne oblicza bezpieczeństwa*, Białystok 2015.

Kosiński J., *Paradygmaty cyberterroryzmu*, Warszawa 2015.

Mądrzejowski W., *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015.

Zubrzycki W. (red.), *Przez przestępczość zorganizowaną do terroryzmu*, Szczytno 2015.

Artykuły

Krawczyk D., *Internet zagrożeniem dla bezpieczeństwa wewnętrznego*, „Horyzonty Bezpieczeństwa" 2016, nr 2 (1) 2.

Krukowski W., *Pojęcie organizacji przestępczej i przestępczości zorganizowanej*, „Prokuratura i Prawo" 2006, nr 1.

Płoszyński Z., *Przestępczość internetowa*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2012, nr 3.

Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.

[55] P. Ciszek, dz. cyt., s. 57.

DANIEL M. ZAWADKA*

WSPÓŁCZESNA PRZESTĘPCZOŚĆ ZWIĄZANA Z PIENIĄDZEM ELEKTRONICZNYM. ROLA ORGANÓW ŚCIGANIA

Abstrakt

Działania przestępcze wymierzone w legalnych posiadaczy kart płatniczych dalej utrzymują się na wysokim poziomie. Powszechność dokonywania płatności kartą sprawia, że przestępcy dalej sięgają do narzędzi jakimi są skimmery oraz uciekają się do ataków phishingowych z wykorzystaniem socjotechniki, licząc na naiwność swoich potencjalnych ofiar. Płatności elektroniczne są ponadto dla przestępców jedną z częściej wybieranych form „prania pieniędzy". Wobec tak powszechnej i rozwiniętej gałęzi przestępczości, obojętne nie pozostają organy ścigania, dążąc do podnoszenia poziomu wykrywalności sprawców.

Słowa kluczowe: pieniądz elektroniczny, skimming, phishing, carding.

Przestępczość w sektorze płatności bezgotówkowych i akceptacji kart płatniczych stanowi w ostatnich latach znaczny odsetek wśród przestępstw związanych z kradzieżą, finansami i szeroko pojętą przestępczością gospodarczą, oraz zorganizowaną. Na tę sytuację istotne przełożenie ma postępujący proces dematerializacji pieniądza, oraz powszechność dokonywania rozliczeń finansowych i zapłat za produkty bądź usługi za pośrednictwem karty płatniczej lub poprzez inne formy elektronicznego dostępu do rachunku bankowego. Za sprawą postępu technologicznego elektroniczna rewolucja obiegu pieniądza dotyczy już praktycznie każdego. Nowoczesne formy kontaktu z bankiem drogą elektroniczną, stały się już standardem, w wyniku czego te tradycyjne siedziby i placówki banków spychane są na margines uzupełniania bankowości internetowej[1]. Pomijając te najstarsze formy bezgotówkowych płatności, za jakie możemy uznać polecenia przelewu, polecenia zapłaty, czeki

* Daniel M. Zawadka – student studiów magisterskich bezpieczeństwa wewnętrznego na UTH im. Heleny Chodkowskiej w Warszawie. W przeszłości związany z sektorem akceptacji kart płatniczych, współpracował z czołowymi acquirerami na polskim rynku. Kontakt e-mail: daniel.zawadka@uth.pl

[1] A. Prokopiuk, *Wybrane aspekty rozwoju e-bankowości w Polsce*, [w:] T. Mikulska, J. Sikorski (red.), *Stan i perspektywy rozwoju współczesnej bankowości*, Białystok 2014, s. 145.

rozrachunkowe, weksle[2] czy nawet przelewy internetowe, a skupiając się stricte na akceptacji kart płatniczych, właściwym wydaje się stwierdzenie, że opanowały one niemalże wszystkie gałęzie branży handlowo-usługowej. Kartą możemy zapłacić prawie wszędzie, nie tylko w standardowym sklepie stacjonarnym, ale również przez Internet, czy w różnego rodzaju urządzeniach samoobsługowych. Akceptacja kart płatniczych jest możliwa w biletomatach komunikacji miejskiej, czy na dworcach kolejowych, które umożliwiają pasażerom bezpieczną formę płatności zbliżeniowej, zwanej również bezstykową, opartą na technologii NFC, opartą na radiokomunikacji krótkiego zasięgu na pasmie wysokich częstotliwości, która pozwala na szybką wymianę danych pomiędzy kartą a czytnikiem na odległość do kilku centymetrów[3]. Tego typu czytniki zbliżeniowe są bardzo powszechnie stosowane zarówno w biletomatach jak i w automatach vendingowych oferujących kawę, zimne napoje, czy przekąski, parkomatach, czy chociażby na stacjach warszawskiego systemu rowerów miejskich Veturilo.

Z uwagi na przedstawioną wyżej wygodę, mobilność i powszechność występowania czytników kart płatniczych w niemalże każdej gałęzi branży handlowo-usługowej, a także szybkość dokonywania transakcji, oraz bezpieczeństwo wynikające z braku konieczności noszenia przy sobie gotówki przez społeczeństwo, sposób działania przestępców czyhających na szanse okradzenia innych obywateli naturalnie uległ zmianie. Aktualne modus operandi sprawców uwzględnia przede wszystkim uzyskiwanie nieuprawnionego elektronicznego dostępu do środków zgromadzonych na kontach swoich ofiar, natomiast typologia przestępczości tego typu z uwagi na rozległość przedmiotową i zróżnicowanie form dysponowania pieniądzem elektronicznym, jest zagadnieniem dosyć obszernym, które w dodatku ulega ciągłym przekształceniom z racji wdrażanych zabezpieczeń technologicznych ze strony środowisk bankowych i organizacji płatniczych. Podobnie wygląda kwestia dostosowania do ewoluującej przestępczości, metodyki czynności podejmowanych przez środowiska bankowe i organy ścigania. Zauważalny jest również wzrost świadomości samych posiadaczy kart w kwestii bezpieczeństwa posługiwania się instrumentami, jakie daje im bankowość elektroniczna, lecz mimo tego według banków oraz organów ścigania to ciągle człowiek jest najsłabszym ogniwem, szczególnie wobec stosowanej przez przestępców socjotechniki w kontekście wyłudzania danych umożliwiających elektroniczny dostęp do pieniędzy zgromadzonych koncie bankowym.

Definicja pieniądza elektronicznego

Treść ustawy o usługach płatniczych[4] rozdziela pojęcia instrumentu płatniczego definiowanego jako zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego. A także odrębne pojęcie pieniądza elektronicznego, określonego jako wartość pienięż-

2 S. Flajterski, B. Świecka, *Elementy finansów i bankowości*, Warszawa 2007, s. 265–266.

3 A. Grzybowska, *Innowacyjne rozwiązania na rynku usług płatniczych*, [w:] T. Mikulska, J. Sikorski (red.), *Stan i perspektywy rozwoju współczesnej bankowości*, Białystok 2014, s. 115.

4 Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tekst jednolity Dz.U. 2016 poz. 1572.

ną przechowywaną elektronicznie, w tym magnetycznie, wydawaną, z obowiązkiem jej wykupu, w celu dokonywania transakcji płatniczych, akceptowaną przez podmioty inne niż wyłącznie wydawca pieniądza elektronicznego[5]. Wcześniej na obszarze Unii Europejskiej również wprowadzono mocą stosownej dyrektywy[6] pojęcie pieniądza elektronicznego. Jej znowelizowana wersja opracowana przez Parlament Europejski i Radę, zastępująca poprzednią w roku 2009, określa pieniądz elektroniczny jako wartość pieniężną przechowywaną elektronicznie, w tym magnetycznie, stanowiącą prawo do roszczenia wobec emitenta, która jest emitowana w zamian za środki pieniężne w celu dokonywania transakcji płatniczych i akceptowana przez osoby fizyczne lub prawne inne niż emitent pieniądza elektronicznego[7]. Dodatkowo w literaturze można spotkać się z dwiema postaciami pieniądza elektronicznego, określonego jako:

- produkt bazujący o technologię kart procesorowych, tzw. elektroniczną portmonetkę (z ang. *electronicpurse, multipurpose prepaid card*),
- produkt wykorzystujący oprogramowanie, przy pomocy którego posiadacz może dokonać płatności w Internecie, tzw. pieniądz sieciowy (z ang. *network based, software basedproduct*)[8].

Wydawanie instrumentu pieniądza elektronicznego jest natomiast czynnością bankową *sensu stricto*[9].

Skimming – najpowszechniejsze przestępstwo godzące w legalnych posiadaczy kart płatniczych

Postęp technologiczny wymusił szereg zmian również na przestępcach, którzy z kradzieży tradycyjnych portfeli, przekierowali swoje zainteresowanie na elektroniczne portmonetki, jakimi są karty płatnicze. Według ustawy o usługach płatniczych, kartą płatniczą nazywamy kartę uprawniającą do wypłaty gotówki lub umożliwiającą złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego, akceptowaną przez akceptanta w celu otrzymania przez niego należnych mu środków[10]. W literaturze polskojęzycznej nie ma jednego wspólnego określenia co do charakteru prawnego karty płatniczej. Podkreślany jest jednak fakt, że karta nie jest nową typową formą pieniądza bezgotów-

5 Tamże, s. 4–6.

6 Dyrektywa 2000/46/EC Parlamentu Europejskiego i Rady z dnia 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalności, Dz. U. L 275/39 z 21 października 2000 r.

7 Dyrektywa 2009/110/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE, Dz. U. L 267/7 z 10 października 2009 r.

8 R. Janowicz, *Pieniądz elektroniczny na świecie*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych*, Szczytno 2003, s. 21.

9 A. Mikos-Sitek, P. Zapadka, *Polskie prawo bankowe. Wybrane zagadnienia*, Warszawa 2011, s. 178.

10 Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tekst jednolity Dz.U. 2016 poz. 1572.

kowego, gdyż posiadacz dysponuje środkami zgromadzonymi na rachunku bankowym[11], tylko raczej jako klucz dostępu[12], lub instrument dostępu do środków zgromadzonych na rachunku bankowym, za pomocą którego możliwa jest wypłata gotówki z bankomatu lub dokonywanie zapłaty[13].

Skimming jest bezprawnym skopiowaniem informacji zapisanych na pasku magnetycznym karty, oraz przechwyceniem kodu PIN (niezbędnego do autoryzacji transakcji na szkodę legalnego posiadacza karty), bez wiedzy i zgody posiadacza, w celu sfałszowania karty przez wykonanie jej fizycznego duplikatu, mającego posłużyć do przestępczego obciążenia rachunku bankowego prawowitego posiadacza karty[14]. Informacja zapisana na pasku magnetycznym, która jest dla przestępców interesująca, zawarta jest w praktyce na dwóch z trzech ścieżek paska magnetycznego karty. Zawartość ścieżek paska magnetycznego karty określa norma ISO-7811. Pierwsza z nich, alfanumeryczna zawiera dane posiadacza karty, czyli imię, nazwisko, numer karty, oraz informacje dodatkowe jakimi są: data ważności, zastrzeżenia lub typ, a także kod CVV/CVC2. Druga z nich, typowo numeryczna zawiera powtórzony numer karty i informacje dodatkowe[15]. Forma zapisu danych na pasku magnetycznym karty płatniczej pod względem technologicznym nie różni się od poziomu skomplikowania zapisu danych na dyskietce, czy kasecie magnetofonowej. Przy użyciu urządzeń stosunkowo niedrogich i dostępnych w przestępczym półświatku, a także dzięki dobrodziejstwu medium jakim jest Internet, wraz z całym zgromadzonym w sieci zasobem porad i koncepcji skutecznego kopiowania zawartości kart i ich fałszowania, przestępcze *know-how* jest aktualnie dostępne dla każdego obywatela – internauty, rozważającego zboczenie z drogi uczciwej egzystencji w społeczeństwie. Popyt potencjalnych sprawców na coraz to bardziej zminimalizowane i pasujące (np. do elementów bankomatów) skimmery, jest istotnym czynnikiem dalszego i trwałego rozwoju produkcji narzędzi przestępstwa tego typu.

Zjawisko skimmingu możemy dodatkowo podzielić na dwie kategorie, z uwagi na miejsce oraz urządzenie z wykorzystaniem którego sprawca dopuszcza się przestępstwa odczytania danych zapisanych na karcie płatniczej. Pierwszą z nich jest skimming w punkcie handlowo-usługowym, który polega na zeskanowaniu informacji z paska magnetycznego karty płatniczej w momencie dokonywania płatności, najczęściej przez nieuczciwego sprzedawcę lub pracownika[16]. Do tego rodzaju procederu używa się np. miniaturowych, mieszczących się w dłoni skimmerów wyposażonych w baterię oraz wbudowaną pamięć zdolną pomieścić określoną ilość danych. Rozmiar urządzenia ma w tym przypadku znaczenie, jeśli sprawca stojąc w pobliżu prawnego posiadacza karty, sczytuje z niej dane w sposób niezauważalny dla klienta, wykorzystując urządzenie trzymane w dłoni, lub zamocowane przy kasie pod blatem. Poza odczytaniem zawartości paska magnetycznego, sprawcom

---

11 M. Pacak, *Ustawa o elektronicznych instrumentach płatniczych. Komentarz*, Warszawa 2013, s. 64.

12 A. Michór, *Kartypłatnicze*, [w:] W. Góralczyk (red.), *Problemy współczesnej bankowości. Zagadnienia prawne*, Warszawa 2014, s. 265.

13 A. Mikos-Sitek, P. Zapadka, dz. cyt., s. 178.

14 K. Mikołajczyk, *Przestępstwa związane z wykorzystywaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10(6), s. 104.

15 J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 160.

16 B. Kowalski, *Problematyka przestępstw dotyczących kart płatniczych na przykładzie skimmingu i cardingu*, „Przegląd Policyjny" 2015, Nr 4(120), s. 170.

potrzebny jest jeszcze kod PIN, który mogą osobiście podejrzeć w momencie wpisywania go przez klienta – posiadacza karty, na klawiaturze terminala płatniczego, lub PinPada podłączonego do terminala, a także poprzez nakierowanie monitoringu w lokalu na klawiaturę służącą do wpisywania PIN-u. Drugą z form skimmingu jest bankomatowa odmiana tego przestępstwa. Polega ona na nielegalnej modyfikacji budowy bankomatu ATM, mającej na celu zamontowanie urządzenia służącego do kopiowania danych z paska magnetycznego karty[17]. Skimmery przymocowuje się w miejscu slotu-gniazda do którego wkładamy kartę w bankomacie aby pobrać z niego gotówkę (lub ją wpłacić jeśli mamy do czynienia z urządzeniem z funkcją wpłatomatu). Najczęściej przybierają one formę nakładki komponującej się z obudową, lub są dokładną repliką elementu obudowy. Poza skopiowaniem zawartości paska magnetycznego, przestępcy muszą ponadto uzyskać kod PIN niezbędny do pełnego wykorzystania potencjalnej sklonowanej karty. W tym celu wykorzystują dopasowane nakładki na klawiaturę bankomatu, które poprzez umiejscowienie tuż nad właściwą klawiaturą „przekazują" do bankomatu kod PIN oraz komendy zatwierdzane na klawiaturze przez nieświadomego przestępczego procederu posiadacza karty. Ponadto rejestrują wpisywane cyfry, albo zapisując je na module pamięci opartej najczęściej na kartach SD lub microSD, albo bezpośrednio przesyłając je drogą radiową do komputera, lub innego urządzenia znajdującego się w zasięgu – najczęściej w samochodzie zaparkowanym niedaleko bankomatu ATM. Dane mogą być również przesyłane bezpośrednio na drugi koniec świata za pomocą modułu łączności GPRS opartego na karcie SIM, wykorzystującej transmisje danych internetowych. Istotne w urządzeniu jest również alternatywne źródło zasilania, najczęściej w postaci baterii lub miniaturowego akumulatora.

Inną z form uzyskiwania kodu PIN przez sprawców skimmingu jest instalowanie miniaturowej kamery skierowanej na klawiaturę bankomatu. W tej sferze pomysłowość przestępców również nie zna granic. Wykorzystują oni różnego rodzaju doczepiane listwy reklamowe, wypukłe naklejki z logotypami, czy nawet doczepiane do bankomatów pojemniki na ulotki z ofertą banku[18]. Zminiaturyzowane urządzenie charakteryzujące się wydajnością w przestępczym procederze powinno być w stanie rejestrować obraz przez kilka lub kilkanaście godzin, co wymusza na konstruktorach wykorzystanie miniaturowego lecz pojemnego nośnika pamięci, oraz kolejnego alternatywnego źródła zasilania w postaci baterii lub niewielkiego akumulatora. Wyższym poziomem zaawansowania technologicznego wśród metod uzyskiwania kodu PIN wyróżniają się przestępcy, którzy opanowali dodatkowo technologię przechwytywania numeru z sygnału elektromagnetycznego oraz wykorzystywania śladu termicznego palców ofiary z klawiatury bankomatu[19]. Zjawisko skimmingu z uwagi na potencjalny większy zysk sprawców, najczęściej dotyka bankomaty w dobrych lokalizacjach turystycznych, oraz te niezlokalizowane w oddziałach bankowych, do których jest swobodny dostęp i z których korzysta duża liczba osób, gdyż w takich miejscach nikogo nie dziwią ślady zużycia mechanicznego na bankomacie, które mogłyby wskazywać na próby modyfikowania obudowy bankomatu, lub inną podejrzaną działal-

17 Tamże, s. 168.

18 J. Gąsiorowski, P. Podsiedlik, *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej*, Dąbrowa Górnicza 2015, s. 112.

19 J. Kosiński, dz. cyt., s. 159.

ność, ani fakt, że w większych miastach lub obiektach turystycznych w pobliżu bankomatu ciągle znajdują się ludzie[20].

Skimming jest przestępstwem charakterystycznym z uwagi na swój międzynarodowy wymiar. Z racji wyższego poziomu zabezpieczeń przyjętych przez organizacje płatnicze z jakim mamy do czynienia w Europie, w porównaniu z zarówno Ameryką Północną jak i Południową, na co ogromny wpływ ma wprowadzony tzw. standard EMV, finalizowanie przestępczego procederu w postaci wypłacania pieniędzy z kont Polaków czy ogólnie Europejczyków, ma miejsce na terenie obu Ameryk, gdzie zabezpieczenia bankowe są na znacznie gorszym poziomie, a udział w rynku kart z mikroprocesorem jest niestety w dalszym ciągu znikomy. W ciągu ostatnich lat większość nielegalnych wypłat środków z kont naszych obywateli w oparciu o sfałszowane karty płatnicze, miała miejsce głównie w Ameryce Południowej[21]. Analizując doniesienia prasowe i kroniki policyjne, nietrudno zauważyć, że na terenie Polski w związku ze skimmingiem najczęściej zarzuty stawiane są obywatelom Mołdawii, Bułgarii i Rumunii[22], którzy prowadzą u nas zorganizowaną działalność przestępczą. Atrakcyjność Polski jako terytorium działania zorganizowanych grup przestępczych z udziałem cudzoziemców wynika głównie z postrzegania RP jako kraju bezpiecznego, stabilnego i rozwiniętego ekonomicznie, którego gospodarka posiada duży potencjał rozwoju, a co za tym idzie możliwości jej nielegalnej eksploatacji. Do tego dochodzi fakt członkostwa w UE i strefie Schengen oraz centralnego położenia w Europie na trasie szlaków komunikacyjnych łączących wschód z zachodem kontynentu[23].

Phishing

Phishing jest rodzajem oszustwa internetowego, które ma na celu kradzież tożsamości, czyli poufnych danych osobistych, np. numerów kart kredytowych, haseł do systemów bankowych, czy haseł do portali oferujących aukcje internetowe. Termin ten pochodzi z języka angielskiego od sformułowania *password hervesting fishing*, oznaczającego łowienie haseł. Samo przestępstwo polega na nakłonieniu użytkownika do samodzielnego wpisania poufnych danych na specjalnie przygotowanej stronie internetowej, mającej imitować oryginalną stronę instytucji (np. banku internetowego, serwisu aukcyjnego, czy internetowego serwisu płatności), pod którą podszywają się oszuści[24]. Sprawcy najczęściej wysyłają do ofiar spreparowane listy elektroniczne, pochodzące rzekomo z banku, wymuszając na poszkodowanym natychmiastowy kontakt drogą elektroniczną pod legendą odblokowania konta, weryfikacji danych karty dla przedłużenia jej ważności, ponownej jej aktywacji, dodania nowej aplikacji, czy poprawy procedur bezpieczeństwa dokonywanych transak-

20 B. Kowalski, dz. cyt., s. 169.

21 *Kradzież w Polsce, wypłata w Peru*, „Rzeczpospolita" z dn. 12.01.2015 r.

22 *Nie zawsze warto kartą*, „Dziennik Trybuna" z dn. 11.02.2015 r.

23 K. Laskowska, *Działalność zorganizowanych grup przestępczych z udziałem cudzoziemców w Polsce w latach 2004–2013 w świetle policyjnych badań statystycznych*, „Przegląd Policyjny" 2016, nr 3(123), s. 18.

24 R. Wilczewski, *Phishing – popełnianie i zwalczanie*, [w:] J. Kosiński, S. Kmiotek (red.), *Przestępczość teleinformatyczna*, Szczytno 2011, s. 258.

cji[25]. Charakteryzując zjawisko przestępczości w bankowości elektronicznej na przykładzie phishingu, nie sposób nie wspomnieć o tworzonym przez cyberprzestępców złośliwym oprogramowaniu, które uważane jest za jedno największych zagrożeń dla bankowości elektronicznej. Poprzez złośliwe oprogramowanie cyberprzestępcy próbują pozyskać nasze środki finansowe lub tylko dane, które są potrzebne do pozyskania tychże środków. Poza trojanami Rbot, Sinowal czy Limbo2, popularnymi kilkanaście lat temu, na polskim rynku bankowym spustoszenie swego czasu siał trojan nazywany Zeus lub Zbot, który modyfikował transakcje elektroniczne poprzez podmienienie numeru rachunku odbiorcy oraz wysokości kwoty. Zmodyfikowana wersja Zeusa była dodatkowo w stanie podmienić stronę bankową generując prośbę o podanie pełnego hasła, a także wyłudzała dane telefonu klienta, służącego do odbierania kodów autoryzacyjnych, infekowała telefon klienta banku złośliwym oprogramowaniem, a w efekcie finalnym dokonywała transakcje w imieniu klienta. W ostatnich latach również zarejestrowano w Polsce przypadki ataków socjotechnicznych z wykorzystaniem trojana Zeus w wersjach Citadel i 2P2, inspirujących klienta do wykonania rzekomo testowej transakcji, wyłudzając tym sposobem dane logowania i środki finansowe przez naiwność internautów. Natomiast za wschodnią granicą naszego kraju zdarzały się przypadki instalowania trojanów w bankomatach poprzez nawiercenie obudowy w miejscu wewnętrznego gniazda USB i podpięcie pendriva z automatycznie instalującym się złośliwym oprogramowaniem, które rejestrowało i umożliwiało przestępcom pozyskanie wpisywanego kodu PIN oraz danych z drugiej ścieżki paska magnetycznego karty płatniczej[26].

Autorzy publikacji z dziedziny cyberprzestępczości wskazują również na możliwość pozyskiwania danych o kartach płatniczych z terminali POS, poprzez odpowiednio spreparowane oprogramowanie i przesyłanie danych na pomocą różnych form łączności – np. bluetooth lub Wi-Fi, lub zapisywania ich we wmontowaną nielegalnie w POS wymienną kartę pamięci[27]. Jednakże z uwagi na technologiczny wymiar skomplikowanej aplikacji obsługującej płatności w terminalu oraz nadzoru jej przez systemy TMS należące do acquirerów lub kooperujących z nimi podmiotów, jest to raczej trudny a z pewnością szerzej nieznany wymiar przestępczości terminalowej, w który swój wkład teoretycznie musiałby mieć akceptant jakim jest przedsiębiorca dzierżawiący terminal płatniczy.

Cyberlaundering – „pranie pieniędzy" za pośrednictwem pieniądza elektronicznego

Pojawienie się nowych technologii umożliwiających dokonywanie natychmiastowych transferów pieniężnych, może przełożyć się na ułatwienie zadania przestępcom w procederze prania pieniędzy[28]. Efektem tego katalog legalizacji środków pochodzących z prze-

[25] J. Gąsiorowski, P. Podsiedlik, dz. cyt., s. 147.

[26] P. Olszar, *Złośliwe oprogramowanie w bankowości elektronicznej*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Szczytno 2013, s. 307–316.

[27] J. Kosiński, dz. cyt., s. 162.

[28] D. Cyman, *Elektroniczne instrumenty płatnicze a bezpieczeństwo użytkowników rynku finansowego*, Warszawa 2013, s. 245.

stępstw wzbogacił się o pojęcie *cyberlaunderingu* – wygodnej i bezpiecznej legalizacji z wykorzystaniem transakcji elektronicznych, dokonywanej najczęściej przez sieć internetową. D. Cyman wśród popularnych elektronicznych instrumentów płatniczych wskazuje na wykorzystywanie systemu kart przedpłaconych, które z uwagi na swoją anonimowość są idealną formą transgranicznego transferu środków pieniężnych, w szczególności z wykorzystaniem kart wydawanych w rajach podatkowych, gdzie obowiązują rygorystyczne regulacje dotyczące tajemnicy bankowej[29].

Jerzy Kosiński w kontekście prania pieniędzy w wymiarze cyberprzestępczości, a co za tym idzie wykorzystaniu elektronicznych instrumentów płatniczych, wymienia trzy formy legalizacji środków finansowych pochodzących z przestępstwa, jakimi są:

- *moneymulles* – rekrutowani na niszowych portalach oferujących pracę, która polega na dokonywaniu transferu otrzymywanych od przestępców kwot na wskazane konta bankowe, w zamian za ustaloną kwotę prowizji. W tym procederze konta praczy zakłada się w bankach, których klienci mają być ofiarami dokonywanych przestępstw finansowych, co pozwala na szybki transfer pieniędzy pomiędzy rachunkami w tym samym banku;
- internetowe gry on-line o charakterze MMORPG, w których internetowi gracze korzystają z wirtualnych kredytów wykupowanych i wymienialnych na realne pieniądze. Przy użyciu wielu kont, łączących graczy z wielu krajów możliwe jest szybkie wprowadzenie, transfer międzynarodowy, oraz powrót do wpłacającego lub wypłata środków poza granicami;
- mikropralnie polegające na wykorzystywaniu usług podobnych do PayPal w połączeniu z płatnościami mobilnymi i tradycyjnymi usługami płatniczymi, poprzez przenoszenie pieniędzy różnymi środkami transferowania w postaci niewielkich kwot przelewanych z dużą częstotliwością, co utrudnia powstrzymywanie prania brudnych pieniędzy[30].

Działania podejmowane przez organy ścigania

Bezpieczeństwo prawne transakcji jest zespołem regulacji prawnych wyznaczających określone zachowania, które mają być podejmowane przez osoby i instytucje, których dotyczą te przepisy[31]. W przypadku stwierdzenia odstępstw od wyznaczonych zachowań, uzyskanych w ramach zgłoszenia osoby poszkodowanej, instytucji finansowej, organizacji płatniczej, czy zauważenia tego podczas prowadzenia postepowania w innej sprawie, lub w wyniku podejmowanych czynności operacyjno-rozpoznawczych, reagują na to uprawnione organy ścigania, wszczynając postepowanie przygotowawcze[32].

---

29 Tamże, s. 246.

30 J. Kosiński, dz. cyt., s. 156.

31 *Bezpieczeństwo prawne transakcji dokonywanych kartami płatniczymi*, „Gazeta Prawna" z dn. 11.12.2008 r.

32 Z uwagi na właściwości wynikające z ustaw szczególnych, a także z k.p.k., do realizacji czynności procesowych w związku z przestępczością kartową właściwa jest Policja, lub Żandarmeria Wojskowa – lecz wyłącznie w stosunku do żołnierza pełniącego czynną służbę wojskową, wobec którego ŻW prowadzi postepowania przygotowawcze z pełnej kwalifikacji określonej treścią całego k.k.

Organy ścigania mają zapewnioną pomoc umocowaną w k.p.k. którą mogą otrzymać od osób mających wiedzę na temat przestępstw kartowych, np. skimmingu w punkcie handlowo-usługowym, gdzie na pierwszej linii reagowania na przestępczy proceder sczytywania zawartości paska magnetycznego, stoją potencjalni świadkowie, czyli np. pracodawca, lub pracownik, który zauważył fakt skanowania kart płatniczych przez kasjera. Pracodawca ponadto na podstawie art. 15 § 3 k.p.k. ma obowiązek podjęcia pełnej współpracy z organami ścigania[33], w tym przez przekazanie monitoringu, czy pełnych danych pracownika, który był sprawcą przestępstwa[34].

Policja funkcjonująca w oparciu o zapisy stosownej ustawy[35] oraz szeregu rozporządzeń ministra właściwego ds. wewnętrznych, czy zarządzeń Komendanta Głównego Policji, reagowanie na stwierdzone przestępstwa w sektorze płatności bezgotówkowych i akceptacji kart płatniczych, powierza komórkom do walki z przestępczością gospodarczą, lub komórkom dochodzeniowo-śledczym, określając je jako właściwe do prowadzenia postepowań przygotowawczych w tym zakresie, z uwagi na postrzeganie ww. rodzaju przestępczości jako przestępczość gospodarczą[36]. W każdym Wydziale dw. z PG w Komendach Wojewódzkich Policji oraz KSP, do których kompetencji należy prowadzenie czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych, w odniesieniu do przestępstw dokonywanych w obrocie bankowym i kapitałowym, związanych z obrotem gospodarczym, czy związanych z legalizacją dochodów uzyskanych z działalności przestępczej, a także fałszerstwa środków płatniczych (z wyłączeniem pieniędzy)[37], znajdują się funkcjonariusze ze specjalistycznym przeszkoleniem w zakresie zwalczania przestępstw z udziałem kart płatniczych. Posiadają oni niezbędną wiedzę oraz kontakty robocze z emitentami kart[38], a także gromadzą informacje o przestępstwach stwierdzonych przez komórki terenowe policyjnych garnizonów[39]. Ich praca jest koordynowania przez Wydział do walki z Przestępczością Gospodarczą Biura Kryminalnego KGP. Policjanci tych komórek wspierają ponadto programy profilaktyczne emitentów kart i NBP w zakresie edukacji społecznej dla wzrostu świadomości o niebezpieczeństwach, jakie czyhają na użytkowników kart[40]. W strukturach Policji znajduje się również eksperckie stanowisko krajowego koordynatora

---

33 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, tekst jednolity Dz.U. 2016 poz. 1749.

34 B. Kowalski, dz. cyt., s. 171.

35 Ustawa z dnia 6 kwietnia 1990 r. o Policji, tekst jednolity Dz.U. 2016 poz. 1782.

36 Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

37 http://www.policja.waw.pl/pl/stoleczna-policja/wydzialy-ksp/wydzial-do-walki-z-prze/85,Wydzial-do-walki-z-Przestepczoscia-Gospodarcza.html [dostęp: 29.09.2017].

38 S. Górnicki, *Zalecenia metodyczne w zakresie gromadzenia dowodów w postępowaniach przygotowawczych w sprawach o przestępstwa kradzieży, fałszerstwa bankowych kart płatniczych oraz wprowadzania do obrotu sfałszowanych bankowych kart płatniczych*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, Szczytno 2003, s. 106.

39 J. Biegański, Ł. Nowacki, *Zasady współpracy banków i agentów rozliczeniowych z organami ściągania*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, Szczytno 2003, s. 111.

40 http://www.policja.pl/pol/aktualnosci/70983,Policjanci-o-skimmingu-podczas-dni-otwartych-w-NBP.html [dostęp: 29.09.2017].

ds. przestępczości kartowej, odpowiedzialnego za współpracę funkcjonariuszy zajmujących się tą problematyką z zagranicznymi kolegami, w ramach sieci krajowych ekspertów w oparciu o szyfrowane łącza wymiany informacji (Siena) pomiędzy państwami członkowskimi Europolu[41].

Z uwagi na międzynarodowy charakter przestępczości zorganizowanej związanej z wykorzystaniem kart płatniczych[42], w jej zwalczaniu bardzo istotną rolę odgrywa współpraca międzynarodowa. W ramach Europejskiego Urzędu Policji, jakim jest Europol, w jego Departamencie Operacyjnym funkcjonuje od 2003 r. zespół zadaniowy AWF Terminal (ang. *Analitycal Work File Terminal*), który powstał z inicjatywy Belgów w celu znalezienia powiązań między odrębnymi dochodzeniami oraz ułatwienia międzynarodowej wymiany informacji przy dochodzeniach dotyczących zorganizowanych siatek przestępczych zaangażowanych w proceder skimmingu[43]. Europejska wymiana informacji na temat przestępczości kartowej może polegać na wymianie raportów o powiązaniach, zawierających podstawowe informacje na temat powiązań kryminalnych pomiędzy osobami rozpracowywanymi w różnych krajach, oraz związku pomiędzy skimmingiem, a wypłatami oraz prowadzonymi w tych sprawach śledztwach przez członków Europolu. Drugą z form są raporty analityczne zawierające dogłębną analizę struktury przestępczej, obszaru działalności, oraz wyciągnięte wnioski co do kierunków dalszej współpracy międzynarodowej w konkretnej sprawie. Raporty uwzględniają dane przetwarzane w bazach danych, za jaką można uznać CardChecker, pozwalający ustalić wydawcę większości kart płatniczych emitowanych na świecie[44]. Europol w ramach AWF Terminal kładzie nacisk na wzajemne wsparcie i poza spotkaniami operacyjnymi i koordynacyjnymi organizowanymi przy prowadzaniu konkretnych spraw na płaszczyźnie międzynarodowej, a także wdrożonym systemem wczesnego ostrzegania przed zidentyfikowanym nowym modus operandi sprawców, czy nowymi technikami i urządzeniami służącymi m.in. do skimmingu, na co dzień zajmuje się wsparciem strategicznym partnerów współpracujących. Przejawia się to w szkoleniach dotyczących bezgotówkowych oszustw płatniczych, wydawaniu anglojęzycznych podręczników na ten temat, spotkaniach eksperckich i konferencjach pozwalających na wymianę doświadczeń pomiędzy koordynatorami krajowymi, czy stworzeniu mechanizmu pozwalającego na składanie sprawozdań statystycznych przestępczości kartowej z poszczególnych państw. Ponadto organizowane są spotkania z przedstawicielami organizacji płatniczych czy emitentów, gdzie funkcjonariusze zapoznają się z nowymi środkami bezpieczeństwa stosowanymi w kartach płatniczych oraz omawiają trendy współczesnej przestępczości w sektorze płatności bezgotówkowych. Europol ponadto zainicjował powstanie kolejnych grup roboczych jakimi są Centrum Informacji o Przestępczości Finansowej (ang. *Financial Crime Information Centre* – FCIC), czy zespół EAST (ang. *European ATM Security Team*), zajmujący się opracowaniem strategii działania wobec przestępczości uderzającej w ban-

41 M. Skowronek, J. Cholewiński, *Operacja kryptonim IASI*, [w:] J. Kosiński, S. Kmiotek (red.), *Przestępczość teleinformatyczna*, Szczytno 2011, s. 236.

42 W. Mądrzejowski, *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015, s. 89.

43 Europol, *Bezgotówkowe oszustwa płatnicze*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. Materiały konferencyjne*, Szczytno 2006, s. 155.

44 M. Skowronek, J. Cholewiński, dz. cyt., s. 237.

komaty. W ramach ATM Terminal. Europol ponadto wspiera kwestię analizy technicznej sfałszowanych kart płatniczych w oparciu o UCS – Uniwersalny System Klasyfikacji Sfałszowanych Kart Płatniczych (ang. *Universal Calssification System fot Counterfeit Payment Cards*), za sprawą którego istnie możliwość rozpoznawania i szukania powiązań pomiędzy przestępstwami kartowymi z różnych państw europejskich dzięki bazą wyników technicznego badania kart, ich fotografii i informacji technicznych nt. sfałszowanych kart[45].

W Polsce kryminalistyczne badania kart płatniczych przeprowadza Zakład Badań Dokumentów i Technik Audiowizualnych Centralnego Laboratorium Kryminalistycznego Policji, lub zespoły bądź sekcje właściwe do badań dokumentów z Laboratoriów Kryminalistycznych Komend Wojewódzkich (lub Stołecznej) Policji. Dodatkowo CLKP stara się poszerzyć zakres przetwarzanych katalogów danych, o bazę elektronicznych środków płatniczych[46]. W kwestii ustaleń teleinformatycznych w związku z przestępstwami kartowymi, z uwagi na przeznaczenie właściwe są komórki do walki z cyberprzestępczością, koordynowane przez Biuro do Walki z Cyberprzestępczością KGP. Wspominane piony co istotne – nie prowadzą pracy procesowej[47].

Kwestię działań podejmowanych przez funkcjonariuszy Policji w odniesieniu do zidentyfikowanej przestępczości w sektorze płatności bezgotówkowych i akceptacji kart płatniczych, regulują m.in. zarządzenie pf-634 Komendanta Głównego Policji z dnia 30 czerwca 2006 r. w sprawie metod i form wykonywania przez Policję czynności operacyjno-rozpoznawczych[48] (z późn. zm.), a także decyzja nr 252 Komendanta Głównego Policji z dnia 18 kwietnia 2008 r. w sprawie programu kursu specjalistycznego w zakresie zwalczania przestępczości gospodarczej (z późn. zm.)[49][50].

W kwestii ustalenia informacji o dowodach przy stwierdzeniu przestępczości kartowej, S. Górnicki wskazuje na typologię źródeł w oparciu o poszczególne podmioty funkcjonujące na rynku transakcji bezgotówkowych:

- akceptant płatności (punkt handlowo-usługowy):
  przesłuchanie pracowników (kasjerów) obsługujących podejrzaną transakcję, lub stwierdzony fraud pozwala na:
  a. ustalenie rysopisu domniemanego sprawcy,
  b. zabezpieczenie oryginału dokumentu potwierdzającego dokonanie płatności bezgotówkowej,
  c. zabezpieczenie nagrań monitoringu akceptanta, lub z obiektu gdzie znajduje się punkt handlowo-usługowy akceptanta;
- bank – emitent i właściciel karty:
  współpraca z emitentem karty płatniczej pozwala organom ścigania na:

45 Europol, dz. cyt., s. 156–160.

46 http://clk.policja.pl/clk/clkp/historia/historia/66039,Historia-laboratorium.html [dostęp: 29.09.2017].

47 Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

48 Dokument niepublikowany.

49 Dz. Urz. KGP poz. 58, z 2013 r. poz. 13, oraz z 2015, poz. 21.

50 Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

a. uzyskanie wszystkich informacji na temat kwestionowanych transakcji dokonanych przy użyciu skradzionej lub sfałszowanej karty,
b. wskazanie agenta rozliczającego daną transakcję,
c. wskazanie faktycznego posiadacza karty;

- acquirer – agent rozliczeniowy, centrum operacyjno-rozliczeniowe acquirera:
  Współpraca organów ścigania z agentem rozliczeniowym polega na:
  a. ustalenie adresu akceptanta kwestionowanych transakcji;
  b. ustalenie miejsca gromadzenia dokumentacji z przeprowadzonych transakcji;
  c. uzyskanie opinii i informacji na temat prawidłowości przeprowadzenia transakcji u danego akceptanta:
     I. czy pojawiały się fraudy?
     II. czy występowały rażące naruszenia procedury akceptacji kart płatniczych, bądź inne okoliczności mogące podważać zaufanie do prawidłowości obsługiwania terminala POS przez personel placówki?
- organizacja płatnicza również może udzielić informacji organom ścigania, jeśli informacje z powyższych źródeł nie pozwalają na pełne wyjaśnienie okoliczności zdarzenia, aczkolwiek podmiotem dedykowanym do udzielania niezbędnych informacji na temat karty płatniczej dla potrzeb postepowania karnego, jest emitent karty (bank wydawca lub organizacja płatnicza), którego dane są nadrukowane na jej rewersie[51].

Podsumowanie

Specyfikacja zagrożeń związanych z obrotem bezgotówkowym skupia się wokół naruszenia tajności danych, nieautoryzowanego dostępu do systemu, czy zablokowania pewnych usług bankowych[52]. Za zagrożenie można również uznać samą szybkość wymiany i dostępność informacji dotyczących sposobów popełniania przestępstw, a także wykorzystywanie luk organizacyjnych, technologicznych czy prawnych[53]. Powszechność obrotu bezgotówkowego w wielu formach, przekłada się ponadto na szeroki wachlarz zdefiniowanych działań przestępczych, m.in.: kradzieży karty płatniczej, fałszerstwa karty płatniczej, posługiwania się kartami płatniczymi niedoręczonymi do prawnego posiadacza, wyłudzenia karty w oparciu o wniosek z nieprawdziwymi danymi, *skimmingu* karty bankomatowej, *cardingu* – czyli dysponowania cudzymi środkami płatniczymi z wykorzystaniem danych cudzej karty płatniczej, *phishingu* i *vishingu* – czyli kradzieży tożsamości, *pharmingu* – czyli przekierowania do fałszywej strony internetowej, *sniffingu* – czyli podsłuchu w Internecie, *tamperingu* – czyli penetracji w celu przechwycenia danych oraz *spoofingu* – czyli podszywania się pod inną tożsamość.

Problematyka bezpieczeństwa transakcji dokonywanych kartami płatniczymi jest zdaniem R. Kaszubskiego wypadkową działań podejmowanych zarówno przez wydawców, agentów rozliczeniowych, akceptantów i posiadaczy kart. Nie sposób nie zgodzić się

[51] S. Górnicki, dz. cyt., s. 104–105.
[52] W. Chmielarz, *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa 1999, s. 105.
[53] D. Cyman, dz. cyt., s. 237.

z kolejnym twierdzeniem wspomnianego autora, iż tylko w przypadku właściwego funkcjonowania tych wszystkich elementów składowych systemu, możliwe będzie utrzymanie w Polsce dotychczasowego, ocenianego jako bardzo wysoki, w porównaniu do innych krajów, poziomu bezpieczeństwa rynku kart płatniczych[54].

Tytuł w języku angielskim:
MODERN CRIMINALITY ASSOCIATED WITH ELECTRONIC MONEY: THE ROLE OF POLICE INVESTIGATOR

Bibliografia

Dokumenty i materiały źródłowe

Ustawa z dnia 6 kwietnia 1990 r. o Policji, tekst jednolity Dz.U. 2016 poz. 1782.

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, tekst jednolity Dz.U. 2016 poz. 1749.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tekst jednolity Dz.U. 2016 poz. 1572.

Dyrektywa 2000/46/EC Parlamentu Europejskiego i Rady z dnia 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalności, Dz. U. L 275/39 z 21 października 2000 r.

Dyrektywa 2009/110/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE, Dz. U. L 267/7 z 10 października 2009 r.

Dz. Urz. KGP poz. 58, z 2013 r. poz. 13, oraz z 2015. poz. 21.

Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

Książki i artykuły

Biegański J., Nowacki Ł., *Zasady współpracy banków i agentów rozliczeniowych z organami ściągania*, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, Kosiński J. (red.), Szczytno 2003.

Chmielarz W., *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa 1999.

Cyman D., *Elektroniczne instrumenty płatnicze a bezpieczeństwo użytkowników rynku finansowego*, Warszawa 2013.

Europol, *Bezgotówkowe oszustwa płatnicze*, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. Materiały konferencyjne*, Kosiński J. (red.), Szczytno 2006.

Flajterski S., Świecka B., *Elementy finansów i bankowości*, Warszawa 2007.

Gąsiorowski J., Podsiedlik P., *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej*, Dąbrowa Górnicza 2015.

Górnicki S., *Zalecenia metodyczne w zakresie gromadzenia dowodów w postępowaniach przygotowawczych w sprawach o przestępstwa kradzieży, fałszerstwa bankowych kart płatniczych oraz wprowadzania do*

[54] *Bezpieczeństwo prawne transakcji dokonywanych kartami płatniczymi*, „Gazeta Prawna" z dn. 11.12.2008 r.

obrotu sfałszowanych bankowych kart płatniczych, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, J. Kosiński (red.), Szczytno 2003.

Grzybowska A., *Innowacyjne rozwiązania na rynku usług płatniczych*, [w:] *Stan i perspektywy rozwoju współczesnej bankowości*, Mikulska T., Sikorski J. (red.), Białystok 2014.

Janowicz R., *Pieniądz elektroniczny na świecie*, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych*, Kosiński J. (red.), Szczytno 2003.

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Kowalski B., *Problematyka przestępstw dotyczących kart płatniczych na przykładzie skimmingu i cardingu*, „Przegląd Policyjny" 2015, Nr 4(120).

Laskowska K., *Działalność zorganizowanych grup przestępczych z udziałem cudzoziemców w Polsce w latach 2004–2013 w świetle policyjnych badań statystycznych*, „Przegląd Policyjny" 2016, nr 3(123).

Mądrzejowski W., *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015.

Michór A., *Karty płatnicze*, [w:] *Problemy współczesnej bankowości. Zagadnienia prawne*, Góralczyk W. (red.), Warszawa 2014.

Mikołajczyk K., *Przestępstwa związane z wykorzystywaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10(6).

Mikos-Sitek A., Zapadka P., *Polskie prawo bankowe. Wybrane zagadnienia*, Warszawa 2011.

Olszar P., *Złośliwe oprogramowanie w bankowości elektronicznej*, [w:] *Przestępczość teleinformatyczna*, Kosiński J. (red.), Szczytno 2013.

Pacak M., *Ustawa o elektronicznych instrumentach płatniczych. Komentarz*, Warszawa 2013.

Prokopiuk A., *Wybrane aspekty rozwoju e-bankowości w Polsce*, [w:] *Stan i perspektywy rozwoju współczesnej bankowości*, Mikulska T., Sikorski J. (red.), Białystok 2014.

Skowronek M., Cholewiński J., *Operacja kryptonim IASI*, [w:] *Przestępczość teleinformatyczna*, Kosiński J., Kmiotek S. (red.), Szczytno 2011.

Wilczewski R., *Phishing – popełnianie i zwalczanie*, [w:] *Przestępczość teleinformatyczna*, Kosiński J., Kmiotek S. (red.), Szczytno 2011.

Prasa i inne

Bezpieczeństwo prawne transakcji dokonywanych kartami płatniczymi, „Gazeta Prawna" z dn. 11.12.2008 r.

Kradzież w Polsce, wypłata w Peru, „Rzeczpospolita" z dn. 12.01.2015 r.

Nie zawsze warto kartą, „Dziennik Trybuna" z dn. 11.02.2015 r.

Źródła internetowe

http://clk.policja.pl/

http://www.policja.waw.pl/

http://www.policja.pl/

ALEKSANDRA NOWICKA*

MEDIALNY FENOMEN BEZPIECZEŃSTWA

Abstrakt

Przedmiot analizy stanowić będzie współistnienie systemu bezpieczeństwa i mediów. Szczególny nacisk położony zostanie na dualny charakter owych powiązań. Po pierwsze, analizie poddany zostanie sposób doboru informacji dotyczących kwestii bezpieczeństwa oraz ich prezentacji. Po drugie, zwrócona zostanie uwaga na realizację funkcji informacyjnej, identyfikacyjnej oraz integracyjnej mediów w systemie bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo, media, przestępczość.

„Współistnienie" systemu bezpieczeństwa i mediów jest zagadnieniem niezmiernie interesującym, jak również budzącym liczne kontrowersje. Co ciekawe, analizowana tematyka nie doczekała się jak dotychczas pokaźnej reprezentacji w literaturze przedmiotu. Na wstępie do niniejszych rozważań, należy zaakcentować dwoistość omawianego zagadnienia. Czym innym bowiem jest medialny obraz szeroko rozumianego bezpieczeństwa i zagadnień pokrewnych, jak chociażby zjawisko przestępczości, a czym innym udział mediów we właściwym funkcjonowaniu systemu bezpieczeństwa.

Pierwszy aspekt odnosi się bezpośrednio do tego w jaki sposób dziennikarze opisują i informują społeczeństwo o kwestiach powiązanych z bezpieczeństwem. Ta sfera stanowi idealne pole do popisu dla reporterów szukających taniej sensacji i chwytliwego tematu, który przyczyni się do wzrostu oglądalności konkretnego programu czy nakładów gazety, dla której pracują. W tym kontekście głównie będzie mówiło się o wspomnianej kontrowersyjności powiązanej z subiektywną selekcją informacji.

* Aleksandra Nowicka – absolwentka bezpieczeństwa wewnętrznego (studia I i II stopnia) w Instytucie Nauk Politycznych UW. Obecnie doktorantka na Wydziale Nauk Politycznych i Studiów Międzynarodowych UW oraz studentka kryminologii (studia II stopnia) w Instytucie Profilaktyki Społecznej i Resocjalizacji UW. Zainteresowania naukowe: kryminologia feministyczna, systemy zarządzania kryzysowego we współczesnych państwach, dziedziczenie cech przestępczych. Kontakt e-mail: nowiko@vp.pl

Drugi aspekt odnosi się natomiast do funkcji i zadań jakie środki masowego przekazu pełnią na rzecz obywateli, co bezpośrednio przekłada się na społeczną świadomość i poczucie bezpieczeństwa.

W tym miejscu należy także zwrócić uwagę na pewną, charakterystyczną zmianę jaka zaszła (zwłaszcza) w rodzimych mediach od lat 80. XX wieku w komunikowaniu na temat bezpieczeństwa. Za ową sytuację odpowiada ewolucja pojęcia bezpieczeństwo. W czasach zimnej wojny jedynymi podmiotami stosunków międzynarodowych były suwerenne państwa narodowe. Z kolei zagrożenie mogło mieć jedynie charakter jednowymiarowy – zewnętrzny. Nie powinno więc dziwić, że ówczesne społeczeństwo miało dostęp tylko do informacji dotyczących sytuacji militarnej poza granicami państwa lub o ewentualnym zagrożeniu wymierzonym we władze państwowe. Po upadku Związku Socjalistycznych Republik Radzieckich i zmianie ładu geopolitycznego na świecie przeformułowano koncepcję bezpieczeństwa. Od tej pory to jednostka stała się podmiotem bezpieczeństwa, a zagrożenia zyskały różnorodny i wszechobecny charakter. Z tego też powodu współcześnie informacje dotyczące kwestii bezpieczeństwa odnoszą się do niemal każdego aspektu życia społecznego. Tak szerokie podejście do owego zagadnienia w mediach pozostaje w zgodzie z kryterium przedmiotowym podziału bezpieczeństwa, na podstawie którego wyróżniamy bezpieczeństwo: ekologiczne, kulturowe, ekonomiczne, polityczne, społeczne oraz militarne[1]. Ze względu na powyższe w niniejszej pracy będą pojawiały się odwołania do różnorodnych aspektów bezpieczeństwa jak również zagadnień pokrewnych np., przestępczości, aczkolwiek bezpośrednio powiązanych z przedmiotem analizy.

Środki masowego przekazu w imieniu społeczeństwa są kontrolerem właściwego oraz zgodnego z prawem funkcjonowania systemu bezpieczeństwa. „Nie do wyobrażenia jest istnienie ustroju demokratycznego bez kontroli jego funkcjonowania w świecie mediów. Każda władza publiczna musi czuć na swych plecach ich oddech”[2]. Poprzez realizację funkcji: informacyjnej, edukacyjnej oraz kontrolnej[3] środki masowego przekazu stają się swego rodzaju spoiwem pomiędzy organami władzy państwowej, a obywatelem. Co istotne, podstawę prawną do ich urzeczywistnienia stanowi konstytucja RP i zawarte w niej przepisy dotyczące wolności mediów, wyrażania własnych poglądów oraz pozyskiwania informacji. Jednak zapisana w konstytucji wolność mediów nie oznacza, że dziennikarze mają prawo zdobyć i przekazać każdą informację bez względu na sposób i okoliczności jej pozyskania, a także skutki jakie w opinii publicznej może ona wywołać. „Art. 14. Rzeczpospolita Polska zapewnia wolność prasy i innych środków społecznego przekazu. Art. 54 1. Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. Art. 61 1. Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie,

---

1 M. Brzeziński, *Rodzaje bezpieczeństwa państwa*, [w:] Sulowski S., Brzeziński M., (red.), *Bezpieczeństwo wewnętrzne państwa wybrane zagadnienia*, Warszawa 2009, s. 34.

2 C. Kulesza, *System wymiaru sprawiedliwości a media*, Białystok 2009, s. 19.

3 *Sądowe ABC – poradnik dla dziennikarzy*, źródło: http://www.krs.pl/pl/rzecznik-prasowy/zbior-dobrych-praktyk/p,1/3717,sadowe-abc-poradnik-dla-dziennikarzy [dostęp: 23.10.2017], s. 3.

w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. 2. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu. 3. Ograniczenie prawa, o którym mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa"[4].

Polska konstytucja gwarantuje każdemu człowiekowi równy dostęp do pozyskiwania informacji oraz wyrażania własnych opinii. Jednak należy zwrócić szczególną uwagę na wskazaną fakultatywną możliwość ograniczenia owego prawa między innymi ze względu na ochronę porządku publicznego oraz bezpieczeństwa. Oznacza to, że w sytuacji, w której kolegialne organy władzy publicznej pochodzące z powszechnych wyborów (np. sejmowa komisja ds. służb specjalnych) procedować będą kwestie, które mogą przyczynić się do wystąpienia rozruchów społecznych lub przedmiotem ich zainteresowania staną się informacje objęte jedną z klauzul: ściśle tajne, tajne, poufne lub zastrzeżone dziennikarze, a co za tym idzie ogół społeczeństwa nie będą mieli do nich dostępu. Prawodawca w aneksie do Ustawy o ochronie informacji niejawnych z 22 stycznia 1999 r. przytoczył egzemplifikacje zagadnień, które mogą zostać objęte klauzulami, a co za tym idzie ich procedowanie utajnione przed środkami masowego przekazu i obywatelami. Są to na przykład: „Informacje dotyczące zagrożeń zewnętrznych bezpieczeństwa państwa o charakterze militarnym, plany i prognozowanie obronne oraz wynikające z nich decyzje i zadania; Planowanie, realizacja, wyniki badań naukowych i prac badawczo-rozwojowych o szczególnie ważnym znaczeniu dla obronności i bezpieczeństwa państwa; Szczegółowe informacje dotyczące organizacji, form i metod pracy operacyjnej Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego oraz byłego Urzędu Ochrony Państwa i byłych Wojskowych Służb Informacyjnych, a także ich kierunki pracy operacyjnej i zainteresowań; Plany obrony cywilnej państwa oraz plany obrony cywilnej województw; Zadania ministrów, centralnych organów administracji rządowej, wojewodów, a także innych konstytucyjnych organów władzy publicznej, związane z osiąganiem podwyższonej gotowości obronnej państwa"[5]. Należy tutaj także wspomnieć o utajnianiu niektórych rozpraw sądowych, zwłaszcza tak zwanych „głośnych procesów", które bulwersują społeczeństwo, a których przebieg lub rezultat może doprowadzić do wspomnianych zamieszek.

Innym problemem związanym z komunikowaniem zagadnień związanych z bezpieczeństwem jest stosunek samych dziennikarzy do powierzonych im obowiązków. W myśl art. 10 Ustawy prawo prasowe z 26 stycznia 1984 r. „Zadaniem dziennikarza jest służba społeczeństwu i państwu. Dziennikarz ma obowiązek działania zgodnie z etyką zawodową i zasadami współżycia społecznego, w granicach określonych przepisami prawa"[6]. Niestety, ale większość dziennikarzy nadal nie zdaje sobie sprawy bądź nie rozumie idei służby społeczeństwu i państwu, i swój zawód sprowadza jedynie do roli sprzedawcy „towaru",

4 *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Dz.U. 1997, nr 78, poz. 483.

5 *Ustawa z dania 22 stycznia 1999 r. o ochronie informacji niejawnych*, Dz.U. 1999, nr 11, poz. 95.

6 *Ustawa z dnia 26 stycznia 1984 r. prawo prasowe*, Dz.U. 1984, nr 5, poz. 24.

który w tym wypadku przybiera postać chwytliwej informacji i taniej sensacji powiązanej z ludzką krzywdą[7].

Należy w tym miejscu zwrócić uwagę na istotny problem selekcji informacji, będący jednocześnie implikacją głównego celu funkcjonowania mediów, jakim jest osiągnięcie jak największego zysku. Nie dziwi więc, że środki masowego przekazu tak chętnie informują obywateli o przestępczości, zamachach terrorystycznych czy wyciekach ściśle tajnych informacji lub niewłaściwie przeprowadzonych przetargach w Siłach Zbrojnych. Oczywiście, głównym celem nie jest wcale idea podniesienia społecznej świadomości i wiedzy, a jedynie znalezienia „chwytliwego" i „poczytnego" tematu. „Relacje kryminalne są pokupnym towarem każdej prasy (…). Nigdy nie oddają one prawdziwej natury przestępczości. Zauważono, że o tym, czy przekazuje się wiadomość o przestępstwie, nie decyduje sam fakt przestępstwa, ale okoliczności przestępstwa, rola w społeczeństwie sprawcy lub ofiary, a nawet zabawne okoliczności sprawy, szczególnie gdy chodzi o przestępstwo mniejszej wagi. Do tego spostrzeżenia dorzuca się następne, że skoro dziennikarze zauważają, iż takie wiadomości budzą zaciekawienie czytelników, to wzmacniają ich wartość medialną, kładąc nacisk na ich wyjątkowość, co prowadzi oczywiście do przesady, sensacyjności i naddramatyczności"[8]. Co więcej, idealnym dopełnieniem, dla historii przestawionej w takiej konwencji, będzie wykrycie spisku lub nieprawidłowości związanych z pracą organów ścigania, władz państwowych lub innych podmiotów odpowiedzialnych za porządek publiczny i bezpieczeństwo. Interesującym jest fakt, że nie sprzedają się tytuły mówiące o sukcesach kampanii prewencyjnych lub wdrożeniu najnowszych zabezpieczeń technicznych na ulicach polskich miast czy rozbiciu groźnej grupy przestępczej. Sukcesy i pozytywny wizerunek osób lub instytucji dla przeciętnego obywatela nie są niczym interesującym, a wręcz nudnym. Jedynie informacje, które w negatywnym świetle przedstawiają bohatera konkretnego reportażu są w stanie wzbudzić zaciekawienie poszczególnych jednostek, które w ten sposób zyskują szansę na podniesienie własnej samooceny w porównaniu z panem X lub panią Y, którzy na przykład dopuścili się zbrodni.

Co więcej, tak selektywne przekazywanie informacji związanych z funkcjonowaniem systemu bezpieczeństwa, a więc instytucji, mechanizmów, procedur prawnych itd. może przyczynić się do spadku społecznego zaufania wobec wskazanych podmiotów i procedur. Spotęgować owo odczucie może nadreprezentacja negatywnych komunikatów w mass mediach. Społeczeństwo dostaje szczątkowe informacje, tylko i wyłącznie o tzw. chwytliwych i szokujących sprawach. „Społeczeństwo karmione informacjami o groźnych przestępstwach kształtuje swoją opinię na podstawie obrazu malowanego przez media. Wierzy zatem, że często popełnia się zabójstwa (skoro tyle się o nich pisze, to z pewnością są często popełniane), że masowa jest pedofilia, a na co drugim rogu ulicy czyha rozbójnik"[9]. Na tej podstawie rodzą się niepoparte faktami wyobrażenia o skali i strukturze przestępczości w Polsce, a dalej idącym skutkiem jest wygłaszanie populistycznych teorii o potrzebie

---

7 J. Sobczak, *Dziennikarz sprawozdawca sądowy. Dylematy i zasadzki*, [w:], *Media i sądy pro bono et malo. Wzajemne relacje w służbie demokratycznego państwa prawa. Materiały pokonferencyjne*, źródło: http://www.krs.pl/pl/konferencje/p,2 [dostęp: 23.10.2017], s. 17.

8 C. Kulesza, dz. cyt., s. 14.

9 Tamże, s. 14.

surowego karania – skoro tylu w naszym kraju mamy zabójców oraz gwałcicieli. Oczywiście permanentne faszerowanie odbiorców tymi doniesieniami sprawia także, że umacniają oni swoje przekonanie co do bezradności oraz bezczynności władz państwowych, lokalnych oraz służb mundurowych. Jednak jak wskazują statystyki policyjne, „ulubione" przez dziennikarzy przestępstwa przeciwko życiu i zdrowiu oraz wolności seksualnej i obyczajności, w których dominować będzie retoryka dramatu, szoku i niedowierzania stanowią margines przestępstw w Polsce. Na przykład w roku 2014 wszczęto 553 postępowania z art. 148 k.k. (zabójstwo), 2444 z art. 197 k.k. (zgwałcenie) oraz 2156 z art. 200 k.k. (seksualne wykorzystanie małoletniego). Podczas gdy mało intrygujące dla mediów pospolite przestępstwa przeciwko mieniu – stanowią znaczący odsetek przestępstw, np. w roku 2014 wszczęto 144149 postępowań art. 278 k.k. (kradzież), 99957 z art. 279 k.k. (kradzież z włamaniem) oraz 7628 z art. 280 k.k. (rozbój)[10]. Jednak kolosalną różnicę dla dziennikarza stanowi możliwość napisania – „Zabójstwo w Boguchwale. Prokuratura: syn wbił matce trzy noże w plecy"[11], aniżeli o tym, że Kowalskiemu ktoś ukradł stary rower.

Co ciekawe, Dagmara Woźniakowska-Fajst, wskazała, iż aby sprzedać informację związaną z przestępczością, a co za tym idzie z bezpieczeństwem, musi ona posiadać osiem charakterystycznych i niezbędnych cech.

Po pierwsze, natychmiastowość – sprawa musi dotyczyć epizodów, które dopiero co się wydarzyły. Ze względu na ograniczony czas antenowy oraz miejsce w rubryce, dziennikarz nie będzie przytaczał szczegółowych informacji dotyczących początku sprawy, która np. wydarzyła się dziesięć lat temu. Co więcej, tego typu artykuł zmusiłby czytelnika lub widza do refleksji, wspomnień – pewnej formy wysiłku umysłowego, co rzecz jasna nie jest wskazane, ani nie jest celem redaktora. Informacja ma być podana na gorąco i najlepiej bezrefleksyjnie. Dlatego też, w mediach rzadko pojawiają się informacje o przestępstwach białych kołnierzyków – bowiem ciągną się one latami. Jeżeli już się pojawiają, to za sprawą znanych sprawców lub znanych ofiar. Egzemplifikację stanowić może sprawa Amber Gold – gdzie obecnie chyba mało kto wie o co tak naprawdę chodzi? Większość osób będzie natomiast kojarzyło wątek syna Premiera Donalda Tuska[12], czy ciąży, w którą w zakładzie karanym zaszła żona głównego podejrzanego z funkcjonariuszem służby więziennej[13]. Co ciekawe, po wyciszeniu wskazanych powyżej tematów, proces w mediach ożył na nowo za sprawą sędzi Lidii Jedynak, która przewodniczy składowi sędziowskiemu. Pani sędzia została posądzona o powiązania z trójmiejskim deweloperem, który utrzymuje kontakty z jednym ze świadków w toczącym się postępowaniu, po tym jak zrobiono im zdjęcie w trójmiejskim lokalu. Rzecz jasna, dziennikarze nie skupili się na merytoryczności pracy

---

10 *Statystyka Policji*, źródło: http://statystyka.policja.pl/st/kodeks-karny [dostęp: 23.10.2017].

11 A. Janik, *Zabójstwo w Boguchwale. Prokuratura: syn wbił matce trzy noże w plecy*, źródło: http://www.nowiny24.pl/wiadomosci/rzeszow/a/zabojstwo-w-boguchwale-prokuratura-syn-wbil-matce-trzy-noze-w-plecy,9849634/ [dostęp: 23.10.2017].

12 *Michał Tusk wiedział, że pracuje dla oszusta*, źródło: http://www.se.pl/wiadomosci/polska/michal-tusk-wiedzia-ze-pracuje-dla-oszusta_274121.html [dostęp: 24.10.2017]; *Michał, „książątko" Tusk. Tak żyje syn króla Europy*, źródło: http://wpolityce.pl/polityka/218295-michal-ksiazatko-tusk-tak-zyje-syn-krola-europy, [dostęp: 24.10.2017].

13 *Żona szefa Amber Gold urodziła. Ojcem klawisz*, źródło: http://www.fakt.pl/wydarzenia/polska/katarzyna-p-zona-bylego-wlasciciela-amber-gold-urodzila/bc0xpwm [dostęp: 24.10.2017].

sędzi i tego w jaki sposób prowadzi postępowanie – co powinno być przedmiotem ich zainteresowania, bowiem ten aspekt nie byłby intrygujący dla odbiorcy. Szczegółowo natomiast przeanalizowali życie prywatne „bohaterki" doniesień medialnych, a na tej podstawie wysnuli liczne „teorie" w jaki sposób owo prywatne spotkanie może wpłynąć na przebieg sprawy[14].

Po drugie, dramatyzacja – treść, a z pewnością tytuł musi mieć dramatyczny wydźwięk by przyciągnąć odbiorcę. Przykładów w polskiej prasie nie brakuje „Dożywocie dla bestii. To ohydny morderca, przed którym trzeba chronić społeczeństwo"[15], „Szokujące zeznania Kajetana P., chciał zjeść ofiarę jak…" już sam nagłówek jest wystarczająco tajemniczy i wywołujący dreszczyk emocji. Jednak autor artykułu posunął się nieco dalej i w tekście umieścił m.in. następujące sformułowania „Ścigano go po całej Europie, a niezłomny zespół prokuratorów wydusił z niego zeznania, które mrożą krew w żyłach (…) Hannibal z Żoliborza jest zwyrodnialcem. Opowiedział wtedy, że zbrodnia była krokiem do doskonałości"[16].

Po trzecie, personalizacja, która poniekąd powiązana jest z dramatyzacją. Tylko i wyłącznie opisanie tragicznych losów konkretnej ofiary lub szczegółów z życia sprawcy spowoduje, że dana historia wstrząśnie odbiorcami. Spersonalizowane sprawy stają się dla odbiorcy bardziej realne.

Po czwarte, uproszczenia. Wielu dziennikarzy, co jest niezmiernie bulwersujące, podaje suche, bezrefleksyjne informacje. Istotne jest również to, że rzadko kiedy starają się obiektywnie oraz wieloczynnikowo ocenić przyczyny, przebieg i skutki konkretnego zdarzenia. W literaturze przedmiotu wskazuje się wręcz na tzw. „dyżurne czynniki: dzieciobójstwo wyjaśnia się biedą, rozboje bezrobociem, a korupcję – społeczną akceptacją"[17]. W celu obalenia tych mitów wystarczy zapoznać się chociażby z wynikami Polskiego Badania Przestępczości[18].

Po piąte, uwiarygodnienie podanych informacji przez opinie autorytetów. Ten aspekt powinien stanowić walor prezentowanego przez dziennikarza materiału. Wątpliwa jednak jest sytuacja, kiedy autorzy materiału tak dobierają ekspertów by ci jedynie potwierdzili opinie prezentowane przez dziennikarza lub proszą o ustosunkowanie się do danych szczątkowych, a nieraz wyrwanych z kontekstu.

---

14 R. Rosiejka, *Amber Gold: KRS zbada sprawę sędzi po publikacji „Newsweeka"*, źródło: http://wiadomosci.wp.pl/kat,50352,title,Amber-Gold-KRS-zbada-sprawe-sedzi-po-publikacji-Newsweeka,wid,18684756,wiadomosc.html [dostęp: 24.10.2017]; W. Cieśla, Krzymowski M., *Sędzia u „Jaworka*", źródło: http://www.newsweek.pl/polska/bankiet-i-podejrzane-kontakty-afera-z-sedzia-z-procesu-amber-gold,artykuly,403935,1.html [dostęp: 24.10.2017].

15 P. Jędzura, *Dożywocie dla bestii. To ohydny morderca przed, którym trzeba chronić społeczeństwo*, źródło: http://www.gazetalubuska.pl/artykuly-archiwalne/art/7798847,dozywocie-dla-bestii-to-ohydny-morderca-przed-ktorym-trzeba-chronic-spoleczenstwo,id,t.html [dostęp: 24.10.2017].

16 *Szokujące zeznania Kajetana P., chciał zjeść ofiarę jak…*, źródło: http://www.se.pl/wiadomosci/polska/szokujace-zeznania-kajetana-p-chcial-zjesc-ofiare-jak_910669.html [dostęp: 24.10.2017].

17 D. Woźniakowska-Fajst, *Media a przestępczość*, [w:] *Społeczno-polityczne konteksty współczesnej przestępczości w Polsce*, Warszawa 2013, s. 373.

18 A. Siemaszko, *Polskie badanie przestępczości (PBP) 2007–2009: analiza wybranych rezultatów*, [w:] *Archiwum kryminologii,* tom XXXI, Warszawa 2009.

Po szóste i siódme seksualność oraz przemoc. Dlatego też, obiektem zainteresowania mediów stają się sprawy o zgwałcenie, pedofilię lub molestowanie seksualne. Zestawienie niewinnej ofiary z bestialskim i bezwzględnym sprawcom, bez wątpienia poruszy tysiące odbiorców. Z tego też powodu od kilku dni w mediach elektronicznych dominują nagłówki „Kapral Anna. Mobbing i molestowanie w Żandarmerii Wojskowej”[19], „Anna poskarżyła się na molestowanie w wojsku. Co zrobił Macierewicz?”[20].

Po ósme, bliskość, zarówno w ujęciu przestrzennym jak i kulturowym. Kolizja drogowa w małej wiosce będzie żywotnym problemem dla społeczności lokalnej, nie zainteresuje natomiast wydawców programów informacyjnych czołowych stacji czy gazet. Co więcej, dla obywatela naszego państwa, które jest jednolite pod względem: narodowościowym, religijnym i kulturowym kwestie terroryzmu separatystycznego, czy naruszania prawa człowieka w państwach azjatyckich są tak abstrakcyjnymi zjawiskami, że media nie odczuwają potrzeby szczegółowego informowania o tych przestępstwach[21].

Jednak w tym kontekście należy zwrócić uwagę na fenomen terroryzmu religijnego, który bez względu na miejsce zamachu, przebieg, ofiary oraz sprawcę jest tak intrygującym zagadnieniem, że media będą nim „żyły” przez kilka kolejnych dni. Widzowie i słuchacze będą w pierwszej kolejności informowani o najnowszych szczegółach zdarzenia oraz o postępach prowadzonego śledztwa. Co więcej, badania prowadzone przez Mię Bloom, wykazały, że jeżeli sprawcą zamachu terrorystycznego jest kobieta, informacja taka staje się około osiem razy bardziej medialna aniżeli przy analogicznej sytuacji, w której zamachowcem byłby mężczyzna[22].

Konotacje terroryzmu z mediami stanowią odrębny niezmiernie interesujący przedmiot analiz. Ze względu na ograniczone możliwości, w tym miejscu należy tylko zaakcentować charakterystyczną dualność tych powiązań. Z jednej strony media o czym już wspomniano informują o zdarzeniu, zagrożeniu lub skutkach oraz podjętych przez społeczność międzynarodową procedurach zwalczania i zapobiegania. Z drugiej, co istotne media stanowią idealne narzędzie do komunikacji w rękach terrorystów, służące do osiągania zamierzonych przez nich celów. To świetny środek do propagandy, promocji, zbierania funduszy, rekrutowania nowych członków, a co najważniejsze szerzenia strachu. Eksperci z dziedziny bezpieczeństwa coraz częściej stawiają jak najbardziej zasadne pytanie – gdzie znajduje się granica między informowaniem o terroryzmie, a szerzeniem jego idei i czy nie została już dawno przekroczona przez dziennikarzy rządnych sensacji?[23]. To pytanie bez wątpienia

---

19 M. Wyrwał, *Kapral Anna. Mobbing i molestowanie w Żandarmerii Wojskowej*, źródło: http://wiadomosci.onet.pl/tylko-w-onecie/kapral-anna-mobbing-i-molestowanie-w-zandarmerii-wojskowej/bcg2k2z [dostęp: 24.10.2017].

20 *Anna poskarżyła się na molestowanie w wojsku. Co zrobił Macierewicz?*, źródło: http://www.fakt.pl/wydarzenia/polska/anna-poskarzyla-sie-na-molestowanie-w-wojsku-macierewicz-umyl-od-sprawy-rece/nkjj187 [dostęp: 24.10.2017].

21 D. Woźniakowska-Fajst, dz. cyt., s. 372–375.

22 M. Bloom, *Seeing the New Face of Terrorism*, źródło: https://www.youtube.com/watch?v=KOTyVBhpTEM, [dostęp: 24.10.2017].

23 L. Dyczewski, *Terroryzm w mediach: sensacja i spektakl, odpowiedzialność i informacja*, [w:] *Polityka medialna instytucji państwowych w obszarze zagrożeń terrorystycznych. Kwartalnik Biura Bezpieczeństwa Narodowego*, tom 9, s. 117–118.

będzie przedmiotem jeszcze wielu analiz, jednak szanse na uzyskanie jednoznacznej odpowiedzi zdają się być nikłe.

Przytoczone powyżej cechy komunikatów mają sprawić, że staną się one rozchwytywane przez społeczeństwo. Jednak są to elementy noszące znamiona manipulacji informacją. Wiele bowiem z nich w celu dopasowania się do wskazanych wytycznych wyrywanych jest z kontekstu lub nieco ubarwianych. Poprzez zastosowanie takich mechanizmów przeciętny obywatel nieposiadający dodatkowo przygotowania merytorycznego nie będzie w stanie pojąć oraz właściwie zinterpretować podanych informacji. Dzięki takim zabiegom w społeczeństwie utrwalane są pewne schematy myślenia oraz percepcji zdarzeń, a co gorsza stereotypy. Dla porównania warto w tym miejscu wskazać cechy informacji i przekazu tak by był on obiektywny i dawał szansę każdemu obywatelowi na wyrażenie własnej opinii na dany temat.

Po pierwsze, informacja powinna być prawdziwa – a więc dotyczyć zdarzeń, które rzeczywiście się wydarzyły.

Po drugie, dokładność – informacja powinna zawierać szczegółowy opis zdarzenia. Dziennikarz nie może dodawać lub odejmować pewnych treści wedle własnego uznania.

Po trzecie, kontekstowość – należy unikać wyizolowania informacji, powinna być podana w powiązaniu z innymi podobnymi wydarzeniami, osadzona w konkretnych warunkach społecznych lub środowiskowych oraz w oparciu o dotychczasową wiedzę na dany temat.

Po czwarte, informacja musi być wiarygodna – to znaczy bazować na kilku godnych zaufania i udokumentowanych źródłach.

Po piąte, jednoznaczna – dziennikarz powinien podać przyczyny, przebieg, skutki oraz czas, miejsce i osoby biorące udział w zdarzeniu.

Po szóste, informacja powinna być wolna od komentarza, w celu umożliwienia każdemu widzowi, słuchaczowi lub czytelnikowi wypracowania własnego zdania i opinii na dany temat.

Po siódme, zrozumiałość i jasność językowa – nie należy stosować zbyt skomplikowanych i rzadko używanych pojęć, które mogą być niezrozumiałe dla odbiorcy. Co więcej, dziennikarze powinni unikać określeń wartościujących oraz wzbudzających zbędne emocje.

Po ósme, poszanowanie godności osoby ludzkiej i prawa – przekazywane informacje nie mogą godzić w godność osobistą zarówno bohaterów opisywanego zdarzenia jak i odbiorców. Pozyskanie informacji, jej treść oraz przekaz muszą być zgodne z przepisami obowiązującego prawa.

Po dziewiąte, ważność – informacja może wywrzeć bezpośredni wpływ na życie poszczególnych jednostek, grup jak i całych społeczności lokalnych.

Po dziesiąte, przewidywalność – informacje dotyczą zdarzeń, które się wydarzyły lub mogą wydarzyć w najbliższej przyszłości[24].

Jak już wspominano, środki masowego przekazu stanowią nieodzowny element ludzkiej egzystencji i zajmują w niej istotne miejsce. Owa pozycja mediów wynika bez wątpienia z chęci permanentnego dostępu do najświeższych oraz rzetelnych informacji. Nie bez przyczyny XXI wiek określony został mianem – ery informacji, w której dostęp do danych ma ogromną wartość lub nawet można się pokusić o stwierdzenie, że jest bezcenny. Należy

[24] Tamże, s. 123–124.

jednak mieć na uwadze, że media nie tylko informują. Odpowiedzialne są także za realizację trzech innych funkcji: identyfikacji personalnej, integracji oraz rozrywki. Ostatnia z nich nie zostanie poddana analizie, bowiem nie odnosi się do przedmiotu rozważań[25].

Funkcja informacyjna realizowana jest poprzez uczenie się, poszukiwanie rady w sprawach bieżących oraz zaspokojenie ciekawości i ogólnych zainteresowań społeczeństwa[26]. Funkcja informacyjna stanowi zasadniczy element współistnienia mediów i systemu bezpieczeństwa. Programy informacyjne przyczyniają się nie tylko do wzrostu świadomości społecznej dotyczącej potencjalnych zagrożeń, ale również mechanizmów prewencyjnych. Są dla większości obywateli pierwszym źródłem informacji o zmieniających się przepisach prawa oraz społeczno-politycznej sytuacji w kraju i na arenie międzynarodowej. Środki masowego przekazu w XXI wieku stały się efektywnym narzędziem służącym do komunikowania wykorzystywanym między innymi przez policję. To poprzez serwisy informacyjne poszczególnych stacji telewizyjnych jak i radiowych społeczeństwo dowiaduje się o prowadzonych przez tę formację kampaniach mających przyczynić się do zmniejszenia współczynnika przestępczości. Egzemplifikację stanowią takie projekty jak: Krajowa Mapa Zagrożeń Bezpieczeństwa; Kochasz? Powiedz STOP Wariatom Drogowym; Seniorze Nie Daj Się Oszukać![27].

W tym miejscu nie można nie odnieść się także do roli mediów w mechanizmach zarządzania kryzysowego oraz komunikowania w sytuacjach kryzysowych. Jako podstawowe błędy w komunikowaniu w sytuacji kryzysowej wskazuje się: „wprowadzanie opinii publicznej w błąd, brak komunikacji i lekceważenie zagrożenia, rozpoczynanie walki z kryzysem w momencie, w którym zostanie on już ujawniony, obojętne stanowisko na przejawy zagrożenia, traktowanie mediów jak wroga oraz posługiwanie się niezrozumiałym językiem zarówno dla odbiorców komunikatu jak i współpracowników”[28]. Z tego powodu partycypacja środków masowego przekazu jest tak istotna w procedurach zarządzania kryzysowego na każdym jego etapie. Media przede wszystkim dostarczają danych o zbli-

---

25 Powszechnie przyjęło się uważać, że główną funkcją mediów jest informowanie społeczeństwa oraz jego edukacja. Z badań Krajowej Rady Radiofonii i Telewizji, wynika, że największą oglądalnością cieszą się nie programy informacyjne, publicystyczne czy edukacyjne, ale te które mają zapewnić widzom rozrywkę. Dlatego też w roku 2016 najchętniej oglądanymi programami w różnych stacjach telewizyjnych były: transmisje z mistrzostw świata w narciarstwie klasycznym oraz piłce nożnej, teleturnieje np. jaka to melodia, seriale: m jak miłość, na dobre i na złe, programy typu reality show: mali giganci, masterchef, twoja twarz brzmi znajomo. Jedynie Fakty TVN-u znalazły się na jednym z pierwszych miejsc, najchętniej oglądanych programów tej stacji. Inne audycje tego typu w pozostałych stacjach zajmują miejsca daleko poza „podium”. Zob. *Najpopularniejsze audycje w I kwartale 2016 r. Dobowa oglądalność programów – raport*, źródło: http://www.krrit.gov.pl/Data/Files/_public/Portals/0/kontrola/program/tv/kwartalne/najpopularniejsze-audycje-w-i-kw.2016.-dobowa-ogladalnosci-programow.pdf [dostęp: 24.10.2017]. Zob. *Najpopularniejsze audycje w III kwartale 2016 r. Dobowa oglądalność programów – raport*, źródło: http://www.krrit.gov.pl/Data/Files/_public/Portals/0/kontrola/program/tv/kwartalne/najpopularniejsze-audycje-w-iii-kw.2016.-dobowa-ogladalnosci-programow.pdf [dostęp: 24.10.2017].

26 B. Dobek-Ostrowska (red.), *Nauka o komunikowaniu. Podstawowe orientacje teoretyczne*, Wrocław 2001, s. 49.

27 *Działania Policji*, źródło: http://zyjbezpiecznie.policja.pl/zb/aktualnosci [dostęp: 24.10.2017].

28 *Materiały szkoleniowe z tematu Efektywna komunikacja ze szczególnym uwzględnieniem sytuacji kryzysowych*, źródło: https://dsc.kprm.gov.pl/sites/default/files/pliki/47.pdf [dostęp: 24.10.2017].

żającym się żywiole, środkach i krokach jakie należy podjąć by zminimalizować lub zniwelować zagrożenie oraz o przebiegu sytuacji kryzysowej. Monitorują także sytuację po zakończeniu akcji ratowniczej w celu rozpowszechnienia apeli o konkretną pomoc. Poprzez udział mediów na każdym etapie zarządzania kryzysowego społeczeństwo jest świadome jak należy się przygotować do nadchodzącego kryzysu, jak zachować w trakcie jego trwania oraz jakie kroki podjąć po jego zakończeniu. Dobrze poinstruowani obywatele bez wątpienia przyczyniają się do szybszego i efektywnego przeprowadzenia akcji ratunkowej, a co za tym idzie do zminimalizowania negatywnych skutków kryzysu. Ze względu na powyższe środki masowego przekazu, ze szczególnym uwzględnieniem lokalnych mediów zostały wskazane przez ustawodawcę odpowiednio w Ustawie o stanie klęski żywiołowej z 18 kwietnia 2002 r.[29], Ustawie o stanie wyjątkowym z 21 czerwca 2002 r.[30] oraz Ustawie o stanie wojennym z 29 sierpnia 2002 r.[31], jako podmioty, które nieodpłatnie i niezwłocznie zobowiązane są do przekazywania obywatelom treści rozporządzeń oraz zarządzeń dotyczących bieżącej sytuacji kryzysowej.

Funkcja informacyjna bezpośrednio łączy się z funkcją identyfikacji personalnej oraz integracji. Pierwsza z nich odpowiada za przekazywanie i tworzenie pożądanych wzorów zachowań społecznych, wzmacnianie osobistych wartości jak również identyfikację z wartościami innych. Druga zaś stanowi podstawę komunikowania społecznego (konwersacji społecznych), substytut faktycznych kontaktów towarzyskich oraz pomoc w wykonywaniu ról społecznych[32]. Media poprzez angażowanie się we wspomniane już programy prewencyjne czy profilaktyczne kreują społeczną świadomość. Widz, słuchacz lub czytelnik otrzymuje swego rodzaju scenariusz działania, który prowadzi do społecznie pożądanego, a co za tym idzie racjonalnego i świadomego zachowania w konkretnych sytuacjach kryzysowych. Przykład stanowić mogą kampanie dotyczące: udzielania pierwszej pomocy przedmedycznej, zachowania się podczas wystąpienia klęsk żywiołowych, zamieszek oraz postępowania na wypadek stania się ofiarą oszustwa np. metodą na wnuczka lub na policjanta.

Co więcej, środki masowego przekazu poprzez przekazywane informacje o bieżącej sytuacji w kraju, zagranicą oraz o funkcjonowaniu służb odpowiedzialnych za zapewnienie porządku publicznego i bezpieczeństwa dają szansę każdej jednostce na określenie własnego poczucia bezpieczeństwa lub zagrożenia. Należy także podkreślić, że poprzez komunikowanie o potencjalnych lub zaistniałych sytuacjach kryzysowych wzmacniane jest poczucie jedności w społeczeństwie. Wizja prawdopodobnego zagrożenia i krzywdy sprawia, że automatycznie wzmacniane są relacje interpersonalne (prymat dobra zbiorowego nad indywidualnym) oraz niektóre wartości na przykład równość wszystkich ludzi, tolerancja, współczucie, empatia itp.

Reasumując, współistnienie mediów oraz szeroko rozumianego bezpieczeństwa jest zagadnieniem niezmiernie złożonym. Z jednej strony przedmiot rozważań jak i zagadnienia

---

29 *Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*, Dz.U. 2002, nr 62, poz. 558.

30 *Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym*, Dz.U. 2002, nr 113, poz. 985.

31 *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, Dz.U. 2002, nr 156, poz. 1301.

32 B. Dobek-Ostrowska (red.), dz. cyt., s. 49.

pokrewne pojawiają się w każdym serwisie informacyjnym czy gazecie. Co więcej, można pokusić się o stwierdzenie, że w wielu wypadkach stanowią idealny i chwytliwy temat zastępczy gdy na przykład na rodzimej scenie politycznej nie wydarzy się nic godnego uwagi. Mass media w ten sposób stają się dobrym nośnikiem informacji odpowiedzialnym za podwyższanie społecznej świadomości dotyczącej kwestii bezpieczeństwa. Kreują także społecznie pożądane wzorce postaw i zachowań. Z drugiej strony tematyka bezpieczeństwa daje dziennikarzom doskonałą sposobność do manipulowania ludzkimi masami oraz tworzenia „chwytliwych" tytułów nie zawsze zgodnych ze stanem faktycznym. Bez wątpienia realizowane przez media funkcje informacyjna, integracyjna i identyfikacyjna w kontekście bezpieczeństwa są niezmiernie istotne i mogą przynieść wymierne skutki w aspekcie prewencyjnym i profilaktycznym. Jednak główny problem pojawia się na etapie utrwalania pewnych stereotypów wśród niewyedukowanego społeczeństwa. Jedynie skonfrontowanie medialnych doniesień z wiedzą merytoryczną daje szansę na racjonalną i obiektywną analizę oraz ocenę prezentowanych zjawisk i zdarzeń. Co więcej, odrębny wątek, który mógłby się stać przedmiotem kolejnych rozważań stanowi zagadnienie emanowania przemocą przy poruszaniu w mediach kwestii związanych z bezpieczeństwem. Problem ten został zaakcentowany przy omawianiu granicy między informowaniem o terroryzmie, a propagowaniem jego idei. W literaturze przedmiotu istnieje bowiem spór o to czy medialne doniesienia dotyczące zamachów terrorystycznych, drastycznych gwałtów lub innych zbrodni, które często przenoszone są do scenariuszy programów takich jak „*Kryminalni*", „*W-11 Wydział Śledczy*", „*Komisariat*" i wielu innych, przez przypadek nie stają się niechlubnym wzorcem do naśladowania zwłaszcza dla młodzieży? Na chwilę obecną jest to pytanie pozostające bez odpowiedzi i bez wątpienia wymagające dalszych, pogłębionych analiz.

Tytuł w języku angielskim:
THE PHENOMENON OF SECURITY IN THE MEDIA

Bibliografia

Materiały źródłowe

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483.

Ustawa z dania 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz.U. 1999, nr 11, poz. 95.

Ustawa z dnia 26 stycznia 1984 r. prawo prasowe, Dz.U. 1984, nr 5, poz. 24.

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz.U. 2002, nr 62, poz. 558.

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. 2002, nr 113, poz. 985.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. 2002, nr 156, poz. 1301.

Działania Policji, źródło: http://zyjbezpiecznie.policja.pl/zb/aktualnosci [dostęp: 24.10.2017].

Materiały szkoleniowe z tematu Efektywna komunikacja ze szczególnym uwzględnieniem sytuacji kryzysowych, źródło: https://dsc.kprm.gov.pl/sites/default/files/pliki/47.pdf [dostęp: 24.10.2017].

Najpopularniejsze audycje w I kwartale 2016 r. Dobowa oglądalność programów – raport, źródło: http://www.krrit.gov.pl/Data/Files/_public/Portals/0/kontrola/program/tv/kwartalne/najpopularniejsze-audycje-w-i-kw.2016.-dobowa-ogladalnosci-programow.pdf [dostęp: 24.10.2017].

Najpopularniejsze audycje w III kwartale 2016 r. Dobowa oglądalność programów – raport, źródło:http://www.krrit.gov.pl/Data/Files/_public/Portals/0/kontrola/program/tv/kwartalne/najpopularniejsze-audycje-w-iii-kw.2016.-dobowa-ogladalnosci-programow.pdf [dostęp: 24.10.2017].

Sądowe ABC – poradnik dla dziennikarzy, s. 3, źródło: http://www.krs.pl/pl/rzecznik-prasowy/zbior-dobrych-praktyk/p,1/3717,sadowe-abc-poradnik-dla-dziennikarzy [dostęp: 23.10.2017].

Sobczak J., *Dziennikarz sprawozdawca sądowy. Dylematy i zasadzki*, s. 17, [w:], *Media i sądy pro bono et malo. Wzajemne relacje w służbie demokratycznego państwa prawa. Materiały pokonferencyjne*, źródło: http://www.krs.pl/pl/konferencje/p,2 [dostęp: 23.10.2017].

Statystyka Policji, źródło: http://statystyka.policja.pl/st/kodeks-karny [dostęp: 23.10.2017].

Publikacje zwarte

Dobek-Ostrowska B. (red.), *Nauka o komunikowaniu. Podstawowe orientacje teoretyczne*, Wrocław 2001.

Kulesza C., *System wymiaru sprawiedliwości a media*, Białystok 2009.

Artykuły

Anna poskarżyła się na molestowanie w wojsku. Co zrobił Macierewicz?, źródło: http://www.fakt.pl/wydarzenia/polska/anna-poskarzyla-sie-na-molestowanie-w-wojsku-macierewicz-umyl-od-sprawy-rece/nkjj187 [dostęp: 24.10.2017].

Brzeziński M., *Rodzaje bezpieczeństwa państwa*, [w:] Sulowski S., Brzeziński M., (red.), *Bezpieczeństwo wewnętrzne państwa wybrane zagadnienia*, Warszawa 2009.

Cieśla W., Krzymowski M., *Sędzia u „Jaworka*", źródło: http://www.newsweek.pl/polska/bankiet-i-podejrzane-kontakty-afera-z-sedzia-z-procesu-amber-gold,artykuly,403935,1.html [dostęp: 24.10.2017].

Dyczewski L., *Terroryzm w mediach: sensacja i spektakl, odpowiedzialność i informacja*, [w:] *Polityka medialna instytucji państwowych w obszarze zagrożeń terrorystycznych. Kwartalnik Biura Bezpieczeństwa Narodowego*, tom 9, s. 117–118.

Janik A., *Zabójstwo w Boguchwale. Prokuratura: syn wbił matce trzy noże w plecy*, źródło: http://www.nowiny24.pl/wiadomosci/rzeszow/a/zabojstwo-w-boguchwale-prokuratura-syn-wbil-matce-trzy-noze-w-plecy,9849634/ [dostęp: 23.10.2017].

Jędzura P., *Dożywocie dla bestii. To ohydny morderca przed, którym trzeba chronić społeczeństwo*, źródło: http://www.gazetalubuska.pl/artykuly-archiwalne/art/7798847,dozywocie-dla-bestii-to-ohydny-morderca-przed-ktorym-trzeba-chronic-spoleczenstwo,id,t.html [dostęp: 24.10.2017].

Michał, „książątko" Tusk. Tak żyje syn króla Europy, źródło: http://wpolityce.pl/polityka/218295-michal-ksiazatko-tusk-tak-zyje-syn-krola-europy [dostęp: 24.10.2017].

Michał Tusk wiedział, że pracuje dla oszusta, źródło: http://www.se.pl/wiadomosci/polska/michal-tusk-wiedzia-ze-pracuje-dla-oszusta_274121.html [dostęp: 24.10.2017].

Rosiejka R., *Amber Gold: KRS zbada sprawę sędzi po publikacji „Newsweeka"*, źródło: http://wiadomosci.wp.pl/kat,50352,title,Amber-Gold-KRS-zbada-sprawe-sedzi-po-publikacji-Newsweeka,wid,18684756,wiadomosc.html [dostęp: 24.10.2017].

Siemaszko A., *Polskie badanie przestępczości (PBP) 2007–2009: analiza wybranych rezultatów*, [w:] *Archiwum kryminologii*, tom XXXI, Warszawa 2009.

Szokujące zeznania Kajetana P., chciał zjeść ofiarę jak…, źródło: http://www.se.pl/wiadomosci/polska/szokujace-zeznania-kajetana-p-chcial-zjesc-ofiare-jak_910669.html [dostęp: 24.10.2017].

Woźniakowska-Fajst D., *Media a przestępczość*, [w:] *Społeczno-polityczne konteksty współczesnej przestępczości w Polsce*, Warszawa 2013.

Wyrwał M., *Kapral Anna. Mobbing i molestowanie w Żandarmerii Wojskowej*, źródło: http://wiadomosci.onet.pl/tylko-w-onecie/kapral-anna-mobbing-i-molestowanie-w-zandarmerii-wojskowej/bcg2k2z [dostęp: 24.10.2017].

Żona szefa Amber Gold urodziła. Ojcem klawisz, źródło: http://www.fakt.pl/wydarzenia/polska/katarzyna-p-zona-bylego-wlasciciela-amber-gold-urodzila/bc0xpwm [dostęp: 24.10.2017].

Źródła internetowe

Bloom M., *Seeing the New Face of Terrorism*, źródło: https://www.youtube.com/watch?v=KOTyVBhpTEM, [dostęp: 24.10.2017].

TAMAR LORTKIPHANIDZE*

KOREAŃSKA REPUBLIKA LUDOWO-DEMOKRATYCZNA – MOCARSTWO ATOMOWE?

Abstrakt

W niniejszym artykule omówiono problem północnokoreańskiego programu nuklearnego i opisano motywy i genezę dążenia Korei Północnej do zdobycia broni nuklearnej. Rozwój programu nuklearnego Korei Północnej od wielu lat stanowi zagrożenie nie tylko dla bezpieczeństwa regionu Azji Wschodniej, ale również dla pokoju na całym świecie. Społeczność międzynarodowa do dziś próbuje powstrzymać władze północnokoreańskie przed zwiększeniem skali zdolności nuklearnych. W artykule dokonano analizy kryzysu północnokoreańskiego od początku programu nuklearnego i omówiono możliwe próby jego rozwiązania.

Słowa kluczowe: Korea Północna, program nuklearny, broń jądrowa, nieproliferacja.

Postępy programu nuklearnego i rakietowego Koreańskiej Republiki Ludowo-Demokratycznej destabilizują sytuację w regionie Azji Pacyfiku. Kolejne testy rakietowe i nuklearne Korei Północnej bezpośrednio zagrażają bezpieczeństwu nie tylko regionu, zaangażowanych mocarstw, ale również całego świata. Mimo tego, iż konflikt ma jak na razie wymiar retoryczny, kryzys w relacjach reżimu północnokoreńskiego z Zachodem narasta. Jakie zagrożenie reprezentuje Korea Północna wobec świata? Korea Północna to nieprzewidywalny gracz na arenie międzynarodowej. Strategia prowokacji i tzw. szantażu nuklearnego jest jednym ze sposobów przyciągnięcia uwagi społeczności międzynarodo-

* Tamar Lortkiphanidze – absolwentka studiów licencjackich i magisterskich kierunku stosunki międzynarodowe (specjalizacja: dyplomacja współczesna) na UW. Absolwentka studiów licencjackich i magisterskich kierunku zdrowie publiczne zarządzanie w ochronie zdrowia) na Warszawskim Uniwersytecie Medycznym. Obecnie doktorantka (II rok) na Wydziale Nauk Politycznych i Studiów Międzynarodowych (nauki o bezpieczeństwie). Rozprawę doktorską przygotowuje o geopolityce Kaukazu Południowego. Interesuje się obszarem poradzieckim, szczególnie Rosją oraz krajami Partnerstwa Wschodniego. Wśród zainteresowań badawczych szczególne miejsce zajmuje również kontynent europejski oraz region Bliskiego i Dalekiego Wschodu. Kontakt e-mail: tamarlortkiphanidze@gmail.com

wej. Ale warto zastanowić się, czy reżim północnokoreański zdecyduje się na aktywną politykę nuklearną w konflikcie ze Stanami Zjednoczonymi i z azjatyckimi sojusznikami USA? Czy któraś ze stron podejmie decyzję o rozpoczęciu konfliktu zbrojnego? Analizując historię stosunków amerykańsko-północnokoreańskich, można stwierdzić, że do tej pory po okresach zaostrzenia retoryki nie dochodziło do konfliktów zbrojnych. Analizując kryzys północnokoreański, warto przyjrzeć się historii programu nuklearnego Koreańskiej Republiki Ludowo-Demokratycznej i zobaczyć kiedy i jak to się zaczęło.

Północnokoreański program nuklearny został zapoczątkowany w 1952 roku pod wpływem Związku Radzieckiego. Koreańska Republika Ludowo-Demokratyczna uzyskała pierwszy reaktor atomowy w darze od Związku Radzieckiego. Już w 1962 roku Korea Północna stworzyła swój własny Instytut Energii Atomowej. Istotną przyczyną zainteresowania się bronią nuklearną przez Koreę Północną był atak atomowy na Hiroszimę i Nagasaki. Po wojnie koreańskiej, kiedy Amerykanie rozmieścili głowice atomowe w Korei Południowej, władze Korei Północnej uświadomiły sobie, że gwarancję bezpieczeństwa dla kraju stanowi broń nuklearna. Pod naciskiem Związku Radzieckiego Korea Północna przystąpiła do traktatu o nieproliferacji broni jądrowej w 1985 roku i ujawniła Międzynarodowej Agencji Energii Atomowej fakt istnienia instalacji atomowych w Jongbion. Po wycofaniu amerykańskiej broni atomowej z Korei Południowej w 1992 roku, Korea Południowa zawarła z Północną traktat o ogłoszeniu Półwyspu Koreańskiego strefą wolną od broni jądrowej. Mimo bycia stroną układu o nieproliferacji broni nuklearnej, Korea Północna w 1992 roku, zawarła z Międzynarodową Agencją Energii Atomowej porozumienie o zabezpieczeniach. Zgodnie z deklaracją, Korea Północna posiadała siedem ośrodków atomowych i około 90 gram plutonu[1].

W 1992 roku Korea Północna ujawniła stan posiadanych materiałów rozszczepialnych. Inspektorzy Międzynarodowej Agencji Energii Atomowej stwierdzili, że Korea Północna pozyskała więcej materiału rozszczepialnego, niż zadeklarowała. Z 90 gramów zadeklarowanego plutonu, istnienie 60 gramów zostało potwierdzone przez agencję, natomiast oddzielenie pozostałych 30 gram według przedstawicieli Korei Północnej zakończyło się niepowodzeniem, więc ta część plutonu znajdowała się na składowisku odpadów radioaktywnych.

Pod koniec sierpnia 1992 roku Międzynarodowej Agencji Energii Atomowej przeprowadziła kolejną inspekcję. W związku z istniejącymi rozbieżnościami, ówczesny dyrektor generalny Międzynarodowej Agencji Energii Atomowej podjął decyzję o przeprowadzeniu specjalnej inspekcji, na co Koreańczycy jednak nie wyrazili zgody. Koreańczycy nawet grozili wystąpieniem z układu o nieproliferacji. Podczas spotkania zarządu Międzynarodowej Agencji Energii Atomowej w sprawie Koreańskiej Republiki Ludowo-Demokratycznej, przedstawiciele agencji po raz pierwszy w historii istnienia tej instytucji podzielili się informacją, pochodzącą od wywiadu państwa członkowskiego – od Stanów Zjednoczonych. Pojawiła się informacja o współpracy Korei Północnej z Pakistanem i Iranem w sprawie rozwijania programu budowy broni atomowej[2].

[1] P. Lipold, *Zagrożenie terrorem nuklearnym w polityce zagranicznej Iranu i Korei Północnej*, Wrocław 2012, s. 138.

[2] M. Elbaradei, *The Age of Deception: Nuclear Diplomacy in Treacherous Times*, London 2011, s. 49–50.

Napięcie między Koreańską Republiką Ludowo-Demokratyczną a Międzynarodową Agencją Energii Atomowej trwało do 1994 roku. Latem 1994 roku między Stanami Zjednoczonymi oraz Koreą Północną doszło do zawarcia porozumienia, na podstawie którego Korea Północna miała wstrzymać program nuklearny w zamian za dostarczenie jej dwóch reaktorów lekkowodnych i pokrycie zapotrzebowania na energię. Utworzono Organizację Rozwoju Energetycznego Półwyspu Koreańskiego – KEDO[3]. Korea Północna zdecydowała się nie wycofywać się z traktatu o nieproliferacji i zobowiązała się do wznowienia swojego uczestnictwa w NPT[4]. Uprawnienia Międzynarodowej Agencji Energii Atomowej zostały natomiast ograniczone. Agencja miała jedynie monitorować proces wyłączenia z użytku ośrodków atomowych w Jongbjon. Koreańczycy, z powodu opóźnienia dostarczenia dwóch lekkowodnych reaktorów energetycznych, jednak nie wstrzymywali programu nuklearnego[5]. Stosunki między Stanami Zjednoczonymi a Koreą Północną zaczęły się poprawiać, o czym może świadczyć wizyta ówczesnej sekretarz stanu USA Madeleine Albright w Korei Północnej[6]. Stosunki między tymi krajami pogorszyły się po dojściu do władzy G.W. Busha, który w 2002 roku Koreę Północną zaliczył do „osi zła". Ówczesny asystent sekretarza stanu ds. Azji Wschodniej i Pacyfiku, James Kelly, w swoim raporcie zarzucił Korei Północnej prowadzenie tajnego programu wzbogacania uranu. Stany Zjednoczone zażądały przeprowadzenia inspekcji północnokoreańskiego programu wzbogacania uranu. Zawieszono dostawy mazutu do Korei Północnej za pośrednictwem instytucji KEDO[7].

W odpowiedzi na ostrą politykę Zachodu, Korea Północna zerwała porozumienie i zaczęła ponownie rozwijać program nuklearny w reaktorze w Jongbjon. Władze Korei Północnej zagroziły również wycofaniem się z traktatu o nieproliferacji broni nuklearnej i niewpuszczeniem inspektorów Międzynarodowej Agencji Energii Atomowej do kraju. Sytuacja znacznie się pogorszyła – rząd koreański zażądał od agencji usunięcia plomb i sprzętu monitorującego z ośrodka w Jongbjon. Później dyrektor generalny Departamentu Energii Atomowej Korei Północnej zażądał wycofania inspektorów Międzynarodowej Agencji Energii Atomowej. Zarząd agencji potępił działania Korei Północnej i zażądał przywrócenia monitoringu programu nuklearnego w Korei. W odpowiedzi na to, 10 stycznia 2003 roku, Korea Północna ogłosiła wycofanie się z traktatu o nieproliferacji broni. Koreańska Republika Ludowo-Demokratyczna wypowiedziała również traktat o strefie bezatomowej na Półwyspie Koreańskim. W związku z ówczesną napiętą sytuacją w Iraku, Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych nie podjęła stosownych kro-

---

3 KEDO – Organizację Rozwoju Energetycznego Półwyspu Koreańskiego utworzono w 1995 roku. Stany Zjednoczone, Japonia oraz Korea Południowa w ramach tej instytucji zobowiązały się wybudować obiecane lekkowodne reaktory energetyczne. Przed uruchomieniem tych reaktorów, te kraje miały dostarczać Korei Północnej 500 tysięcy metrów sześciennych ciężkiego oleju opałowego rocznie.

4 NPT – Układ o nierozprzestrzenianiu broni jądrowej.

5 *Treaties and Regimes*, źródło: http://www.nti.org/treaties-and-regimes/us-dprk-agreed-framework/ [dostęp: 5.10.2017].

6 *Albright Greeted With a Fanfare by North Korean*, źródło: http://www.nytimes.com/2000/10/24/world/albright-greeted-with-a-fanfare-by-north-korea.html?pagewanted=all [dostęp: 5.10.2017].

7 http://www.armscontrol.org/print/1253 [dostęp: 5.10.2017].

ków i nie uchwaliła żadnej rezolucji w tej sprawie. Społeczność międzynarodowa nawet nie potępiła zachowania Korei Północnej[8].

W celu uregulowania kryzysu nuklearnego rozmowy od sierpnia 2003 roku prowadzono w formacie spotkań sześciostronnych (Chińska Republika Ludowa, Japonia, Korea Południowa, Rosja, Stany Zjednoczone oraz Korea Północna). W 2005 roku udało się przełamać impas: wspólne oświadczenie sześciu negocjatorów zawierało zgodę Koreańskiej Republiki Ludowo-Demokratycznej na zaprzestanie prowadzenia programu budowy broni nuklearnej. Korea Północna zobowiązała się również do ponownego podpisania traktatu o nieproliferacji broni jądrowej i do wydania zezwolenia na inspekcje Międzynarodowej Agencji Energii Atomowej. Warto podkreślić, że Korea Północna zgodziła się na te posunięcia w zamian za pomoc energetyczną. Ten chwilowy sukces został zakończony po zamrożeniu przez Departament Skarbu Stanów Zjednoczonych północnokoreańskich funduszy w Banco Delta Asia w Makau pod zarzutem, że miały niby związek z praniem brudnych pieniędzy[9].

W odpowiedzi na to 9 października 2006 roku Korea Północna przeprowadziła pierwszą próbę nuklearną, co oznaczało, że Koreańska Republika Ludowo-Demokratyczna dołączyła do grona państw posiadających broń jądrową. Do dnia dzisiejszego potencjał nuklearny tego kraju spełnia wiele funkcji zarówno w polityce wewnętrznej, jak i zewnętrznej – podkreśla nie tylko rozwój naukowy i technologiczny, ale również prestiż tego kraju. Od tamtego czasu władze północnokoreańskie używają program nuklearny jako kartę przetargową do uzyskania pomocy zagranicznej. Reżim północnokoreański do dnia dzisiejszego jest przekonany, że broń nuklearna jest najlepszym środkiem odstraszania wrogo nastawionych państw.

Rada Bezpieczeństwa ONZ potępiła test nuklearny i nałożyła sankcje na Koreę Północną. Społeczność międzynarodowa stała przed wyzwaniem rozprzestrzeniania się broni masowego rażenia, więc w celu rozładowania napięcia Stany Zjednoczone udostępniły Koreańczykom zamrożone fundusze. W lutym 2007 roku po otrzymaniu pomocy humanitarnej rząd Korei Północnej zgodził się na zaprzestanie rozwoju programu nuklearnego w Jongbjon i na wpuszczenie inspektorów Międzynarodowej Agencji Energii Atomowej do kraju. Co ciekawe, w drugiej połowie 2007 roku inspektorzy agencji potwierdzili zamknięcie ośrodków jądrowych w Korei Północnej[10].

W związku z tym, iż na podstawie wspólnego porozumienia to Stany Zjednoczone prowadziły demontaż instalacji nuklearnych w Korei Północnej, status Międzynarodowej Agencji Energii Atomowej był niejasny. W związku z tym, że Korea Północna wycofała się z traktatu o nieproliferacji broni jądrowej, ten kraj już nie był zobowiązany do przestrzegania zobowiązań układu. Mimo przełamania impasu między Zachodem a Koreańską Republiką Ludowo-Demokratyczną, ten kraj wciąż znajdywał się na liście państw sponsorujących terroryzm, więc w październiku 2008 roku Korea Północna zakazała inspektorom Międzynarodowej Agencji Energii monitorowania prac w ośrodku nuklearnym w Jongbjon. W odpowiedzi na to, w celu rozładowania sytuacji, Stany Zjednoczone usunęły Koreę Pół-

8 M. Elbaradei, dz. cyt., s. 98–100.

9 *Press Releases*, źródło: https://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx [dostęp: 7.10.2017].

10 *Factsheets*, źródło: https://www.armscontrol.org/factsheets/dprkchron [dostęp: 7.10.2017].

nocną z listy państw „osi zła". Następnego dnia inspektorzy agencji powrócili do Korei Północnej[11].

W kwietniu 2009 roku Korea Północna wystrzeliła satelitę. Rada Bezpieczeństwa ONZ potępiła Koreę za przeprowadzenie testu rakietowego pocisku balistycznego dalekiego zasięgu. W kwietniu 2009 roku po zawieszeniu negocjacji, reżim północnokoreański podjął decyzję o zaprzestaniu inspekcji Międzynarodowej Agencji Energii Atomowej. 25 maja 2009 roku Korea Północna przeprowadziła drugą próbę nuklearną. Ujawniono również północnokoreański program wzbogacania uranu, o co podejrzewano ten kraj od dawna. W trakcie negocjacji w cyklu spotkań sześciostronnych Korea Północna stosowała strategię otwartości na dialog i deklarowała gotowość do ustępstw, ale następnie nie wypełniała przyjętych wcześniej zobowiązań i uciekała do prowokacji i eskalacji napięć. Przykładem takiej polityki było przeprowadzenie dwóch prób jądrowych[12].

Co prawda oficjalnych danych na temat programu nuklearnego Korei Północnej wciąż nie ma, ale w drugiej połowie 2010 roku Korea Północna ujawniła, że osiągnęła zdolność wzbogacania uranu. Korea Północna rozwinęła współpracę z Syrią i Iranem, polegającą na sprzedaży materiałów i technologii nuklearnych, a także rakietowych. Na początku 2012 roku ponownie doszło do ocieplenia relacji na linii Zachód-Korea Północna – w zamian za pomoc humanitarną od Zachodu, w lutym 2012 roku Korea Północna zgodziła się zaprzestać rozwoju programu nuklearnego i wzbogacania uranu. Po wystrzeleniu rakiety dalekiego zasięgu w kwietniu 2012 roku, stosunki z Zachodem zaczęły ponownie się pogarszać.

W lutym 2013 roku została przeprowadzona kolejna próba atomowa. Dowodziło tego odnotowanie wstrząsów sejsmicznych około 5 stopni w skali Richtera w północnej części Korei Północnej. Dopiero później władze północnokoreańskie oficjalnie się przyznały do przeprowadzenia próby nuklearnej[13]. Warto zaznaczyć, że reaktor w Jongbjon został ponownie uruchomiony w 2013 roku. We wrześniu 2015 w mediach koreańskich pojawiła się informacja, że podejmuje się działania w celu podnoszenia jakości i zwiększenia liczby instalacji nuklearnych w kraju[14].

6 stycznia 2016 roku Korea Północna przeprowadziła czwartą próbę nuklearną. Po zarejestrowaniu wstrząsów sejsmicznych w Korei Północnej przez Zachód, ten kraj oświadczył, że przeprowadził udaną próbę bomby wodorowej, co wywołało sceptyczne reakcje ekspertów zachodnich[15]. Społeczność międzynarodowa wątpiła, by Korea Północna poczyniła takie postępy, ponieważ bomba wodorowa jest groźniejszą i potężniejszą bronią[16].

---

11 *Korea*, źródło: http://www.theguardian.com/korea/subsectionmenu/0,,854619,00.html%20 [dostęp: 7.10.2017].

12 Ł. Kulesa, *Perspektywy zakończenia północnokoreańskiego programu jądrowego*, Biuletyn „PISM", nr 10 (424), z 22 lutego 2007 r.

13 *North Korea Nuclear Test Earthquake*, źródło: http://www.theguardian.com/world/2013/feb/12/north-korea-nuclear-test-earthquake [dostęp: 10.10.2017].

14 *North Korea*, źródło: http://www.nti.org/country-profiles/north-korea/ [dostęp: 10.10.2017].

15 *Nuclear proliferation case studies*, źródło: http://www.world-nuclear.org/information-library/safety-and-security/non-proliferation/appendices/nuclear-proliferation-case-studies.aspx [dostęp: 10.10.2017].

16 *North Korea Major Announcement artificial Earthquake. Nuclear Test site live*, źródło: http://www.theguardian.com/world/live/2016/jan/06/north-korea-major-announcement-artificial-earthquake-nuclear-test-site-live [dostęp: 10.10.2017].

7 lutego 2016 roku Korea Północna wystrzeliła rakietę dalekiego zasięgu. Rząd koreański poinformował, że umieszczono w ten sposób satelitę na orbicie. Korea Północna ponownie złamała rezolucje Rady Bezpieczeństwa ONZ. Jak widać, możliwość uzyskania porozumienia z Koreą Północną przekreślały próby jądrowe przeprowadzone w latach 2006, 2009, 2013 i 2016 w czasie trwania rozmów z reżimem północnokoreańskim.

Media od dawna wieszczą o nieuchronności wojny Korei Północnej z Zachodem. Warto pamiętać, że Korea Północna mimo tego, że jest jednym z najbiedniejszych państw, z drugiej strony jest krajem najbardziej zmilitaryzowanym. Powszechny pobór wojskowy dotyczy zarówno mężczyzn, jak i kobiet. Mówi się, że armia północnokoreańska jest czwartą pod względem liczebności armią świata, czyli zaraz po Chinach, USA i Indiach[17].

W bieżącym roku kryzys północnokoreański jeszcze bardziej się zaostrzył. W 2017 roku Korea Północna przeprowadziła już 15 prób rakiet balistycznych. Trzeba pamiętać, że na początku 2017 roku Stany Zjednoczone wysłały dodatkowe siły zbrojne na Półwysep Koreański. 4 lipca bieżącego roku Korea Północna przeprowadziła pierwszy test międzykontynentalnej rakiety balistycznej, która wylądowała w Morzu Japońskim. Kilka tygodni później, w lipcu 2017 roku przeprowadzono test rakiety, która może dolecieć do Alaski. Warto podkreślić, że reżim północnokoreański użył pocisków Hwasong-14, które można uzbroić w głowicę nuklearną i mają dosyć duży zasięg (taki pocisk może dosięgnąć wybrzeży Stanów Zjednoczonych).

We wrześniu bieżącego roku Korea Północna podczas próby nuklearnej użyła bombę wodorową – tak jak podały media północnokoreańskie, ta bomba wodorowa jest przeznaczona do montażu na międzykontynentalnych pociskach balistycznych. Takie zachowanie reżimu północnokoreańskiego świadczy o dużym postępie w dążeniu do uzyskania przez Północną Koreę międzykontynentalnego pocisku z głowicą nuklearną, która mogłaby dosięgnąć Stanów Zjednoczonych.

Próby nuklearne przeprowadzone w lipcu i we wrześniu 2017 roku wywołały ostrą reakcję nie tylko Stanów Zjednoczonych, ale również innych ważnych graczy – między innymi Rosji i Chin, które nie przestrzegały międzynarodowych sankcji w stosunku do reżimu północnokoreańskiego. Ryzyko wybuchu konfliktu zbrojnego w regionie Azji Wschodniej jest bardzo duże, ale mimo to aktorzyna scenie międzynarodowej na razie ograniczają się do zaostrzenia retoryki.

Warto pamiętać, że od czasów objęcia rządów przez Kim Dzong Una w 2011 roku Koreańska Republika Ludowo-Demokratyczna dokonała wielkiego postępu w pracach nad rakietami dalekiego zasięgu. Po przeprowadzeniu próby nuklearnej we wrześniu 2017 roku, reżim północnokoreański pokazał, że ma zdolność do wytworzenia rakiet o zasięgu międzykontynentalnym. Mimo tego, że wiedza na temat zdolności militarnej Koreańskiej Republiki Ludowo-Demokratycznej jest niepewna, szacuje się, że obecnie Korea Północna dysponuje około 30–60 głowicami jądrowymi.

Warto podkreślić, że broń jądrowa ułatwia przetrwanie reżimu politycznego Korei Północnej. Taka broń stanowi instrument wzmacniający pozycję negocjacyjną tego kraju. Koreańska Republika Ludowo-Demokratyczna jako jedyna do tej pory jednostronnie ze

[17] W. Dziak, K. Sajewski, *Korea Północna-wewnętrzne wektory trwania*, Warszawa 2016, s. 137.

skutkiem natychmiastowym (bez zastosowania trzymiesięcznego okresu wypowiedzenia) wystąpiła z reżimu nieproliferacji[18].

Nałożenie sankcji przez Radę Bezpieczeństwa ONZ nie przynosiło rezultatu – Korea Północna wciąż grozi zwiększeniem potencjału nuklearnego. Presja społeczności międzynarodowej nie skłania reżimu północnokoreańskiego do denuklearyzacji. Kryzys północnokoreański ukazał słabości społeczności międzynarodowej. Rada Bezpieczeństwa ONZ nie potrafi zaradzić temu kryzysowi. Korea Północna raczek nigdy nie zgodzi się na całkowitą denuklearyzację[19].

Analizując dotychczasowe relacje Federacji Rosyjskiej i Chińskiej Republiki Ludowej z Koreą Północną, łatwo zauważyć, że te dwa państwa będące stałymi członkami Rady Bezpieczeństwa ONZ nie przestrzegają nałożonych międzynarodowych sankcji, o czym świadczy wielkość obrotów handlowych z Koreańską Republiką Ludowo-Demokratyczną (wielkość obrotów handlowych ChRL z KRLD to 5 mld dolarów, a Rosji – 100 mln dolarów)[20]. Taka polityka dwóch mocarstw wobec Korei Północnej pozwala Koreańskiej Republice Ludowo-Demokratycznej ignorować międzynarodowe sankcje oraz kontynuować i rozwijać program nuklearny.

Zagadnienie programu nuklearnego Korei Północnej od lat pozostaje problemem nierozwiązanym. Perspektywy jego pozytywnego rozwiązania kończą się na etapie deklaracji przedstawicieli państw zachodnich. Ograniczony dostęp do wiarygodnych informacji o sytuacji wewnętrznej w Korei Północnej utrudnia przewidywanie przyszłości tego państwa. Wobec wyżej wymienionych szans na denuklearyzację Korei Północnej należy dążyć do zahamowania rozwoju jej programu nuklearnego.

W marcu bieżącego roku, minister spraw zagranicznych Chińskiej Republiki Ludowej zaproponował tzw. plan podwójnego zamrożenia, zgodnie z którym Korea Północna miałaby zrezygnować z testów nuklearnych i rakietowych w zamian za rezygnację przez Koreę Południową i USA z instalacji i ćwiczeń wojskowych na półwyspie koreańskim. Czy istnieje szansa przywrócenia formatu rozmów tzw. szóstki[21]? Raczej nie, ponieważ reżim północnokoreański nigdy nie zgodzi się na całkowitą denuklearyzację. W związku z tym, że północnokoreańska strategia nuklearna nie opiera się na wiarygodnym arsenale, stwarza możliwość ciągłego manipulowania i blefowania. Ale w razie poważnego kryzysu na Półwyspie Koreańskim zwiększa się ryzyko użycia broni nuklearnej.

Kryzys północnokoreański zaostrzył się we wrześniu bieżącego roku. Korea Północna osiągnęła zdolności militarne, które najbardziej zagrażają bezpieczeństwu Stanów Zjednoczonych. W związku z tym pytanie, jak Stany Zjednoczone chcą skłonić reżim północnokoreański do rozwiązania tego problemu – zdecydują się na użycie siły zbrojnej, czy przełożą wszystkich starań do uregulowania kryzysu w sposób pokojowy (negocjacje, inne środki

---

18 B.G. Jun, *Cyclical Patterns of North Korean Nuclear Negotiations: 1987–2012*, [w:] *Assessment of the Nuclear Programs of Iran and North Korea*, New York 2013, s. 59.

19 J. Durkalec, *Perspektywy denuklearyzacji Korei Północnej*, Biuletyn „PISM", nr 16 (881), z 10 lutego 2012 r.

20 A. Legucka, *Rosja wobec kryzysu północnokoreańskiego*, Biuletyn „PISM", nr 92 (1534), z 3 października 2017 r.

21 Szóstka – negocjacje prowadzone nad programem nuklearnym Korei Północnej przez ChRL, Japonię, Koreę Południową, Rosję, USA i Koreę Północną w latach 2003–2009.

dyplomatyczne)? Zmiana reżimu Kimów w Korei Północnej lub akceptacja stanu obecnego – czyli dążenia Korei Północnej do uzyskania pełnych zdolności nuklearnych jest raczej mało prawdopodobne i mogłoby przynieść ze sobą bardzo niebezpieczne skutki.

Po przeanalizowaniu polityki Koreańskiej Republiki Ludowo-Demokratycznej jedna rzecz jest pewna – reżim północnokoreański traktuje osiągnięcie zdolności militarnych jako zabezpieczenie władzy, więc mimo sankcji gospodarczych i izolacji międzynarodowej, Korea Północna będzie dalej rozwijać program nuklearny.

Mimo tego, iż elita amerykańska uważa, że wojna z Koreą Północną jest nie do uniknięcia, raczej żadna strona nie jest zainteresowana rozpoczęciem konfliktu zbrojnego – chodzi o to, że takie rozwiązanie nie opłacałoby się żadnej ze stron. Wojna zakończyłaby się klęską Koreańskiej Republiki Ludowo-Demokratycznej, ale jest obarczona dużym ryzykiem ofiar śmiertelnych w regionie Azji Wschodniej i może nawet w Stanach Zjednoczonych.

Podsumowując, jedynym sposobem wywarcia skutecznego nacisku na reżim północnokoreański jest zgodność społeczności międzynarodowej, w szczególności wszystkich stałych członków Rady Bezpieczeństwa ONZ i rzeczywiste egzekwowanie sankcji, czyli odcięcie wszystkich źródeł finansowania programu nuklearnego Korei Północnej. W tym celu potrzebna jest ścisła współpraca między takimi mocarstwami jak Stany Zjednoczone, Federacja Rosyjska i Chińska Republika Ludowa.

Co do możliwości zawarcia efektywnego porozumienia między Koreą Północną a państwami zachodnimi, większość ekspertów uważa, że państwa zaangażowane w uregulowanie kryzysu północnokoreańskiego muszą dojść do kompromisu – w zamian za zahamowanie, lub nawet za zaprzestanie północnokoreańskiego programu nuklearnego Stany Zjednoczone też muszą pójść na ustępstwa i muszą ograniczyć aktywność militarną nie tylko w Korei Południowej, ale w całym regionie. Co jest raczej trudne do wyobrażenia, ponieważ Stany Zjednoczone raczej nie pójdą na większe ustępstwa, co będzie skutkować jeszcze większym wsparciem dla reżimu północnokoreańskiego udzielonego przez Federację Rosyjską i ChRL.

Tytuł w języku angielskim:
NORTH KOREA AS A NUCLEAR EMPIRE?

Bibliografia

Publikacje zwarte

Dziak W., Sajewski K., *Korea Północna-wewnętrzne wektory trwania*, Warszawa 2016.

Elbaradei M., *The Age of Deception: Nuclear Diplomacy in Treacherous Times*, London 2011, s. 49–50.

Lipold P., *Zagrożenie terrorem nuklearnym w polityce zagranicznej Iranu i Korei Północnej*, Wrocław 2012.

Artykuły

Albright Greeted With a Fanfare by North Korean, źródło: http://www.nytimes.com/2000/10/24/world/albright-greeted-with-a-fanfare-by-north-korea.html?pagewanted=all [dostęp: 5.10.2017].

Durkalec J., *Perspektywy denuklearyzacji Korei Północnej*, Biuletyn „PISM", nr 16 (881), z 10 lutego 2012 r.

Factsheets, źródło: https://www.armscontrol.org/factsheets/dprkchron [dostęp: 7.10.2017].

Jun B.G., *Cyclical Patterns of North Korean Nuclear Negotiations: 1987–2012*, [w:] *Assessment of the Nuclear Programs of Iran and North Korea*, New York 2013, s. 59.

Korea, źródło: http://www.theguardian.com/korea/subsectionmenu/0,,854619,00.html%20 [dostęp: 7.10.2017].

Kulesa Ł., *Perspektywy zakończenia północnokoreańskiego programu jądrowego*, Biuletyn „PISM", nr 10 (424), z 22 lutego 2007 r.

Legucka A., *Rosja wobec kryzysu północnokoreańskiego*, Biuletyn „PISM", nr 92 (1534), z 3 października 2017 r.

North Korea, źródło: http://www.nti.org/country-profiles/north-korea/ [dostęp: 10.10.2017].

North Korea Major Announcement artificial Earthquake. Nuclear Test site live, źródło: http://www.theguardian.com/world/live/2016/jan/06/north-korea-major-announcement-artificial-earthquake-nuclear-test-site-live [dostęp: 10.10.2017].

North Korea Nuclear Test Earthquake, źródło: http://www.theguardian.com/world/2013/feb/12/north-korea-nuclear-test-earthquake [dostęp: 10.10.2017].

Nuclear proliferation case studies, źródło: http://www.world-nuclear.org/information-library/safety-and-security/non-proliferation/appendices/nuclear-proliferation-case-studies.aspx [dostęp: 10.10.2017].

Treaties and Regimes, źródło: http://www.nti.org/treaties-and-regimes/us-dprk-agreed-framework/ [dostęp: 5.10.2017].

Press Releases, źródło: https://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx [dostęp: 7.10.2017].

Źródła internetowe

http://www.armscontrol.org/print/1253 [dostęp: 5.10.2017].

MICHAŁ PIOTR BROMIŃSKI*

ZJAWISKO MIGRACJI A TERRORYZM – BEZPIECZEŃSTWO UE W DRUGIEJ DEKADZIE XXI W.

Abstrakt

Coraz istotniejszym problemem związanym z niespokojną sytuacją na Bliskim Wschodzie, oraz problemami ekonomicznymi Białorusi, Ukrainy i – w mniejszym stopniu – Rosji jest kwestia legalnej i nielegalnej imigracji z tych terytoriów do Unii Europejskiej. Istotne jest uzyskanie odpowiedzi na pytanie, w jaki sposób napływ imigrantów ma wpływ na wszystkie sfery bezpieczeństwa – począwszy od zagrożeń terrorystycznych, po problematykę ekonomii i przestępczości pospolitej. W jaki sposób integracja imigrantów ma wpływ na minimalizowanie ryzyka wystąpienia z ich strony zagrożenia? Celem artykułu jest analiza zróżnicowanych motywacji, którymi kierują się imigranci przy podejmowaniu decyzji o wyjeździe, zbadanie wpływu migracji na kształt i funkcjonowanie rynku, a także próba przeanalizowania wzajemnej korelacji między nasilającymi się w Europie aktami terroru, a skalą imigracji.

Słowa kluczowe: migracja, bezpieczeństwo, terroryzm, imigranci ekonomiczni.

Przekształcenia zachodzące obecnie w strukturach Unii Europejskiej – zarówno polityczne, jak i społeczne wymuszają konieczność zdefiniowania pojęcia bezpieczeństwa na nowo. W Europie pojawiają się zagrożenia wcześniej niewystępujące, a te przejawiające do tej pory charakter incydentalny intensyfikują się. Wobec takiej dynamiki zmian kluczowym jest określenie czy zarówno cała Unia Europejska, jak i wszystkie jej kraje członkowskie zostały wyposażone w odpowiednie narzędzia, zarówno prawne, jak i wykonawcze nie-

* Michał Piotr Bromiński – Absolwent kierunku Bezpieczeństwo Wewnętrzne Wydziału Nauk Politycznych i Studiów Międzynarodowych UW. Student kierunku Mechatronika Wydziału Mechatroniki WAT oraz studiów magisterskich Kryminalistyka w Centrum Nauk Sądowych UW. Zainteresowania: rozwiązania prawne i technologiczne w szeroko pojętej przestrzeni bezpieczeństwa publicznego i międzynarodowego. Pasjonat balistyki i zastosowania nowoczesnych technologii w służbie bezpieczeństwa. Kontakt e-mail: michal.brominski@gmail.com

zbędne do realizacji zadań z zakresu zapewniania ludności ochrony w czasie rzeczywistym, ale również skutecznej profilaktyki kryminalnej.

Ważne jest, by usystematyzować terminologię, bowiem nawet niektórzy politycy czy dziennikarze nie potrafią w pełni poprawnie posługiwać się siatką pojęciową niejednokrotnie przecież myloną w komunikatach medialnych.

Mianem cudzoziemca natomiast określa się osobę, która nie posiada obywatelstwa kraju, w którym w danej chwili pozostaje[1].

Imigrantami nazywa się te osoby, które opuszczają swój kraj z zamiarem pozostania (zamieszkania) poza jego granicami na terytorium innego państwa[2]. Z punktu widzenia swoich ojczyzn są natomiast emigrantami.

Imigrant, to według Organizacji Narodów Zjednoczonych osoba przebywająca w kraju niebędącym jej miejscem pochodzenia przez okres dłuższy, niż 12 miesięcy, bądź legitymująca się obywatelstwem innego państwa[3]. Imigrantów można podzielić na proaktywnych i reaktywnych.

Proaktywni imigranci przybywają z jasno wyklarowanym celem – pracy zarobkowej, założenia bądź prowadzenia działalności handlowej etc. Są to więc w przeważającej mierze imigranci ekonomiczni.

Grupą ryzyka stanowiącą przedmiot zainteresowania służb bezpieczeństwa stanowią natomiast imigranci reaktywni[4]. W tej właśnie grupie znajdziemy najwięcej nielegalnych imigrantów, a także transmigrantów (zintegrowanych zarówno w kraju, do którego przybyli, jak i w kraju macierzystym)[5].

W świetle obecnie rosnącego lęku o bezpieczeństwo pośród obywateli UE największym zagrożeniem zdają się być ataki terrorystyczne. Jak się je definiuje? Jest to: „użycie przemocy wobec innych z pogwałceniem prawa, mające spowodować zastraszenie lub wymuszenie na określonej podgrupie ustępstw i określonych działań. Może być motywowane politycznie, kryminalnie lub religijnie[6]". Ponadto należy rozróżniać akty terrorystyczne od terroru kryminalnego. Podstawową różnicą między tymi dwoma zjawiskami są motywy, jakimi kierują się sprawcy.

Obserwacja zmian jakie mają obecnie miejsce w Europie, ich dynamika i fakt, że nigdy wcześniej imigracja na taką skalę nie miała miejsca oraz jej w większym stopniu obiektywne, niż subiektywne przesłanki łączące intensywność zjawiska z kwestiami związanymi z bezpieczeństwem sprawiają, że jest tematem tak istotnym z punktu widzenia analizy zagrożeń, jakie mogą pojawiać się w krajach Wspólnoty.

---

1 *Pojęcia i definicje*, organizacja Chlebem i solą, źródło: http://uchodzcy.info/infos/pojecia-i-definicje/ [dostęp: 09.2017 r.].

2 Tamże.

3 M. Wójcik-Żołądek, *Współczesne procesy migracyjne: definicje, tendencje, teorie*, „Studia BAS", nr 4/40, s. 10.

4 A. Richmond, *Reactive migration: Sociological perspectives on refugee movements*, „Journal of refugee studies" 1993, nr 6(1), s. 10–11.

5 M. Nowicka, *Europa jako wspólna przestrzeń społeczna – metodologiczne kwestie badania społeczeństwa i integracji społecznej w Europie na przykładzie mobilności przestrzennej*, s. 35.

6 Atak terrorystyczny, Projekt EDB, źródło: http://edbtwarda.cba.pl/?page_id=6 [dostęp: 09.2017 r.].

Migracje – Białoruś, Ukraina, Rosja

Rosnące bezrobocie, brak poczucia bezpieczeństwa, wysoka korupcja i bardzo wyraźnie zarysowane różnice zamożności między grupami społecznymi skłaniają wschodnich sąsiadów Polski do emigracji na zachód, który oferuje wyższe zarobki pozwalające na poprawę jakości życia, odzwierciedlane np. przez średni dochód *per capita* (dla Ukrainy wynosił on w 2014 roku około 180 euro, podczas gdy w Polsce było to średnio 670 euro)[7].

Główną przyczyną migracji ze wschodu będą więc czynniki związane z ekonomią oraz stabilną sytuacją geopolityczną członków Unii, a także jej solidnie ugruntowaną polityką wewnętrzną, które to czynniki implikują wysokie poczucie bezpieczeństwa.

W przypadku migracji z terytoriów Ukrainy, Rosji i Białorusi nie istnieje żadna konotacja między imigrantami przyjeżdżającymi z tych państw, a zamachami terrorystycznymi w Europie. W przypadku tego kierunku migracji kluczową kwestią związaną z bezpieczeństwem będzie przestępczość pospolita[8], przemyt[9] i nielegalne zatrudnienie[10]. Jak pokazują policyjne statystyki udział obcokrajowców w procentowej liczbie sprawców odnotowanych przestępstw stanowi znikomy odsetek, który dodatkowo spada przy jednoczesnym wzroście wykrywalności.

Migracja z terenów Białorusi, Ukrainy i Rosji nie stanowi zagrożenia z kilku istotnych powodów – identyfikacji geograficznej, podobieństwa obyczajów, języka oraz wspólnej historii które sprawiają, że imigranci ci asymilują się w Polsce bardzo szybko, tu zakładają rodziny (niejednokrotnie mieszane), są przyjmowani dużo chętniej i zdecydowanie rzadziej spotykają się z dyskryminacją, nienawiścią czy prześladowaniami, niż np. imigranci z Bliskiego Wschodu.

O ile przestępczość jest zjawiskiem powszechnym i mieszczącym się w granicach norm wyznaczanych policyjnymi statystykami, o tyle przyspieszony rozwój państw Europy Zachodniej w porównaniu np. z Ukrainą, przesuwanie kapitału ludzkiego z I i II do III sektora gospodarki oraz niż demograficzny implikują braki kadrowe w gałęziach niezbędnych dla funkcjonowania społeczeństwa ale wymagających fizycznie i nisko opłacanych, jak rolnictwo, przetwórstwo czy budownictwo.

Jak podkreślają eksperci Ośrodka Studiów Wschodnich (OSW), Polska jest jedynym krajem europejskim, w którym zauważalny jest duży wzrost imigracji ze wschodu, zwłaszcza Ukrainy. W tym przypadku istotny jest podział na imigrację stałą i czasową. Jak podkreśla OSW imigracja stała (długoterminowa) oscyluje cały czas na takim samym poziomie, natomiast gwałtowny wzrost odnotowuje się w wydawaniu zezwoleń czasowych

---

7 S. Pivovarov, *Polskę zalali ukraińscy imigranci*, 29 października 2015, źródło: https://pl.sputniknews.com/polska/201510291314829-Polska-Ukraina-Imigranci/ [dostęp: 09.2017 r.].

8 Dane statystyczne, Komenda Główna Policji, źródło: http://www.statystyka.policja.pl/st/wybrane-statystyki/przestepczosc-cudzozie/50867,dok.html [dostęp: 09.2017 r.].

9 M. Pawlak, *Kontrabanda na północno-wschodniej granicy. Jak skutecznie walczyć z przemytem?*, 24 czerwca 2016, źródło: http://niezalezna.pl/82379-kontrabanda-na-polnocno-wschodniej-granicy-jak-skutecznie-walczyc-z-przemytem [dostęp: 09.2017 r.].

10 H. Rabiega, *Kary nie zniechęcają do zatrudniania nielegalnych imigrantów*, 29 lipca 2014, źródło: http://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/812611,kary-nie-zniechecaja-do-zatrudniania-nielegalnych-imigrantow.html [dostęp: 09.2017 r.].

(w związku z podejmowaną np. pracą okresową albo w celach turystycznych, na których jednak Ukraińcy podejmują nielegalne zatrudnienie). Imigracja z Ukrainy ma swoje podłoże przede wszystkim w niskich zarobkach, braku poczucia bezpieczeństwa i jest związana z pogarszającą się tam sytuacją ekonomiczną[11].

Rozwój ekonomiczny państw prowadzi do bogacenia się społeczeństw. Coraz lepsze wykształcenie sprawia, że poszukuje się dobrze płatnych miejsc pracy, najczęściej w strukturach międzynarodowych korporacji lub otwierając własną działalność gospodarczą. W takiej sytuacji, aby nie dopuścić do wzrostu kosztów produkcji, a co za tym idzie cen towarów, niezwykle wygodne dla przedsiębiorców i gospodarki kraju jest pozyskiwanie niewykwalifikowanej, bądź słabo wykwalifikowanej siły roboczej w postaci proaktywnych imigrantów ekonomicznych, dla których nawet najniższa stawka w Polsce wciąż będzie wielokrotnością wynagrodzenia, które mogliby otrzymać w swoich ojczyznach za taki sam ekwiwalent godzinowy.

Wielu ludzi uważa, że cudzoziemcy odbierają Polakom miejsca pracy. W znakomitej większości przypadków jest to nieprawda – z jednym wyjątkiem. Imigranci zazwyczaj decydują się pracować „na czarno", gdzie gotówka przepływa z ręki do ręki, a pracodawca nie odprowadza odpowiednich składek ani nie ubezpiecza pracownika, który nie oponuje wobec takich praktyk za cenę zatrudnienia i możliwości zarobku. W takiej sytuacji pracodawca mając do wyboru dwóch pracowników: świadomej swoich praw i gotowej ich dochodzić osoby o niskich bądź żadnych kwalifikacjach, a równie niewykwalifikowanego, ale skrajnie spolegliwego cudzoziemca, który podejmie się każdej, nawet najcięższej (3xD – dirty, difficult, dangerous)[12] pracy zawsze wybierze tego drugiego. Bardzo chętnie zatrudniani są zwłaszcza zagraniczni pracownicy sezonowi (np. w rolnictwie), przed czym pracodawców nie zniechęca nawet nowa, bardziej sformalizowana, płatna procedura i ochrona pracowników w postaci narzucenia minimalnej kwoty wynagrodzenia[13].

Choć Polska wypracowała narzędzia do ograniczania takich praktyk i karania za nie (Ustawa o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium RP, czy wspomniane wcześniej zaostrzanie procedur zatrudnienia pracowników sezonowych), to jednak skala nielegalnego zatrudnienia wciąż pozostaje bardzo duża (kontrole inspektorów wykazały tego typu nieprawidłowości w połowie podmiotów objętych kontrolą)[14].

Jednym z poważniejszych zagrożeń związanych z imigracją na kierunku wschodnim, o którym należy wspomnieć, jest wykorzystywanie transmigrantów (związanych zarówno z krajem macierzystym, jak i tym, do którego migrują) do przemytu broni (jak również narkotyków, czy towarów objętych akcyzą). Tylko w pierwszej połowie tego roku doszło do dwóch takich prób, z których jedną było usiłowanie wwozu na teren RP okrętowej armaty

---

11 M. Jaroszewicz, *Kryzysowa migracja Ukraińców*, Ośrodek Studiów Wschodnich, 19 października 2015, źródło: https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2015-10-19/kryzysowa-migracja-ukraincow [dostęp: 09.2017 r.].

12 A. Adamczyk, *Migracje zagraniczne do Polski, a problem bezpieczeństwa społeczno-politycznego*, s. 231.

13 M. Rzemek, *Cudzoziemcy: do 2018 r. łatwiej o pracę Ukraińców*, 7 marca 2017, źródło: http://www.rp.pl/Cudzoziemcy/303079977-Cudzoziemcy-do-2018-r-latwiej-o-prace-Ukraincow.html#ap-1 [dostęp: 09.2017 r.].

14 I. Czerniejewska, *Pracownicy bez granic Raport krajowy Polska*, Warszawa 2014, s. 5.

przeciwlotniczej produkcji sowieckiej AK-630 kalibru 30 mm[15] (jedna z zatrzymanych osób narodowości ukraińskiej na stałe mieszka w Polsce). Jak informuje portal defence24.pl takie próby przemytu są elementem testowania szczelności wschodnich granic Unii Europejskiej przez Federację Rosyjską[16].

Emigracja z Europy Wschodniej ma więc odmienny wymiar od tej z Bliskiego Wschodu, nie tylko ze względu na motywację ale także w zakresie bezpieczeństwa i rodzajów zagrożeń jakie może za sobą nieść, a które są najczęściej zagrożeniami typowymi, znanymi i mieszczącymi się w pojęciu tzw. „przestępczości pospolitej".

Migracje – Bliski Wschód

Jeszcze kilka lat temu pojęcie „kryzysu imigracyjnego" nie funkcjonowało, a już na pewno nie w formie tak bardzo budzącej lęk wśród europejskiej społeczności i nie generowało tak dalece posuniętych komplikacji, związanych z kontrolą i rozlokowaniem cudzoziemców w krajach Wspólnoty.

Wg systemu klasyfikacji rodzajów migracji istotna jest analiza czynników wypychających i przyciągających. Decyzja o opuszczeniu ojczyzny podejmowana jest w skutek braku zapewnienia elementarnej potrzeby – bezpieczeństwa, rozumianego nie tylko w ujęciu potocznym i wąskim tego słowa rozumieniu – jako fizyczne bezpieczeństwo osób i ich bliskich – ale także szerzej, jako bezpieczeństwa ekonomicznego, niedostatków żywności i dachu nad głową[17].

Wyróżnia się, w zależności od regionu, kilka przyczyn intensyfikacji kryzysu imigracyjnego. W przypadku krajów takich, jak Tunezja, Algieria, Jordania i Libia podkreśla się „Arabską Wiosnę", czyli gigantyczne protesty ludności, związane z dużym bezrobociem, rosnącymi cenami żywności, korupcją oraz nepotyzmem na wysokich szczeblach władzy[18]. Należy tutaj zauważyć, jak podkreśla J. Todenhöfer (pierwszy zachodni dziennikarz w „Państwie Islamskim"), że w skutek interwencji militarnej USA, która odsunęła od władzy sunnitów, możliwe było objęcie dominującej roli przez salafickich terrorystów i utworzenie kalifatu pod nazwą tak zwanego „Państwa Islamskiego"[19]. Kalifat ten w następstwie prowadzonych przez siebie działań zbrojnych, prześladowań i okrucieństw, których się dopuszczał, doprowadził do wyklarowania się gigantycznych ruchów migracyjnych na Bliskim Wschodzie.

---

15 M. Dura, *Okrętowa armata przemycana z Ukrainy do Polski. Realne zagrożenie?*, 6 kwietnia 2017, źródło: http://www.defence24.pl/574828,okretowa-armata-przemycana-z-ukrainy-do-polski-realne-zagrozenie [dostęp: 09.2017 r.].

16 Portal defence24.pl, *Kolejna próba przemytu broni z Ukrainy do Polski*, 17 kwietnia 2017, źródło: http://www.defence24.pl/580435,kolejna-proba-przemytu-broni-z-ukrainy-do-polski [dostęp: 09.2017 r.].

17 M. Wójcik-Żołądek, *cyt. wyd.*, s. 27.

18 M. Bieniek, *Uchodźcy. Dlaczego uciekają?*, 14 stycznia 2016, źródło: http://www.newsweek.pl/swiat/uchodzcy-trzy-glowne-przyczyny-wielkiej-emigracji-z-afryki,artykuly,370503,1.html [dostęp: 09.2017 r.].

19 W. Osiński, *Pierwszy zachodni dziennikarz w Państwie Islamskim*, 17 sierpnia 2015, źródło: http://www.newsweek.pl/swiat/jurgen-todenhofer-pierwszy-zachodni-dziennikarz-w-panstwie-islamskim,artykuly,368795,1.html [dostęp: 09.2017 r.].

Zajęcie terytoriów w Syrii i Iraku utwierdziło islamistów w przekonaniu, że mają szansę na zaprowadzenie hegemonii na opanowanym obszarze i zachęca do prowadzenia dalszych działań zbrojnych. Wojna tymczasem przybiera na sile, a tylko do tej pory wysiedlonych z obszarów ogarniętych działaniami zbrojnymi zostało ok. 4,5 mln ludzi, którzy zmierzają do Europy z nadzieją na azyl zadeklarowany przez niemiecką kanclerz Angelę Merkel, co zostało odczytane wprost jako zaproszenie[20].

Zakończone sukcesami powstanie w Tunezji i Egipcie pociągnęło za sobą podobne ruchy w Libii, gdzie jednak Muammar al-Kaddafi, poprzez skierowanie wojska do ich tłumienia, spowodował wybuch krwawego konfliktu wewnętrznego. Katastrofa gospodarcza i całkowity brak bezpieczeństwa skłonił setki Libijczyków do poszukiwania azylu właśnie w Europie. Sytuacja nie uległa uspokojeniu nawet po załagodzeniu konfliktu, bowiem kraj ze zrujnowaną ekonomią i zniszczoną infrastrukturą stał się nieatrakcyjny – w żaden sposób nie rokował pozytywnie na przyszłość. Imigranci z Libii są problemem zwłaszcza dla Włochów, których kolonią była niegdyś Libia i głownie tam się kierują[21] (do końca 2015 roku było to ponad 50 tys. uchodźców).

Nie bez znaczenia jest również sytuacja polityczna w skrajnie zmilitaryzowanym kraju, jakim jest Erytrea. Kraj liczący pięć milionów mieszkańców dysponuje 320 tys. armią, która poza obroną służy również w rolnictwie, czy na budowach – przy tym wszystkim nie posiadając nawet budżetu (średni żołd to 10 dolarów miesięcznie). Erytreę co miesiąc opuszcza około pięciu tysięcy osób. To właśnie z Erytrei Polska wyraziła gotowość na przyjęcie dwóch tysięcy uchodźców[22].

Nie bez znaczenia dla intensyfikacji ruchów migracyjnych ma nastawienie do imigracji prezentowane przez kraje mogące stać się potencjalnymi azylami. Stanowiska reprezentowane przez kanclerz Angelę Merkel i François Hollande, a będące wizytówką zapraszającą uchodźców do Europy nie mają podłoża czysto humanitarnego, a są silnie nacechowane ekonomicznie. Wg statystyk za mniej, niż 40 lat liczba obywateli Niemiec ma spaść poniżej liczby obywateli Francji. Prowadzona do tej pory polityka prorodzinna poniosła fiasko, a niż demograficzny pogłębiał się. Wobec takiego zagrożenia niemieckiej stabilności gospodarczej i zachwiania rynku jako jedyną szansą na uzupełnienie braków na rynku pracy zdawało się być wykorzystanie nowoprzybyłych imigrantów – stąd tak proimigracyjna polityka prowadzona przez władze tego kraju[23].

Niska stopa bezrobocia, wysoki poziom świadczeń socjalnych, duża łatwość w uzyskaniu zatrudnienia na stanowiskach niewymagających praktycznie żadnych kwalifikacji spowodowana rosnącym wykształceniem Niemców i poszukiwaniem przez nich pracy zwłaszcza w sektorach usługowych lub ich samozatrudnieniu, to główne czynniki świad-

---

20 M. Bieniek, cyt. wyd.

21 Tamże.

22 O. Górczyński, *Erytrea, czyli państwo-więzienie. Stamtąd pochodzą uchodźcy, których przyjmie Polska*, portal Wirtualna Polska, 23 lipca 2017, źródło: https://wiadomosci.wp.pl/erytrea-czyli-panstwo-wiezienie-stamtad-pochodza-uchodzcy-ktorych-przyjmie-polska-6027734616581249a [dostęp: 09.2017 r.].

23 M. Fabisiak, *Dlaczego Niemcy zaprosili uchodźców do Europy? „Pomagają ofiarom wojny" i nie tylko*, 10 września 2015, źródło: https://wiadomosci.wp.pl/dlaczego-niemcy-zaprosili-uchodzcow-do-europy-pomagaja-ofiarom-wojny-i-nie-tylko-6027693645431425a [dostęp: 09.2017 r.].

czące o atrakcyjności Niemiec jako celu imigracji na tle innych państw, które również oferują uchodźcom pomoc i azyl[24].

Integracja muzułmanów ze społecznością europejską możliwa jest jedynie częściowo. Dla imigrantów z Bliskiego Wschodu Europejczycy wciąż pozostają odmieńcami, wyznawcami religii, która głosi herezje o jedynym i słusznym wyznaniu – Islamie. Choć wznoszone są nowe meczety, centra kultury islamu, a muzułmanie zyskują coraz większe przywileje, to nie dążą do integracji ze społecznością europejską, a preferują pozostawanie w zamkniętych społecznościach. Każda krytyka islamu poczytywana jest jako ksenofobia i nawoływanie do nienawiści[25].

Polityka proimigracyjna niesie jednak za sobą coraz bardziej negatywne następstwa. M. Duszczyk zauważa w panelu konferencji „Konsekwencje kryzysu imigracyjnego dla Niemiec i Unii Europejskiej", że kryzys ten powoduje zwiększanie się obostrzeń funkcjonowania strefy Schengen i ulegające intensyfikacji tendencje narodowe, które nie tylko zmieniają sposób postrzegania Wspólnoty przez kraje do niej należące, ale również mogą prowadzić do opuszczania przez nie Unii. Uważa on, że działania polityków zmierzające do integracji z uchodźcami nastąpiły zanim Europejczycy byli do owej integracji gotowi, co dodatkowo ją utrudnia (można tu wspomnieć np. o intensyfikujących się wpływach ruchów narodowych o skrajnych poglądach, które zyskują coraz to większe rzesze popleczników)[26]. Ponadto sami uchodźcy stwarzają trudności nie znając procedury udzielania azylu (wniosek złożony o azyl w kraju, do którego dotarło się w pierwszej kolejności), a natychmiast żądają udzielenia azylu w Niemczech.

Imigranci, a sprawa turecka

Jednym z rozwiązań kryzysu imigracyjnego mającym na celu ograniczenie napływu wcześniej niezweryfikowanych imigrantów była umowa z listopada 2015 roku, zawarta między Brukselą a Ankarą, na mocy której wszyscy imigranci, którzy nielegalnie przedostali się na terytorium Grecji, mieliby być odsyłani do Turcji. Turcja natomiast w zamian za przyjmowanie ich uzyskałaby wznowienie rozmów o przyjęcie jej w poczet członków Wspólnoty, a dodatkowo otrzymałaby w pierwszym etapie 3 miliardy euro jako zapomogę dla Syryjczyków pozostających na jej terytorium, a ponadto zniesienie wiz dla swoich obywateli[27]. Według ustaleń za jednego syryjskiego nielegalnego imigranta cofniętego z Grecji do Turcji Unia przyjmie jednego syryjskiego uchodźcę przebywającego w tureckich obozach. Zwiększy to pewność, że ów uchodźca nie jest terrorystą (wcześniejsza weryfika-

24 Tamże.

25 K. Izak, *Zagrożenie terroryzmem i ekstremizmem w Europie na podstawie wybranych przykładów. Teraźniejszość, prognoza ewolucji i kierunki rozwoju*, Przegląd Bezpieczeństwa Wewnętrznego, 5/11, s. 120.

26 B. Rudawski, *„Konsekwencje kryzysu migracyjnego dla Niemiec i Unii Europejskiej". Sprawozdanie z konferencji*, 8 czerwca 2016, źródło: https://pl.boell.org/pl/2016/06/08/konsekwencje-kryzysu-migracyjnego-dla-niemiec-i-unii-europejskiej-sprawozdanie-z [dostęp: 09.2017 r.].

27 PAP, *Spór o migrantów. Turcja niezadowolona, Bruksela stawia warunki*, 22 sierpnia 2016, źródło: http://www.tvn24.pl/wiadomosci-ze-swiata,2/umowa-ue-turcja-ws-migrantow,670322.html [dostęp: 09.2017 r.].

cja po stronie tureckiej) oraz podwyższy jakość kontroli napływającej ludności poprzez „podwójne filtrowanie" – najpierw po stronie tureckiej, a następnie europejskiej. Dzięki zawartemu porozumieniu udało się w bardzo dużym stopniu ograniczyć napływ nielegalnych imigrantów ze wschodu Morza Śródziemnego[28].

Miało to jednak swoje obwarowania. Unia uzależniła zniesienie wiz i kontynuację rozmów o członkostwie od spełnienia 72 kryteriów (zgodnie z porozumieniem zawartym w Brukseli w listopadzie 2015 roku, rozszerzanym w oświadczeniu UE-Turcja z marca 2016 r.)[29]. Jednym z nich była reforma prawa antyterrorystycznego, która nie została przeprowadzona. Ponadto jej zapisy zostały wykorzystane do stłumienia próby puczu wojskowego i zastosowania daleko idących reperkusji wobec wielu tysięcy tureckich obywateli oskarżanych o współpracę z armią celem obalenia Recepa Erdogana[30].

Porozumienie zawarte między Unią, a Turcją dało Ankarze kartę przetargową w negocjacjach ze Wspólnotą w postaci ok. 3,5 miliona uchodźców, którzy obecnie przebywają wstrzymani w swojej podróży do Europy na terenie Turcji. Eksperci oceniają, że w przypadku wejścia w życie groźby Erdogana wprost mówiącego o otwarciu granicy jeżeli Unia nie przestanie naciskać Turcji w sprawie przeprowadzenia reform politycznych, a zwłaszcza rewizji ustawy antyterrorystycznej (dającej rządowi zbyt szerokie uprawnienia), fala imigrantów zaleje Europę i nie będzie ona w stanie poradzić sobie ani z zabezpieczeniem granic i kontrolą przybywających, ani utrzymać ich na swoim terytorium (wyżywienie, rozlokowanie, pomoc socjalna), bo nie ma sił i środków by sprostać takiej liczbie imigrantów jednocześnie[31].

Tymczasem po roku od podpisania umowy turecki premier Numan Kurtulmus stwierdza, że w związku z niewywiązaniem się Unii z zobowiązań potwierdzonych zawartym porozumieniem (konkretnie nieprzyznania wiz obywatelom Turcji, mimo że to ona wciąż nie przeprowadziła wymaganych reform) zostanie ono zerwane. Choć lęk przed 3 milionami Syryjczyków obecnie przebywającymi w Turcji jest silny, to jednak według ekspertów takich, jak np. Adam Balcer (Wise Europa) zerwanie umowy byłoby dużo bardziej brzemienne w skutkach dla Ankary, niż Brukseli. Wg Balcera w zorganizowanych i nadzorowanych przez Turków obozach żyje jednie około 10% uchodźców, podczas gdy reszta jest rozproszona po całym kraju, toteż wysiedlenie wszystkich byłoby technicznie praktycznie niemożliwe. Obecnie granice Europy są dużo lepiej strzeżone, system filtrowania przepływu ludności szczelniejszy, a straż graniczna bardziej wyczulona. Dodatkowo Turcja prowadzi z Europą wymianę handlową szacowaną na 145 miliardów euro i w przypadku zerwania umowy, co pogorszyłoby i tak napiętą relację między oboma partnerami, nie była-

---

28 PAP, *Komisarz UE: Umowa z Turcją ws. migracji działa mimo ostrych wypowiedzi*, 27 marca 2017, źródło: http://www.gazetaprawna.pl/artykuly/1030700,umowa-z-turcja-ws-migracji-dziala-mimo-ostrych-wypowiedzi.html [dostęp: 09.2017 r.].

29 Komunikat prasowy, *Oświadczenie UE–Turcja*, 18 marca 2016 roku, źródło: http://www.consilium.europa.eu/pl/press/press-releases/2016/03/18-eu-turkey-statement/ [dostęp: 09.2017 r.].

30 PAP, *Komisarz UE: Umowa z Turcją…*, *cyt. wyd.*

31 PAP, *„Zaleją was imigranci". Turcja grozi Unii Europejskiej, że otworzy swoje granice*, 25 listopada 2016, źródło: http://wiadomosci.dziennik.pl/swiat/artykuly/536323,turcja-erdogan-grozi-otwarciem-granic-do-ue-dla-migrantow.html [dostęp: 09.2017 r.].

by w stanie w żaden sposób zniwelować strat spowodowanych ewentualnymi embargami i innymi represjami ekonomicznymi[32].

Wobec widma takich sankcji i niemożności spełnienia gróźb A. Balcer uważa, że zaognianie konfliktu stanowi jedynie wewnętrzną grę polityczną Turcji, mającą na celu przekonanie niezdecydowanego elektoratu o poglądach prawicowych do osoby prezydenta Erdogana poprzez budowę jego wizerunku jako surowego, zdecydowanego i pewnego siebie przywódcy, który walczy o żywotne interesy swojego państwa i jego obywateli, czym przekonałby do wzięcia udziału w referendum konstytucyjnym jak najwięcej niezdecydowanych, prawicowych wyborców[33].

Terroryzm

Polimorfizm zjawiska terroryzmu i występowanie w różnorakich odmianach (od terroryzmu klasycznego przez cyberterroryzm, po ekoterroryzm) stanowi problem w sformułowaniu jednolitej definicji terroryzmu, czego nie potrafiła dokonać nawet Organizacja Narodów Zjednoczonych[34].

Jak podkreśla S. Wojciechowski terroryzm jest sumą wielu elementów. Składają się nań m.in. zaplanowane działania o niszczycielskim charakterze (które łamią obowiązujące prawo). Mogą one być motywowane różnorako, m.in. politycznie, religijnie etc. i podjęcie ich ma przynieść określone skutki. Ponadto przedmiotem takie ataku miałoby być państwo, podmiot międzynarodowy lub ich elementy składowe (instytucje, infrastruktura itd.), choć działania te mogą być również wymierzone w zwykłych obywateli[35].

Terroryzm, jako zjawisko międzynarodowe i poniekąd ponadnarodowe, jest ściśle związany z ruchami ludności, czyli tzw. migracją. R. Leiken podkreśla, że obecnie dla terrorystów migracja jest narzędziem służącym do przedostania się na terytorium państwa, które terroryści zamierzają zaatakować[36]. Terroryści, którym uda się dotrzeć do państwa obranego za cel mogą podjąć dwojakie działania: mogą działać od razu, bezpośrednio po przybyciu przygotowując i przeprowadzając zamach, bądź ukryć się w tłumie autochtonów, symulując asymilację i normalne życie tworząc tzw. „uśpioną komórkę"[37] mającą oczekiwać na rozkazy, prowadzić rekrutację, gromadzić materiały lub stanowić wsparcie dla aktywnych terrorystów.

Celem działania terrorystów są więc nie zabójstwa czy niszczenie wybranych obiektów, ale osiągnięcie konkretnego, zamierzonego celu poprzez wywarcie odpowiedniej presji

---

32 WP Wiadomości, *Wicepremier Turcji mówi, że umowa z UE jest nieważna. Czy Europę zaleje fala migrantów?*, 14 marca 2017, źródło: https://wiadomosci.wp.pl/wicepremier-turcji-mowi-ze-umowa-z-ue-jest-niewazna-czy-europe-zaleje-fala-migrantow-6100943037998209a [dostęp: 09.2017 r.].

33 Tamże.

34 S. Wojciechowski, *Terroryzm. Analiza pojęcia, Przegląd Bezpieczeństwa Wewnętrznego*, 1/09.

35 Tamże.

36 R. Raczyński, *Wpływ migracji międzynarodowych na bezpieczeństwo wewnętrzne państwa*, Bezpieczeństwo. Teoria i praktyka, nr 2, 2015 r.

37 I. Latkowska, *Samobójcze zamachy terrorystyczne jako rodzaj gry politycznej (w kontekście bezpieczeństwa XXI wieku)*, Prace Naukowe Akademii im. Jana Długosza w Częstochowie, 11 lipca 2015, Częstochowa.

psychologicznej i wzbudzenie strachu w jednostce (bądź jednostkach, państwach, rządach) decyzyjnej.

Europol ocenia jednak, że nie ma związku pomiędzy intensyfikacją działań terrorystów, a rosnącym napływem ludności z Bliskiego Wschodu. Jedynie 10% wszystkich ataków terrorystycznych w Europie przeprowadzanych jest przez dżihadystów (uczestników „świętej wojny Islamu z niewiernymi") i choć ginie w nich sumarycznie 95% wszystkich ofiar zamachów w Europie, to jednak z zestawienia zamachów naniesionych na linię chronologiczną kryzysu imigracyjnego (od 2015 roku) wynika, że nie zachodzi korelacja między wzmożonym napływem imigrantów, a częstotliwością ataków terrorystycznych o podłożu religijnym (islamistycznym) – pozostała ona bez zmian[38].

Rzecz jasna, terroryści wykorzystują wzmożony ruch na granicy do przedostania się do Europy, czego dowodem są np. zamachy we Francji z listopada 2015 roku, ale według Europolu takie zjawisko jest marginalne. Otwarte natomiast pozostaje pytanie, czy statystyki te odzwierciedlają stan faktyczny, bowiem w Europie funkcjonuje obecnie około 400 terrorystów z tzw. „Państwa Islamskiego", którzy mają autonomię w wyborze celów i sposobie ataku (jak podają źródła Associated Press w wywiadach irackim i europejskich)[39].

W przypadku zamachu w Paryżu z listopada 2015 roku francuskie służby ustaliły, że dwóch spośród sprawców zamachu (w organizację którego były zaangażowane trzy skoordynowane grupy terrorystyczne) legitymowało się syryjskimi paszportami, które zostały odnotowane przez Greków zaledwie miesiąc wcześniej podczas przyjmowania imigrantów[40]. Otwartym pozostaje pytanie, czy owi zamachowcy dostali się do Europy wykorzystując sfałszowane paszporty, czy tez posłużyli się prawdziwymi dokumentami uzyskanymi innymi kanałami (np. odkupienie od innego imigranta, który już znalazł się w Europie, bądź pozyskanie ich od kogoś, kto zginął w drodze do Grecji).

Do organizacji i „duchowego przywództwa" wyżej wspomnianego zamachu przyznało się tzw. ISIS (Islamskie Państwo Iraku i Syrii)[41], co nie zostało oficjalnie potwierdzone przez żadne służby, jednakże wobec braku innych potencjalnych mocodawców przyznających się do sprawstwa (choćby kierowniczego) można domniemywać, że terroryści co najmniej utrzymywali kontakt z przedstawicielami Kalifatu Islamskiego. Jest to o tyle bardziej prawdopodobne, że ISIS od dawna ostrzegało Europę przed swoimi wysłannikami,

---

38 *95 procent ofiar zamachów ginie z rąk dżihadystów. Dane Europolu*, 27 czerwca 2017, źródło: http://www.tvn24.pl/wiadomosci-z-kraju,3/zagrozenie-terrorystyczne-w-europie-raport-europolu,752307.html [dostęp: 09.2017 r.]. Por. A. Zięba, *Oczekując nieoczekiwanego: zagrożenie terrorystyczne w Unii Europejskiej*, [w:] Z. Siemiątkowski, A. Zięba (red.), *Służby specjalne we współczesnym państwie*, Warszawa 2016, s. 221–230.

39 ARB, *400 terrorystów Daesh gotowych do ataku w Europie, 24 marca 2016*, źródło: http://www.rp.pl/Terroryzm/160329707-400-terrorystow-Daesh-gotowych-do-ataku-w-Europie.html#ap-1 [dostęp: 09.2017 r.].

40 Adrian o., *Zamachy w Paryżu: terroryści dostali się do Europy jako uchodźcy*, 15 listopada 2015, źródło: http://pl.blastingnews.com/europa/2015/11/zamachy-w-paryzu-to-dzielo-uchodzcow-coraz-wiecej-na-to-wskazuje-00648773.html [dostęp: 09.2017 r.].

41 Polish Express, *ISIS, ILIS, DAESH, czy Państwo Islamskie: która nazwa jest właściwa i czemu jest ich tak wiele*, 8 grudnia 2015, źródło: http://www.polishexpress.co.uk/isis-ilis-daesh-czy-panstwo-islamskie-ktora-nazwa-jest-wlasciwa-czemu-jest-ich-tak-wiele [dostęp: 09.2017 r.].

których będzie kierowało do Europy – ukrytych w tłumie imigrantów docierających m.in. do Grecji[42].

Pierwsze ostrzeżenia odnoszące się do możliwości przenikania terrorystów do Europy pod pozorem poszukiwania azylu pojawiły się właśnie w połowie 2015 roku, kiedy norweska gazeta Dagbadet opublikowała artykuł (powołując się na źródła w norweskim wywiadzie), w którym opisała, że istnieją dowody na to, że wśród imigrantów przedostających się do Europy są nie tylko liczni wysłannicy ISIS, ale także innego ugrupowania terrorystycznego – Frontu Al-Nusra[43]. Wspomniany Front Al-Nusra jest zbrojną organizacją islamskich terrorystów do niedawna będący siatką Al-Kaidy działającą w Syrii. Powstał w 2011 roku i był reakcją na totalitarne rządy reżimu Baszara al-Asada, przeciwko któremu walczył[44]. Amerykańscy specjaliści oceniają jednak, że zabieg ten jest jedynie wybiegiem, mającym budować bojownikom własną markę, a niezależność od Al-Kaidy będzie jedynie pozorna, dlatego też USA wciąż poczytuje Front jako poważne zagrożenie i jako takie zamierza go zwalczać.

Nie ulega również wątpliwości, że kryzys imigracyjny ułatwia potencjalnym terrorystom podróżowanie do Europy z wykorzystaniem nie tylko pozyskanych w sposób nielegalny lub sfałszowanych, ale również autentycznych dokumentów. Wskutek prowadzonych działań zbrojnych Kalifat wszedł w posiadanie znacznych ilości paszportów libijskich, irackich i syryjskich, z fałszowania i handlu którymi uczynił intratne źródło finansowania swojej działalności. Pozyskał on również możliwość wyposażania potencjalnych terrorystów w doskonałe dokumenty bez konieczności fałszowania ich od podstaw (de facto na oryginalnych drukach). Stanowi to tak duży problem, ze francuski minister spraw wewnętrznych, Bernard Cazeneuve, nawołuje do stworzenia europejskiej agencji, która zajmowałaby się wyłącznie kontrolą dokumentów na podstawie których imigranci są wpuszczani do Europy[45].

Raport Europolu zwraca również uwagę na istotną kwestię łatwości werbunku i radykalizacji imigrantów przez już obecnych w Europie werbowników, np. w osobach imamów o skrajnie radykalnych poglądach. Dużo łatwiej zwerbować osobę o podobnych poglądach, religii czy obyczajach, niż Europejczyka, którego styl życia, priorytety i poglądy znacznie różnią się od tych, które usiłowano by mu perswadować. Ponadto wg Associated Press w granicach Unii znajduje się wciąż 400 przeszkolonych, islamskich terrorystów gotowych do działania, podczas gdy tylko w 2016 roku w związku z zagrożeniem terrorystycznym o podłożu religijnym (radyklanego islamu) aresztowano wg Europolu 687 osób[46].

---

42 Adrian o., *Zamachy w Paryżu…*, *cyt. wyd.*

43 Tamże.

44 CNN, *Front Al-Nusra odłącza się od Al-Kaidy*, 31 lipca 2016, źródło: https://www.wprost.pl/swiatowe-dni-mlodziezy-krakow-2016/10017256/Front-Al-Nusra-odlacza-sie-od-Al-Kaidy.html [dostęp: 09.2017 r.].

45 ABC washingtonexaminer.com, *Państwo Islamskie fałszuje paszporty na skalę przemysłową. Potwierdzają to także Amerykanie*, 27 stycznia 2016, źródło: http://www.pch24.pl/panstwo-islamskie-falszuje-paszporty-na-skale-przemyslowa--potwierdzaja-to-takze-amerykanie,40855,i.html [dostęp: 09.2017 r.].

46 BBC News, *Europol: Liczba ofiar terrorystów w UE wzrosła w ciągu roku niemal 38-krotnie*, 21 lipca 2016, źródło: https://www.wprost.pl/swiat/10016046/Europol-Liczba-ofiar-terrorystow-w-UE-wzrosla-w-ciagu-roku-niemal-38-krotnie.html [dostęp: 09.2017 r.].

Jednym z poważniejszych zagrożeń jest wykorzystywanie przez terrorystów międzynarodowej sieci Internet. W „Sprawozdaniu w sprawie zapobiegania radykalizacji (…)" podkreśla się, że obecnie istniejące rozwiązania prawne mające na celu ograniczanie bądź całkowite uniemożliwianie publikowania w Internecie treści związanych z werbunkiem, szkoleniem i produkcją materiałów wybuchowych oraz przygotowywania zamachów wymuszają konieczność prowadzenia dialogu z dostawcami usług teleinformatycznych w Europie, by wspólnie wypracować rozwiązania – zarówno te techniczne, jak i prawne – umożliwiające znaczne ograniczenie możliwości publikacji w/w treści, a w przypadku ich pojawienia się – błyskawiczne usunięcie[47]. Należałoby również ustalić, jaki procent zradykalizowanych terrorystów przenika do Europy nie z zamiarem przeprowadzenia bezpośredniego uderzenia ale w celach szkoleniowych, prowadzenia rekrutacji, dostarczania rozkazów i przekazywania informacji (zwłaszcza transmigranci) czy organizacji wyposażenia i prowadzenia tzw. „białego wywiadu".

Unia konstatuje, że jednym z kluczowych działań w przestrzeni cyfrowej jest prowadzenie kontrnarracji do tej werbowników i radykalnych islamistów w taki sposób, by uwrażliwiać odbiorcę na wszelkie przejawy zradykalizowanego przekazu, nagabywania i próby werbunku tak, aby obywatel Unii był świadomy i odporny na nowe typy zagrożeń na które może natknąć się w sieci. Wspólnota w sprawozdaniu podkreśla również konieczność rozszerzenia takich działań uświadamiających na państwa trzecie, nie będące stowarzyszonymi[48].

Unia w raporcie podkreśla również, że konieczne jest rozbijanie sieci terrorystycznych, które najskuteczniej można osiągnąć poprzez skuteczne ściganie przestępstw skarbowych (ukrywanie majątku, uchylanie się od opodatkowania) bowiem to one są głównymi źródłami finansowania terroryzmu[49].

Ciekawa jest jeszcze jedna informacja zawarta w uzasadnieniu do raportu. Szacuje się mianowicie, że 5000 obywateli europejskich opuściło kontynent, by walczyć w szeregach terrorystów – zwłaszcza wskazuje się tu Irak oraz Syrię. Według International Centre for the Study of Radicalisation and Political Violence jest wśród nich 1200 Francuzów – dwukrotnie więcej, niż obywateli Niemiec[50].

Zagrożenie terrorystyczne należy więc wyeliminować skupiając się na przyczynach jego powstania. Są to: wojna na Bliskim Wschodzie destabilizująca region i zmuszająca tysiące ludzi do opuszczenia swoich domostw i ucieczki celem ratowania życia, co stwarza terrorystom warunki do wmieszania się w tłum i przeniknięcia na terytorium Europy. Inna, ale równie istotna, to szerząca się radykalizacja uchodźców i rodzimych obywateli Unii Europejskiej prowadzona przede wszystkim za pośrednictwem radykalnych imamów, a także sieci Internet.

---

47 R. Dati, *Sprawozdanie w sprawie zapobiegania radykalizacji oraz rekrutacji obywateli europejskich przez organizacje terrorystyczne*, (2015/2063(INI)), Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, 3 listopada 2015.

48 Tamże.

49 Tamże, podrozdział X.

50 TVN24 BiS, *W walce o dżihad. Europejczycy w szeregach ISIS*, 10 sierpnia 2016, źródło: http://tvn24bis.pl/ze-swiata,75/europejczycy-w-szeregach-isis,667488.html [dostęp: 09.2017 r.].

Zagrożenie terrorystycznej jest obecnie jednym z największych wyzwań, z jakimi muszą się zmierzyć europejskie służby. Terroryzm wraz ze swoimi metodami działań, a także celami strategicznymi nieustannie ewoluuje co sprawia, że wciąż pozostaje najtrudniejszym do ujawnienia i zapobieżenia niebezpieczeństwem. Zagrożenie stanowią przede wszystkim osoby, które usiłują przedostać się do Europy pod pozorem poszukiwania azylu wraz z gigantyczną falą imigrantów, która utrudnia pełną i dokładną weryfikacje każdego z osobna.

Mimo że deklaracje i rozwiązania prawne przyjmowane przez Unię Europejską oraz opracowywane przez nią raporty świadczą o bezsprzecznym rosnącym zagrożeniu i nie można nie zauważać, że jest ono powiązane ze wzrostem imigracji zwłaszcza z Bliskiego Wschodu, to jednak obserwując poczynania Wspólnoty odnosi się nieodparte wrażenie, że nowe rozwiązania i regulacje prawne wprowadzane są z opóźnieniem i nie nadążają za bieżącymi wydarzeniami oraz podejmowane są ze swoistą nieśmiałością (np. uchwała o potępieniu zamachu, zamiast błyskawicznej odpowiedzi w postaci odpowiedniej regulacji, która dałaby właściwym służbom niezbędne narzędzia do uniemożliwienia jego powtórzenia).

Zwalczanie terroryzmu

Wobec pojawienia się nowych technik działania terrorystów oraz intensyfikacji ich działań niezbędnym było wypracowanie nowych metod walki z terroryzmem.

Polska, jako członek Unii Europejskiej aktywnie angażuje się nie tylko w dyskurs odnośnie poprawy bezpieczeństwa, ale również aktywnie bierze udział w opracowywaniu odpowiednich rozwiązań legislacyjnych oraz międzynarodowej współpracy i wymianie doświadczeń funkcjonariuszy służb bezpieczeństwa. Polscy funkcjonariusze na przykład aktywnie uczestniczą w szkoleniach organizowanych przez Europol i nieustannie pracują nad opracowywaniem coraz skuteczniejszych procedur operacyjnych[51]. Skuteczna walka z terroryzmem nie może polegać na wystosowywaniu oficjalnych not, wzywaniu do zaprzestania działań i poddania się. Musi być równie bezlitosna i skuteczna co działania terrorystów (tylko dzięki takiemu podejściu Brytyjczykom udało się ukrócić fale zamachów w latach 90.)[52].

O planowanym zamachu zanim ma on miejsce (jak pokazują dane wywiadowcze) wie wcześniej kilkadziesiąt do kilkuset osób. Należy przede wszystkim zacieśnić współpracę i poprawić obieg informacji między poszczególnymi służbami członków Unii Europejskiej. Zamachy w Paryżu miały miejsce, bowiem Belgowie nie udostępnili posiadanych informacji o zamachowcach Francuskim służbom. Później owi terroryści przenieśli się z powrotem do Belgii, bowiem Francja nie dysponowała wystarczającymi danymi wywiadowczymi, by zatrzymać ich, zanim przekroczą granicę[53].

---

51 K. Liedel, *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa. Zarządzanie bezpieczeństwem*, Warszawa 2010.

52 M. Nowicki, *Belgowie latami tolerowali terrorystów*, 23 marca 2016, źródło: http://www.newsweek.pl/opinie/jak-europa-powinna-walczyc-z-terroryzmem-,artykuly,382579,1.html [dostęp: 09.2017 r.].

53 Tamże.

Choć nowe metody walki z terrorystami, jak skatalogowane, udostępnione wszystkim członkom wspólnoty bazy danych biometrycznych obywateli i terrorystów, system miejskiego monitoringu wizyjnego obejmujący coraz większe obszary Europy, czy mikrofony kierunkowe w miejscach publicznych wciąż zdają się być przerażająco mało skuteczne w walce z terroryzmem[54].

W kwietniu 2016 roku w Londynie miały miejsce targi Security and Counter terror Expo, prezentujące 300 firm z całego świata (bezpieczeństwo publiczne to biznes, którego sektor prywatny wyceniany jest na ok. 30 miliardów dolarów).

Jedną ze stosowanych i wciąż ulepszanych (początkowo robili to ludzie, eksperci, obecnie zastąpiły ich wciąż udoskonalane algorytmy i systemy kamer) jest technologia SPOT (Screening Passengers by Observation Techniques). Polega ona na obserwacji tłumu pasażerów i każdego z osobna, i analizowaniu jego zachowania m.in. na podstawie mimiki i mikromimiki twarzy, mowy ciała (sztywna postawa, ręce w kieszeniach lub torbach, pocenie się, stopień rozszerzenia źrenic, nadmierna bladość etc.)[55].

Początek 2015 przyniósł uruchomienie ogromnej bazy fotografii przestępców, należącej do Interpolu, a do której dostęp mają służby ze 190 krajów. Równolegle Chiny uruchomiły program FtF (Facing the Future) – system monitoringu wizyjnego porównujący twarze widziane obiektywem kamery z posiadaną bazą danych w czasie rzeczywistym[56].

Choć wydawać by się mogło, że systemy monitoringu porównujące twarze podróżnych z bazą danych przestępców powinny mieć wysoką skuteczność, to jednak waha się ona w okolicach 60–70%. Ponadto systemy odpowiedzialne za analizę tętna, źrenic i mikromimiki są z kolei nazbyt skuteczne – wskazują jako potencjalnego przestępcę zestresowanych przed kolejną ważną transakcją biznesmenów, czy rodziny rozemocjonowane faktem czekania na dawno niewidzianego bliskiego. Niewątpliwie systemy te są przyszłością, jednakże czeka je jeszcze wiele lat, zanim będą perfekcyjnie realizować zadania przed nimi postawione.

Inną techniką zwalczania terrorystów, zanim w ogóle nastąpi próba ataku jest inwigilacja. Marokańskie służby przy wjeździe do kraju gromadzą każdą, nawet z pozoru zupełnie nieistotną daną. Dzięki temu możliwe było dwukrotne ostrzeżenie Niemiec o planowanym zamachu (każde z doniesień okazało się być prawdą) – podobnie trafne były ich ostrzeżenia skierowane w stronę Francji. Chodzi tu nie tyle nawet o skrajnie niebezpieczną i praktycznie niewykonalną infiltrację komórek terrorystycznych poprzez wprowadzenie tam agenta – obecnie równie dużo informacji dostarcza zwyczajna obserwacja miast czy codziennych rytuałów ich obywateli. Każdy policjant jest uczulony na to, że gazeciarz, taksówkarz czy bezdomny, których regularnie widują każdego dnia może stanowić zagrożenie i to zagrożenie będzie trzeba natychmiast wyeliminować[57].

---

54 M. Rybarczyk, *Jak walczyć z terrorystami? Nowe metody nie są skuteczne*, 27 listopada 2015, Focus 10/2015, źródło: http://www.focus.pl/artykul/jak-walczyc-z-terrorystami-nowe-metody-nie-sa-skuteczne [dostęp: 09.2017 r.].

55 Tamże.

56 Tamże.

57 M. Narbutt, *Infiltracja popłaca. Marokańskie służby specjalne dwukrotnie alarmowały Niemcy, że Tunezyjczyk Anis Amri planuje zamach*, 26 grudnia 2016, źródło: https://wpolityce.pl/swiat/320935-infiltracja-poplaca-marokanskie-sluzby-specjalne-dwukrotnie-alarmowaly-niemcy-ze-tunezyjczyk-anis-amri-planuje-zamach?strona=2 [dostęp: 09.2017 r.].

Podsumowanie

Migracja z krajów Białorusi, Ukrainy i (w mniejszym stopniu) Rosji była zjawiskiem powszechnym i obserwowanym na długo przed pojawieniem się tzw. „kryzysu imigracyjnego". Miała ona przede wszystkim charakter ekonomiczny i z racji podobieństw między imigrantami, a obywatelami krajów, do których owi imigranci przybywali (zwłaszcza kulturowych, religijnych i obyczajowych) nie generowała tak intensywnych sprzeciwów i nienawiści wśród obywateli autochtonicznych. Powodowana była wyłącznie ekonomią, ponadto pojawianie się wielu imigrantów miało charakter cykliczny, ale okresowy (pracownicy sezonowi). Wypełnianie przez nich luk na rynku pracy związanych zwłaszcza z ciężką pracą fizyczną i zawodami z grupy 3xD, których wykonywania mało kto się podejmuje było i jest bardzo pożądane przez pracodawców.

Migracje na kierunku wschodnim stanowią więc bardzo dużą szansę na wypełnienie luk na europejskim rynku pracy (co przyczyni się z kolei do utrzymania stabilności rynku) przy jednoczesnym znikomym wzroście zagrożenia ze strony imigrantów (poza minimalnym wzrostem przestępczości).

Główną przyczyną migracji z terenów Bliskiego Wschodu są konflikty zbrojne i związane z nimi nagminne łamanie praw człowieka, a co za tym idzie całkowity brak poczucia bezpieczeństwa pośród ludności cywilnej i brak szans na poprawę sytuacji zarówno politycznej, jak i ekonomicznej w najbliższej przyszłości. Nie bez znaczenia dla intensywności i celów migracji z Bliskiego Wschodu pozostają również oświadczenia składane przez przywódców państw członkowskich Unii Europejskiej oraz przejrzyste i przychylne obcokrajowcom prawo azylowe. Imigracja na tym kierunku generuje jednak bardzo duży ruch, w którym z łatwością mogą przedostać się terroryści. Jest to zagrożenie nieobserwowalne np. w przypadku imigracji z Białorusi, Ukrainy czy Rosji. Za czynniki wypychające w tym przypadku można uznać brak bezpieczeństwa na terenach imigrantom macierzystych, utratę dobytku i zanik wszelkich więzi z opuszczanym regionem. Czynnikami przyciągającymi będą zwłaszcza niskie bezrobocie, łatwość w uzyskaniu świadczeń socjalnych i znaczna ich wysokość, łatwość uzyskania zatrudnienia (zwłaszcza w zawodach nie wymagających żadnych kwalifikacji) oraz podejście władz krajów członkowskich (jak np. Niemcy czy Francja), które same zapraszają imigrantów. Zagrożenie, które może wyłaniać się z tego obrazu ma swoje podłoże nie w imigracji jako takiej, ale w sposobie, w jaki terroryści wykorzystują ruchy dużych grup ludności do przedostania się do Europy, odmienności wiary i obyczajów obcokrajowców, ich braku chęci asymilacji i postawach niektórych imigrantów, zakładających życie w Europie na koszt państw udzielających im azylu (brak chęci integracji, pracy, uczynienie z pomocy socjalnej jedynego źródła dochodu etc.). Migracje z Bliskiego Wschodu są jednak nierozerwalnie kojarzone przede wszystkim z przenikającym zagrożeniem terrorystycznym, przed którym ostrzegając lęk i nienawiść potęguje wielu szanowanych dziennikarzy i polityków. jak należałoby się więc przygotować do neutralizacji takich zagrożeń i całkowitego uniemożliwienia przenikania dżihadystów do Europy?

Kluczowymi wyzwaniami, jakie staja przed służbami bezpieczeństwa na pierwszej linii frontu walki z terroryzmem jest wypracowywanie coraz skuteczniejszych metod weryfikacji dużych grup imigrantów, wskazywanie i izolowanie potencjalnych zagrożeń. Wewnątrz Europy natomiast najistotniejszymi są: wyśledzenie i likwidacja uśpionych i aktywizują-

cych się komórek terrorystycznych oraz nieustanna obserwacja i w razie potrzeby reagowanie wszędzie tam, gdzie może dochodzić do nawoływania do przyłączenia się do świętej wojny, głoszenie nienawiści do Europejczyków, czy wszelkie próby werbunku.

Równie poważnym niebezpieczeństwem są te jednostki, które nie będąc wcześniej wyznawcami islamu pod wpływem werbowników i radykalnych nauk duchownych imamów postanowiły skanalizować swoją nienawiść do świata i ubrać ją w barwy religii.

Jeszcze jednym obszarem, który powinien pozostawać pod nieustannym nadzorem służb jest globalna sieć Internet, gdzie dochodzi do wyszukiwania potencjalnych kandydatów na terrorystę, weryfikacji jego cech osobowościowych, a wreszcie indoktrynacji i szkolenia.

Równie dużym zagrożeniem są także sfrustrowane jednostki w Europie nie mające związku z dżihadem, ale dokonujące zamachów na własną rękę, do których następnie przyznają się (głównie islamskie) organizacje terrorystyczne.

W trakcie konferencji „Konsekwencje kryzysu imigracyjnego dla Niemiec i Unii Europejskiej" interesują obserwację opisał profesor Andrzej Sakson. Według niego w Polsce ma miejsce coś, co określił mianem „socjologicznego fenomenu" – nasilają się nastroje antyimigranckie, a grupy skrajnie narodowe o poglądach rasistowskich i ksenofobicznych zyskują znaczny pogłos, mimo braku imigrantów w kraju[58].

Obecny wzrost liczby potencjalnych i realnych zagrożeń w Europie stawia poważne wyzwanie przed Brukselą. Niezbędne jest bowiem opracowanie odpowiednich rozwiązań prawnych, które dadzą organom wykonawczym odpowiednie możliwości prowadzenia działań związanych nie tylko z zapobieganiem zagrożeniom, ale także pozwalające na prowadzenie działań wyprzedzających takich, jak m.in. szeroko zakrojona obserwacja i inwigilacja osób podejrzanych w ramach bardziej uproszczonej, niż ta obecnie stosowana procedury (niektóre państwa europejskie zaczynają już wprowadzać takie rozwiązania).

Natomiast ponad wszystko pożądanym jest, aby podejmowane przez władze ustawodawcze i wykonawcze kroki nadążały, a nawet wyprzedzały mające obecnie miejsce w Europie dynamiczne przemiany społeczne i polityczne, bo tylko wyprzedzenie działań terrorystów może zagwarantować ich całkowite unieszkodliwienie.

Tytuł w języku angielskim:
MIGRATION AND TERRORISM – SECURITY OF THE EU IN THE SECOND DECADE OF 21st CENTURY

Bibliografia

Publikacje zwarte

Adamczyk A., *Migracje zagraniczne do Polski, a problem bezpieczeństwa społeczno-politycznego*, „Przegląd Strategiczny 2013", nr 2, s. 219–237.

Czerniejewska I., *Pracownicy bez granic Raport krajowy Polska*, Warszawa 2014.

[58] B. Rudawski, *cyt. wyd.*

Hoffman B., *Oblicza terroryzmu*, Warszawa 2001.

Perek R., *Terroryzm. Rola i miejsce Policji w jego zwalczaniu*, Katowice 2013.

Siemiątkowski Z., Zięba A. (red.), *Służby specjalne we współczesnym państwie*, Warszawa 2016.

Szafrański J. (red.), *Współczesne zagrożenia terroryzmem oraz metody działań antyterrorystycznych*, Szczytno 2007.

Artykuły

ABC washingtonexaminer.com, *Państwo Islamskie fałszuje paszporty na skalę przemysłową. Potwierdzają to także Amerykanie*, 27 stycznia 2016, źródło: http://www.pch24.pl/panstwo-islamskie-falszuje-paszporty-na-skale-przemyslowa--potwierdzaja-to-takze-amerykanie,40855,i.html [dostęp: 09.2017 r.].

ARB, *400 terrorystów Daesh gotowych do ataku w Europie, 24 marca 2016*, źródło: http://www.rp.pl/Terroryzm/160329707-400-terrorystow-Daesh-gotowych-do-ataku-w-Europie.html#ap-1 [dostęp: 09.2017 r.].

Atak terrorystyczny, Projekt EDB, źródło: http://edbtwarda.cba.pl/?page_id=6 [dostęp: 09.2017 r.].

BBC News, *Europol: Liczba ofiar terrorystów w UE wzrosła w ciągu roku niemal 38-krotnie*, 21 lipca 2016, źródło: https://www.wprost.pl/swiat/10016046/Europol-Liczba-ofiar-terrorystow-w-UE-wzrosla-w-ciagu-roku-niemal-38-krotnie.html [dostęp: 09.2017 r.].

Bieniek M., *Uchodźcy. Dlaczego uciekają?*, 14 stycznia 2016, źródło: http://www.newsweek.pl/swiat/uchodzcy-trzy-glowne-przyczyny-wielkiej-emigracji-z-afryki,artykuly,370503,1.html [dostęp: 09.2017 r.].

Chlebem i solą, *Pojęcia i definicje*, organizacja Chlebem i solą, źródło: http://uchodzcy.info/infos/pojecia-i-definicje/ [dostęp: 09.2017 r.].

CNN, *Front Al-Nusra odłącza się od Al-Kaidy*, 31 lipca 2016, źródło: https://www.wprost.pl/swiatowe-dni-mlodziezy-krakow-2016/10017256/Front-Al-Nusra-odlacza-sie-od-Al-Kaidy.html [dostęp: 09.2017 r.].

Dane statystyczne, Komenda Główna Policji, źródło: http://www.statystyka.policja.pl/st/wybrane-statystyki/przestepczosc-cudzozie/50867,dok.html [dostęp: 09.2017 r.].

Dati R., *Sprawozdanie w sprawie zapobiegania radykalizacji oraz rekrutacji obywateli europejskich przez organizacje terrorystyczne*, (2015/2063(INI)), Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych [dostęp: 3.11.2016].

Dura M., *Okrętowa armata przemycana z Ukrainy do Polski. Realne zagrożenie?*, 6 kwietnia 2017, źródło: http://www.defence24.pl/574828,okretowa-armata-przemycana-z-ukrainy-do-polski-realne-zagrozenie [dostęp: 09.2017 r.].

Fabisiak M., *Dlaczego Niemcy zaprosili uchodźców do Europy? „Pomagają ofiarom wojny" i nie tylko*, 10 września 2015, źródło: https://wiadomosci.wp.pl/dlaczego-niemcy-zaprosili-uchodzcow-do-europy-pomagaja-ofiarom-wojny-i-nie-tylko-6027693645431425a [dostęp: 09.2017 r.].

Górczyński O., *Erytrea, czyli państwo-więzienie. Stamtąd pochodzą uchodźcy, których przyjmie Polska*, portal Wirtualna Polska, 23 lipca 2017, źródło: https://wiadomosci.wp.pl/erytrea-czyli-panstwo-wiezienie-stamtad-pochodza-uchodzcy-ktorych-przyjmie-polska-6027734616581249a [dostęp: 09.2017 r.].

Izak K., *Zagrożenie terroryzmem i ekstremizmem w Europie na podstawie wybranych przykładów. Teraźniejszość, prognoza ewolucji i kierunki rozwoju*, Przegląd Bezpieczeństwa Wewnętrznego, 5/11.

Jaroszewicz M., *Kryzysowa migracja Ukraińców*, Ośrodek Studiów Wschodnich, 19 października 2015, źródło: https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2015-10-19/kryzysowa-migracja-ukraincow [dostęp: 09.2017 r.].

95 procent ofiar zamachów ginie z rąk dżihadystów. Dane Europolu, 27 czerwca 2017, źródło: http://www.tvn24.pl/wiadomosci-z-kraju,3/zagrozenie-terrorystyczne-w-europie-raport-europolu,752307.html [dostęp: 09.2017 r.].

Kiełt A., *Przeciwdziałanie terroryzmowi jako element działań na rzecz bezpieczeństwa państwa*, źródło: www.wspia.eu/file/20336/29-KIEŁT+ALDONA.pdf [dostęp: 09.2017 r.].

Komunikat prasowy, *Oświadczenie UE–Turcja*, 18 marca 2016 roku, źródło: http://www.consilium.europa.eu/pl/press/press-releases/2016/03/18-eu-turkey-statement/ [dostęp: 09.2017 r.].

Latkowska I., *Samobójcze zamachy terrorystyczne jako rodzaj gry politycznej (w kontekście bezpieczeństwa XXI wieku)*, Prace Naukowe Akademii im. Jana Długosza w Częstochowie, 11 lipca 2015, Częstochowa.

Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa. Zarządzanie bezpieczeństwem*, Warszawa 2010.

mb, TVN24 BiS, *W walce o dżihad. Europejczycy w szeregach ISIS*, 10 sierpnia 2016, źródło: http://tvn24bis.pl/ze-swiata,75/europejczycy-w-szeregach-isis,667488.html [dostęp: 09.2017 r.].

Narbutt M., *Infiltracja popłaca. Marokańskie służby specjalne dwukrotnie alarmowały Niemcy, że Tunezyjczyk AnisAmri planuje zamach*, 26 grudnia 2016, źródło: https://wpolityce.pl/swiat/320935-infiltracja-poplaca-marokanskie-sluzby-specjalne-dwukrotnie-alarmowaly-niemcy-ze-tunezyjczyk-anis-amri-planuje-zamach?strona=2 [dostęp: 09.2017 r.].

Nowicka M., *Europa jako wspólna przestrzeń społeczna – metodologiczne kwestie badania społeczeństwa i integracji społecznej w Europie na przykładzie mobilności przestrzennej*.

Nowicki M., *Belgowie latami tolerowali terrorystów*, 23 marca 2016, źródło: http://www.newsweek.pl/opinie/jak-europa-powinna-walczyc-z-terroryzmem-,artykuly,382579,1.html [dostęp: 09.2017 r.].

O. Adrian, *Zamachy w Paryżu: terroryści dostali się do Europy jako uchodźcy*, 15 listopada 2015, źródło: http://pl.blastingnews.com/europa/2015/11/zamachy-w-paryzu-to-dzielo-uchodzcow-coraz-wiecej-na-to-wskazuje-00648773.html [dostęp: 09.2017 r.].

Osiński W., *Pierwszy zachodni dziennikarz w Państwie Islamskim*, 17 sierpnia 2015, źródło: http://www.newsweek.pl/swiat/jurgen-todenhofer-pierwszy-zachodni-dziennikarz-w-panstwie-islamskim,artykuly,368795,1.html [dostęp: 09.2017 r.].

PAP, *Komisarz UE: Umowa z Turcją ws. migracji działa mimo ostrych wypowiedzi*, 27 marca 2017, źródło: http://www.gazetaprawna.pl/artykuly/1030700,umowa-z-turcja-ws-migracji-dziala-mimo-ostrych-wypowiedzi.html [dostęp: 09.2017 r.].

PAP, *Spór o migrantów. Turcja niezadowolona, Bruksela stawia warunki*, 22 sierpnia 2016, źródło: http://www.tvn24.pl/wiadomosci-ze-swiata,2/umowa-ue-turcja-ws-migrantow,670322.html [dostęp: 09.2017 r.].

PAP, *„Zaleją was imigranci". Turcja grozi Unii Europejskiej, że otworzy swoje granice*, 25 listopada 2016, źródło: http://wiadomosci.dziennik.pl/swiat/artykuly/536323,turcja-erdogan-grozi-otwarciem-granic-do-ue-dla-migrantow.html [dostęp: 09.2017 r.].

Pawlak M., *Kontrabanda na północno-wschodniej granicy. Jak skutecznie walczyć z przemytem?*, 24 czerwca 2016, źródło: http://niezalezna.pl/82379-kontrabanda-na-polnocno-wschodniej-granicy-jak-skutecznie-walczyc-z-przemytem [dostęp: 09.2017 r.].

Piekarski M., *Strategia i taktyka terrorystów*, artykuł po raz pierwszy został opublikowany na stronach Dolnośląskiego Ośrodka Studiów Strategicznych w roku 2004.

Pivovarov S., *Polskę zalali ukraińscy imigranci*, 29 października 2015, źródło: https://pl.sputniknews.com/polska/201510291314829-Polska-Ukraina-Imigranci/ [dostęp: 09.2017 r.].

Polish Express, *ISIS, ILIS, DAESH, czy Państwo Islamskie: która nazwa jest właściwa i czemu jest ich tak wiele*, 8 grudnia 2015, źródło: http://www.polishexpress.co.uk/isis-ilis-daesh-czy-panstwo-islamskie-ktora-nazwa-jest-wlasciwa-czemu-jest-ich-tak-wiele [dostęp: 09.2017 r.].

Portal defence24.pl, *Kolejna próba przemytu broni z Ukrainy do Polski*, 17 kwietnia 2017, źródło: http://www.defence24.pl/580435,kolejna-proba-przemytu-broni-z-ukrainy-do-polski [dostęp: 09.2017 r.].

Rabiega H., *Kary nie zniechęcają do zatrudniania nielegalnych imigrantów*, 29 lipca 2014, źródło: http://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/812611,kary-nie-zniechecaja-do-zatrudniania-nielegalnych-imigrantow.html [dostęp: 09.2017 r.].

Raczyński R., *Wpływ migracji międzynarodowych na bezpieczeństwo wewnętrzne państwa*, Bezpieczeństwo. Teoria i praktyka, nr 2, 2015 r.

Richmond A., *Reactive migration: Sociological perspectives on refugee movements*, Journal of refugee studies, 1993, nr 6(1).

Rudawski B., *„Konsekwencje kryzysu migracyjnego dla Niemiec i Unii Europejskiej". Sprawozdanie z konferencji*, 8 czerwca 2016, źródło: https://pl.boell.org/pl/2016/06/08/konsekwencje-kryzysu-migracyjnego-dla-niemiec-i-unii-europejskiej-sprawozdanie-z [dostęp: 09.2017 r.].

Rybarczyk M., *Jak walczyć z terrorystami? Nowe metody nie są skuteczne*, 27 listopada 2015, Focus 10/2015, źródło: http://www.focus.pl/artykul/jak-walczyc-z-terrorystami-nowe-metody-nie-sa-skuteczne [dostęp: 09.2017 r.].

Rzemek M., *Cudzoziemcy: do 2018 r. łatwiej o pracę Ukraińców*, 7 marca 2017, źródło: http://www.rp.pl/Cudzoziemcy/303079977-Cudzoziemcy-do-2018-r-latwiej-o-prace-Ukraincow.html#ap-1 [dostęp: 09.2017 r.].

Wojciechowski S., *Terroryzm. Analiza pojęcia, Przegląd Bezpieczeństwa Wewnętrznego*, 1/09.

Wójcik-Żołądek M., *Współczesne procesy migracyjne: definicje, tendencje, teorie*, „Studia BAS", nr 4/40.

WP Wiadomości, *Wicepremier Turcji mówi, że umowa z UE jest nieważna. Czy Europę zaleje fala migrantów?*, 14 marca 2017, źródło: https://wiadomosci.wp.pl/wicepremier-turcji-mowi-ze-umowa-z-ue-jest-niewazna-czy-europe-zaleje-fala-migrantow-6100943037998209a [dostęp: 09.2017 r.].

MICHAŁ SZOTEK*

OBLICZA TERRORYZMU ISLAMSKIEGO W EUROPIE I PRÓBY PRZECIWDZIAŁANIA

Abstrakt

Działalność terrorystyczna ekstremistów islamskich w Europie z każdym kolejnym rokiem staje się coraz trudniejsza do wychwycenia przez służby państw europejskich. Terroryści cały czas zmieniają metody działania, co umożliwia im uniknięcie zdekonspirowania. Nowe oblicze terroryzmu związane jest zużywaniem przeróżnych nieznanych wcześniej narzędzi do przeprowadzania zamachów terrorystycznych przez ekstremistów islamskich, dzięki czemu są oni zawsze krok przed służbami. Postrzeganie zagrożenia jakim stał się obecny terroryzm islamski na przestrzeni ostatnich lat, jest efektem wzmożonej aktywności tzw. „samotnych wilków" ale nie tylko ich.

Słowa kluczowe: terroryzm islamski, zamach terrorystyczny, ekstremiści islamscy, samotny wilk.

Wprowadzenie

W niniejszej pracy autor opisuje zjawisko, które w ostatnim czasie przekształciło się w jedno z największych zagrożeń współczesnej Europy. Zjawisko terroryzmu islamskiego można postrzegać w wymiarze narodowym oraz międzynarodowym. Mianowicie zjawisko terroryzmu islamskiego jest zagrożeniem dla systemów bezpieczeństwa nie tylko poszczególnych krajów Wspólnoty Europejskiej, ale przez swój transgraniczny charakter stało się wyzwaniem dla wszystkich państw Unii Europejskiej. Użycie terminu „terroryzm islamski" może być uznawane za określenie zbyt ogólne, ponieważ oczywiście nie każdy wyznawca islamu jest terrorystą, jednak należy pamiętać, że sprawcy zamachów z ostatnich lat głoszą jednoznacznie, że działają w obronie islamu. Zamachowcy walczą z gorszącą, wyniszczającą i zepsutą kulturą państw zachodnich. Celem każdego państwa jest zapewnienie bez-

* Michał Szotek – student studiów magisterskich na kierunku Bezpieczeństwo Wewnętrzne na Uniwersytecie Warszawskim. Absolwent studiów licencjackich na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Zainteresowania badawcze koncentrują się wokół tematyki przeciwdziałania zjawisku terroryzmu islamskiego, narastającego radykalizmu postaw w Europie oraz kryzysu migracyjnego w Europie. Kontakt e-mail: miguel.szotek@gmail.com

pieczeństwa swoim obywatelom, jednak jak można tego dokonać w sytuacji, gdy oblicze terroryzmu islamskiego zmienia się cały czas. Terroryzm jaki znaliśmy z wydarzeń jakie miały miejsce w Madrycie w 2004 r. oraz Londynie w 2005 r., to historia. Możemy zaobserwować, że terroryzm islamski zmienia i rozwija nowe swoje sposoby działania[1].

Przedmiotem badań w niniejszej publikacji jest określenie czym jest terroryzm islamski w Europie, scharakteryzowanie zagrożeń jakie wynikają z jego obecnej postaci, analiza poszczególnych zamachów oraz podjętych działań, jakie zostały wyciągnięte wnioski w związku z przeprowadzonymi zamachami. Dodatkowo celem niniejszego artykułu jest dokonanie analizy metod jakie stosują terroryści islamscy, aby zaprowadzić w Europie atmosferę terroru i chaosu. Artykuł ma na celu ukazanie jak niebezpiecznym zjawiskiem jest terroryzm islamski dla systemów bezpieczeństwa państw europejskich oraz dla całej cywilizacji europejskiej. Wnioski z analizy sytuacji problemowej i tematu pracy były pryncypium do sformułowania głównego problemu badawczego, który brzmi w sposób następujący: **Czy w dobie rosnącego fundamentalizmu islamskiego, można nadal czuć się bezpiecznie w Europie?**

Wieloaspektowość głównego problemu badawczego oraz potrzeba nadania odpowiedniego kierunku badaniom, dowodzi konieczności sformułowania problemów szczegółowych:

1. Czym jest terroryzm islamski?
2. Jakie zagrożenie istnieje ze strony tzw. „Samotnych wilków"?
3. Ile razy służby były krok przed zamachowcami a ile razy niestety ale krok za nimi?
4. Jak długo kraje europejskie będą zmagać się ze terroryzmu islamskiego?

W celu uzyskania odpowiedzi na postawiony w pracy badawczej problem główny oraz problemy szczegółowe należy postawić hipotezę główną. Hipoteza główna brzmi następująco: metody i działania jakie prowadzone są przez europejskie służby do zapobiegania terroryzmowi islamskiego nie prowadzą do zahamowania tendencji rosnącej jaką przejawia terroryzm ekstremistyczny. Mając na względzie zwiększenie poziomu bezpieczeństwa, służby wprowadzają liczne modyfikacje w swoich systemach bezpieczeństwa, jednak ostatnie zamachy terrorystyczne pokazują, że zmiany nie przynoszą w pełni zamierzonych efektów.

Przy napisaniu niniejszego artykułu podstawę stanowiły materiały źródłowe oraz literatura podmiotu. Źródła stanowiły akty prawne i publikacje internetowe. Należy wymienić tu takie pozycje jak *Radykalizacja poglądów religijnych w społecznościach muzułmańskich wybranych państw Unii Europejskiej: Polska, Holandia, Wielka Brytania* pod redakcją Damiana Szlachtera, powyższa pozycja opisuje metody oraz działania jakie stosują służby w celu zwalczania zjawiska terroryzmu i radykalizmu oraz *Ewolucja terroryzmu motywowanego ideologią religijną* autorstwa Artura Wejksznera, który w swojej publikacji skupia się na wyjaśnieniu sposobu działania salafickiego ruchu globalnego dżihadu.

Literatura przedmiotu, która jest dostępna, jest nieaktualna w niektórych aspektach związanych z terroryzmem islamskim, przykładem są metody i działania, które stosowane są do przeciwdziałania zjawisku jakim jest terroryzm islamski, otóż tylko nowsze publi-

[1] Onet, *Madryt 2004. To był najkrwawszy zamach w Europie*, źródło: http://wiadomosci.onet.pl/swiat/madryt-2004-to-byl-najkrwawszy-zamach-w-europie/e79lzzk [dostęp: 12.09.2017].

kacje mają opisane nowe strategie działania wobec tego zagrożenia. Spowodowane jest to dynamiką z jaką postępują, zmiany w systemach prawnych państw europejskich a również modyfikację metod i działań, które należy dostosowywać do tego jak zmienia się zjawisko ekstremizmu islamskiego.

Dla służb bezpieczeństwa państw europejskich atak terrorystyczny jest zjawiskiem trudnym do przewidzenia oraz co grosza do zapobieżenia. Osoby biorące udział w zamachach często są jedynie narzędziem wykorzystywanym przez terrorystów. Ekstremiści natomiast w każdy możliwy sposób wysyłają komunikat, w kierunku rządów państw europejskich, aby je zastraszyć i zmusić do podjęcia ustępstw[2]. Największym zagrożeniem dla bezpieczeństwa wewnętrznego krajów Unii Europejskiej a zarazem dla samych obywateli UE jest obawa przed kolejnym zamachem terrorystycznym. Należy zdefiniować czym jest terroryzm. Według ustaleń szczytu NATO w Pradze w 2002 r. jest to „Bezprawne lub groźne użycie siły lub przemocy przeciw osobom indywidualnym lub mieniu, zmierzające do zniewolenia lub zastraszenia rządów lub społeczeństw dla osiągnięcia celów politycznych, religijnych lub ideologicznych[3]".

Analizując dynamikę zmian w działaniach terrorystów, podczas zamachów, które miały miejsce w Europie możemy dostrzec, że jeszcze nigdy w historii państw Europy terroryzm religijny nie był tak dużym wyzwaniem. Intensywność zjawiska terroryzmu islamskiego w połączeniu z problemem kryzysu migracyjnego, który trwa od 2014 r., może spowodować stopniową radykalizację postaw Europejczyków wobec ludności muzułmańskiej. Już teraz można dostrzec zmiany nastrojów politycznych w społeczeństwach europejskich, które zaczynają odczuwać zagrożenie ze strony społeczności muzułmańskiej, przykładem jest uzyskanie we wrześniowych wyborach do Bundestagu ok. 13% poparcia przez AfD czyli skrajnie prawicową partię na niemieckiej scenie politycznej. Subiektywne przesłanki łączące z kwestiami związanymi z bezpieczeństwem sprawiają. Wszystko to sprawia, że temat terroryzmu islamskiego i jego „nowego oblicza w Europie" stał się jednym z największych zagrożeń jakie mogą mieć miejsce w krajach całej Europy.

Terroryzm islamski

Terroryzm islamski, jest formą terroryzmu o charakterze religijnym. Zanim scharakteryzowany zostanie terroryzm islamski, należy wyszczególnić, na czym opiera się Islam. Mianowicie religia islamu, oprócz systemu wierzeń, jest nie jednokrotnie czynnikiem, który umacnia oraz utrwala więzi, które zachodzą w przykładowej grupie. Islam jest religią, która określa nie tylko stosunek wyznawcy do Boga, jednakże ukazuje swoim wyznawcom cały system społeczny, wszelkie normy prawne oraz zachodzące stosunki międzyludzkie[4]. Poja-

---

2 M. Kubik, *Terroryzm jako strategia komunikacyjna*, [w:] K. Liedel, P. Piasecka, *Terroryzm wczoraj i dziś. Księga pamiątkowa na 10-lecie Centrum Badań nad Terroryzmem Collegium Civitas*, Warszawa 2015, s. 23.

3 BBN, *Terroryzm – zagrożenie globalne i lokalne*, źródło: https://www.bbn.gov.pl/download/1/1034/rozdzial1.pdf [dostęp: 12.09.2017].

4 P. Guła, *Terroryzm międzynarodowy, w tym islamski. Zarys problemu*, WSPol, Szczytno 2009, s. 23.

wia się na każdym kroku w życiu swojego wyznawcy, między innymi dlatego w islamie nie ma rozdziału życia religijnego od świeckiego. Wyżej wspominane cechy powodują, że ludność muzułmańską łatwiej zjednoczyć, wykorzystują hasła, które wypływają z religii. Co ważne dla terrorystów islamskich, porównywanie wszystkich wymiarów życia z treściami, które zapisane są Koranie, stworzyło wygodną możliwość do swobodnej interpretacji słów Koranu, a co za tym idzie dostosować zawarte prawdy do swoich celów. Przykładowo zakaz samobójstwa, który zapisany jest w Koranie został odrzucony przez przywódcę Palestyńskiego Islamskiego Dżihadu[5]. Fathi Szikaki stwierdził, że ciemiężony lud, aby móc się bronić przed innym ludem, musi odnaleźć inne sposoby walki. Podsumowując, samobójcy, którzy giną w obronie ludności islamskiej nie naruszają zasad wiary islamu, a nawet jako dla męczenników droga do raju jest dla nich otwarta. Wyżej opisana interpretacja w pełni zaprzecza dotychczasowemu rozumieniu nauk zawartych w świętej księdze islamu[6].

Dodatkowo ważne jest wyjaśnienie pojęcia dżihadu, które obecnie jest nietrafnie interpretowane. Dżihad to wysiłki oraz starania jakie podejmuje muzułmanin, aby na świecie panowała sprawiedliwość, dobro oraz, aby podjąć działania mające na celu szerzenia islamu. Sam dżihad należy dzielić na[7]:

- wielki – jest to praca nad sobą, by być lepszym człowiekiem, podjęcie działań, które mają na celu poprawę jednostki, czyli podjęcie walki ze wszelkimi swoimi słabościami oraz wadami;
- mały – jest to od górny obowiązek zbrojnej walki w momencie, gdy atakowana jest jednostka, społeczność czy wiara muzułmańska i muzułmański sposób życia. W czasie, gdy jest islam jest zagrożony i atakowany z zewnątrz oraz inne środki działania skończyły się.

Błędna skrajna interpretacja dżihadu małego forma wyznacza walkę zbrojną, która ma spowodować panowanie islamu nad światem. Taki model dżihadu małego jest wybierany przez przeróżne fanatyczne islamskie ugrupowania terrorystyczne, mające zradykalizowane poglądy. Terroryzm islamski wykorzystuję religię islamu do realizacji swoich celów politycznych oraz usprawiedliwiania swoich bezprawnych, krwawych zamachów, które mają wzbudzić strach i terror[8].

Szef Bin Laden Issue Station, doświadczony oficer oraz analityk Michael Scheuer wprowadził do terminologii pojęcie terroryzmu globalnego, inaczej globalnego dżihadu. Według Michaela Scheuera, dla takich terrorystów nie występuje pojęcie neutralności, otóż każde państwo, które prowadzi walkę a nawet potępia terroryzm, jest zagrożone zamachem terrorystycznym. Należy pamiętać, że terroryści uderzają w określone obiekty. Głównym celem ekstremistów jest ludność cywilna. Jest to związane z tym, że ludność cywilna jest podatna na różnego rodzaju manipulacje, poruszenie, strach, które może wywołać zamach terrorystyczny. Wydarzenia z Francji z lat 2015–2016 mogą posłużyć jako przykład, kiedy

5 A. Krawczyk, *Terroryzm ugrupowań fundamentalistycznych na obszarze Izraela w drugiej połowie XX wieku*, Toruń 2007.

6 P. Guła, dz. cyt., s. 24.

7 M. Sadowski, *Dżihad – Święta wojna w islamie*, Przegląd Bezpieczeństwa Wewnętrznego nr 8 (5) 2013, s. 41.

8 M. Tomczak, *Ewolucja terroryzmu. Sprawcy – metody – finanse*, Instytut Zachodni, Poznań 2010, s. 175.

dla terrorystów najważniejsze było uderzyć w noncombatant targets[9], czyli tzw. cele niewalczące, *w* rezultacie czego zabić jak najwięcej cywili. Tym, co chcieli uzyskać terroryści był natychmiastowy medialny rozgłos o masowym ataku na cywili. Należy pamiętać, że dla terrorystów nie jest najważniejszy tylko obiekt, na który dokonują zamach, tak samo ważne okoliczności jak i wcześniej wspomniany cel jaki zostanie osiągnięty po przeprowadzonym zamachu. Akt przemocy ma na celu dotarcie do jak najszerszej grupy odbiorów, natomiast sama akcja bardzo często jest dokładnie zaplanowana a działania są dokonywane z pełną świadomością konsekwencji, nie ma tutaj mowy o wystąpieniu zjawiska przypadku. Terroryzm islamski, który cechuje się specyficznymi religijnymi regułami i nakazami jest destrukcyjny oraz jest znacznie krwawszy w skutkach. Islamiści stosują przeważnie terroryzm masowy, ich akty terroru są bardzo często wymierzane przeciwko ludziom wyznającym odmienną religię, jednak w wielu sytuacjach ofiarami zamachów są również muzułmanie. Podsumowując, istnieją dwa powody, dla których terroryści islamscy stosują przemoc[10], otóż w sposób pośredni i bezpośredni. Ten pierwszy ma na celu zastraszenie poprzez zamachy jak największej ilości cywili oraz wpłynięcie na rządy krajów zachodnich, aby odstąpiły albo podjęcia pewne działania. Bezpośredni powód, to eliminacja możliwie jak największej ilości innowierców, przykładowo poprzez używanie do przeprowadzania zamachów porwanych samolotów, ładunków wybuchowych, broni krótkiej i coraz częściej broni białej[11].

Istotnym czynnikiem mającym znaczący wpływ na terroryzm islamski jest bieda i ubóstwo. Brak godnych warunków życia, wzbudza agresje i złość, które są efektem końcowym frustracji. Dodatkowo niewystarczający dostęp do edukacji powoduje, że fanatycy religijni mają ułatwioną możliwość wdrażania swojej ideologii zagubionym jednostkom. Bardzo często ekstremiści islamscy obwiniają „świat zachodu" o wszelkie zło, jakie dotyka muzułmanów na świecie. Manipulując ludźmi, ukazują, kto jest winny ubóstwu, kreując wroga, którego należy unicestwić. Nie należy jednak generalizować terrorystów jako osoby pochodzące wyłącznie z biednych warstw społecznych. Wielu fanatycznych bojowników pochodzi ze średnich warstw społecznych, a nawet posiada wyższe wykształcenie, będąc członkami zamożnych rodzin islamskich, które nigdy nie doświadczyły skrajnej nędzy[12]. Należy mieć na uwadze, że według R. Borkowskiego terroryzm i ekstremizm w obecnej postaci, ma podłoże oparte w większym stopniu na aspektach kulturowych oraz politycznych. Znaczniej w mniejszym stopniu opiera się on na przyczynach socjoekonomicznych. Ekstremistom islamskim, żyjącym w Europie, korzystającym ze wszystkiego co związane z kulturą zachodu, wdraża się, że winnymi uciskowi i nędzy, jaka dotyka ich braci w wierze w krajach arabskich są państwa Zachodu. Między innymi dlatego nawołuje się ich do podjęcia walki, która będzie prowadzona bezpośrednio na terytorium państw Zachodu[13]. Postawiony w taki sposób cel, budzi w nich poczucie misji, która została im powierzo-

[9] *Patterns of Global Terrorism*, Office of the Cordinator for Counterterrorism, Serwis internetowy Departamentu Stanu USA, U.S. Department of State, http://www.state.gov// [dostęp: 12.09.2017].

[10] B. Hołyst, *Terroryzm*, t. 1, Wyd. LexisNexis, Warszawa 2011, s. 51–107.

[11] Tamże, s. 51–107.

[12] M. Tomczak, *Ewolucja terroryzmu. Sprawcy – metody – finanse*, Instytut Zachodni, Poznań 2010, s. 175.

[13] R. Borkowski, *Terroryzm ponowoczesny Studium z antropologii polityki*, Toruń 2006, s. 20–70.

na oraz którą należy wykonać z powodu wyższych wartości. Według przeanalizowanych danych, terrorysta, który bierze udział w zamachach w Europie zazwyczaj jest jednostką, która ma obywatelstwo danego kraju europejskiego lub przebywa w nim jakiś czas. Dodatkowo korzysta z zachodniego stylu życia, jednakże pomimo tego wszystkiego co zostało wyżej wspomniane, to ulega hasłom skrajnej ideologii islamskiej. Najczęściej są to osoby wieku pomiędzy 18 a 30 rokiem życia. Osoby wyznaczone do indoktrynacji tak młodej jednostki korzystają z tego, że osoby w bardzo młodym wieku wykazują jeszcze nieukształtowaną osobowość, dlatego łatwo nimi manipulować. W stosowaniu metod manipulacji młodą jednostką, pomagają sytuacje, w których osoba taka doznaje zderzenia z rzeczywistością. Wszelki idealizm, staje się nieprawdą. Młode osoby czują się oszukane, a co za tym idzie niejednokrotnie rośnie w nich reakcja buntu, braku akceptacji na zaistniały stan rzeczy, chcą walczyć z okrutną rzeczywistością. Ostatnim ważnym czynnikiem, który pomaga w zindoktrynowaniu oraz zradykalizowaniu jednostki jest ukazanie, że za wszelkie niepowodzenia życiowe czy traumatyczne przeżycia z dzieciństwa winnymi są kraje szeroko pojętego Zachodu. Natomiast „skrzywdzone" jednostki otrzymują w zamian poczucie akceptacji, bezpieczeństwa. Postawy taki jednostek są chwalone przez resztę grupy, stają się one jej ważnymi członkami[14].

Madryt i Londyn, miasta połączone wspólną tragedią

Historia terroryzmu islamskiego, który jest dzisiaj znany w Europie rozpoczęła się od zamachów, które miały miejsce w Madrycie w 2004 roku i rok później w Londynie. Zamachy zostały przeprowadzone przy użyciu ładunków wybuchowych umieszczonych w środkach komunikacji miejskiej[15].

Zamachy w Madrycie były odwetem za interwencję państw koalicji sprzymierzonych pod egidą USA w Iraku. Mianowicie po zamachach z 11 września 2001 r. wiele krajów europejskich, w tym Hiszpania, stanęło ramię w ramię ze Stanami Zjednoczonymi Ameryki do walki przeciwko terroryzmowi. Po około dwóch latach Al-Kaida[16] dokonała krwawego odwetu za wyżej wspomnianą interwencję w Iraku. 11 marca 2004 r. doszło do eksplozji 10 z 13 ładunków wybuchowych, które umiejscowione były w pociągach madryckiej kolei podmiejskiej. Według ogólnodostępnych informacji, w zamachach w Madrycie zginęło 191 osób, natomiast aż 1841 zostało rannych. Początkowo cień wszelkich podejrzeń ze strony hiszpańskich władz padł na członków separatystycznej organizacji ETA[17], której celem jest walka o niepodległość Kraju Basków. Jednakże

[14] M. Tomczak, *Ewolucja terroryzmu. Sprawcy – metody – finanse*, Instytut Zachodni, Poznań 2010, s. 176–178.

[15] Gazeta Prawna, *Najważniejsze zamachy terrorystyczne w Europie w ostatnich latach*, źródło: http://www.gazetaprawna.pl/artykuly/1048402,zamachy-terrorystyczne-w-europie-w-ostatnich-latach.html [dostęp: 12.09.2017].

[16] *Al-Kaida*, (arab. *zasada*) organizacja terrorystyczna o międzynarodowym zasięgu (terroryzm międzynarodowy) założona w 1988 przez Osamę bin Ladena, źródło: http://portalwiedzy.onet.pl/124701,,,,al_kaida,haslo.html [dostęp: 12.09.2017].

[17] *ETA*, Euskadi Ta Askatasuna, Kraj Basków i Wolność, tajna, separatystyczna organizacja działająca w Hiszpanii, walcząca przy pomocy metod terrorystycznych (głównie terroru indywidualnego, wymierzonego

przedstawiciele ETA natychmiastowo oznajmili, że żaden członek ich organizacji nie brał udziału w zamachu w stolicy Hiszpanii. Hiszpańskie służby znalazły w dniu zamachu dowody, które wskazały, że sprawcy zamachu nie należeli do ETA. W porzuconym białym samochodzie dostawczym służby hiszpańskie odnalazły siedem kolejnych detonatorów, szereg materiałów oraz instrukcji głosowych będących w języku arabskim. Na miejscu przestępstwa została znaleziona karta telefoniczna, która należała do Dżamala Zougama, który należał do madryckiej komórki terrorystycznej. Zapisy połączeń głosowych pozwoliły dotrzeć do znaczącej liczby terrorystów[18]. Zougam oraz dwóch innych członków madryckiej komórki terrorystycznej zostało aresztowanych przez hiszpańskie służby kolejnego dnia po zamachu. Cel polityczny terrorystów został spełniony, ponieważ wybuch miał miejsce parę dni przed wyborami do parlamentu hiszpańskiego, a nowy premier Hiszpanii Jose Luisem Rodriguez Zapatero od razu po wygranych wyborach parlamentarnych ogłosił, że natychmiastowo zostanie wycofany z Iraku hiszpański kontyngent liczący 1300 żołnierzy[19]. „Bliźniaczym" atakiem, który miał miejsce w Madrycie był zamach w Londynie 7 lipca 2005 r. Pomiędzy godziną 8.40 a 9.50 doszło do 3 eksplozji w pociągach londyńskiego metra oraz jednego wybuchu w londyńskim autobusie. Użyte ładunki wybuchowe zabiły 56 osób, natomiast raniły około 300. Zamach spowodował potężny paraliż komunikacyjny 6 milionowego Londynu. Cała komunikacja miejska została zawieszona, tak więc paraliż trwał około dwa dni. Oba zamachy ukazują pewne podobieństwa, otóż ładunki wybuchowe eksplodowały w godzinach porannego szczytu, kiedy środki miejskiego transportu w europejskich miastach są zazwyczaj przepełnione. Ataki zostały przeprowadzone bez jasnej i klarownej zapowiedzi, otóż terroryści grozili atakami odwetowymi za interwencję zbrojna w Iraku. Nikt nie spodziewał się, że terroryści są w stanie na terenie Hiszpanii i Wielkiej Brytanii skonstruować ładunki wybuchowe o tak dużej sile rażenia. Oba wydarzenia łączy również idea dążenia do spowodowania jak największej liczby ofiar przez co charakter ataku terrorystycznego miał na celu wywołanie atmosfery paniki i chaosu w społeczeństwie europejskim[20]. Dwóch zamachowców-samobójców było niewyróżniającymi się w społeczeństwie obywatelami brytyjskimi. Dopiero po pobycie z Lahaur w Pakistanie, wrócili według relacji najbliższych „odmienieni". Na terenie Pakistanu doszło do zradykalizowania się ich poglądów[21].

przeciwko funkcjonariuszom państwa hiszpańskiego) o niepodległość kraju Basków, źródło: http://portalwiedzy.onet.pl/75879,,,,eta,haslo.html [dostęp: 12.09.2017].

18 Polskie Radio, *Zamachy w Madrycie – odwet za Irak*, źródło: http://www.polskieradio.pl/39/156/Artykul/1071933,Zamachy-w-Madrycie-%E2%80%93-odwet-za-Irak [dostęp: 12.09.2017 r.].

19 A. Wejkszner, *Ewolucja terroryzmu motywowanego ideologią religijną*, Poznań 2010, s. 338–341.

20 Wirtualna Polska, *Media o podobieństwach zamachów w Londynie i Madrycie*, źródło: https://wiadomosci.wp.pl/media-o-podobienstwach-zamachow-w-londynie-i-madrycie-6037190996529793a [dostęp: 13.09.2017].

21 Newsweek Polska, *Krwawe puzzle*, źródło: http://www.newsweek.pl/swiat/krwawe-puzzle,16655,1,1.html [dostęp: 15.09.2017].

Zmieniające się oblicze terroryzmu islamskiego

Atak „Samotnych wilków", nie jest zjawiskiem nowym, jednak staje się co raz bardziej powszechny, powoduje to zmianę sposobu postrzegania zagrożenia jakim jest terroryzm opierający się na metodach działania „Samotnych wilków". Należy wytłumaczyć czym się charakteryzują „samotne wilki" na tle zamachów jakie miały miejsce. Za przykład może posłużyć zamach przeprowadzony w Berlinie w 2016 roku, który ukazał, że terroryzm będzie częściej miał postać ataku „samotnego wilka", który atakuje z ukrycia, najważniejsze dla takiej jednostki jest osiągnąć jak największe zaskoczenie, m.in. przeprowadzenie ataku w środku miasta, podczas normalnego dnia lub podczas imprezy masowej. „Samotnego wilka" charakteryzuje[22]:

- jeden sprawca albo kilku współdziałających ze sobą napastników;
- sprawca najczęściej działa w jednym miejscu;
- jak największa liczba ofiar w jednym wydarzeniu;
- kierują sprawcą pobudki ideologiczne/religijne;
- współpracuje z organizacjami mającymi charakter terrorystyczny;
- zamach trwa od kilku minut do kilku godzin (jeśli dochodzi do obławy sił bezpieczeństwa, ponieważ sprawca weźmie zakładników).

Pamiętając o tym, że zamachy przeprowadzane przez grupy terrorystów, kończą się przeważnie masakrą, której efektem końcowym jest duża liczba ofiar, to jednak zamachy przeprowadzane przez pojedyncze jednostki wywołują większe poczucie zagrożenia. Jest to spowodowane wywołaniem lęku, atmosfery strachu przed każdą inną jednostką. W takim wypadku boimy się nie tylko „dziwnej" grupy ludzi, ale również każdej jednostki, która jest w naszym otoczeniu. Wydarzenia z ostatnich lat pokazały, że każdy może być terrorystą, nie sposób jest w tłumie ludzi wyselekcjonować taką podejrzaną jednostkę.

Z analizy wynika, że radykalizacja „samotnych wilków" nie ma miejsca w zorganizowanych strukturach. Jednostki radykalizują się w we własnym domu, przeważnie używając komputera lub innych urządzeń mobilnych. Do radykalizacji dochodzi podczas czytania w Internecie treści, które wzbudzają w nich gniew oraz nienawiść do świata zachodniego. W Internecie znajdują informację, wskazówki, instrukcje jak zabijać „niewiernych". Niekoniecznie muszą być członkami skrajnych organizacji, nie wymagają przechodzenia skomplikowanych szkoleń. Bardzo często osoby takie mają różne problemy o podłożu psychicznym. Umożliwia im to stawanie się zimnymi mścicielami, którzy wymierzają sprawiedliwość za wyrządzone krzywdy doznane z ręki „niewiernych". Stają się bojownikami walczącymi o lepszą, w ich mniemaniu, muzułmańską Europę. Dlatego przewidzenie, która jednostka z milionów ludzi stanie się muzułmańskim terrorystą jest praktycznie niewykonalne[23].

[22] PolskaTimes, *Samotne wilki, czyli terroryzm w wersji 2.0*, źródło: http://www.polskatimes.pl/artykul/872693, samotne-wilki-czyli-terroryzm-w-wersji-20,id,t.html [dostęp: 15.09.2017].

[23] G. Lindenberg, *Przyszłością terroryzmu są zamachy pojedynczych osób*, źródło: https://euroislam.pl/przyszloscia-terroryzmu-sa-zamachy-pojedynczych-osob/ [dostęp: 17.09.2017].

Trzy czynniki sprawiają, że możliwe zagrożenie ze strony indywidualnych terrorystów będzie wzrastać[24]:

1. Jednostki takie są bardzo trudne do wychwycenia przez służby bezpieczeństwa.
2. Samo-radykalizacja jednostki oraz bezproblemowe zdobycie narzędzi niezbędnych do przeprowadzenia zamachu.
3. Instrukcje jak przeprowadzić zamach są ogólnodostępne w Internecie dla takich jednostek. Bardzo duża część zamachów, na których wzorują się „samotne wilki" przeprowadzana była bez użycia broni palnej. Zamachowcy korzystali z narzędzi, które są możliwe do zdobycia wszędzie czyli: np. noże oraz samochody, ostatnie wydarzenia z Europy pokazują, że ten typ zamachów będzie się upowszechniać.

Należy mieć na uwadze, że zamachy dokonywane przy użyciu przykładowo noża lub samochodu nie dokonują takiej masakry „niewinnych" osób jak zamachy bombowe lub atak przy użyciu broni palnej[25]. Najistotniejszym efektem końcowym nie jest ilość ofiar, lecz wywołanie atmosfery grozy, wzbudzenie jak najgorszych nastrojów społecznych, pokazanie jak wiele można przeprowadzić takich zamachów, w tak prosty sposób. Najgorszym z możliwych scenariuszy jest sytuacja w której do zamachów tego typu wykorzystywane byłyby również kobiety oraz dzieci. W takiej sytuacji, możliwe, że taki zamach mógłby zostać przeprowadzony dosłownie w każdym możliwym miejscu i czasie w Europie. Im częstotliwość takich zamachów zwiększa się, tym bardziej społeczeństwo odczuwa strach i zagrożenie, które towarzyszy na każdym kroku[26]. W momencie, gdy zamachy mają miejsce w każdej możliwej przestrzeni życia człowieka, to społeczeństwo zaczyna odczuwać poczucie, że w żadnym miejscu nie jest już bezpiecznie. W każdym miejscu możemy stać się ofiarą zamachu, a dodatkowo, służby nie są w stanie uniemożliwić każdego możliwego ataku ze strony „samotnych wilków"[27]. W sytuacji wzrostu poczucia zagrożenia przy jednoczesnym zjawisku bezsilności, dochodzi do spadku zaufania do państwa, jako suwerena, które w najważniejszych dokumentach gwarantuje zapewnienie bezpieczeństwa swoim obywatelom. Elity rządzące, które za pomocą aparatu bezpieczeństwa nie potrafią bronić własnych obywateli przed zamachowcami tracą posłuch w społeczeństwie, a właśnie to przyświeca terrorystom, aby nikt nie czuł się bezpiecznie tam gdzie przebywa[28]. Według eksperta ds. bezpieczeństwa z Centrum Analiz Strategicznych i Bezpieczeństwa mjr Mariusza Kordowskiego „organizacje terrorystyczne przejawiają jednak swoją aktywność po której można je poznać i śledzić" natomiast „osoby indywidualne z dnia na dzień mogą postanowić, że coś zrobią". „Samotny wilk" bardzo szybko planuje dokonanie zamachu, co powoduje, że jest przeważnie nieuchwytny dla służb. Dlatego według eksperta z Centrum

---

24 Tamże.

25 B. Wieliński, *Samochód – broń terrorystów nr 1. Bo zachodnich miast nie da się zabezpieczyć przed atakami z jej użyciem*, źródło: http://wyborcza.pl/7,75399,21541047,samochod-bron-terrorystow-nr-1-bo-zachodnich-miast-nie-da.html [dostęp: 17.09.2017].

26 G. Lindenberg, *cyt. wyd.*

27 CNN, *Atak „samotnych wilków". Nowa fala terroryzmu?*, http://wiadomosci.onet.pl/atak-samotnych-wilkow-nowa-fala-terroryzmu/r86vf [dostęp: 17.09.2017].

28 TVP Info, *Samotne wilki…*, *cyt. wyd.*

Analiz Strategicznych i Bezpieczeństwa zjawisko „samotnych wilków" będzie problemem i zarazem wyzwaniem, który czeka całą Europę[29].

Analiza wybranych zamachów

Do zamachu terrorystycznego w Berlinie doszło 19 grudnia 2016 r. podczas trwania jarmarku bożonarodzeniowego, atak terrorystyczny został wykonany za pomocą ciężarówki. Rozpędzona ciężarówka wjechała w przechodniów będących na zamkniętej ulicy. Warto zwrócić uwagę, że *modus operandi* tego zamachu terrorystycznego był podobny do aktu terroru, który został przeprowadzony parę miesięcy wcześniej w Nicei. Zamach miał miejsce około godziny 20, miejsce zamachu zostało wybrane nie bez powodu. Mianowicie jarmark bożonarodzeniowy był zatłoczony, dlatego był bardzo dobrym celem dla terrorysty. Aktu terroru dokonał 24 letni Tunezyjczyk Anis Amri[30]. Po zamachu terrorysta uciekł z miejsca zdarzenia. Następnego dnia po zamachu, tzw. Państwo Islamskie przyznało się do przeprowadzenia aktu terroru, co należy jednak odbierać z dystansem. Biorąc pod uwagę charakter propagandy jaka jest prowadzona przez dżihadystów, możemy dojść do wniosku, że każdy zamach w imię islamu jest przydatny do realizacji swoich celów i chętnie wezmą odpowiedzialność za niego na swoje barki. W Berlinie w grudniowym zamachu zginęło 12 osób, natomiast około 50 zostało rannych[31].

W marcu i w czerwcu w 2017 r. w Londynie zostały przeprowadzone dwa bliźniacze zamachy terrorystyczne, w których zostały wykorzystane pojazdy mechaniczne oraz noże. Oba zostały dokonane na mostach londyńskich, na London Bridge oraz na Moście Westminsterskim. Argumentem dlaczego przechodnie na mostach stali się celami terrorystów, jest on zrozumiały[32]. Z mostu człowiek ma ograniczoną możliwość ucieczki, co ułatwia dokonanie krwawego zamachu. W obu zamachach zginęło 12 osób, natomiast około 100 zostało rannych. Po zamachu na moście Westminsterskim tzw. Państwo Islamskie ogłosiło, że atak był przez nich przygotowany, jednak dochodzenie brytyjskiej policji wskazało, że zamachowiec nie miał żadnych powiązań z ugrupowaniami terrorystycznymi, natomiast jego poglądy uległy radykalizacji[33].

Kolejnymi i zarazem ostatnimi analizowanymi zamachami są zamachy, które miały miejsce w Katalonii w sierpniu 2017 r. Analogicznie jak w powyższych zamachach w tych

---

29 Polskie Radio, *„Samotne…*, *cyt. wyd.*

30 PAP, *Zamach w Berlinie. Policyjny nalot na dwa mieszkania. Wysoka nagroda za pomoc w ujęciu podejrzanego Tunezyjczyka*, źródło: http://www.polskieradio.pl/5/3/Artykul/1706917,Zamach-w-Berlinie-Policyjny-nalot-na-dwa-mieszkania-Wysoka-nagroda-za-pomoc-w-ujeciu-podejrzanego-Tunezyjczyka [dostęp: 18.09.2017].

31 PAP, *Podejrzany o zamach na jarmarku w Berlinie nie żyje*, źródło: http://wiadomosci.onet.pl/swiat/zamach-w-berlinie-podejrzany-anis-amri-nie-zyje/tsp36ms [dostęp: 18.09.2017].

32 M. Orłowski, *Londyn: zamach terrorystyczny. 4 zabitych i 40 rannych w okolicy brytyjskiego parlamentu*, źródło: http://wyborcza.pl/7,75399,21533444,pilne-strzaly-przed-parlamentemwlondynie.html?disableRedirects=true [dostęp: 21.09.2017].

33 Independent, *Khalid Masood: London attacker had no links to Isis or al-Qaeda, says Met Police*, źródło: http://www.independent.co.uk/news/uk/home-news/khalid-masood-london-attack-isis-al-qaeda-no-links-police-a7652696.html [dostęp: 21.09.2017].

dwóch również zostały użyte pojazdy mechaniczne oraz noże, jednakże według ustaleń hiszpańskich służb mogło dojść do eksplozji ładunku wybuchowego. Otóż w nocy z 16 na 17 sierpnia, tak więc przed zamachami, w domu jednorodzinnym w Alcanar doszło do wybuchu. Alcanar w Hiszpanii jest postrzegane przez hiszpańskie służby jako centrum operacyjne islamistów, którzy dokonali zamachów w Barcelonie i Cambrils. W eksplozji ładunku śmierć poniosła co najmniej jedna osoba, natomiast siedem zostało rannych. Trzeba pamiętać, że na początku hiszpańskie służby nie wiązały wybuchu z jakąkolwiek nielegalną działalnością. Katalońska policja przypuszczała, że najprawdopodobniej doszło do wybuchu gazu, o czym świadczyć miały odnalezione na miejscu butle. Po zamachach, jakie miały miejsce na deptaku La Rambla w Barcelonie oraz w miejscowości Cambrils, jedną z możliwych hipotez katalońskiej policji jest fakt, że eksplozja do jakiej doszło, jest związana z możliwą produkcją materiałów wybuchowych. Z ustaleń hiszpańskich służb wynika, że wybuch w Alcanar sprawił, że islamiści postanowili wykorzystać samochód, aby dokonać masakry na zatłoczonym barcelońskim deptaku. Bilans tego zamachu to 15 osób zabitych oraz około 130 rannych, z czego kilkanaście ciężko[34]. Był to pierwszy na terenie Hiszpanii tak straszliwy zamach terrorystyczny, który został przeprowadzony po zamachach w Madrycie w 2004 r.

Europejskie służby w wielu przypadkach udaremniły przeróżne ataki terrorystyczne, choć miały miejsce sytuacje, gdy zagrożenie atakiem terrorystycznym było uznawane za mało prawdopodobne, a jednak nastąpiło. Należy mieć na uwadze, że służby nie są w stanie zapobiec wszystkim zamachom. Dodatkowo ważne jest, aby pamiętać, że terroryzm islamski potrzebuje rozgłosu, to jest jeden z celów terrorystów. Dlatego każdy udany zamach, jest sukcesem, który dla europejskich służb jest trudny do powstrzymania. Obecnie narzędziem zamachu może być ciężarówka lub inny ogólnie dostępny przedmiot, natomiast za parę lat przykładowo sytuacja może się zmienić i narzędziem zamachu może być dron, a liczba ofiar zamachów będzie się zwiększać[35].

Zapobieganie rozwojowi radykalizacji postaw jako jedna z metod walki z terroryzmem

Zdarza się, że „samotne wilki" zdradzają oznaki radykalizacji swojej osoby poprzez przeróżne wpisy w mediach społecznościowych taki jak Facebook czy Twitter. Zamachom można w pewnym stopniu zapobiegać, ale służby nie mają możliwości kontroli każdej osoby, która na mediach społecznościowych chwali się zaangażowaniem w sprawę o jaką walczy tzw. Państwo Islamskie. Jednakże w sytuacji nadmiernego zaangażowania w sieci takiej jednostki bardzo istotną rolę może odegrać rodzina i znajomi. Osoby z najbliższego kręgu radykalizującej jednostki powinny rozpoznać, kiedy dana jednostka wkracza w etap przygotowania się do dokonania zamachu. Nikt nie ulega radykalizacja nie z dnia

[34] PAP, *20 butli z gazem i potężna eksplozja. Od tego zaczęły się zamachy*, źródło: http://www.tvn24.pl/wiadomosci-ze-swiata,2/zamachy-w-hiszpanii-eksplozja-w-alcanar-powiazana-z-atakami,765379.html [dostęp: 21.09.2017].

[35] W.J. Janik, *Logistyka współczesnego terroryzmu*, Elbląg 2016, s. 25–65.

na dzień. Wiąże się to z psychicznym przygotowaniem to zabicia innego człowieka. Za przykład należy wziąć Larossi Abballa, który ćwiczył podrzynanie gardeł na żywych królikach. Rodziny zamachowców często wykazują zaskoczenie, że ich bliski podjął się takiego czynu, który oni potępiają. Dlatego miedzy innymi tak ważne jest, aby najbliżsi ludzie z kręgu „samotnego wilka" rozpoznali jego proces radykalizacji i zgłosili to odpowiednim służbom[36].

Bardzo ważne, aby możliwi terroryści nie byli wspierani przez swoich współwyznawców, a nawet potępiani w swoich czynach. Wszystkie lokalne społeczności muzułmańskie powinny być negatywnie nastawione wobec terroryzmu. Im większa będzie integracja społeczności muzułmańskiej ze światem zachodnim, tym mniej osób chciało dokonywać zamachów, ponieważ będzie działać przeciwko własnej społeczności. Ważne jest, aby społeczności muzułmańskie postrzegały takich „samotnych wilków" jako morderców, a nie bohaterów i męczenników. W takiej sytuacji wiele osób zrezygnuje z możliwości stania się terrorystą-męczennikiem walczącym za islam z niesprawiedliwym światem zachodu[37].

W wielu przypadkach, gdy dochodzi do rekrutacji jednostki, cały schemat jest podobny a nawet taki sam. Młody muzułmanin zostaje wysłany na studia do Europy, rodzina, z której pochodzi należy przeważnie do grupy wyższej klasy średniej. Student posiada dobre wykształcenie oraz włada biegle kilkoma językami. Dodatkowo sprawnie porusza się sferze nowości technologicznych, w tym obsługi komputera i wielu różnych programów. W momencie, gdy trafia do innego środowiska kulturowego, może dojść do zajścia zjawiska marginalizacji oraz osamotnienia w społeczeństwie. Może to zachęcić go do nawiązania nowych znajomości z osobami, z którymi ma wspólne zainteresowania[38]. W wielu przypadkach radykalizacja następuje w lokalnych meczetach. Początkowo znajomość oparta jest na przestrzeni prywatnej, w której stopniowo pojawiają się dyskusje na tematy związane z religią, kulturą, różnymi tradycjami czy też sytuacją polityczną. Alternatywna radykalizacja zachodzi wśród dzieci imigrantów islamskich, które żyją w świadomości braku możliwości wystąpienia integracji oraz rychłego awansu społecznego, to powoduje, że zaczynają brać udział w przeróżnych działaniach przestępczych. Początkowo są to głównie drobne przestępstwa, jednak po pewnym czasie zachodzi proces radykalizacji wśród niektórych jednostek z takich gangów młodzieżowych, jest to spowodowane faktem, że zaczynają one szukać „lepszej alternatywy"[39].

Ostatnim istotnym aspektem, który może spowodować postawienie znaczącego kroku w walce z tym destrukcyjnym zjawiskiem jakim jest terroryzm islamski, jest ograniczenie w Internecie przeróżnych dostępnych treści, które nakłaniają do stosowania przemocy,

---

36 G. Lindenberg, *cyt. wyd.*

37 M. Piekarski, *Polowanie na „samotne wilki*", źródło:http://www.special-ops.pl/blog/id354,polowanie-na-samotne-wilki/ [dostęp: 22.09.2017].

38 B. Bolachów, *Procesy radykalizacji mniejszości islamskiej w Unii Europejskiej. Od czynników permisywnych do przemocy politycznej*, [w:] D. Szlachter (red. et al.), *Radykalizacja poglądów religijnych w społecznościach muzułmańskich wybranych państw Unii Europejskiej: Polska, Holandia, Wielka Brytania*, Szczytno 2011, s. 45-50. Por. A. Zięba, D. Szlachter, *Countering Radicalisation of Muslim Community Opinions on the EU Level*, "International Studies. Interdisciplinary Political and Cultural Journal", Vol. 17, No. 1/2015, s. 119–144.

39 Tamże, s. 50–57.

agresji, udziału w dżihadzie oraz walki ze całym światem zachodnim. Najważniejsze jest, aby wyżej wspomniane materiały propagandowe, instruktażowe były z sieci na bieżąco usuwane lub blokowane. Służby również powinny monitować głoszenie mowy nienawiści stosowanej przez wielu imamów czy inne osoby uznawane za autorytety w lokalnych społecznościach muzułmańskich. W Wielkiej Brytanii od 2015 roku podejrzani o terroryzm tracą paszporty. Otóż zostało wydane pozwolenie na anulowanie paszportów dla osób, które są podejrzane o terroryzm i są obecnie poza granicami Wielkiej Brytanii. Dodatkowo służby będą wnikliwie na pozwolenie rządu monitorować powroty podejrzanych osób do Wielkiej Brytanii[40]. Nowe przepisy regulują również obowiązek firm, które dostarczają usługi Internetu, aby gromadziły informacje o powiązaniach adresów IP z indywidualnymi użytkownikami Internetu. Wszelkie dane w sprawach związanych z terroryzmem będą przekazywane w ręce policji[41].

Z analizy źródeł należy wyodrębnić brytyjską koncepcje strategii antyterrorystycznej, która wywodzi się z tzw. podejścia maksymalistycznego, skupiając się na wszystkich 4 podłożach walki z terroryzmem, które są wyodrębnione w Strategii Unii Europejskiej w sferze walki z terroryzmem[42]:

1. Zapobieganie (Prevent) – polega na zatrzymywaniu jednostek przed aktywnym bądź biernym wspomaganiem wszelkiej aktywności, która ma charakter terrorystyczny. Celem tego kroku jest zapobieganie zjawisku rosnącej radykalizacji oraz rekrutacji, występującej w Europie jak na Świecie.
2. Ochrona (Protect) – związana jest z efektywnym zabezpieczaniem obywateli oraz wszystkich obiektów użyteczności publicznej przed możliwymi zamachami terrorystycznymi. Podłoże to oparte jest na wzmacnianiu bezpieczeństwa na granicach, transportu oraz infrastruktury krytycznej.
3. Ściganie (Pursue) – polega na poszukiwaniu potencjalnych zagrożeń oraz prowadzeniu dochodzeń, które uniemożliwią terrorystom zaplanowanie, skomunikowanie się i jakąkolwiek podróż po Unii Europejskiej czy innym zakątku świata.
4. Reagowanie (Respond) – związane jest z przygotowaniem państw Unii Europejskiej do skutecznego zarzadzania kryzysowego, pomoc poszkodowanym przez terroryzmu oraz zminimalizowanie powstałych skutków terroryzmu.

Wrogiem dzisiejszej Europy jest radykalny islam, który walczy z demokracją i całym dorobkiem kultury europejskiej, dlatego należy zapobiegać jego rozprzestrzenianiu się wszelkimi możliwymi sposobami, stosując wszystkie możliwe środki prawne[43].

---

40 *Terrorism Act 2006*, http://www.legislation.gov.uk/ukpga/2006/11/contents [dostęp: 12.09.2017].

41 D. Szlachtera (red.), *Radykalizacja poglądów religijnych w społecznościach muzułmańskich wybranych państw Unii Europejskiej: Polska, Holandia, Wielka Brytania*, s. 45–57.

42 The EU Counter-Terrorism Strategy, http://register.consilium.europa.eu [dostęp: 12.09.2017].

43 M. Urzędowska, *„Samotne wilki" i islamscy radykałowie – terroryści groźniejsi dziś niż przed zamachami na WTC?*, źródło: http://wyborcza.pl/1,76842,17019309,_Samotne_wilki__i_islamscy_radykalowie___terrorysci.html [dostęp: 22.09.2017].

Podsumowanie

Zjawisko terroryzmu indywidualnego, które jest obecnie nazywane również terroryzmem „samotnych wilków" albo solo terroryzmem możemy uznać za „nowe oblicze terroryzmu islamskiego". Pierwsza dekada XXI wiek ukazuje, jak terroryzm islamski potrafi się zmieniać i dostosować się do warunków w jakich istnieje. Należy mieć na uwadze, że jest ogromnym zagrożeniem dla szeroko pojętego bezpieczeństwa państw europejskich, zarówno wewnętrznego jak i zewnętrznego. W dzisiejszym świecie pojęcie terroryzmu islamskiego łączy się ze zjawiskiem radykalizacji, która zachodzi w wielu kręgach społeczności muzułmańskiej. Każdy zamach w Europie przybliża nas do stereotypowego postrzegania muzułmanów jako terrorystów. Dlatego należy zrozumieć muzułmanów, którzy bardzo często nie chcą być łączeni za jakimikolwiek grupami terrorystycznymi, wykazując niechęć i odrazę do zamachów przeprowadzanych przez innych wyznawców islamu.

Najważniejsze jest, aby chronić każdego człowieka, szczególnie młodego, przed procesem radykalizacji, ponieważ to młode, zbuntowane osoby ulegają temu strasznemu zjawisku. Należy zwalczać radykalizację postaw bez względu na religię, jaką wyznaje oraz poglądy polityczne jakimi się legitymuje zagrożona jednostka. Z analizy w niniejszej pracy wynika, że najważniejsze jest, aby skutecznie zapobiegać ciągłemu zagrożeniu jakim jest terroryzm islamski w nowej postaci. Ważnym jest, aby nie doprowadzać do eskalacji oraz zapobiegać wszelkim konfliktom, jakie są w stanie wybuchnąć pomiędzy społecznością muzułmańską a europejską. Najnowsza historia Europy na swoich kartach pokazała, w którym kierunku potrafiła zmierzać Europa przez rosnący radykalizm i do czego w efekcie końcowym doprowadził proces radykalizacji społeczeństw na tle rasowym czy religijnym.

Należy również pamiętać, że za zamachami terrorystycznymi stoją ekstremiści islamscy, którzy reprezentują zradykalizowaną część społeczeństwa muzułmańskiego. Dlatego należy wprowadzać wszelkie metody, które będą zwalczać i uniemożliwiać zachodzenia zjawiska radykalizacji postaw, które szczególnie występuje wśród młodych wyznawców islamu. Terroryści islamscy korzystają z Koranu instrumentalnie oraz stosują jego cytaty fragmentarycznie, pomijając jego prawdziwy kontekst. Cele terrorystów były, są i zawsze będą polityczne, islam w ich użyciu jest jedynie użyteczną ideologią do osiągnięcia zamierzonego celu, do którego będą dążyć przy użyciu wszelkich środków.

Badania wykazały, że odpowiedź na pytanie stanowiące problem główny: **Czy w dobie rosnącego fundamentalizmu islamskiego, można nadal czuć się bezpiecznie w Europie?** jest twierdząca. Zarazem można uznać, że dynamika wydarzeń jakie mają miejsce w ostatnich latach w Europie, powoduje, że w krajach europejskich, takich jak Francja, Niemcy, Wielka Brytania, Włochy zagrożonych terroryzmem islamskim nie ma zapewnionego na chwilę obecną odpowiedniego stopnia bezpieczeństwa.

Warto mieć na uwadze, że nie wynika to z braku profesjonalizmu i staranności w działaniach służb, tylko z faktu, że terroryzm islamskich należy postrzegać jako szeroki i złożony problem. Mianowicie służby udaremniły wiele zamachów terrorystycznych, ale dla zamachowców islamskich ważne jest, aby choć jeden akt terroru przebiegł pomyślnie dla nich, a świat po takim zajściu będzie mówił o problemie ekstremizmu islamskiego, m.in. dlatego kraje europejskie najprawdopodobniej przez następne kilkanaście lat będą zmagać się z terroryzmem islamskim.

Obecnie panująca sytuacja geopolityczna w Europie oraz wydarzenia w państwach Europy, ukazuje, że bardzo ważne jest, aby społeczeństwo europejskie zmieniło swoje nastawienie i podejście do terroryzmu islamskiego w wykonaniu m.in. „samotnych wilków", a co za tym idzie równocześnie do radykalizacji postaw wśród młodych muzułmanów, ponieważ tylko tak służby będą mogły zagwarantować realnie bezpieczeństwo wszystkim obywatelom Europy, bez względu na kolor skóry, religię czy poglądy polityczne.

Tytuł w języku angielskim
FACES OF ISLAMIC TERRORISM IN EUROPE AND THE ATTEMPS TO COUNTERACT

Bibliografia

Akty prawne

Terrorism Act 2006.

The European Union Counter-Terrorism Strategy.

Publikacje zwarte

Borkowski R., *Terroryzm ponowoczesny: Studium z antropologii polityki*, Toruń 2006.

Guła P., *Terroryzm międzynarodowy, w tym islamski. Zarys problemu*, WSPol, Szczytno 2009.

Hołyst B., *Terroryzm*, t. 1, Wyd. LexisNexis, Warszawa 2011.

Janik W.J., *Logistyka współczesnego terroryzmu*, Elbląg 2016.

Krawczyk A., *Terroryzm ugrupowań fundamentalistycznych na obszarze Izraela w drugiej połowie XX wieku*, Toruń 2007.

Liedel K., Piasecka P. (red.), *Terroryzm wczoraj i dziś. Księga pamiątkowa na 10-lecie Centrum Badań nad Terroryzmem Collegium Civitas*, Warszawa 2015.

Sadowski M., *Dżihad – Święta wojna w islamie*, Przegląd Bezpieczeństwa Wewnętrznego nr 8 (5) 2013.

Szlachter D. (red. et al.) *Radykalizacja poglądów religijnych w społecznościach muzułmańskich wybranych państw Unii Europejskiej: Polska, Holandia, Wielka Brytania*, Szczytno 2011.

Tomczak M., *Ewolucja terroryzmu. Sprawcy – metody – finanse*, Poznań 2010.

Wejkszner A., *Ewolucja terroryzmu motywowanego ideologią religijną*, Poznań 2010.

Zięba A., Szlachter D., *Countering Radicalisation of Muslim Community Opinions on the EU Level*, „International Studies. Interdisciplinary Political and Cultural Journal", Vol. 17, No. 1/2015.

Publikacje internetowe

BBN, *Terroryzm – zagrożenie globalne i lokalne*, źródło: https://www.bbn.gov.pl/download/1/1034/rozdzial1.pdf [dostęp: 12.09.2017].

CNN, *Atak „samotnych wilków". Nowa fala terroryzmu?*, źródło: http://wiadomosci.onet.pl/atak-samotnych-wilkow-nowa-fala-terroryzmu/r86vf [dostęp: 12.09.2017].

Gazeta Prawna, *Najważniejsze zamachy terrorystyczne w Europie w ostatnich latach*, źródło: http://www.gazetaprawna.pl/artykuly/1048402,zamachy-terrorystyczne-w-europie-w-ostatnich-latach.html [dostęp: 12.09.2017].

Independent, *Khalid Masood: London attacker had no links to Isis or al-Qaeda, says Met Police*, źródło: http://www.independent.co.uk/news/uk/home-news/khalid-masood-london-attack-isis-al-qaeda-no-links-police-a7652696.html.

Lindenberg G., *Przyszłością terroryzmu są zamachy pojedynczych osób*, źródło: https://euroislam.pl/przyszlosc-ia-terroryzmu-sa-zamachy-pojedynczych-osob/.

Newsweek Polska, *Krwawe puzzle*, źródło: http://www.newsweek.pl/swiat/krwawe-puzzle,16655,1,1.html [dostęp: 12.09.2017].

Onet, *ETA*, źródło: http://portalwiedzy.onet.pl/75879,,,,eta,haslo.html [dostęp: 12.09.2017].

Onet, *Madryt 2004. To był najkrwawszy zamach w Europie*, źródło: http://wiadomosci.onet.pl/swiat/madryt-2004-to-byl-najkrwawszy-zamach-w-europie/e79lzzk.

Onet, *Al-Kaida*, (arab. *zasada*), źródło: http://portalwiedzy.onet.pl/124701,,,,al_kaida,haslo.html [dostęp: 12.09.2017].

Orłowski M., *Londyn: zamach terrorystyczny. 4 zabitych i 40 rannych w okolicy brytyjskiego parlament*, źródło:http://wyborcza.pl/7,75399,21533444,pilne-strzaly-przed-parlamentem-wlondynie.html?disableRedirects=true [dostęp: 12.09.2017].

PAP, *20 butli z gazem i potężna eksplozja. Od tego zaczęły się zamachy*, źródło: http://www.tvn24.pl/wiadomosci-ze-swiata,2/zamachy-w-hiszpanii-eksplozja-w-alcanar-powiazana-z-atakami,765379.html [dostęp: 12.09.2017].

PAP, *Podejrzany o zamach na jarmarku w Berlinie nie żyje*, źródło: http://wiadomosci.onet.pl/swiat/zamach-w-berlinie-podejrzany-anis-amri-nie-zyje/tsp36ms [dostęp: 12.09.2017].

PAP, *Zamach w Berlinie. Policyjny nalot na dwa mieszkania. Wysoka nagroda za pomoc w ujęciu podejrzanego Tunezyjczyka*, źródło: http://www.polskieradio.pl/5/3/Artykul/1706917,Zamach-w-Berlinie-Policyjny-nalot-na-dwa-mieszkania-Wysoka-nagroda-za-pomoc-w-ujeciu-podejrzanego-Tunezyjczyka [dostęp: 12.09.2017].

Patterns of Global Terrorism, Office of the Cordinator for Counterterrorism, Serwis internetowy Departamentu Stanu USA, U.S. Department of State, http://www.state.gov [dostęp: 12.09.2017].

Piekarski M., *Polowanie na „samotne wilki"*, źródło: http://www.special-ops.pl/blog/id354,polowanie-na-samotne-wilki/ [dostęp: 12.09.2017].

Polska Times, *Samotne wilki, czyli terroryzm w wersji 2.0*, źródło: http://www.polskatimes.pl/artykul/872693,samotne-wilki-czyli-terroryzm-w-wersji-20,id,t.html [dostęp: 12.09.2017].

Polskie Radio, *„Samotne wilki". Nowe oblicze terroryzmu*, źródło: http://www.polskieradio.pl/130/4212/Artykul/1707008,Samotne-wilki-Nowe-oblicze-terroryzmu [dostęp: 12.09.2017].

Polskie Radio, *Zamachy w Madrycie – odwet za Irak*, źródło: http://www.polskieradio.pl/39/156/Artykul/1071933,Zamachy-w-Madrycie%E2%80%93-odwet-za-Irak [dostęp: 12.09.2017].

TVP Info, *Samotne wilki – najgroźniejsza broń Państwa Islamskiego*, źródło: http://www.tvp.info/26388864/samotne-wilki-najgrozniejsza-bron-panstwa-islamskiego [dostęp: 12.09.2017].

Urzędowska M., *„Samotne wilki" i islamscy radykałowie – terroryści groźniejsi dziś niż przed zamachami na WTC?*, źródło: http://wyborcza.pl/1,76842,17019309,_Samotne_wilki__i_islamscy_radykalowie___terrorysci.html [dostęp: 12.09.2017].

Wieliński B., *Samochód – broń terrorystów nr 1. Bo zachodnich miast nie da się zabezpieczyć przed atakami z jej użyciem*, źródło: http://wyborcza.pl/7,75399,21541047,samochod-bron-terrorystow-nr-1-bo-zachodnich-miast-nie-da.html [dostęp: 12.09.2017].

Strony internetowe

http://www.independent.co.uk
http://www.polskatimes.pl
http://www.polskieradio.pl

http://www.tvp.info.pl
https://euroislam.pl
http://www.state.gov
https://portalwiedzy.onet.pl
https://wiadomosci.wp.pl
https://www.bbn.gov.pl
https://www.gazetaprawna.pl
https://www.newsweek.pl
https://www.onet.pl
https://www.special-ops.pl
https://www.tvn24.pl
https://www.wyborcza.pl
https://www.abw.gov.pl
http://www.legislation.gov.uk
https://register.consilium.europa.eu

ALEKSANDRA GOŁAŚ*

ARTYKUŁ RECENZYJNY KSIĄŻKI FARHADA KHOSROKHAVARA *RADICALIZATION: WHY SOME PEOPLE CHOOSE THE PATH OF VIOLENCE* NEW YORK 2017, THE NEW PRESS, SS. 192

Po 11 września 2001 roku radykalizacja stała się jednym z wiodących zagadnień w ramach studiów nad współczesnym terroryzmem. Przed tą datą koncepcja radykalizacji pozostawała na marginesie obszaru zainteresowania nauk społecznych i ich prób zrozumienia źródeł fascynacji przemocą polityczną[1]. W pracach dotyczących zjawiska terroryzmu skupiano się wówczas przede wszystkim na formach działania organizacji terrorystycznych, zdecydowanie rzadziej zaś na zdefiniowaniu ścieżki, która prowadzi niektóre jednostki do zmiany poglądów, a w efekcie – do stosowania przemocy. Po bezprecedensowych wydarzeniach z początku XXI wieku, amerykańscy przedstawiciele świata nauki wraz z ośrodkami decyzyjnymi i podmiotami odpowiedzialnymi za bezpieczeństwo państwa, rozpoczęli szereg badań nad tzw. źródłami terroryzmu. Radykalizacja stała się jednym z pierwszoplanowych terminów w politykach antyterrorystycznych państw zachodnich, a jej znaczenie umocniło się wraz z fenomenem rodzimego terroryzmu islamskiego i tzw. *foreign fighters*.

Efektem owego zainteresowania badaczy procesem radykalizacji jest szereg publikacji powstałych w tym temacie po 2001 roku. Jedną z prac wartych uwagi jest recenzowana książka francusko-irańskiego socjologa Farhada Khosrokhavar, piastującego stanowisko profesora na jednej z wiodących paryskich uczelni wyższych – Szkole Zaawansowanych Badań w Naukach Społecznych (*École des Hautes Études en Sciences Sociales*, EHESS). Khosrokhavar jest autorem licznych publikacji podejmujących temat islamu we Francji,

* Aleksandra Gołaś – doktorantka na Wydziale Nauk Politycznych i Studiów Międzynarodowych UW, absolwentka kierunku bezpieczeństwo wewnętrzne w INP UW (2017); obszar zainteresowania: radykalizacja społeczności muzułmańskich w Unii Europejskiej (ze szczególnym uwzględnieniem roli zakładów karnych jako miejsc sprzyjających radykalizacji), publikacje: A. Gołaś, *Czynniki i uwarunkowania radykalizacji muzułmanów w zakładach karnych. Studium przypadku Wielkiej Brytanii*, Kwartalnik Ośrodka Analiz Politologicznych UW „e-Politikon", 2017, nr XXIII. Kontakt e-mail: aleksandra.golas@gmail.com

1 F. Khosrokhavar, *Radicalization: Why Some People Choose the Path of Violence*, New York 2017, s. 1; por. A. P. Schmid, *Radicalisation: Topics and Themes*, "Perspectives on Terrorism", 2016, nr 3, s. 26.

a także terroryzmu islamskiego[2]. Jako jeden z pierwszych dokonał diagnozy funkcjonowania islamu w zakładach karnych Francji i Anglii, a w latach 2011–2013 przeprowadził badania w większości więzień francuskich pod kątem procesu radykalizacji[3]. Prace Farhada Khosrokhavar nie są dostępne w języku polskim.

Recenzowana pozycja „Radicalization: Why some people choose the path of violence" w anglojęzycznej wersji pojawiła się na rynku nakładem wydawnictwa The New Press (organizacja non-profit, działająca w interesie publicznym) w 2017 roku. Oryginalnym językiem książki jest francuski, w którym to wydana została dwa lata wcześniej.

Treść książki podzielona jest na 10 rozdziałów problemowych, poprzedzonych 20-stronicowym wprowadzeniem, w którym autor wyjaśnia znaczenie terminu „radykalizacja" (s. 1)[4], a także umiejscawia go w naukach społecznych. Khosrokhavar we wstępie stawia również tezę, iż współcześnie mamy do czynienia z mało intensywną wojną, prowadzoną przez partyzantów i organizacje terrorystyczne, którzy nie mogą zostać pokonani przez tradycyjne armie. Jak zauważa badacz, zachód od końca lat 90. XX wieku doświadcza wzrostu zagrożenia ze strony rodzimego terroryzmu islamskiego, którego społeczna percepcja znaczenie różni się od sposobu postrzegania występujących w niektórych regionach Europy zagrożeń ze strony ugrupowań separatystycznych. Przyczyny takiego stanu rzeczy autor dopatruje się w fakcie, iż przez zdecydowaną większości osób radykalny islam wciąż odbierany jest jako zagrożenie „z zewnątrz" Starego Kontynentu.

W pierwszym rozdziale Khosrokhavar dzieli historię radykalizacji na kilka okresów w oparciu o działalność następujących ugrupowań: XI-wiecznych Asasynów, terroryzm ruchów anarchistycznych przełomu XIX i XX wieku oraz lewicowych w latach 1970–1990, fazy funkcjonowania Al-Kaidy. Przegląd kończy się na Arabskiej Wiośnie, którą autor uznał za „nowy rozdział dżihadyzmu", początkujący pojawienie się odmiennych form radykalizacji. Rozdział ten w fascynujący sposób ukazuje oblicza radykalizacji poprzez analizę procesów społeczno-politycznych, leżących u jej źródeł.

Kolejny rozdział poświęcony jest radykalizacji w świecie muzułmańskim. Zdaniem autora pojawiła się ona w konsekwencji odczuwanego przez wyznawców islamu upokorzenia, a nawet braku nadziei wykształconych młodych pokoleń, zamieszkujących Bliski Wschód. Zdaniem autora, radykalizacja islamistyczna w porównaniu z poprzedzającymi ją ruchami anarchistycznymi i innymi skrajnie lewicowymi, jest zdecydowanie bardziej gwałtowna i nieprzewidywalna, a dżihadyści ochoczo poświęcają się sprawie. Autor podjął również próbę zidentyfikowania różnic i podobieństw w radykalizacji szyickiej i sunnickiej, omówiono również kwestię radykalizacji kobiet.

---

2 Zob. m.in. F. Khosrokhavar, *Inside Jihadism. Understanding jihadi movements worldwide*, London and New York 2009.

3 Zob. F. Khosrokhavar, *Radicalization in Prison: The French Case*, „Politics, Religion & Ideology" 2013, nr 2, s. 284–306.

4 „Radykalizacja odnosi się do procesu, w którym jednostka lub grupa przyjmuje gwałtowną formę działania bezpośrednio związaną z ekstremistyczną ideologią o treści politycznej, społecznej lub religijnej, która kwestionuje ustalony porządek polityczny, społeczny lub kulturowy".

W trzecim rozdziale opisane zostało znaczenie intelektualistów, teoretyków i ideologów ugrupowań islamistycznych oraz ich wpływ na radykalizację wśród społeczności muzułmańskich.

Następna część pracy poświęcona została Internetowi, uznanego przez autora za instrument wzmacniający radykalny przekaz poprzez nową formę komunikacji dżihadystów z podatnymi jednostkami. Zauważone zostało również, iż Internet wykorzystywany jest nie tylko w celu szerzenia propagandy, ale również jako narzędzie do „konkurowania" antagonistycznych ugrupowań terrorystycznych.

Piąty rozdział jest niespełna dwustronicowym sygnałem w złożonym i trudnym problemie finansowania radykalizacji. Autor ogranicza się wyłącznie do zauważenia roli „charytatywnych instytucji" w pozyskiwaniu pieniędzy dla organizacji terrorystycznych.

W dalszej kolejności Khosrokhavar omawia miejsca radykalizacji (jak zauważa mogą to być nieraz całe państwa, regiony, miasta, sąsiedztwa oraz pojedyncze budynki, takie jak szkoły, meczety), podkreślając tym samym lokalny (geograficzny) aspekt zjawiska.

W siódmym rozdziale autor przedstawia niejednoznaczną rolę frustracji w procesie radykalizacji, pomiędzy którymi, jak zauważa, nie występuje bezpośredni związek przyczynowo-skutkowy. Nie mniej jednak zaznacza, że frustracja może mieć wpływ na niektóre jednostki o odpowiednich predyspozycjach psychologicznych.

Zdecydowanie najciekawszym, a zarazem najbardziej rozbudowanym (ponad 60 stron), jest rozdział ósmy recenzowanej pozycji, poświęcony europejskiemu modelowi radykalizacji. Autor odwołuje się w nim do dwóch dominujących obecnie na terenie Europy rodzajów radykalizacji: islamistycznej i skrajnie prawicowej. Poruszone zostały między innymi kwestie katalizatorów popychających jednostki w kierunku stosowania przemocy (w szczególności zaś kombinacja dwóch czynników: poczucia głębokiej dehumanizacji oraz życie w muzułmańskim getcie) oraz ewolucji form oraz modeli radykalizacji na terenie Europy. Autor wprowadził również typologię radykalizacji na: skierowaną na zewnątrz (*ad extra*)/ skierowaną do środka (*ad intra*), narodową/ponadnarodową, mającą miejsce w państwach demokratycznych/mającą miejsce w państwach autorytarnych. Dużo miejsca poświęcono również problemowi radykalizacji w więzieniach.

Kolejny rozdział jest z kolei ukazaniem międzynarodowego charakteru radykalizacji, przejawiającego się obraniem świata muzułmańskiego za „teatr" działań ugrupowań dżihadystycznych, poczynając od irańskiej rewolucji z 1979 roku.

Pracę zamyka dwustronicowy rozdział konfrontujący pojęcia „radykalizacja" i „deradykalizacja".

Jak można wywnioskować z tytułu recenzowanej publikacji, intencją autora była próba odpowiedzi na pytanie, dlaczego niektóre jednostki radykalizują swoje poglądy, w efekcie czego stosują przemoc? Należy zaznaczyć, że znakomita większość pracy skupia się na radykalizacji islamistycznej. Poprzez studium historyczne, ukazujące jak na przestrzeni ostatnich kilku dekad zmieniał się proces radykalizacji, autor w sposób przejrzysty i interesujący przedstawił motywy i czynniki, dla których niektóre jednostki decydują się wkroczyć na ścieżkę radykalizacji, umiejscawiając je ponadto w odpowiednim kontekście politycznym, ekonomicznym, społecznym, religijnym. Walorem opracowania są pojawiające się w niektórych fragmentach nawiązania i porównania schematów radykalizacji islamistycznej ze skrajnie prawicową i lewicową, a także opatrzenie tekstu nie tylko suchymi

faktami, ale również przykładami historii konkretnych osób i całych ugrupowań, potwierdzającymi słowa autora. Nie można nie zgodzić się z autorem, co do faktu, że Europa ma niewielkie doświadczenie z ruchami anty-aborcyjnymi i broniącymi praw zwierząt, a wciąż dominującą jest radykalizacja islamistyczna i skrajnie prawicowa (s. 73). Po lekturze rozdziału poświęconego europejskiemu modelowi radykalizacji pozostaje jednak niewielki niedosyt w dyskusji nad schematem radykalizacji prawicowej. Należy również zaznaczyć, że Khosrokhavar jest francuskim badaczem, stąd też dominujące w pracy informacje oparte są na doświadczeniach kraju pochodzenia badacza, nie mniej jednak pojawia się równie dużo nawiązań do Wielkiej Brytanii.

Zadowalający jest fakt, że Khosrokhavar odniósł się również do radykalizacji kobiet w świecie muzułmańskim, zaznaczając, że ich ścieżka prowadząca finalnie do stosowania przemocy różni się od tej, obieranej przez mężczyzn. Szkoda, że autor nie pokusił się o rozwinięcie tematu radykalizacji kobiet w Europie i ich przyłączania się do tzw. Państwa Islamskiego. Oczywiście jest to cena, jaką należy zapłacić próbując przeprowadzić zwięzłą analizę problemu – nie zawsze możliwe jest uwzględnienie wszystkich kwestii.

Istotną zaletą opracowania jest przystępne przekazanie czytelnikowi teorii radykalizacji, wypracowanych przez nauki społeczne. Autor nie rozwodzi się nad owymi teoriami i nie bierze udziału w tak często występującej w literaturze polemice nad definiowaniem terminu „radykalizacja", przez co książkę czyta się w przyjemny sposób, co ułatwia również styl pisania autora. Publikacja opatrzona jest wstępem i zakończeniem, a także bibliografią zawierającą niespełna 50 pozycji, przeważnie w języku francuskim. Poruszanie się po treści książki ułatwia zamieszczony na końcu indeks. W strukturze pracy wrażenie nie do końca przemyślanych pozostawiają niektóre rozdziały, zajmujące po 2 do 5 stron.

Książka powinna znaleźć szerokie grono odbiorców, zarówno wśród specjalistów praktyków, badaczy przemocy politycznej i studentów, jak również osób, które nurtuje postawione w tytule pytanie. Jest to pozycja z całą pewnością godna polecenia, a temat jak najbardziej aktualny. Mimo wspomnianego wcześniej znaczącego wzrostu ilości publikacji na temat radykalizacji, pozycja nie powiela schematów znanych z innych książek, a doświadczenie jej autora w dziedzinie może zapewnić o jej rzetelności. Wielka szkoda, że publikacje Farhada Khosrokhavar i innych autorów podejmujących temat radykalizacji nie są tłumaczone na język polski.

Tytuł w języku angielskim

BOOK REVIEW FARHAD KHOSROKHAR *RADICALIZATION: WHY SOME PEOPLE CHOOSE THE PATH OF VIOLENCE*, NEW YORK 2017, THE NEW PRESS, PP. 192

KLAUDIA BOGACKA*

SPRAWOZDANIE Z KONFERENCJI DEFENCE SUMMIT 2017 *POLSKA STRATEGIA OBRONNOŚCI. ROLA STRATEGICZNEGO PRZEGLĄDU OBRONNEGO – PLANOWANIE OBRONNE – WYZWANIA W RAMACH NATO*

Abstrakt

Strategiczny Przegląd Obronny opracowany przez Ministerstwo Obrony Narodowej stał się rzeczywistością. Funkcjonowanie raportu w środowisku wymaga podsumowań i wyciągnięcia wniosków. Zajęła się tym II edycja konferencji Defence Summit 2017.

Słowa kluczowe: Strategiczny Przegląd Obronny, obronność, NATO, cyberbezpieczeństwo, militaryzacja Rosji.

Druga edycja redakcyjnego cyklu konferencji Defence Summit 2017 zatytułowana „Polska Strategia obronności. Rola Strategicznego Przeglądu Obronnego – Planowanie Obronne – Wyzwania w ramach NATO" (*Polish Strategy of Defence. Role of the Strategic Defence Review – Defensive Planning – Challenges as part of NATO*) odbyła się 5 grudnia 2017 roku w siedzibie organizatora przedsięwzięcia, dziennika Rzeczpospolita. Pierwsza edycja miała miejsce w marcu bieżącego roku, podczas której uczestnicy dyskutowali na temat bezpieczeństwa narodowego 2017+, innowacyjności dla obronności oraz zderzeniu rozwoju gospodarczego z innowacyjnym sektorem zbrojeniowym. Kolejna poświęcona została Strategicznemu Przeglądowi Obronnemu powstałemu w celu zaspokojenia aktualnych i przyszłych potrzeb Polski w zakresie obronności. Realizacja zamierzeń z przeglądu ma umocnić pozycję Polski w NATO i odgrywać rolę swego rodzaju pomostu działań Sojuszu Północnoatlantyckiego na wschodniej flance. W związku z tym, na potrzeby opracowania dokumentu, przeprowadzono analizę zagrożeń, z którymi potencjalnie mogłaby się zmagać Polska i wojsko w ciągu najbliższych 15 lat. Wybrano model optymalny służący do

* Klaudia Bogacka – studentka III roku bezpieczeństwa wewnętrznego, na specjalizacji administracja porządku publicznego na Uniwersytecie Warszawskim. Prezes Studenckiego Koła Naukowego Bezpieczeństwa Wewnętrznego w roku akademickim 2016/2017. W roku późniejszym wiceprezes Koła. Członkini Kolegium Redakcyjnego czasopisma „Securo". Kontakt e-mail: klaudia.bogacka@poczta.onet.pl

efektywnego odstraszania, dzięki któremu Polska będzie gotowa do prowadzenia efektywnej operacji obronnej nawet w najgorszym wypadku. To są podstawowe informacje sformułowane przez wiceministra obrony narodowej Tomasza Szatkowskiego, również uczestnika drugiej edycji konferencji, które znajdziemy we wstępie do „Koncepcji obronnej", czyli jawnej części raportu.

Dyskusja podczas konferencji skoncentrowała się na próbie odpowiedzi na pytanie, czy Strategiczny Przegląd Obronny stanie się podstawą decyzji o inwestycjach modernizacyjnych i przekształceniach w armii oraz Siłach Zbrojnych RP, które zapewnią skuteczną obronę. W pełnych zaangażowania dywagacjach wzięli udział przedstawiciele kierownictwa Ministerstwa Obrony Narodowej, profesorowie, eksperci wojskowi, zagraniczni analitycy oraz przedstawiciele przemysłu.

Konferencję zainaugurował książę Michael von Liechtenstein, założyciel i fundator Geopolitical Information Services, międzynarodowej platformy eksperckiej i doradczej będącej współorganizatorem wydarzenia. W swoim przemówieniu podkreślał, że siły europejskie, w tym Polska wraz ze swoim potencjałem obronnym i gospodarczym muszą skuteczniej współdziałać w dziedzinie bezpieczeństwa patrząc na obecną sytuację na Ukrainie. Agresja Rosji na Ukrainę była dzwonkiem alarmowym i sygnałem dla innych państw. Książę widzi potrzebę zacieśniania współpracy w ramach sojuszu oraz ekonomicznej koordynacji wysiłków zbrojeniowych w obliczu pojawiających się i eskalujących napięć na kontynencie europejskim.

Rolę, wnioski i rysujące się strategie Strategicznego Przeglądu Obronnego w planowaniu obronnym RP omówił Tomasz Szatkowski. Podsekretarz Stanu w Ministerstwie Obrony Narodowej, odpowiedzialny w rządzie za przeprowadzenie strategicznego przeglądu obronnego był pewien, że choć dokument nie ma nadanej mocy prawnej, po decyzji ministra obrony narodowej stanie się kamieniem węgielnym reform obronnych w Polsce. Stworzy trwałe podstawy do tworzenia polityki obronnej w resorcie. Przyznał, że dotychczas polityka obronna nie rozwijała się w sposób efektywny, dlatego raport ma stać się także narzędziem do tworzenia jej w przyszłości. Powstanie przeglądu było procesem, poczynając od diagnozy środowiska bezpieczeństwa, prognozach, kończąc na rekomendacjach. Wiceminister wskazał, że ministerstwo powinno postawić na rozwój wojsk lądowych wspieranych wzmocnionym lotnictwem w polskim przewężeniu wielkiej Równiny Północnoeuropejskiej, na obszarze historycznej „strefy zgniotu" między Zachodem i Wschodem, ponieważ tak wynika z ustaleń. Podkreślił, że na Bałtyku najpilniejszym rozwiązaniem jest wprowadzenie broni podwodnej nowej generacji z dalekosiężnym orężem w postaci pocisków manewrujących. Wiceminister poruszył również kwestię Wojsk Obrony Terytorialnej, które mają stanowić istotne wsparcie dla sił operacyjnych, a na tyłach skoncentrować się na działaniach antydywersyjnych. Natomiast wojska specjalne mają być oczami i uszami armii skupionymi na zadaniach rozpoznawczych, wskazywaniu lotniczym, artyleryjskim i rakietowym środkom rażenia celów do likwidacji. Podsekretarz stanu odpowiedział na obawy związane z pochłonięciem przez Wojska Obrony Terytorialnej większości funduszy przeznaczonych na modernizację armii. Nie mają one podstaw, ponieważ zasadnicza część budżetu zbrojeniowego trafi do sił operacyjnych – zapewniał. Jedną z rekomendacji przeglądu jest postulat utworzenia w przyszłości kolejnej 4. dywizji zmechanizowanej i wzmocnienie struktur istniejących związków taktycznych. Na szczególną uwagę zasługuje

plan tworzenia systemów antydostępowych, zdolnych do zadawania wrogowi dotkliwych strat. Co ciekawe, inspiracją nie były państwa zachodnie, tylko Chińska Republika Ludowa oraz Federacja Rosyjska – wspomniał wiceminister. Celem jest pozostanie naszego państwa interoperacyjnym z NATO oraz bycie „sanktuarium" dla samych siebie. Z tego względu położono nacisk na rozwój Sił Zbrojnych w aspekcie jakościowym, ilościowym również. Resort odtwarza pierwszy raz od 30 lat ilość, co będzie miało wpływ na jakość – podążając za wypowiedzią podsekretarza stanu. Ponadto, ministerstwo stawia na modernizację obecnych czołgów. Cytując wiceministra Szatkowskiego: czołgi to nie jest przeżytek.

Gen. bryg. Sławomir Wojciechowski, Dowódca Operacyjny RSZ mówił o Strategicznym Przeglądzie Obronnym jako rzeczywistej strategii obronności. Przypomniał, że raport jest trzecim dokumentem tego typu po historycznym przełomie, z czego poprzednicy nie wnieśli zbyt wiele do rzeczywistości wojskowej. Z przekonaniem mówił o realnej szansie wyciągnięcia wniosków z SPO i ich wdrożenia, wyznaczając przy tym strategiczny kierunek polskiej polityki obronnej. Na potwierdzenie tezy wskazał fakt, że to pierwszy przegląd przywracający wojsko obronności, rzeczywiście zaakceptowany przez środowisko.

Wystąpienia podsumował panel dyskusyjny z udziałem osób, które miały bezpośredni wpływ na powstanie raportu, Tomasza Szatkowskiego, gen. bryg. Sławomira Wojciechowskiego, prof. Andrzeja Najgebauera z Wojskowej Akademii Technicznej oraz prof. Huberta Królikowskiego, przedstawiciela Ministerstwa Obrony Narodowej i pracownika Uniwersytetu Jagiellońskiego na temat wyników dokumentu. Wiceminister przyznał, że autorzy dokumentu do programowania rozwoju Sił Zbrojnych po raz pierwszy wykorzystali metody badawcze analityczne przyjęte na Zachodzie. Raport oparty jest na solidnych podstawach badawczych i naukowych. Zaproponowane rozwiązania kolejno testowano używając metodyki gier wojennych oraz weryfikowano w praktyce, chociażby podczas ćwiczeń strategicznych „Zima'17".

W wystąpieniu prof. Andrzeja Najgebauera z Wojskowej Akademii Technicznej poruszone zostały kwestie symulacyjnego i analitycznego wsparcia SPO zaprezentowane na schematach. Przegląd rozpoczyna cykl planowania – realizowany będzie cyklicznie, według powziętych planów, co 4 lata. Profesor wspomniał, że przy planowaniach strategicznych użyte zostały gry RPG (z ang. *role-playing game*).

Redaktor Piasecki podczas panelu dyskusyjnego zadał pytanie dotyczące nowego rodzaju zagrożenia bezpieczeństwa, tym samym skłaniając swoich rozmówców do refleksji nad tematem cyberbezpieczeństwa, tak ważnego w dzisiejszych czasach – czy Strategiczny Przegląd Obronny proponuje skuteczną odpowiedź na powszechne w wirtualnej przestrzeni zagrożenia cybernetyczne? Wiceminister uspokajał, że obrona cybernetyczna ma aktualnie priorytet w armii, a inwestycje w bezpieczeństwo cyfrowe przyspieszyły. Problem ten poruszono również podczas kolejnego panelu dyskusyjnego z udziałem gen. bryg. rez. pilota Dariusza Wrońskiego, Prezesa Centrum Wdrożeniowo-Produkcyjnego Instytutu Technicznego Wojsk Lotniczych, eksperta Warszawskiego Instytutu Inicjatyw Strategicznych (WIIS), prof. Jan Pietrasieńskiego – specjalisty od broni rakietowej, przedstawiciela Wydziału Mechatroniki i Lotnictwa w Wojskowej Akademii Techniczna oraz Nikodema Bończa-Tomaszewskiego – Prezesa Exatela. Nikodem Bończa-Tomaszewski przedstawił cyberatak jako możliwość sparaliżowania paraliżowania państwa, jak kiedyś inwazja na obce terytorium. W przyszłości wojna rozpocznie się właśnie od cyberataku na infrastruk-

turę krytyczną, finansową i telekomunikacyjną. W związku z tym mają powstać wojska cybernetyczne, jako wypadkowa przeprowadzonych analiz. Prezes Exatela stwierdził jednak, że sektor prywatny nie będzie militaryzowany w sposób sowiecki. W dyskusji wypłynął przykry wniosek, że Polską słabością jest nieumiejętność wykorzystania posiadanych inżynierów i ich potencjału.

Ponadto, na konferencji poruszono kwestię militaryzacji Rosji. Prof. Stefan Hedlund z Uniwersytetu Uppsala w Szwecji opowiedział o konsekwencjach rosnącej militaryzacji Rosji – „MAKING RUSSIA GREAT AGAIN". Natomiast militaryzację politycznego myślenia w Rosji pod kątem historycznym przybliżył dr Paweł Kowal z Instytutu Studiów Politycznych Polskiej Akademii Nauk. Wypowiedzi zakończył panel dyskusyjny o znaczeniu inicjatywy Enhanced Forward Presece jako środka do dalszej integracji Sił Zbrojnych RP w strukturach Sojuszu z udziałem prof. Hubert Królikowski – przedstawiciela Ministerstwa Obrony Narodowej i Uniwersytetu Jagiellońskiego, księcia Michaela von Liechtenstein, prof. Stefana Hedlunda i dr Pawła Kowala. Poddano dyskusji obecne wymiary współpracy Rzeczpospolitej i NATO w ramach EFP, EFP jako szansie integracji Sił Zbrojnych RP z NATO oraz przyszłości EFP w kontekście wniosków wypływających z SPO.

Tytuł w języku angielskim

CONFERENCE REPORT DEFENCE SUMMIT 2017 *POLISH STRATEGY OF DEFENCE. ROLE OF THE STRATEGIC DEFENCE REVIEW – DEFENSIVE PLANNING – CHALLENGES AS PART OF NATO*

DANIEL KASPERKIEWICZ*

SPRAWOZDANIE Z ZAJĘĆ PRAKTYCZNYCH *RUN – HIDE – FIGHT – JAK PRZEŻYĆ ZAMACH? POWSTRZYMAJ TERRORYSTĘ!*

Abstrakt

Kolejne wydarzenie z cyklu „W sieci terroru" odbyło się na Uniwersytecie Warszawskim. Tematyką terroryzmu od strony bezpieczeństwa osobistego zajął się Maciej Górski. Ćwiczenia zawierały praktyczne podejście do ewakuacji i zachowania w sytuacjach zagrożenia.

Słowa kluczowe: terroryzm, sytuacje zagrożenia, szkolenie praktyczne, Studenckie Koło Naukowe Bezpieczeństwa Wewnętrznego UW, ewakuacja, bezpieczeństwo, samoobrona.

W piątek, 24 listopada 2017 roku odbyło się kolejne spotkanie z cyklu „W sieci terroru", zatytułowane „Run Hide Fight – jak przeżyć zamach? Powstrzymaj terrorystę!". Poszczególne wydarzenia z cyklu organizowane są na Uniwersytecie Warszawskim przez Studenckie Koło Naukowe Bezpieczeństwa Wewnętrznego oraz Niezależne Zrzeszenie Studentów Uniwersytetu Warszawskiego. Ma on na celu zaznajomić uczestników z tematyką terroryzmu i sposobów reagowania w sytuacji zagrożenia.

Spotkanie w sali 200 budynku Zarządu Samorządu Studentów na Kampusie Głównym poprowadził Maciej Górski, członek specjalistycznych zespołów ochronnych, a także prowadzący przedmiotu ogólnouniwersyteckiego Anty-Terror System. Zajęcia zaczęły się o 16.30 wstępnym konwersatorium, z licznymi odniesieniami do poprzedniego spotkania w cyklu, które prowadzone było przez dr Krzysztofa Liedla. Wyświetlony został film „Run-Hide-Fight: Surviving an Active Shooter Event", stworzony przez władze samorządowe miasta Houston w Teksasie. Na jego bazie omówione zostały poszczególne elementy zachowań w sytuacji zagrożenia. Po zakończeniu części teoretycznej przyszedł czas na wypróbowanie zdobytej wiedzy w praktyce – zanim jednak do tego doszło, przygotowana została wolna przestrzeń na sali i przeprowadzona została rozgrzewka. Prowadzący na

* Daniel Kasperkiewicz – student III roku I stopnia bezpieczeństwa wewnętrznego, prezes Studenckiego Koła Naukowego Bezpieczeństwa Wewnętrznego Uniwersytetu Warszawskiego. Poza studiami pasjonat sztuk walki oraz kryminalistyki. Kontakt e-mail: d.kasperkiewic@student.uw.edu.pl

bazie powtarzanych kilkukrotnie eksperymentów tłumaczył, jak należy zachowywać się w konkretnych sytuacjach. Jako pierwsza zrealizowana została zainscenizowana ewakuacja sali. Po każdym zrealizowanym elemencie Maciej Górski tłumaczył mechanikę wybranego aspektu sytuacji zagrożenia, czerpiąc z pojawiających się błędów. Nie brakowało pytań, ale również nie brakowało odpowiedzi na nie. Z każdym kolejnym elementem grupa poznawała kolejne aspekty bezpiecznej ewakuacji.

Po zakończeniu pierwszej części zajęć praktycznych zrealizowana została druga, dotycząca bezpośrednich sytuacji zagrożenia bronią. Pod właściwą opieką uczestnicy przystąpili do ćwiczeń z atrapami, które przeplatane były teorią zachowań napastników podczas ataku. Przećwiczone zostały zarówno schematy zachowań wobec napastników uzbrojonych w nóż, jak również posiadających broń palną. Na koniec wyświetlony został film o ataku na amerykańską ambasadę, po którym pokrótce omówiono psychologię porwań.

Spotkanie zakończyło się po kilku godzinach intensywnych ćwiczeń podsumowaniem wiedzy zdobytej na szkoleniu, a także zaproszeniem do kontynuowania edukacji w tym kierunku. Podkreślone zostało, że dbanie o swoje bezpieczeństwo to ciągły proces edukacji i zachowywania uważności. Pomimo dużej frekwencji, zajęcia udało się przeprowadzić sprawnie, bez szkód oraz w pozytywnej atmosferze.

Tytuł w języku angielskim:
REPORT OF THE TRAINING-WORKSHOP *RUN – HIDE – FIGHT: HOW TO SURVIVE THE TERRORIST ATACK? STOP THE TERRORIST!*

„SECURO”
Wytyczne dla Autorów

Wymagania redakcyjne

Układ analizy:
- Autor
- Tytuł analizy w języku polskim
- Tytuł analizy w języku angielskim
- Abstrakt: w języku polskim do 600 znaków
- Kluczowe słowa: w języku polskim (max. 5)
- Tekst artykułu
- Bibliografia (bez numeracji poszczególnych pozycji!)
  - materiały źródłowe (dokumenty), publikacje zwarte, artykuły, źródła internetowe
- Nota o Autorze (w tym: kierunek i stopień studiów, adres e-mailowy).

Czcionka: Times New Roman „12”
Akapit: wyrównanie do prawej i lewej, wcięcie: 1,25 cm pierwszy wiersz, 1,5 odstępu między wierszami.
Przypisy polskie: na dole strony, odstępy między wierszami pojedyncze, numeracja ciągła, czcionka „10”, według wzoru:

[1] S. Huntington, *Trzecia fala demokratyzacji*, Warszawa 1995, s. 206.
[1] Tamże, s. 27.
[1] S. Huntington, dz. cyt., s. 28.
[1] M. Cichosz, *Transformacja demokratyczna – przyczyny, przebieg i efekty procesu*, [w:] A. Antoszewski (red.), *Systemy polityczne Europy Środkowo-Wschodniej*, Wrocław 2006, s. 52.
[1] A. Zięba, *Counterterrorism Systems of Spain and Poland: Comparative Studies*, „Przegląd Politologiczny” 2015, nr 3, s. 65–78.
[1] S. Ciesielski, *Restytucja czeczeńskiej autonomii*, źródło: http://www.sciesielski.republika.pl/ czeczenia/ resauto.html [1.03.2016 r.].
[1] *Czarnogórcy wierzą w Unię Europejską*, „Gazeta Wyborcza” z dn. 21.04.2016 r.
[1] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Dz.U. 1997 nr 78 poz. 483.

Tekst podstawowy i przypisy: wyjustowane.
Ustawienia strony: standardowe
Objętość: 30–40 tys. znaków (wraz ze spacjami)
Forma przekazania tekstu: e-mail’em, w edytorze Word na adres: a.gasztold@uw.edu.pl

dr Aleksandra Gasztold
Redaktor Naczelna „Securo”
Instytut Nauk Politycznych
Uniwersytet Warszawski
ul. Nowy Świat 67, p. 201
00-927 Warszawa
http://sknbwuw.cba.pl

ISSN: 2353-6330